



Analysis of Packet to Detect Malware Files

Muhammad Shairoze Malik, Arooj Fatima and Saad Waqas

School of Electrical engineering and computer Sciences, National University of Science and Technology, Islamabad.

Corresponding author: aroofatima72315@yahoo.com, saadwaqas832@gmail.com

Received: 18 September, 2022; Accepted: 18 November, 2022; Published: 20 December, 2022

Abstract:

The article covers the procedure of detecting malicious files from a packet which was responsible to make the system infected, this paper will highlight all the key elements that plays a pivotal role in detecting those files. The primary motivation behind this work is to provide information about those malware files and the detection of those files. This article also describes the use of perfect packet analysis software as well as its key features which can make our analysis simpler. Moreover, this article concludes with the author's perspective regarding the malware analysis.

Keywords: Malware files, Packet analysis software, Malware analysis, Detection

1. Introduction

Malware is the most common attack in the Cyber Security field. Most of the attackers use different malware techniques to gain benefit, it can be in terms of money or can be anything else. Malware can cause a huge damage to the user without his consent. In today's world, it is becoming the most damageable attack. It can affect your system, hardware, data loss and mostly data theft, your network and many other. So, to survive in this world, to control the number of attacks and to investigate malware cases, malware analyst showed their existence. They provide many of the detection procedures or techniques of malware which we can be used to investigate

these cases and to protect our system. Some questions that are being asked in this field are:

- What behavioral changes a malware can cause?
- How to detect the malware?
- What are the procedures of malware analysis?
- How to capture packets?
- What tool should we use to do the analysis?

The word malware is derived from words **MAL**icious **softWARE**. Whereas the word software means the program that targets the safety and integrity of the system is called malware. So, the Malware Analysis is the field

of inspecting malware tests to attempt to extricate important data about their starting point, conduct, and effect. There are many techniques that are used by malware analysts, a person who perform these activities, like Static Analysis and Dynamic Analysis [1]. Static Analysis include analysis of the malicious code without running it i.e., the File Headers, Strings, Hashes whereas the Dynamic Analysis include the analysis of the malicious code in a sandbox or safe environment.

2. IOC's:

IOC's stands for **Indication of Compromise**. These are the forensics evidence of a potential intrusion on a system network. These clues allow security professionals to determine the tactic of an occurred or impending attack IOCs are not always easy to detect, they can be as simple as metadata elements or incredibly complex malicious code and content samples. There are several IOC's which are listed below:

A. IP ADDRESS:

The word IP stands for "Internet Protocol", which can be regard as the set of rules governing the form of data sent via the internet or local network [3]. IP addresses are the unique addresses which can be used to identify the device.

B. DOMAIN NAME:

A domain name is a part of a URL. It is a string of text that maps to a numeric IP address, used to access a website from client servers [4].

C. USER AGENT:

The User-Agent request header is a characteristic string that let servers and network peers

identify the application, operating system, vendor, and version of requesting user-agent [5]. The syntax of use-agent is **User-Agent: <product> / <product-version> <comment>**.

D. HOSTNAME:

A hostname is a label that is assigned to a device connected to a computer network and that is used to identify the device in the various forms of electronic communication such as World Wide Web [4].

E. FILE HASHES:

File hashing is also used for file verification.

3. Tools For Analysis:

There are many tools that we can use to do analysis on the malware like PeStudio, Process Hacker, Process Monitor (ProcMon), ProcDot, Autoruns, Fiddler, IDA PRO, Ghidra. Wireshark is mainly used for the analysis because of its simplicity.



4. Wireshark:

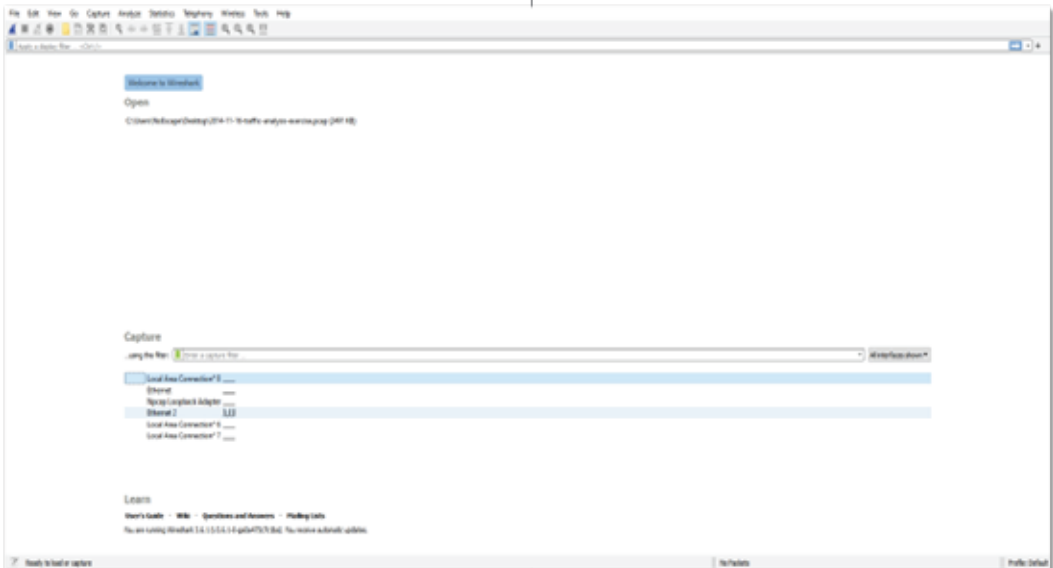
Wireshark is a free and open-source packet analyzer. Wireshark is a tool used for capturing and analyzing PCAPs files. It is used for **network troubleshooting, analysis, software and communication, protocol development and education**. The working of Wireshark is like tcpdump but has a graphical front and integrated sorting and filtering options. All the packet traffic is visible on the interface including uni-cast traffic. Wireshark is a data capturing program that understand the structure of different network protocol and it uses PCAPs to capture packets so it can only capture packets on the type of network that PCAP support. It can also color packets based on

rules that match fields in packets to help the user identify the type of traffic at a glance. Users can change the interface according to their choice [2].

4.1 Wireshark Default View

When you open the Wireshark, you will see this interface. To open a packet, just go to the file in the menu bar. Click open and select your

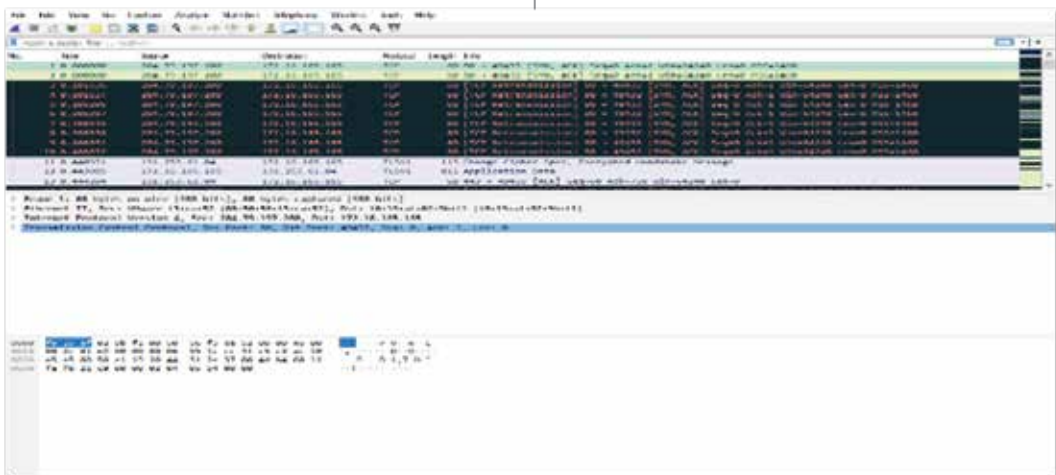
file. From Wireshark, you can also analyze the packets of your machine. All you need to do is choose the Local Area Connection. Another way to capture the local packets is to choose the Start Capturing Packets option with a symbol  on the top left side of the page. And to stop the capturing, click on the option named as Stop Capturing Packets with the  symbol.



4.2 Starting With Wireshark:

Now have a look on Wireshark user interface. The main window shows Wireshark as you

would usually see it after some packets are captured or loaded.



4.3 Wireshark Display Parts

The Wireshark Display has 4 parts as shown in the figure. These parts are also described below [7]:

- Filter Box (1): It is used to filter the packets displayed.
- Packet Listing (2): It shows all packets that satisfied the display filter.
- Packet Detail Windows (3): Display the contents of the currently selected packet.
- Hex Window (4): It displays the hex content of the current packet. The hex window is linked with the packets detail window and with highlight any field selected.

4.4 Changing The Default View:

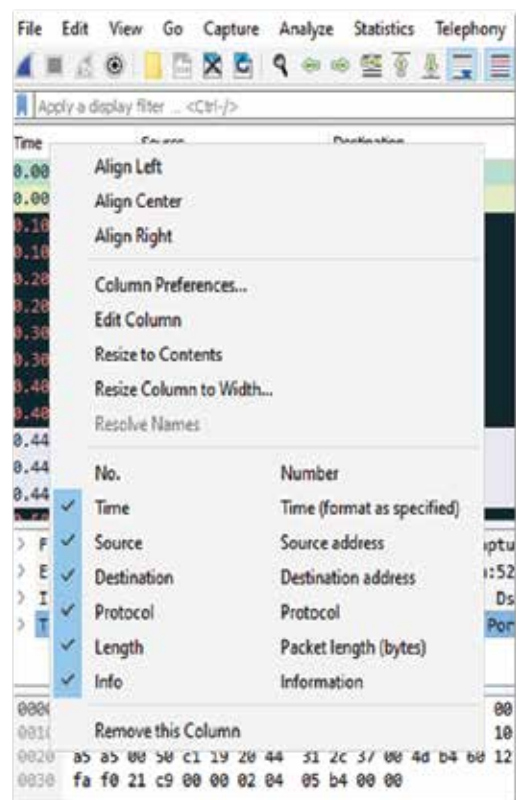
The Default view of Wireshark is not very friendly to every user, so Wireshark gives a functionality to the user to customize the interface of the Wireshark according to their choice or need. The default column in the Wireshark is not ideal in every case. Here comes the need to modify the columns. The default columns are:

- No: It is the frame number from the beginning of the PCAP.
- Time: Seconds are broken down into Nanoseconds.
- Source: Source address.
- Destination: Destination address.
- Protocol: Used in Ethernet Frame, IP Packet, or TCP segment.
- Length: Length of Frame in Bytes.

So, following are the ways to customize the columns in the interface:

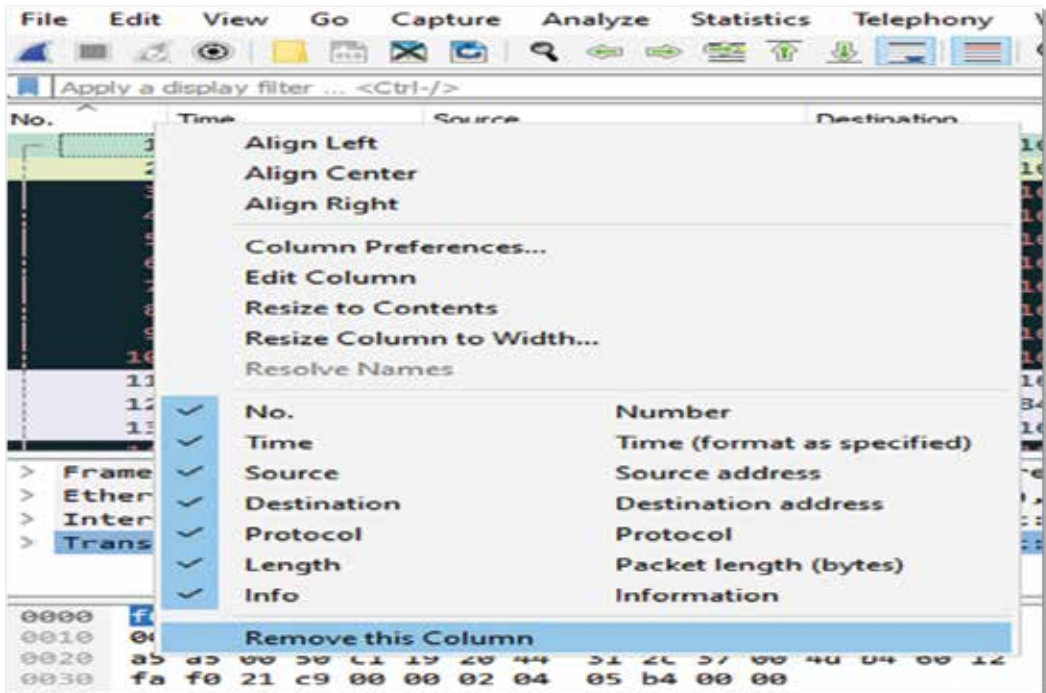
a. Hiding Columns:

We can easily hide the columns in the interface, we can also unhide the columns when there is a need to use the columns. First Right-Click on the Column which you want to hide and then uncheck the column name. And to unhide the column, you just need to check the column name again. Following Figures shows the way how to hide the columns:



b. Removing Columns:

There are some of the columns in the interface which are not required for the analysis like the **NO** column and the **Length** column. We can also remove these columns. For this we just need to Right Click on that column and then Select **Remove this Column** option from the drop-down menu.

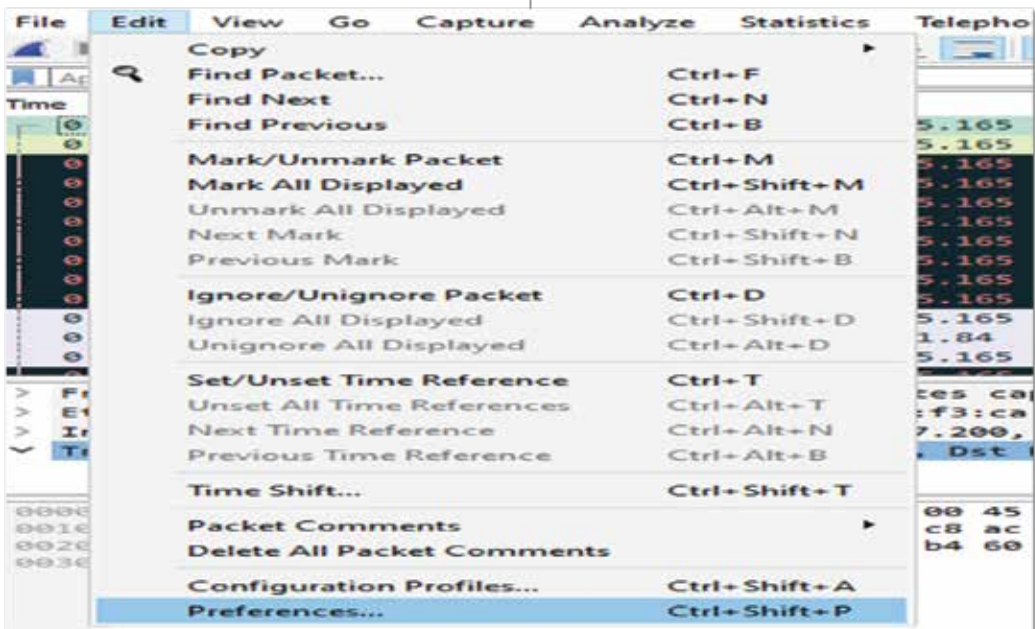


c. Adding Columns:

Wireshark also provide us with the feature which allows us to add the column of our own choice. For Adding the column, you must go through from the number of steps listed below:

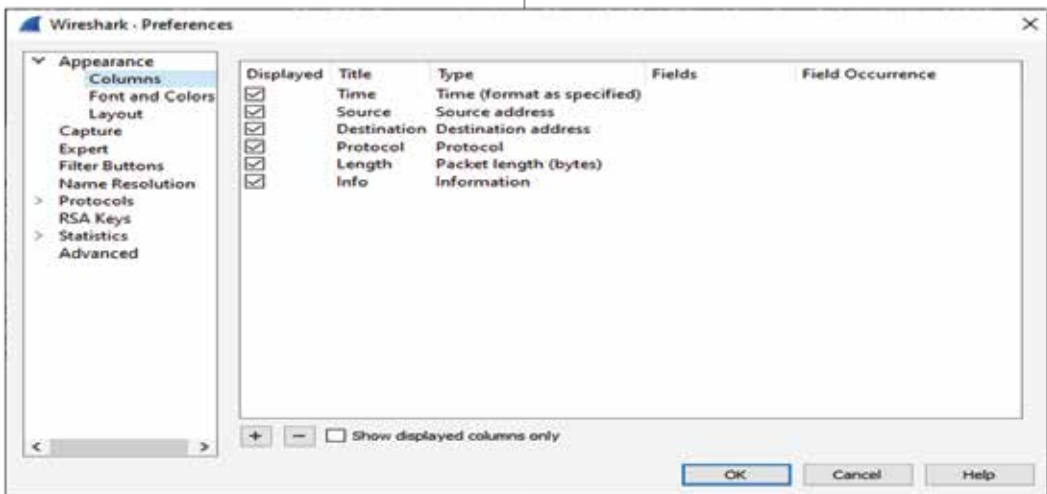
STEP 01:

Go to the **Edit** on the menu and then select **Column Preference** option from the drop-down menu.



The Column Preference Menu List all columns, viewed or hidden at the bottom of the menu there are two buttons **plus (+)** and **minus**

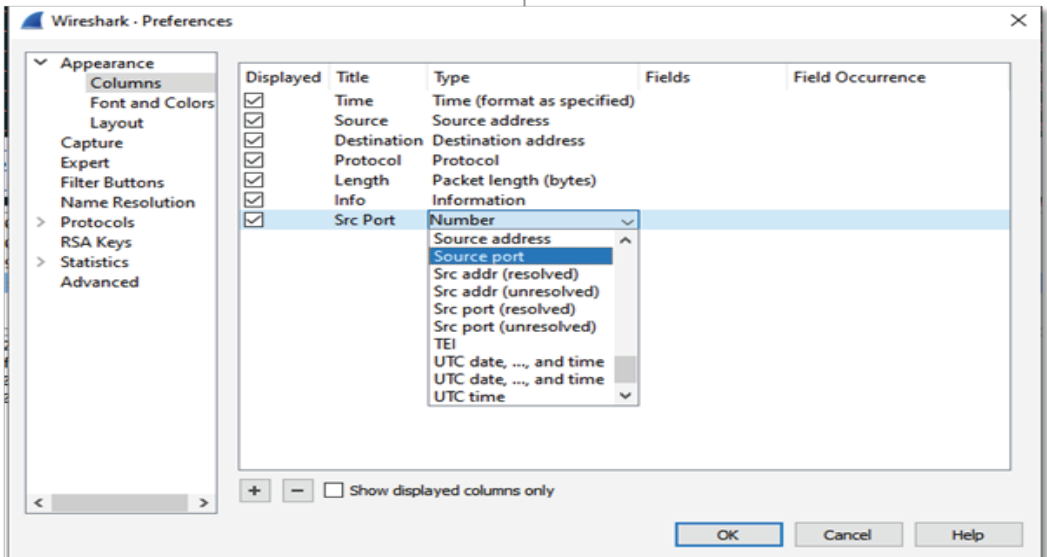
(-) which are used to add or remove the column respectively.



STEP 02:

If you want to add a column, you just need to click on the plus sign, a new row will appear

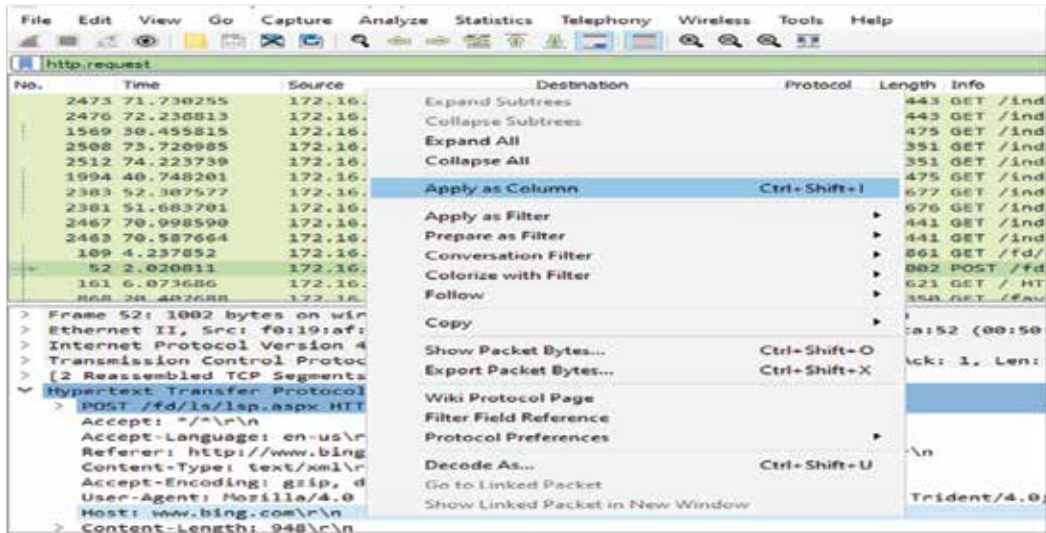
and then rename the Column and select the type of your column.



Same case goes with the removing column. After setting up this click on **OK**. Now, you have successfully changed the columns of the Wireshark interface.

d. Apply As Column:

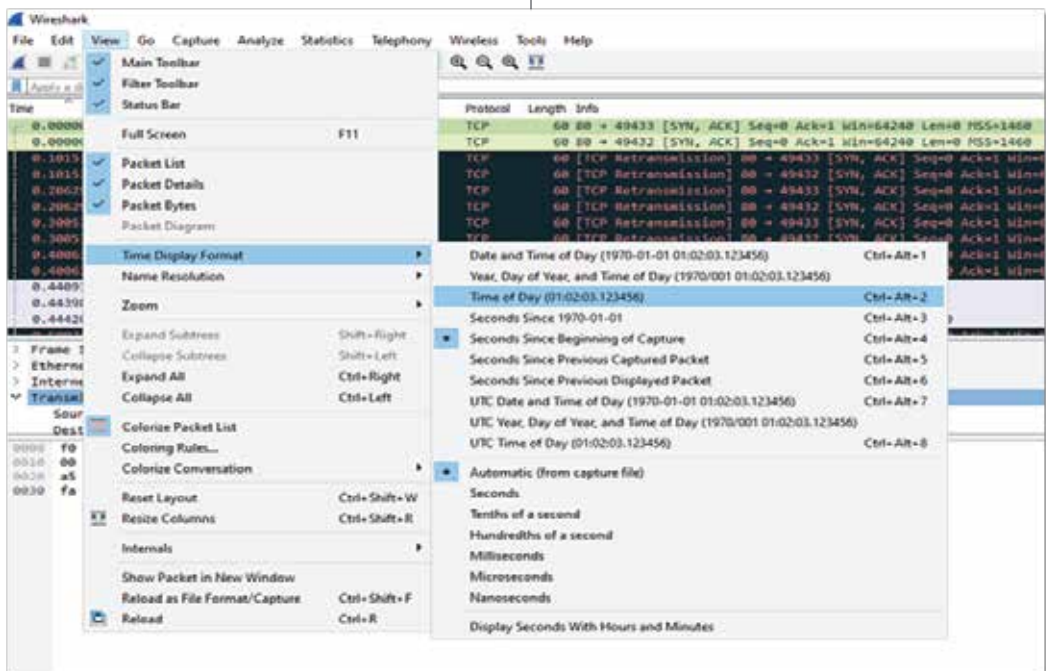
If you want to apply any field from the Packet Window Detail as a column, you need to Right-Click on that field. Choose Apply as Column option and then it will be displayed as column.



e. Time Display:

We can also change the format of the displayed time. The default syntax of the time is seconds broken down into Nanoseconds which in real is like 0.101536. You can also change this

syntax into readable syntax. First Go to the **View** from the **Menu** and then choose **Time Display Format**, now choose the format of your own choice.



5. Detection Of Malware:

Initially, we will check the traffic, if they were

sent in continuous packets, then they will be exportable through Wireshark itself or if not then we have to manually analyze the streams

and packets. Detection of malware includes number of steps:

- Analyze the network traffic present in the packet through protocol hierarchy.
- Check the greater percentage of network protocol i.e., HTTP/HTTPS, SMB etc.
- Analyze all the packets present in the traffic.
- Sort the objects with the Content-Type.
- Locate suspicious files and take hashes of those files by using hashmyfile [8].
- Cross Check the hashes of suspicious files by putting those hashes in Virus Total [9].

Sometimes malicious traffic can also be detected through different destination port for example: victim is connecting through port:80 and attacker is connecting through port:143 sounds malicious.

6. Case Study:

Let's consider a case study [10]. Here we have a packet which contains the logs of malicious files. These files are responsible to make the machine infected. Now we must do some

investigation in that packet to give the answers to some questions listed below. This section of the document covers that how and where to get the information in in the packet.

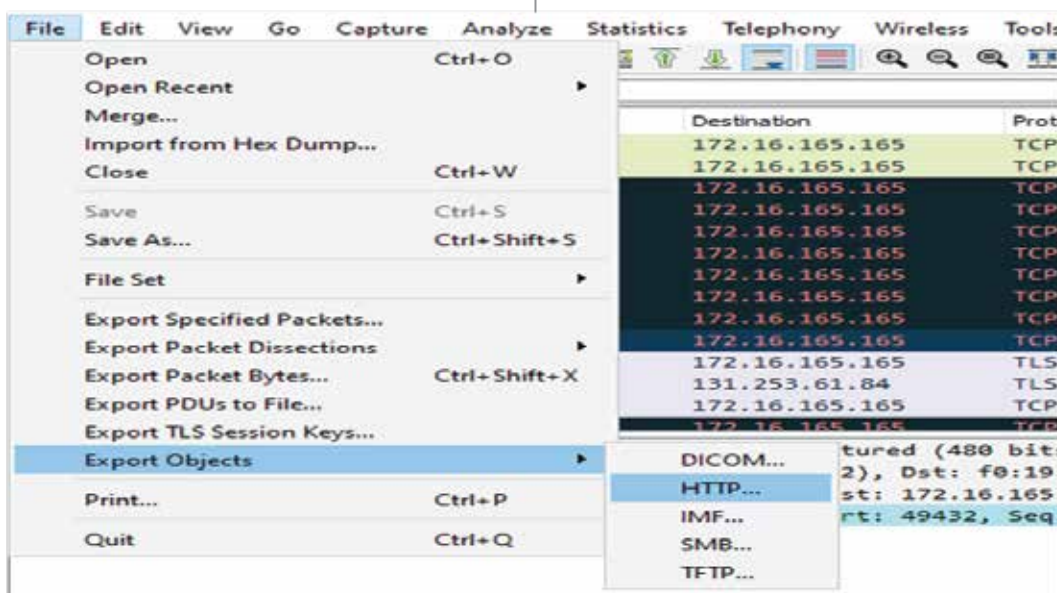
Questions

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

Question No. 01:

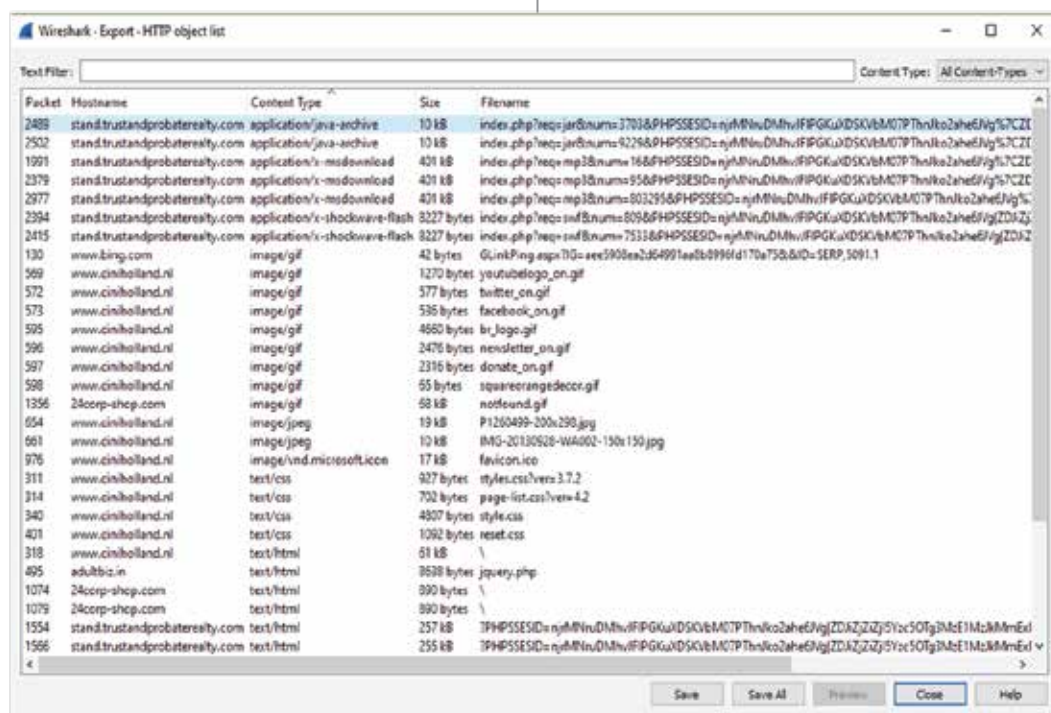
STEP 01:

Go to the file drop-down in the menu bar and then choose Export Objects. Then another drop-down will appear which will show some of the options like HTTP. As most of the traffic in the packet logs were of HTTP, so we will choose HTTP option from the menu.



After doing the above step, a window will appear with the name Wireshark – Export – HTTP object list. It will describe the information of every downloadable material. We can

sort the Content Type alphabetically just by clicking the Content Type. Now save every file.



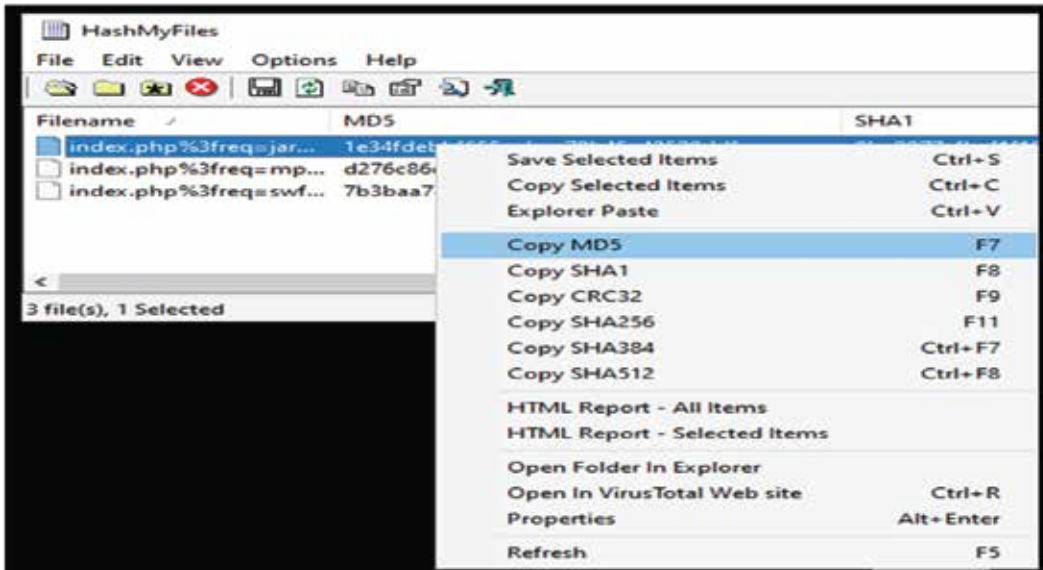
Take hashes of every file you downloaded from the list with the help of *hashmyfiles*

software.



After getting the hashes, copy those hashes of any type one by one and then put those hashes

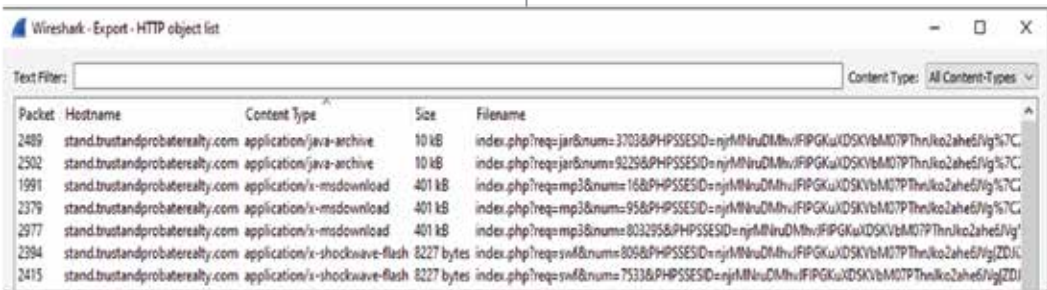
in the virus total that will show if these hashes are infected or not.

**Question No. 02:**

Solution of Question no. 01 shows the infected files. Now the question is to get the URL/Domain of the infected site. Again, follow the steps mentioned in the Question No. 01 till the window appear with the name Wireshark – Export – HTTP object list. In this window, there is a column named as hostname. This column will give us the answer of Question No. 02.

Question No. 03:

We have already found the infected site hostname. Now we are going to find the IP address of that infected site. For this, just put the filter *http.request*. It will only show the logs requested by the user. In the Destination Column, we can easily find the IP address of the infected site.

Question No. 04:

With the same filter, we can find the IP address of the infected machine. The Source Column shows the IP address of the infected machine.

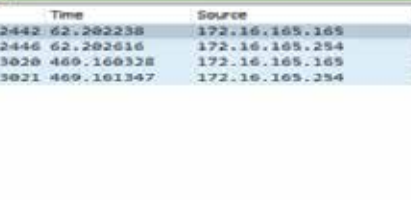
QUESTION NO. 05:

There is more than one way to get the

hostname of the infected machine. Some of them are described below:

WAY 01:

Put the DHCP filter in the filter box. Some of the packets will be shown. Click any of the



The screenshot displays a network traffic analysis interface. The top section shows a list of captured packets. The bottom section provides a detailed view of the selected packet (No. 3021), which is a DHCP message. The details include the relay agent IP address, client MAC address, client hardware address padding, server host name, boot file name, magic cookie, and a list of DHCP options.

No.	Time	Source	Destination
2442	62.202238	172.16.165.165	255.255.255.255
2446	62.202616	172.16.165.254	172.16.165.165
3020	469.160328	172.16.165.165	172.16.165.165
3021	469.161347	172.16.165.254	172.16.165.165

Relay agent IP address: 0.0.0.0
 Client MAC address: f0:19:af:02:9b:fi (f0:19:af:02:9b:fi)
 Client hardware address padding: 000000000000
 Server host name not given
 Boot file name not given
 Magic cookie: DHCP
 > Option: (53) DHCP Message Type (Inform)
 > Option: (61) Client identifier
 ✓ Option: (12) Host Name
 Length: 12
 Host Name: K34EN6u3N-PC
 > Option: (60) Vendor class identifier
 > Option: (55) Parameter Request List
 ✓ Option: (255) End

name of the infected machine.

Question No. 06:

No.	Time	Source	Destination	Protocol	Length	Host	Info
2400	53.160900	172.16.165.165	172.16.165.2	HTTP	118		Refresh NO C34EHLGN-PC(00)
2430	54.060204	172.16.165.165	172.16.165.2	HTTP	118		Refresh NO C34EHLGN-PC(00)
2439	56.160211	172.16.165.165	172.16.165.2	HTTP	118		Refresh NO C34EHLGN-PC(00)
2440	62.502002	172.16.165.165	172.16.165.2	HTTP	92		Name query NO SPAD(00)
2451	64.002559	172.16.165.165	172.16.165.2	HTTP	92		Name query NO SPAD(00)
2453	65.502640	172.16.165.165	172.16.165.2	HTTP	92		Name query NO SPAD(00)

The screenshot shows the Wireshark interface with a packet capture of network traffic. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for common actions like opening files, saving, and zooming.

The main pane displays a list of captured packets. The first packet selected is an HTTP GET request from source IP 172.16.165.165 to destination IP 82.150.140.30. The full request URI is http://www.cinihiolland.nl/wp/. The packet details pane on the right shows the Ethernet II header, indicating it was received from a VMware adapter (VMware_f3:ica:52).

No.	Time	Source	Destination	Protocol	Length	Full request URI
570	11.202403	172.16.165.165	82.150.140.30	HTTP	457	http://www.cinihiolland.nl/wp/
579	11.202596	172.16.165.165	82.150.140.30	HTTP	448	http://www.cinihiolland.nl/wp/
650	12.073745	172.16.165.165	74.125.233.96	HTTP	602	http://www.youtube.com/embed/
868	28.402688	172.16.165.165	82.150.140.30	HTTP	358	http://www.cinihiolland.nl/fav
981	21.787961	172.16.165.165	188.225.73.100	HTTP	505	http://24corp-shop.com/
982	21.787964	172.16.165.165	188.225.73.100	HTTP	585	http://24corp-shop.com/
1076	22.631140	172.16.165.165	188.225.73.100	HTTP	413	http://24corp-shop.com/source
1212	23.664539	172.16.165.165	37.200.69.143	HTTP	695	http://stand.trustandprobatr
1213	23.664644	172.16.165.165	37.200.69.143	HTTP	695	http://stand.trustandprobatr
1509	30.455615	172.16.165.165	37.200.69.143	HTTP	473	http://stand.trustandprobatr
1994	40.748201	172.16.165.165	37.200.69.143	HTTP	475	http://stand.trustandprobatr
2381	51.683701	172.16.165.165	37.200.69.143	HTTP	677	http://stand.trustandprobatr
2488	52.308727	172.16.165.165	37.200.69.143	HTTP	677	http://stand.trustandprobatr

The bottom pane shows the expanded details of the selected packet (Frame 578). It indicates that 457 bytes were captured on the wire (3656 bits) over an Ethernet II interface. The source MAC address is f0:19:af:02:9b:f1 and the destination MAC address is f3:ica:52. The source IP is 172.16.165.165 and the destination IP is 82.150.140.30.

35

7. Conclusion

According to the author and the co-author, detection of malware in a packet is an interesting activity in investigating it. The above-mentioned ways to detect the malware was related to the HTTP traffic. The reader can have a basic understanding of malware analysis in traffic.

8. References:

- [1] I. Ahmed and K. suk Lhee, "Classification of packet contents for malware detection," *Journal in Computer Virology*, vol. 7, no. 4, 2011.
- [2] N. Dutta, N. Jadav, S. Tanwar, H. K. D. Sarma, and E. Pricop, "Introduction to Malware Analysis," in *Studies in Computational Intelligence*, vol. 995, 2022.
- [3] R. S. Kunwar and P. Sharma, "Malware analysis: Tools and techniques," in *ACM International Conference Proceeding Series*, 2016, vol. 04, March-2016.
- [4] B. Dodiya and U. K. Singh, "Malicious Traffic analysis using Wireshark by collection of Indicators of Compromise," *Int J Comput Appl*, vol. 183, no. 53, 2022.
- [5] T. Moore and R. Clayton, "Which malware lures work best? Measurements from a large instant messaging worm," in *eCrime Researchers Summit, eCrime*, vol.5, 2015.
- [6] V. Jain, "Getting Familiar with Wireshark," in *Wireshark Fundamentals*, 2022.
- [7] N. Pachhala, S. Jothilakshmi, and B. P. Battula, "A Comprehensive Survey on Identification of Malware Types and Malware Classification Using Machine Learning Techniques," in *Proceedings - 2nd International Conference on Smart Electronics and Communication, ICOSEC 2021*, 2021.
- [8] X. Zhong, Y. Fu, L. Yu, R. Brooks, and G. K. Venayagamoorthy, "Stealthy malware traffic - Not as innocent as it looks," in *2015 10th International Conference on Malicious and Unwanted Software, MALWARE 2015*, 2016.
- [9] B. A. Mah, "Empirical model of HTTP network traffic," in *Proceedings - IEEE INFOCOM*, 1997, vol. 2.1997.
- [10] M. Yaibuates and R. Chaisricharoen, "A Combination of ICMP and ARP for DHCP Malicious Attack Identification," in *2020 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering, ECTI DAMT and NCON 2020*, 2020.