

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

Isharat Ali¹, Dr. Santosh Kumar Yadav²

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

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

¹mirzaishratali@gamil.com, ²drskyadav@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.

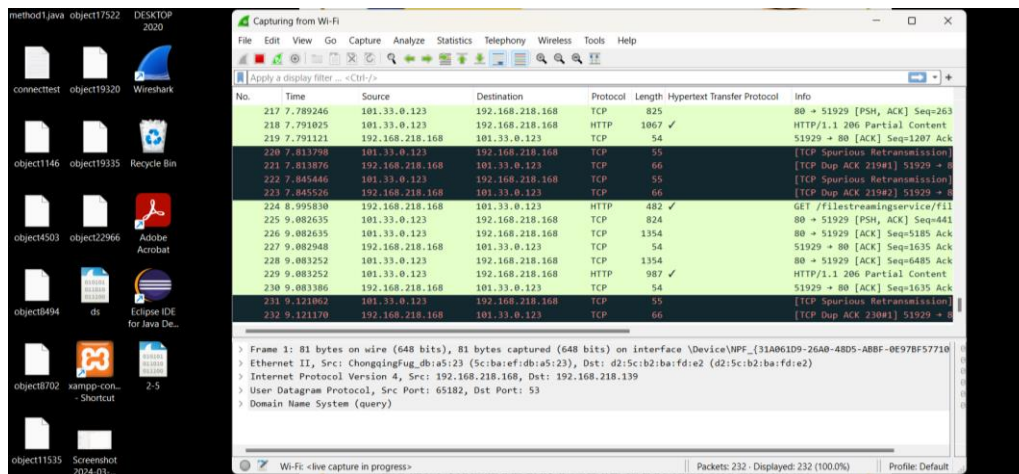
Wireshark is a packet sniffer and analysis tool. It captures network traffic from Ethernet, Bluetooth, wireless (IEEE.802.11), token ring, and frame relay connections, among others, and stores that data for offline analysis.

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.



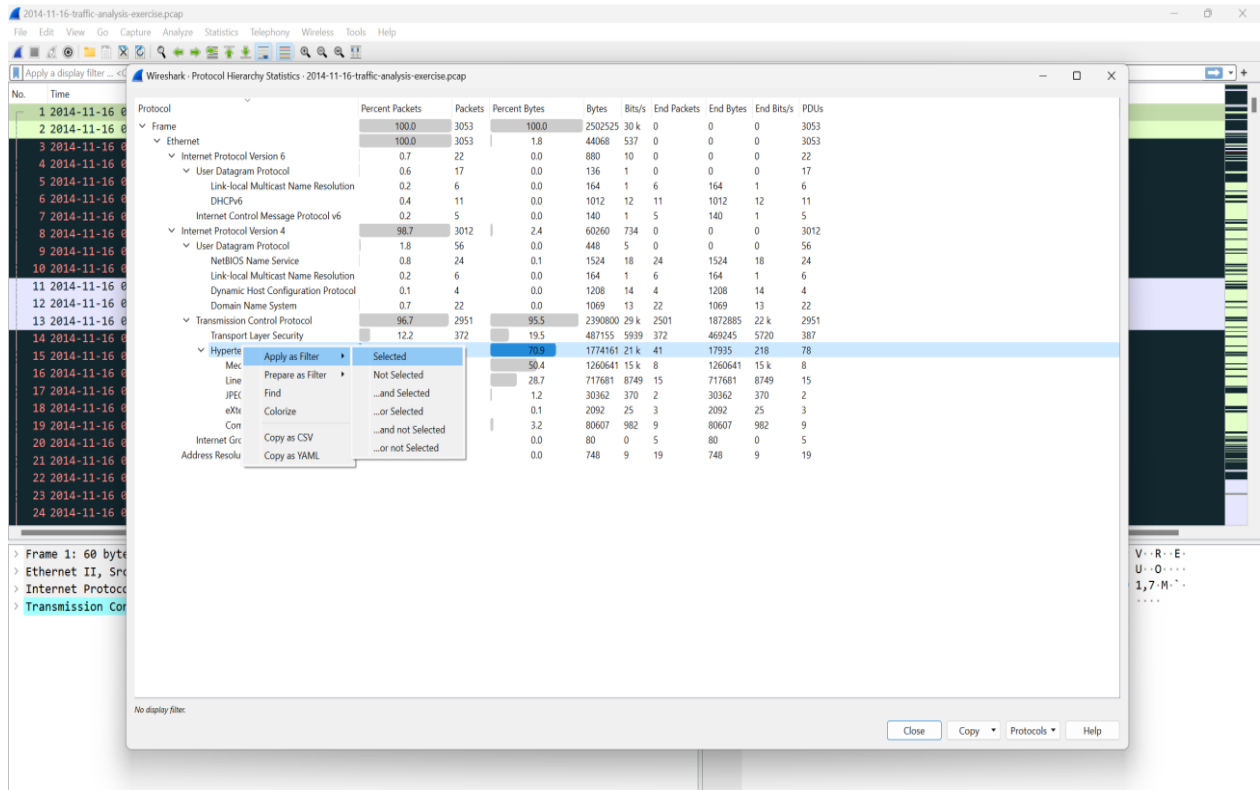
You should only use Wireshark on networks where you have permission to inspect network packets. Using Wireshark to look at packets without permission is illegal.

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?

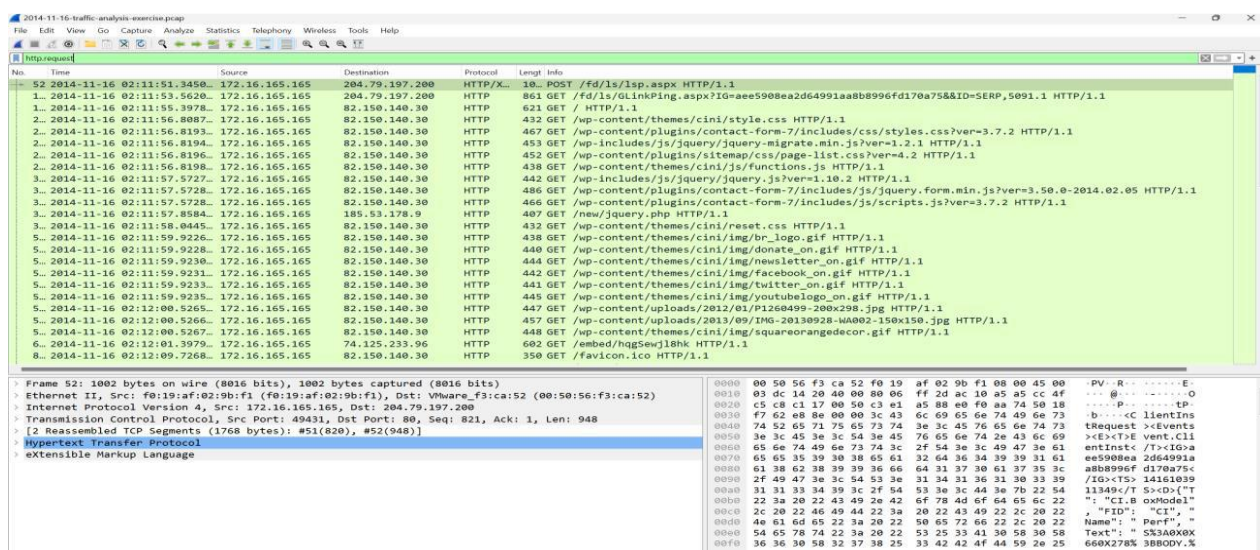
- ❖ What are the infected file(s) downloaded and their hashes?
- ❖ What is URL/ Domain of the infected site?
- ❖ What is the IP address of the infected website?
- ❖ What is the IP address of the infected machine?
- ❖ What is the hostname of the infected machine?
- ❖ What is the mac address of the infected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

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



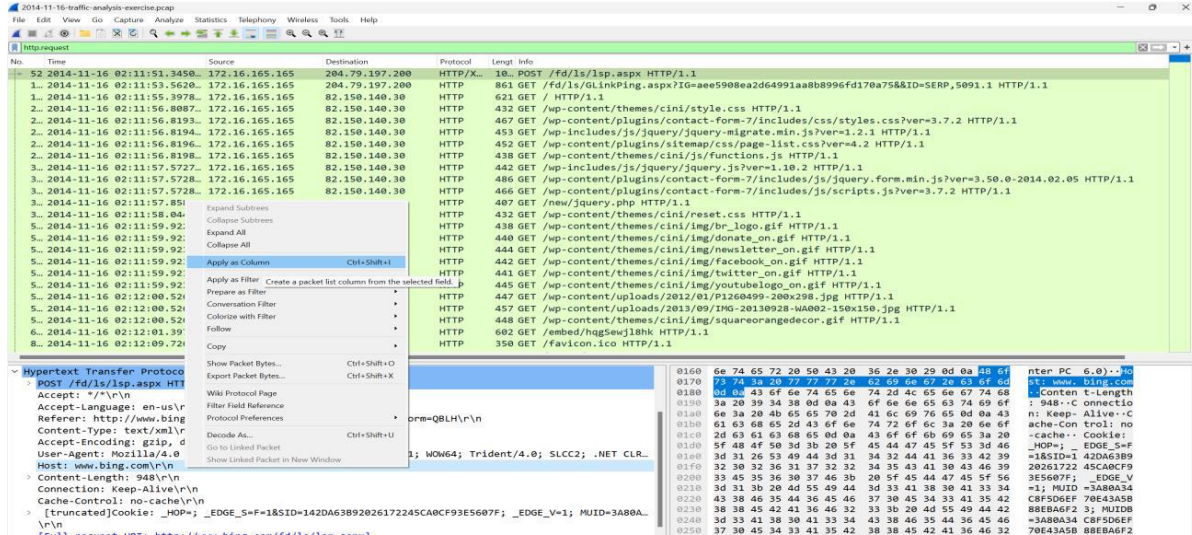
No.	Time	Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
1	2014-11-16 02:11:53.5620	Frame	100.0	3053	100.0	2502525	20 k	0	0	0	3053
2	2014-11-16 02:11:53.5978	Ethernet	100.0	3053	1.8	44068	537	0	0	0	3053
3	2014-11-16 02:11:53.5978	Internet Protocol Version 6	0.7	22	0.0	880	10	0	0	0	22
4	2014-11-16 02:11:53.5978	User Datagram Protocol	0.6	17	0.0	136	1	0	0	0	17
5	2014-11-16 02:11:53.5978	Link-local Multicast Name Resolution	0.2	6	0.0	164	1	6	164	1	6
6	2014-11-16 02:11:53.5978	DHCPv6	0.4	11	0.0	1012	12	11	1012	12	11
7	2014-11-16 02:11:53.5978	Internet Control Message Protocol v6	0.2	5	0.0	140	1	5	140	1	5
8	2014-11-16 02:11:53.5978	Internet Protocol Version 4	98.7	3012	2.4	60260	734	0	0	0	3012
9	2014-11-16 02:11:53.5978	User Datagram Protocol	1.8	56	0.0	448	5	0	0	0	56
10	2014-11-16 02:11:53.5978	NetBIOS Name Service	0.8	24	0.1	1524	18	24	1524	18	24
11	2014-11-16 02:11:53.5978	Link-local Multicast Name Resolution	0.2	6	0.0	164	1	6	164	1	6
12	2014-11-16 02:11:53.5978	Dynamic Host Configuration Protocol	0.1	4	0.0	1208	14	4	1208	14	4
13	2014-11-16 02:11:53.5978	Domain Name System	0.7	22	0.0	1069	13	22	1069	13	22
14	2014-11-16 02:11:53.5978	Transmission Control Protocol	96.7	2951	95.5	230080	29 k	2501	187285	22 k	2951
15	2014-11-16 02:11:53.5978	Transport Layer Security	12.2	372	19.5	407155	5939	372	469245	5720	387
16	2014-11-16 02:11:53.5978	Hypertext Transfer Protocol	70.8	1774	1174161	21 k	41	17935	218	78	1774
17	2014-11-16 02:11:53.5978	Line	59.4	126041	15 k	8	126041	15 k	8	8	126041
18	2014-11-16 02:11:53.5978	JPEG	28.7	717681	8749	15	717681	8749	15	15	717681
19	2014-11-16 02:11:53.5978	eXtensible Markup Language	1.2	30362	370	2	30362	370	2	2	30362
20	2014-11-16 02:11:53.5978	Com	0.1	2092	25	3	2092	25	3	3	2092
21	2014-11-16 02:11:53.5978	Internet Gr	3.2	80607	982	9	80607	982	9	9	80607
22	2014-11-16 02:11:53.5978	Address Resolu	0.0	80	0	5	80	0	5	5	80
23	2014-11-16 02:11:53.5978		0.0	748	9	19	748	9	19	19	748

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



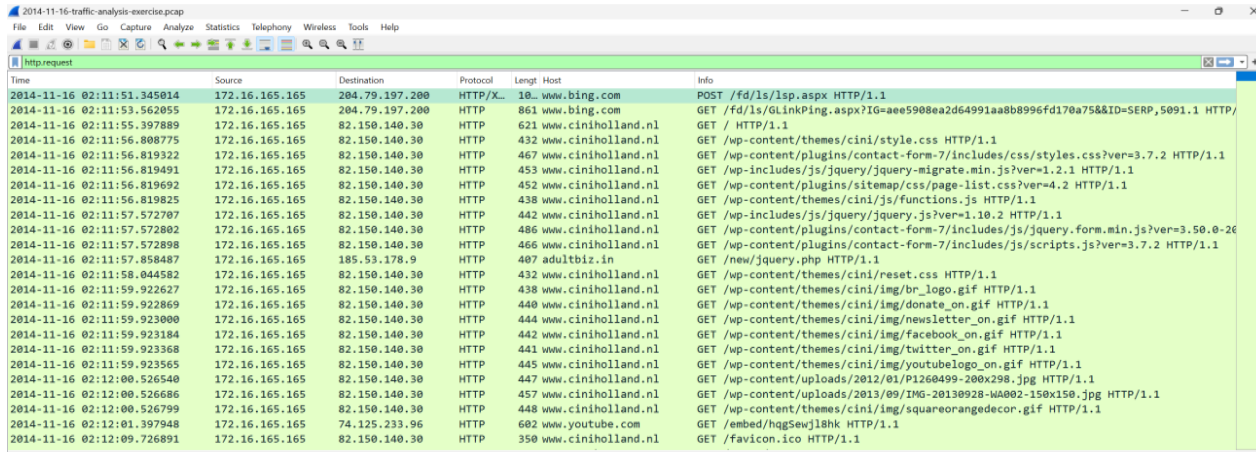
No.	Time	Source	Destination	Protocol	Length	Info
52	2014-11-16 02:11:51.3450	172.16.165.165	204.79.197.200	HTTP/X	30	POST /fd/ls/lsp.aspx HTTP/1.1
1.	2014-11-16 02:11:53.5620	172.16.165.165	204.79.197.200	HTTP	861	GET /fd/ls/LinkPing.aspx?IG=aee5908ea2d64991aa88996fd170a75&&ID=SERP_5091.1 HTTP/1.1
1.	2014-11-16 02:11:56.3978	172.16.165.165	82.150.140.30	HTTP	621	GET / HTTP/1.1
2.	2014-11-16 02:11:56.8087	172.16.165.165	82.150.140.30	HTTP	432	GET /wp-content/themes/cini/style.css HTTP/1.1
2.	2014-11-16 02:11:56.8193	172.16.165.165	82.150.140.30	HTTP	467	GET /wp-content/plugins/contact-form-7/includes/css/styles.css?ver=3.7.2 HTTP/1.1
2.	2014-11-16 02:11:56.8194	172.16.165.165	82.150.140.30	HTTP	453	GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HTTP/1.1
2.	2014-11-16 02:11:56.8196	172.16.165.165	82.150.140.30	HTTP	452	GET /wp-content/plugins/sitemap/css/page-list.css?ver=4.2 HTTP/1.1
2.	2014-11-16 02:11:56.8198	172.16.165.165	82.150.140.30	HTTP	438	GET /wp-content/themes/cini/js/functions.js HTTP/1.1
3.	2014-11-16 02:11:57.5727	172.16.165.165	82.150.140.30	HTTP	442	GET /wp-includes/js/jquery/jquery.js?ver=1.10.2 HTTP/1.1
3.	2014-11-16 02:11:57.5728	172.16.165.165	82.150.140.30	HTTP	486	GET /wp-content/plugins/contact-form-7/includes/js/jquery.form.min.js?ver=3.50.0-2014.02.05 HTTP/1.1
3.	2014-11-16 02:11:57.5728	172.16.165.165	82.150.140.30	HTTP	466	GET /wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=3.7.2 HTTP/1.1
3.	2014-11-16 02:11:57.8584	172.16.165.165	185.53.178.9	HTTP	407	GET /new/jquery.php HTTP/1.1
3.	2014-11-16 02:11:58.0445	172.16.165.165	82.150.140.30	HTTP	432	GET /wp-content/themes/cini/reset.css HTTP/1.1
5.	2014-11-16 02:11:59.9226	172.16.165.165	82.150.140.30	HTTP	438	GET /wp-content/themes/cini/img/br_logo.gif HTTP/1.1
5.	2014-11-16 02:11:59.9228	172.16.165.165	82.150.140.30	HTTP	440	GET /wp-content/themes/cini/img/donate_on.gif HTTP/1.1
5.	2014-11-16 02:11:59.9230	172.16.165.165	82.150.140.30	HTTP	444	GET /wp-content/themes/cini/img/newsletter_on.gif HTTP/1.1
5.	2014-11-16 02:11:59.9231	172.16.165.165	82.150.140.30	HTTP	442	GET /wp-content/themes/cini/img/facebook_on.gif HTTP/1.1
5.	2014-11-16 02:11:59.9233	172.16.165.165	82.150.140.30	HTTP	441	GET /wp-content/themes/cini/img/twitter_on.gif HTTP/1.1
5.	2014-11-16 02:11:59.9235	172.16.165.165	82.150.140.30	HTTP	445	GET /wp-content/themes/cini/img/youtube_logo_on.gif HTTP/1.1
5.	2014-11-16 02:12:00.5265	172.16.165.165	82.150.140.30	HTTP	447	GET /wp-content/uploads/2012/01/P1260499-200x298.jpg HTTP/1.1
5.	2014-11-16 02:12:00.5266	172.16.165.165	82.150.140.30	HTTP	457	GET /wp-content/uploads/2013/09/IMG-20130928-WA002-150x150.jpg HTTP/1.1
5.	2014-11-16 02:12:00.5267	172.16.165.165	82.150.140.30	HTTP	448	GET /wp-content/themes/cini/img/squareorangedecor.gif HTTP/1.1
6.	2014-11-16 02:12:01.3979	172.16.165.165	74.125.233.96	HTTP	602	GET /embed/hqSep18hk HTTP/1.1
8.	2014-11-16 02:12:09.7268	172.16.165.165	82.150.140.30	HTTP	350	GET /favicon.ico HTTP/1.1

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

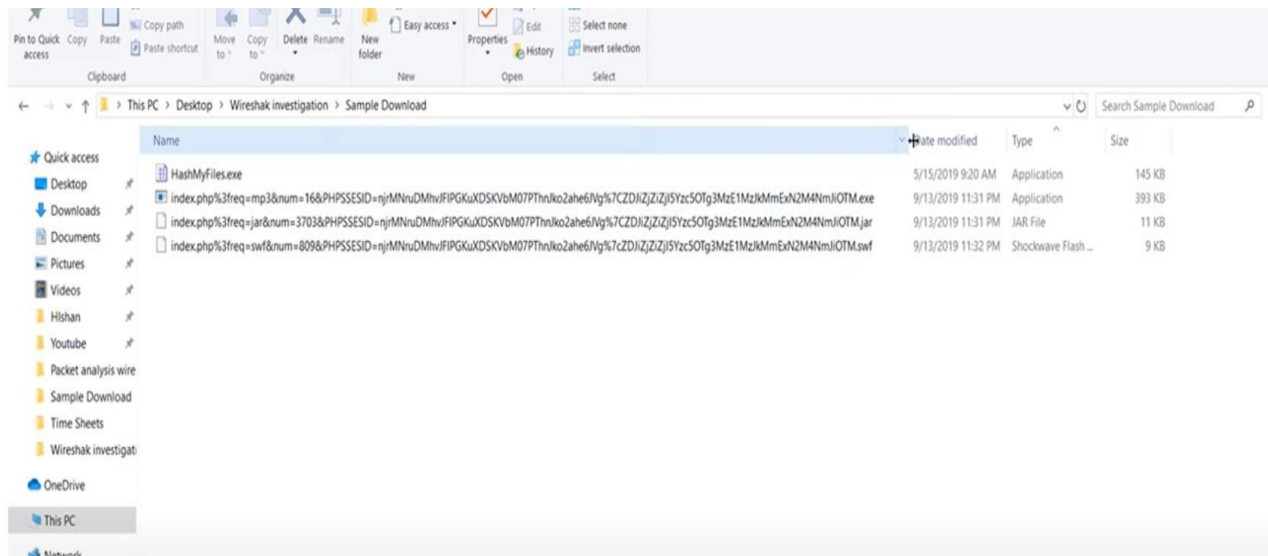


The screenshot shows a Wireshark capture of an HTTP request. The packet list pane is filtered to show the selected packet (No. 52). The packet bytes pane shows the raw data of the request, including the POST body and various headers like Accept, Referer, Content-Type, and User-Agent. The hex-to-ascii conversion is visible at the bottom of the packet bytes pane.

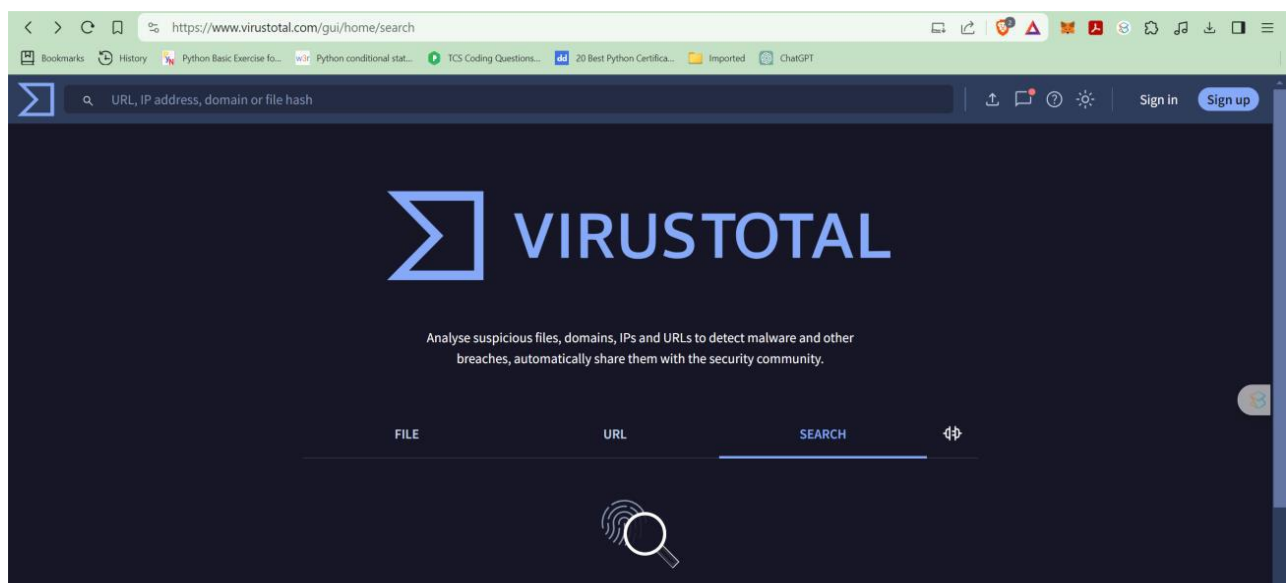
Now check Host Column



The screenshot shows the same Wireshark capture, but now the Host column is visible in the packet list pane. The host column is highlighted, and the packet list pane shows the host names for each packet, such as www.bing.com and www.ciniholland.nl.



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

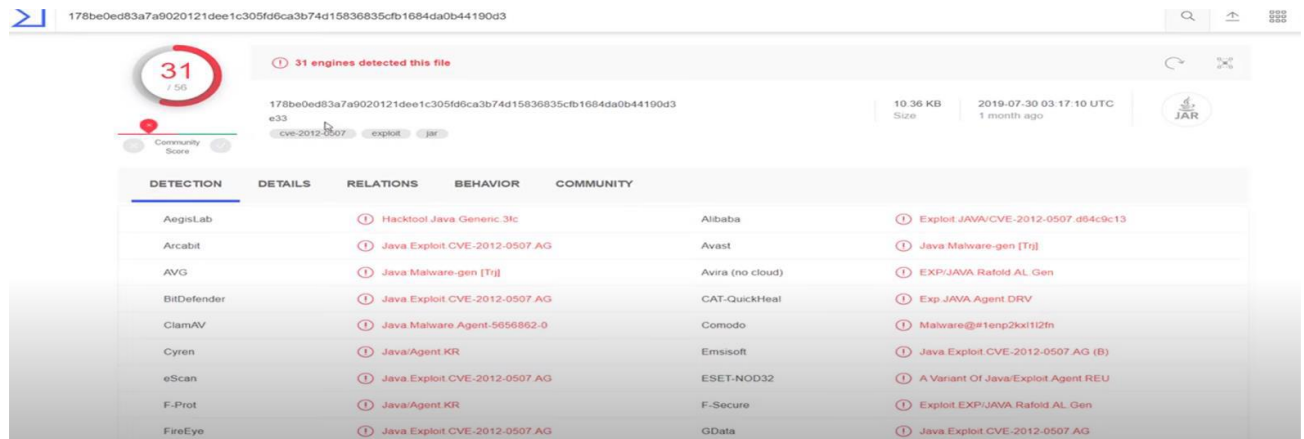
It is the best software to analyze traffic with. It allows capturing and inspecting the packets from all the available network adapters. I also love the packet filtering feature so that I can filter and see the desired types of packets.

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.

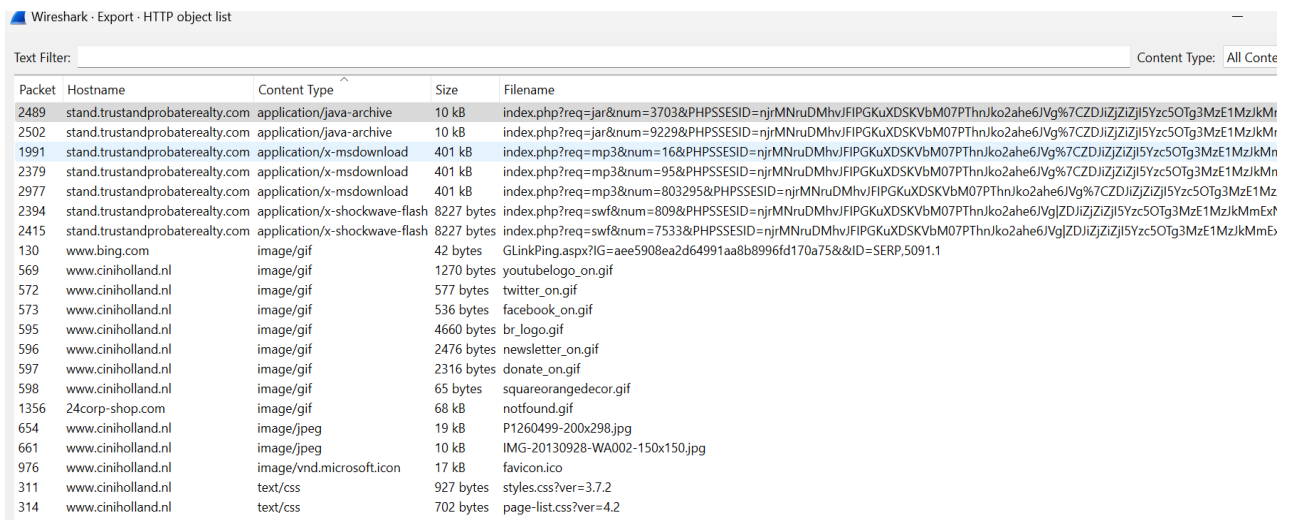
Now, we checked the hash in virus total and found it infected.



DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
AegisLab		Hacktool:Java.Generic.3/c		Exploit:JAVA/CVE-2012-0507_d64c9c13
Arcabit		Java Exploit: CVE-2012-0507 AG		Java Malware-gen [Trj]
AVG		Java Malware-gen [Trj]		EXP:JAVA.Ratofid.AL.Gen
BitDefender		Java Exploit: CVE-2012-0507 AG		Exp:JAVA.Agent.DRV
ClamAV		Java Malware Agent: 5656862.0		Malware@#1enp2kx112fn
Cyren		Java:Agent.KR		Java Exploit: CVE-2012-0507 AG (B)
eScan		Java Exploit: CVE-2012-0507 AG		A Variant Of Java:Exploit Agent REU
F-Prot		Java:Agent.KR		Exploit:EXP:JAVA.Ratofid.AL.Gen
FireEye		Java Exploit: CVE-2012-0507 AG		Java Exploit: CVE-2012-0507 AG

❖ What is URL/ Domain of the infected site?

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



Packet	Hostname	Content Type	Size	Filename
2489	stand.trustandprobater Realty.com	application/java-archive	10 kB	index.php?req=jar&num=3703&PHPSESSID=njrMnruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6Jvg%7CZDjIzjZiZjI5Yzc5OTg3MzE1MzJkM
2502	stand.trustandprobater Realty.com	application/java-archive	10 kB	index.php?req=jar&num=9229&PHPSESSID=njrMnruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6Jvg%7CZDjIzjZiZjI5Yzc5OTg3MzE1MzJkM
1991	stand.trustandprobater Realty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=16&PHPSESSID=njrMnruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6Jvg%7CZDjIzjZiZjI5Yzc5OTg3MzE1MzJkM
2379	stand.trustandprobater Realty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=95&PHPSESSID=njrMnruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6Jvg%7CZDjIzjZiZjI5Yzc5OTg3MzE1MzJkM
2977	stand.trustandprobater Realty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=803295&PHPSESSID=njrMnruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6Jvg%7CZDjIzjZiZjI5Yzc5OTg3MzE1Mz
2394	stand.trustandprobater Realty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=809&PHPSESSID=njrMnruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6Jvg%7CZDjIzjZiZjI5Yzc5OTg3MzE1MzJkM
2415	stand.trustandprobater Realty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=7533&PHPSESSID=njrMnruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6Jvg%7CZDjIzjZiZjI5Yzc5OTg3MzE1MzJkM
130	www.bing.com	image/gif	42 bytes	GLinkPing.aspx?IG=aee5908ea2d64991aa8b8996f170a75&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

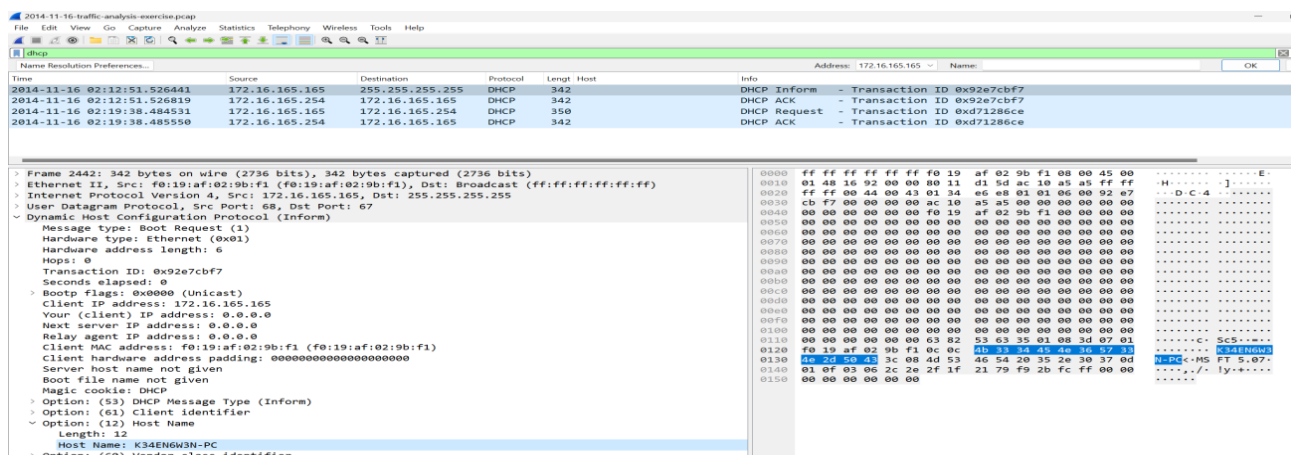
❖ What is the hostname of the infected machine?

K34EN6W3N-PC

❖ What is the mac address of the infected machine ?

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

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 through 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 Prakash Tripathi, Ritendra Goyal, Praveen Kumar Shukla, KLSI. "Introduction to information security and cyber laws". Dreamtech Press. ISBN: 9789351194736, 2015.
4. Cyber Security and Data 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.