International Journal of Innovative Research in Science and Engineering
Volume 10, Issue 05, 2024
www.ijirse.com
ISSN: 2454-9665

ANALYZE NETWORK TRAFFIC USING WIRESHARK TO IDENTIFY SIGNS OF MALWARE COMMUNICATIONS SUCH AS DATA INFILTRATION

Isharat Ali[1], Dr. Santosh Kumar Yadav[2]

[1]Research Scholar (Computer Science, Shri JJT University, Rajasthan, India)

[2]Research Guide (Professor, Computer Science, Shri JJT University, Rajasthan, India)

[1]mirzaishratali@gamil.com, [2]drskyadav@hotmail.com

ABSTRACT

The role of Wireshark is very important in our daily life. Now day by day hackers are spreading malicious content, user can generate message easily reach a large audience or users.

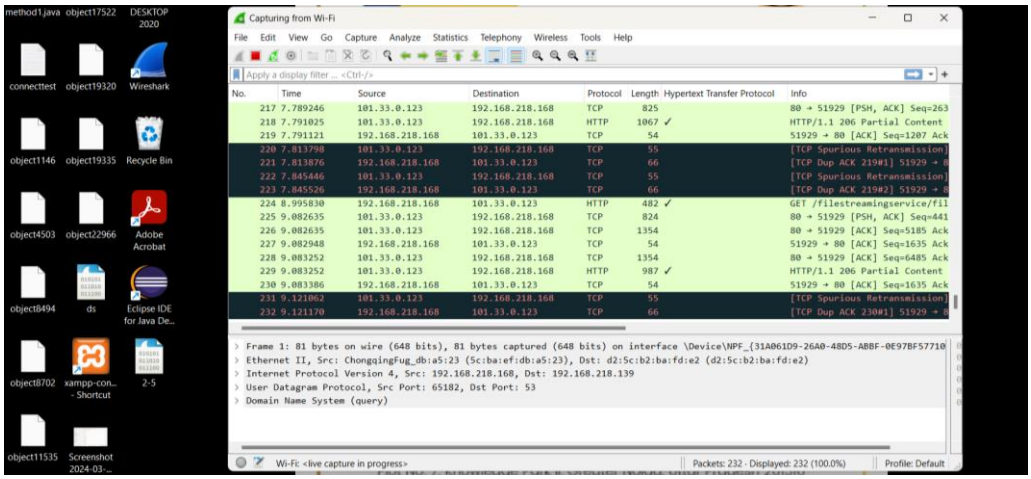
Wireshark is a packet sniffer and analysis tool. It captures network traffic from Ethernet, Bluetooth, wireless (IEEE.802.11), token ring, and frame relay connections, among others, and stores that data for offline analysis. Wireshark allows you to filter the log before the capture starts or during analysis, so you can narrow down and zero in on what you're looking for in the network trace.

Keywords: packet, Ethernet/Bluetooth/WiFi, Sniffer, capture, traffic, malware, infiltration

INTRODUCTION

Wireshark is an open-source network protocol analysis software program, widely considered the industry standard. A global organization of network specialists and software developers supports Wireshark and continues to make updates for new network technologies and encryption methods. Government agencies, corporations, non-profits, and educational institutions use Wireshark for troubleshooting and teaching purposes. There truly isn't a better way to learn low-level networking than to look at traffic under the Wireshark microscope.

International Journal of Innovative Research in Science and Engineering
Volume 10, Issue 05, 2024
www.ijirse.com
ISSN: 2454-9665



Logo of Wireshark

You should only use Wireshark on networks where you have permission to inspect network packets. Using Wireshark to look at packets without permission is illegal.

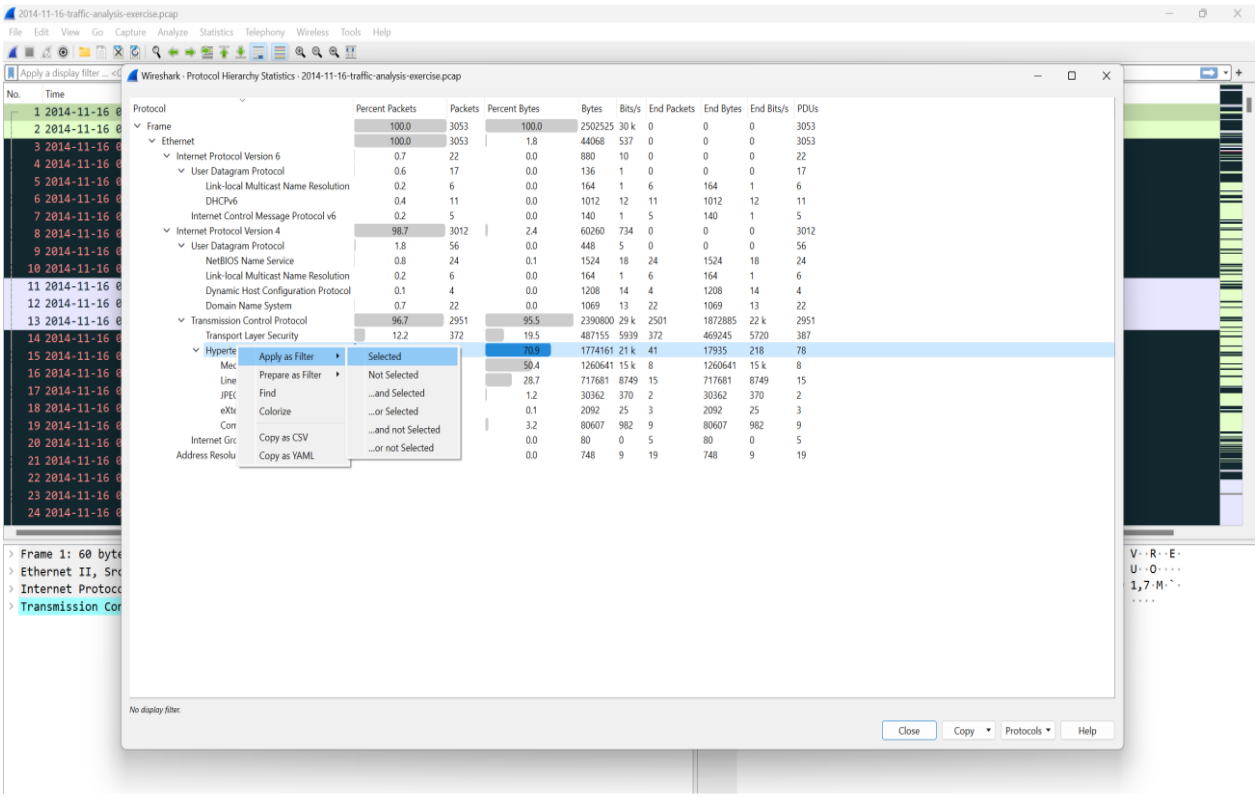
Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable.

What are we looking for?

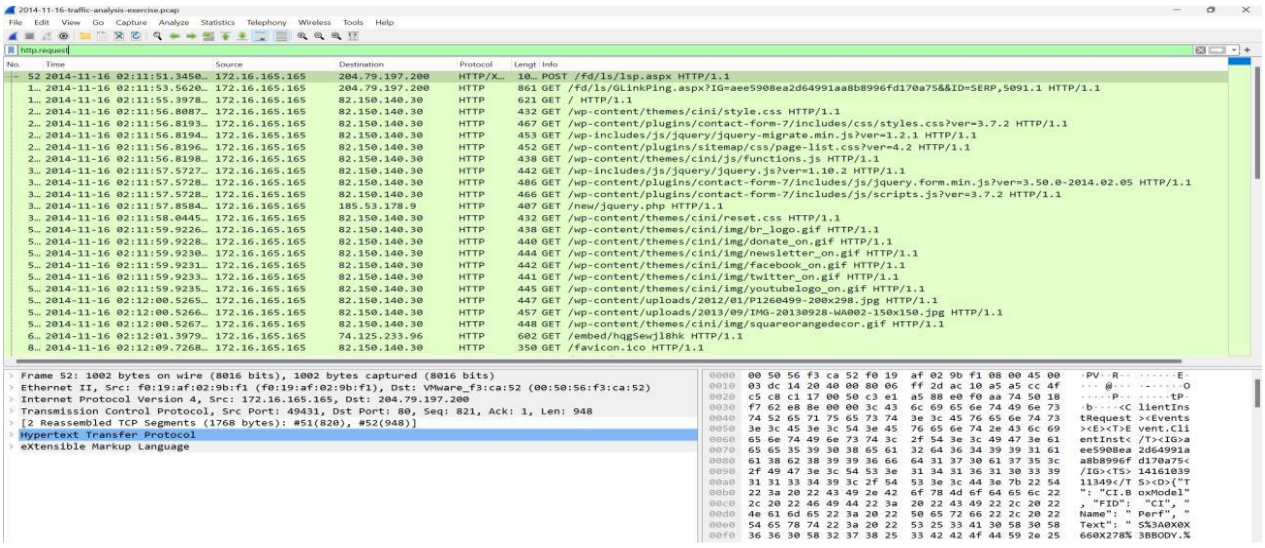
- What are the infected file(s) downloaded and their hashes?
- What is URL/ Domain of the infected site?
- What is the IP address of the infected website?
- What is the IP address of the infected machine?
- What is the hostname of the infected machine?
- What is the mac address of the infected machine?

International Journal of Innovative Research in Science and Engineering
Volume 10, Issue 05, 2024
www.ijirse.com
ISSN: 2454-9665

Check the normal activity of different protocol on the network by checking protocol hierarchy and find the normal information being transferred under different protocols.

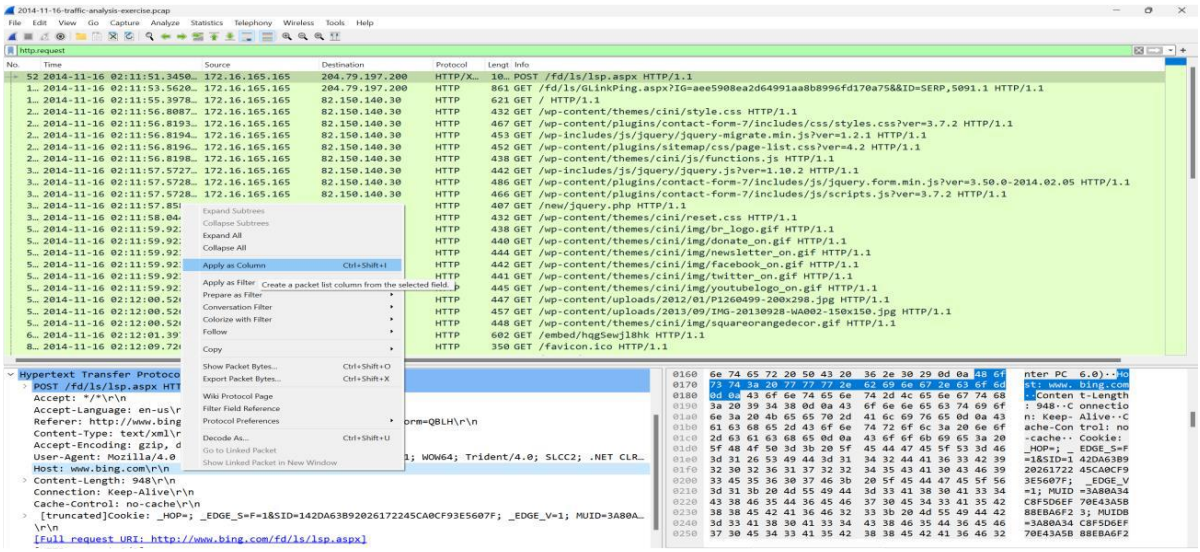


To see only Get and Post Request : Filter ---→ http.request

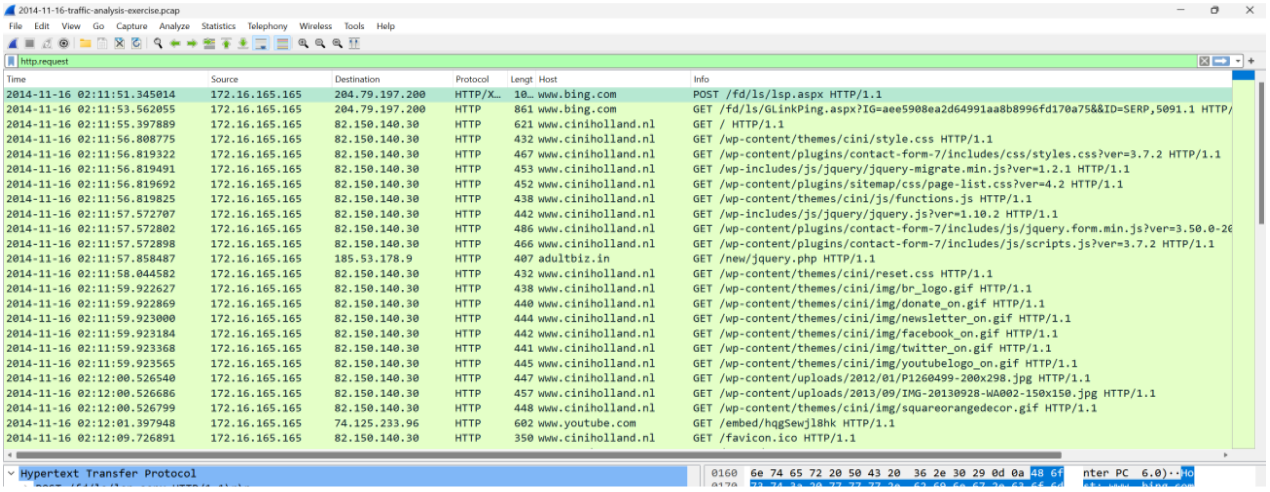


International Journal of Innovative Research in Science and Engineering
Volume 10, Issue 05, 2024
www.ijirse.com
ISSN: 2454-9665

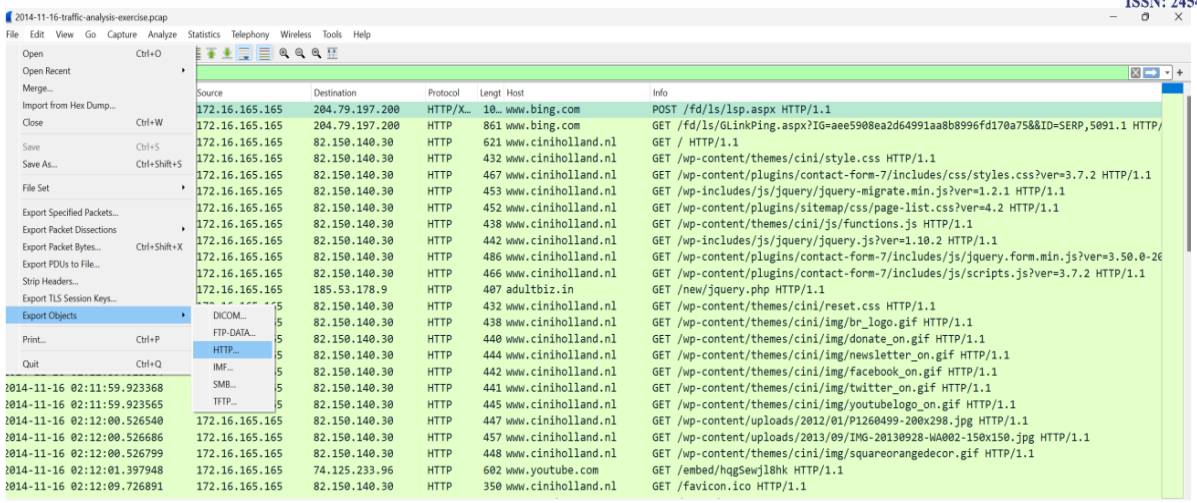
To get the better understanding of destination: Right Click on host user HTTP



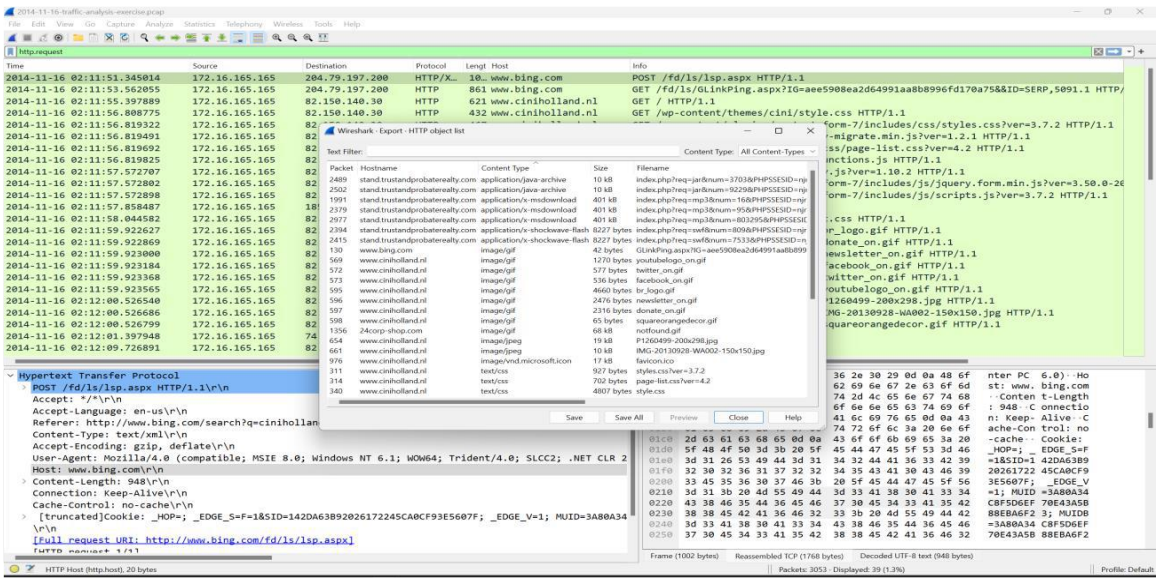
Now check Host Column



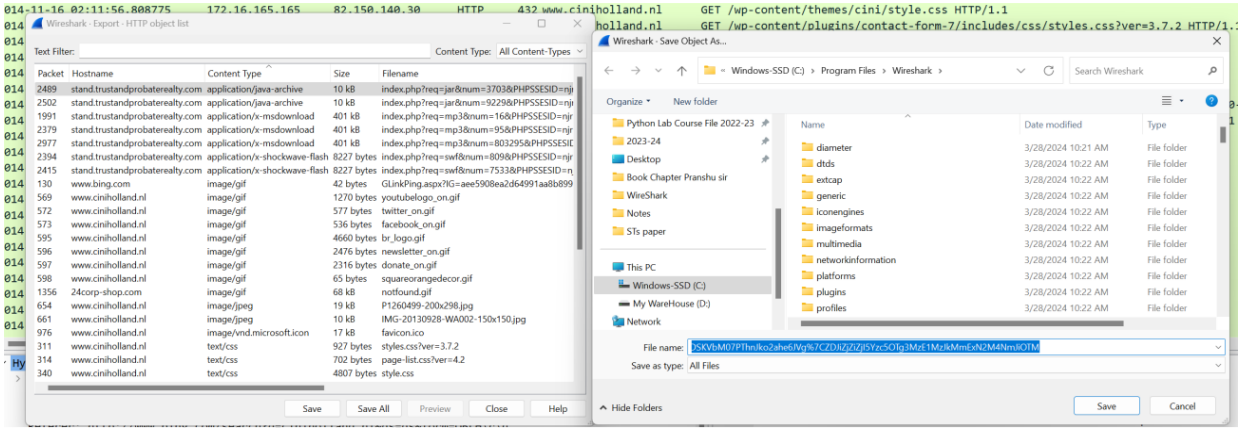
International Journal of Innovative Research in Science and Engineering
Volume 10, Issue 05, 2024
www.ijirse.com
ISSN: 2454-9665



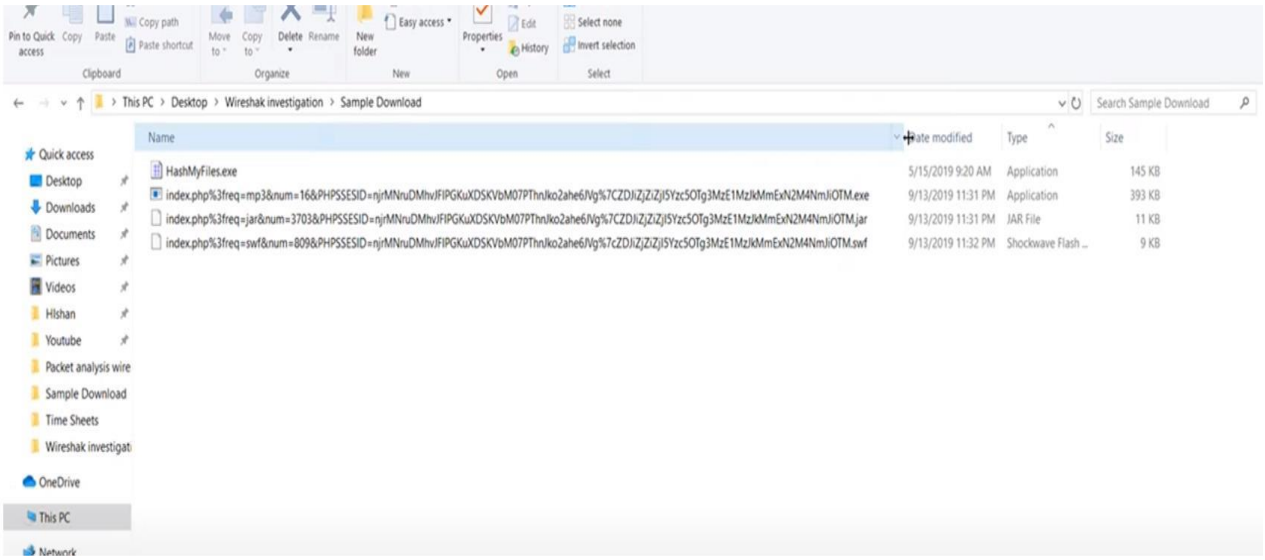
Sort column by Content type



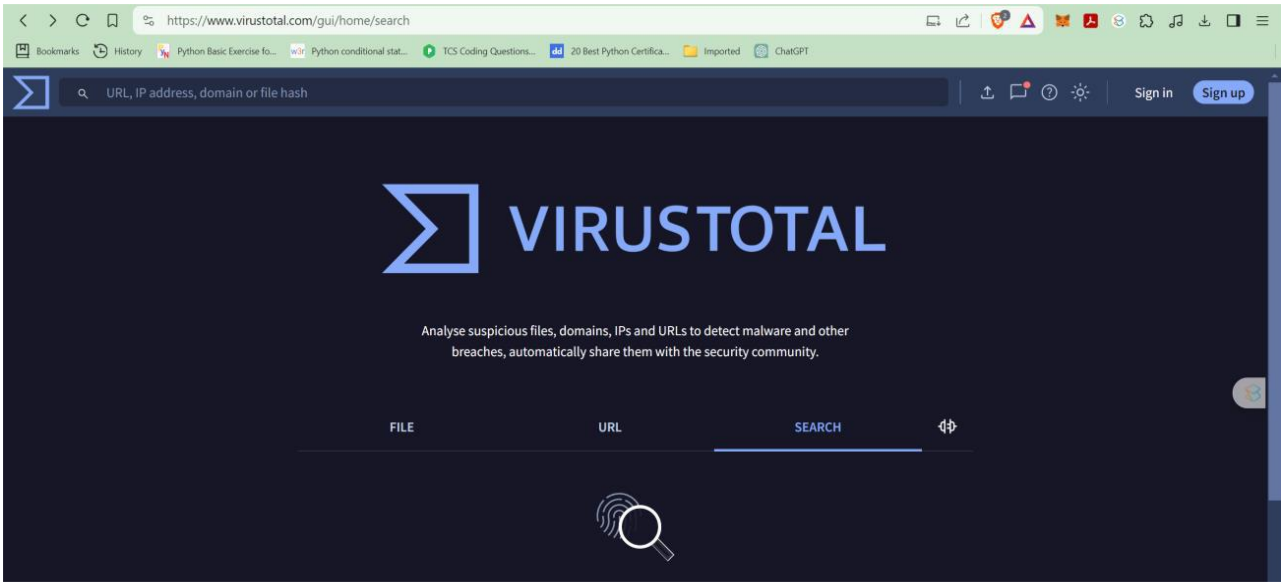
We can save all suspicious files



International Journal of Innovative Research in Science and Engineering
Volume 10, Issue 05, 2024
www.ijirse.com
ISSN: 2454-9665



We can directly upload the files to virus total but we avoid due to confidentiality, instead we find the hash of file and then check for malicious activity.



RESULTS AND DISCUSSION

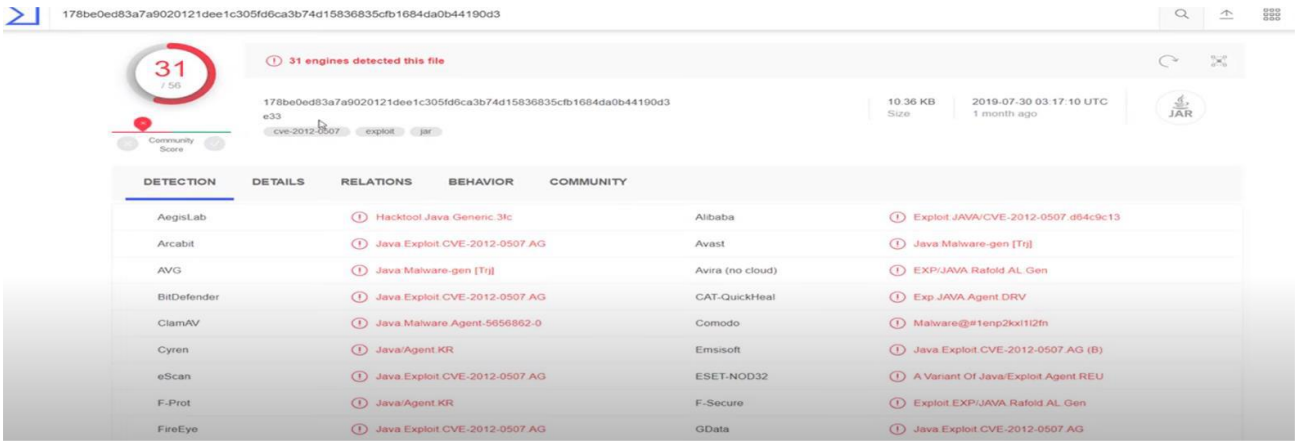
It is the best software to analyze traffic with. It allows capturing and inspecting the packets from all the available network adapters. I also love the packet filtering feature so that I can filter and see the desired types of packets.

Wireshark has many uses, including troubleshooting networks that have performance issues. Cyber security professionals often use Wireshark to trace connections, view the contents of suspect network transactions and identify bursts of network traffic.

Wireshark is a widely used, open source network analyzer that can capture and display real-time details of network traffic. It is particularly useful for troubleshooting network issues, analyzing network protocols and

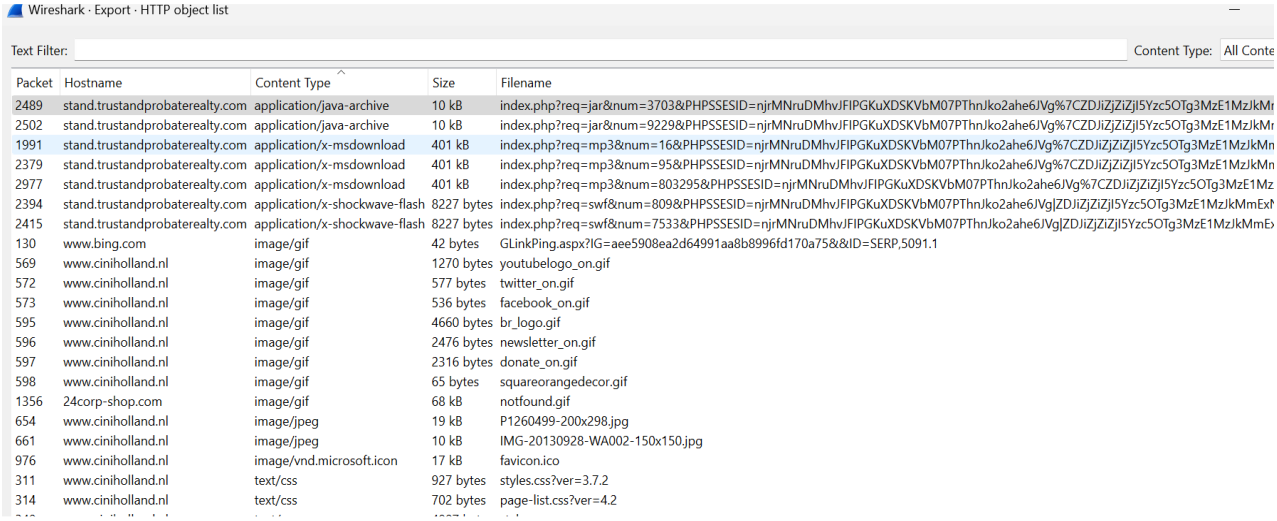
ensuring network security. Networks must be monitored to ensure smooth operations and security.

Now, we checked the hash in virus total and found it infected.



- What is URL/ Domain of the infected site?

Answer: see the host name of infected file. stand.trustandprobaterealty.com



Packet	Hostname	Content Type	Size	Filename
2489	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=3703&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMr
2502	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=9229&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMr
1991	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=16&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMn
2379	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=95&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMn
2977	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=803295&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1Mz
2394	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=809&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExM
2415	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=7533&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmEx
130	www.bing.com	image/gif	42 bytes	GLinkPing.aspx?IG=aee5908ea2d64991aa8b8996fd170a75&&ID=SERP,5091.1
569	www.ciniholland.nl	image/gif	1270 bytes	youtubelogo_on.gif
572	www.ciniholland.nl	image/gif	577 bytes	twitter_on.gif
573	www.ciniholland.nl	image/gif	536 bytes	facebook_on.gif
595	www.ciniholland.nl	image/gif	4660 bytes	br_logo.gif
596	www.ciniholland.nl	image/gif	2476 bytes	newsletter_on.gif
597	www.ciniholland.nl	image/gif	2316 bytes	donate_on.gif
598	www.ciniholland.nl	image/gif	65 bytes	squareorangedecor.gif
1356	24corp-shop.com	image/gif	68 kB	notfound.gif
654	www.ciniholland.nl	image/jpeg	19 kB	P1260499-200x298.jpg
661	www.ciniholland.nl	image/jpeg	10 kB	IMG-20130928-WA002-150x150.jpg
976	www.ciniholland.nl	image/vnd.microsoft.icon	17 kB	favicon.ico
311	www.ciniholland.nl	text/css	927 bytes	styles.css?ver=3.7.2
314	www.ciniholland.nl	text/css	702 bytes	page-list.css?ver=4.2

- What is the IP address of the infected website?

  37.200.69.143

- What is the IP address of the infected machine ?

  172.16.165.165

- What is the hostname of the infected machine?

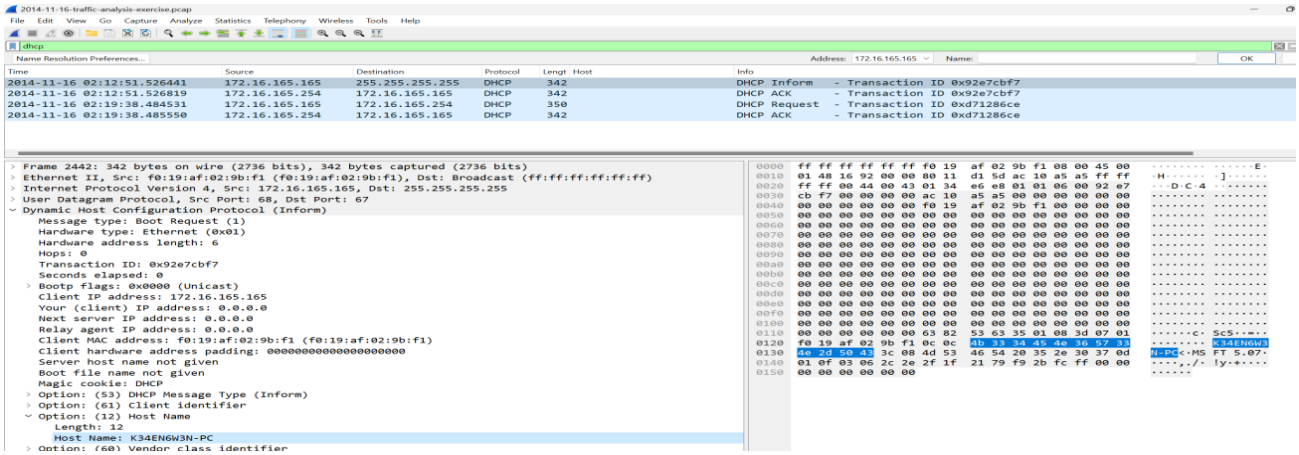
  K34EN6W3N-PC

- What is the mac address of the infected machine ?

  f0:19:af:02:9b:f1

International Journal of Innovative Research in Science and Engineering
Volume 10, Issue 05, 2024
www.ijirse.com
ISSN: 2454-9665

Host name using DHCP:



CONCLUSIONS

In this paper, we had worked about the Real-time Monitoring: Wireshark allows users to capture and analyze live network traffic in real-time, providing insights into the communication between devices on the network. Wireshark plays a crucial role in network security analysis. It allows security professionals to inspect packets for signs of malicious activities, such as suspicious traffic patterns, unauthorized access attempts, or data exfiltration.

Great tool for troubleshooting all kinds of problems and bugs. It works perfectly with any kind of OS and helps to capture all the traffic going trough your network. Great GUI, great filtering and great form of displaying packet captures. It is the best software to analyze traffic.

REFERENCES

1. Sunit Belapure and Nina Godbole, “Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives”, Wiley India Pvt Ltd, ISBN: 978-81- 265-21791, Publish Date 2013.
2. Basta, Basta, Brown, Kumar, Cyber Security and Cyber Laws, 1st edition , Cengage Learning publication.
3. Dr. Surya PrakashTripathi, RitendraGoyal, Praveen Kumar Shukla, KLSI. “Introduction to information security and cyber laws”. Dreamtech Press. ISBN: 9789351194736, 2015.
4. Cyber Security and Date Privacy by Krishan Kumar Goyal , Amit Garg , Saurabh Singhal , HP HAMILTON LIMITED Publication, ISBN-13-978-1913936020
5. Thomas J. Mowbray, “Cybersecurity: Managing Systems, Conducting Testing
6. Investigating Intrusions”, Copyright © 2014 by John Wiley & Sons, Inc, ISBN: 978 - 1-118 -84965 -1.
7. James Graham, Ryan Olson, Rick Howard, “Cyber Security Essentials”, CRC Press, 15-Dec 2010.
8. Anti- Hacker Tool Kit (Indian Edition) by Mike Shema, McGraw-Hill Publication.
9. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.