TrackIT

Introduction to Malware Analysis and Wireshark

Sri Lanka Information Technology

Individual Assignment

IE 2012

System and Network Programming

IT21197550

Nihila Premakanthan

Contents

Introduction 3
Malware 4
Classification of Malware 4
Prevention from Malware 6
Detection from Malware 6
Removal of Malware 6
Protection from Malware 6
Introduction to Malware Analysis 7
Techniques of Malware Analysis 7
Introduction to Wireshark 9
Filtering Packets through HTTP Requests 11
Exporting objects from HTTP 13
Capturing File Properties 25

Introduction

This book is for anyone who wishes to learn about malware and malware analysis. This mainly focuses on the packet analysing tool Wireshark. Further it also recommended to try out the try hack me room named ‘TrackIT’ to get more clear understanding about the malware analysis.

It is Malicious Software. It is a software that is specifically designed to harm computer data in some way. Virus, worm, trojan horse, backdoor, spyware and rootkit are some of the classifications of malware.

The main aim of malware analysis is to study a program's behavior and verify if it has a malicious functionality. It is better to use a virtualization software like VMWare or Virtual Box.

Malware

All malicious software is considered as malware. Software that is used to try to violate the availability, confidentiality, or integrity of a computer system's security policy. Malware aims to give an attacker remote control over an infected machine, broadcast spam from the infected machine to unknowing targets, look into the local network of the affected user, and steal important data.

Viruses, worms, trojan horses, ransomware, bots or botnets, spyware, rootkits, fileless malware, and malvertising are the most prevalent types of malware.

And while a malware attack's ultimate objective—to access user data or destroy the device, typically for financial gain—is frequently the same, the distribution techniques might vary. Some of them may even combine these malware varieties.

Classification of Malware

1. Viruses

   Viruses are a sort of malware that are frequently introduced by victims into an application, program, or system in the form of a piece of code. Viruses are among the most prevalent forms of malware, and they share characteristics with physical viruses in that they both need a host, or a device, to survive.

   They wait to strike until they are activated, maybe by consumers receiving email attachments, which are frequently executable files with the extension.exe. From there, the virus multiplies by making copies of itself and spreading them from machine to computer to cause the most destruction.

2. Worms

   Worms are a kind of malware that self-replicates, much like malware viruses do. However, unlike viruses, worm malware may replicate itself without the assistance of a human and is not host-dependent, therefore it is not required to attach to a piece of software in order to harm it. Software flaws can be the source of worm transmission.

They may also be downloaded from portable media, sent as attachments via emails or direct conversations, or both. When these files are opened, they could connect to a malicious website or launch the computer worm automatically. After being installed, the worm silently starts to work and discreetly infects the computer or even entire networks.

3. Trojan Horse

   Trojans are a sort of malware that impersonates legitimate programs, files, or software in order to trick users into downloading it and unwittingly handing over control of their devices. A trojan can carry out its intended function once it has been installed, whether it be to hurt, interfere with, steal from, or cause another type of harm to your data or network. Trojan malware, also referred to as a Trojan horse or Trojan horse virus, is frequently disseminated through email attachments, website downloads, and direct communications. They require user action to be distributed, just like viruses do. The distinction between malware viruses and trojans is that viruses are host-dependent, whereas trojans are not. Like viruses, Trojans also do not replicate themselves.

4. Ransomware

   As its name suggests, ransomware is a category of malware that demands a ransom. It locks and encrypts the victim's computer or other assets, then requests a ransom to decrypt it. Frequently, victims unintentionally download this particular malware through email attachments or links from unreliable sources. Once installed, the malware may allow hackers to access a device through a backdoor before starting to encrypt the data and locking users out of their devices until they pay a ransom to recover control. It's important to note that ransomware, also known as crypto-malware, is increasingly being paid for in cryptocurrencies.

Prevention from Malware

Malware detection and prevention are accomplished using a range of security technologies. These include content filtering, data leak prevention systems, virtual private networks, firewalls, next-generation firewalls, network intrusion prevention systems (IPS), deep packet inspection (DPI) capabilities, and unified threat management systems. All security solutions should be tested using a variety of malware-based assaults to make sure they are functioning effectively in order to avoid malware. To ensure testing is done against the most recent assaults, a strong, up-to-date collection of malware signatures must be used.

Detection from Malware

Firewalls, IPSs, and sandboxing programs are examples of sophisticated malware analysis and detection techniques. Some malware types, like ransomware, which quickly becomes visible after encrypting your files, are simpler to spot than others. Other malware, such as spyware, may stay on a target system undetected for an adversary to continue having access to it. No matter the sort of malware, what it does, how easily it may be detected, or who uses it, using malware is always done with evil intent.

Removal of Malware

A virus manage to evade detection by antivirus software, malware removal offers solutions used to remove malware from a machine that has been infected.

Protection from Malware

You require an all-encompassing, enterprise-wide malware security approach to safeguard your device from malware. Using a combination of antivirus, anti-spyware, and vulnerability protection technologies combined with URL filtering and Program identification capabilities on the firewall, commodity threats are exploits that are less sophisticated and more readily discovered and blocked.

Introduction to Malware Analysis

Analysing malware has various advantages. First, we can comprehend the malicious actions that the malware intends to carry out. We will be able to identify which machines contain the virus and take corrective action, such as deleting it or even erasing the machine clean and reinstalling everything, as well as upgrade our network and endpoint sensors to detect and stop such activity. Second, by examining the malware's design and coding, we may be able to gather data that could be valuable for attribution—that is, for us to be able to pinpoint the most likely creator and operator. Third, we can more accurately comprehend and forecast the breadth and trend of malware attacks by comparing it with historical as well as geo-location data. In essence, malware analysis forms the cornerstone for identifying and thwarting intrusions.

Deploying a malware instance in an analysis environment is part of a normal malware analysis process. A network sensor may look at traffic to spot potential malware and test it in a sandbox.

Techniques of Malware Analysis

Learning malware behaviors is the process of malware analysis. We need to be able to quickly conduct thorough, dependable, and scalable analyses of samples due to the number and growing complexity of malware. Because malware frequently contains code designed purposely to defy analysis, these program analysis approaches, which were developed to help the software development process frequently need to be modified or expanded for malware analysis. In other words, detecting and getting around anti-analysis techniques is the main issue in malware analysis.

There are mainly two types of malware analysis

1. Static Analysis

   Static analysis involves reviewing the code to judge a program's behavior without actually running it. Static analysis encompasses a broad range of malware analysis methods. The analysis output might not match the actual malware behaviors, which is one restriction. A more serious issue is that malware writers use code encryption and packing to completely circumvent static analysis because they are well aware of its limitations.

2. Dynamic Analysis

In order to spot harmful behavior, dynamic analysis keeps an eye on how malware is executed. Dynamic analysis ignores behaviors that are not triggered by the input but accurately pinpoints program behaviors in accordance with test input scenarios. Additionally, code encryption strategies intended to avoid static analysis can be defeated via dynamical analysis.

Question 1

Setting your software to auto-update is one way you can help protect your business from ransomware. True(T) or False(F)?

T

Question2

Local backup files which are saved on the computer will protect the data from being lost in a ransomware attack. True(T) or False(F)?

F

Introduction to Wireshark

Wireshark is a network packet analyzer. It displays all the details related to the packets captured. This is an open source software and it was also released under the GNU General Public License. Ethernet, Wireless LAN, Bluetooth, USB, and other network media types can all have their traffic captured by Wireshark.

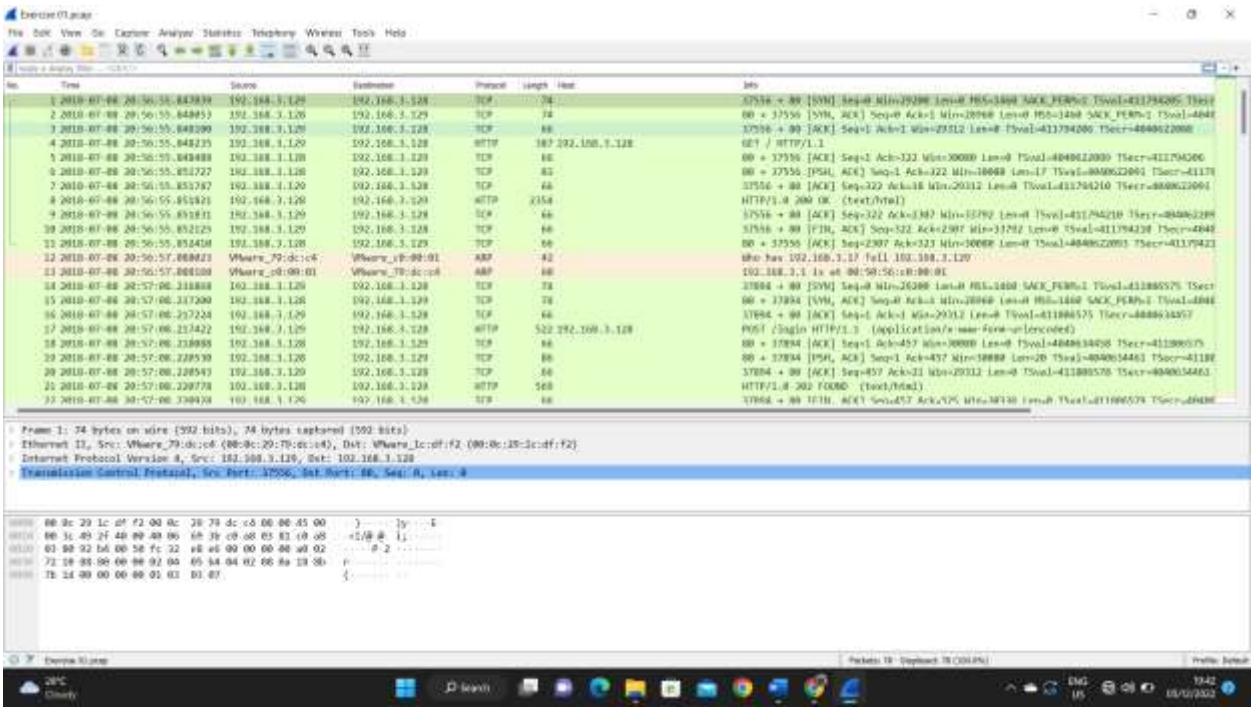
It is used by network security engineers to look at security issues and by network administrators to troubleshoot network issues. Further it is used to test network applications by QA engineers. To debug protocol implementations, developers use it and to learn the internals of network protocols, individuals use it.

Depending on your environment and the size of the capture file you are studying, Wireshark may require a certain number of resources. The numbers listed below should work well for capture files that are modest to medium in size and do not exceed a few hundred MB. More memory and storage space will be needed for larger capture files.

Huge capture files can be created by an active network. Even on a hundred-megabit network, capturing can quickly generate hundreds of megabytes of data. It is always a good idea to get a computer with a quick CPU, plenty of memory, and storage space.

Features of Wireshark

1. This application runs on UNIX and windows platform
2. It captures data packets through a network interface
3. It saves data from the packets captured
4. It filters and searches packets based on certain criteria
5. It imports packets from text files containing hex dumps.
6. It displays detailed protocol information of the packets.



The main window consists parts such as menu, main toolbar, packet list, packet details, packet byte details and status bar.

Following are some functionalities of each part

- Menu - Used to start actions
- Main toolbar - Provide access to frequently used items
- Filter toolbar - Filter packets based on certain criteria
- Packet List - Summary of each packet captured
- Packet Bytes - Display data from packets selected
- status bar - Detailed information about the current program state and captured data

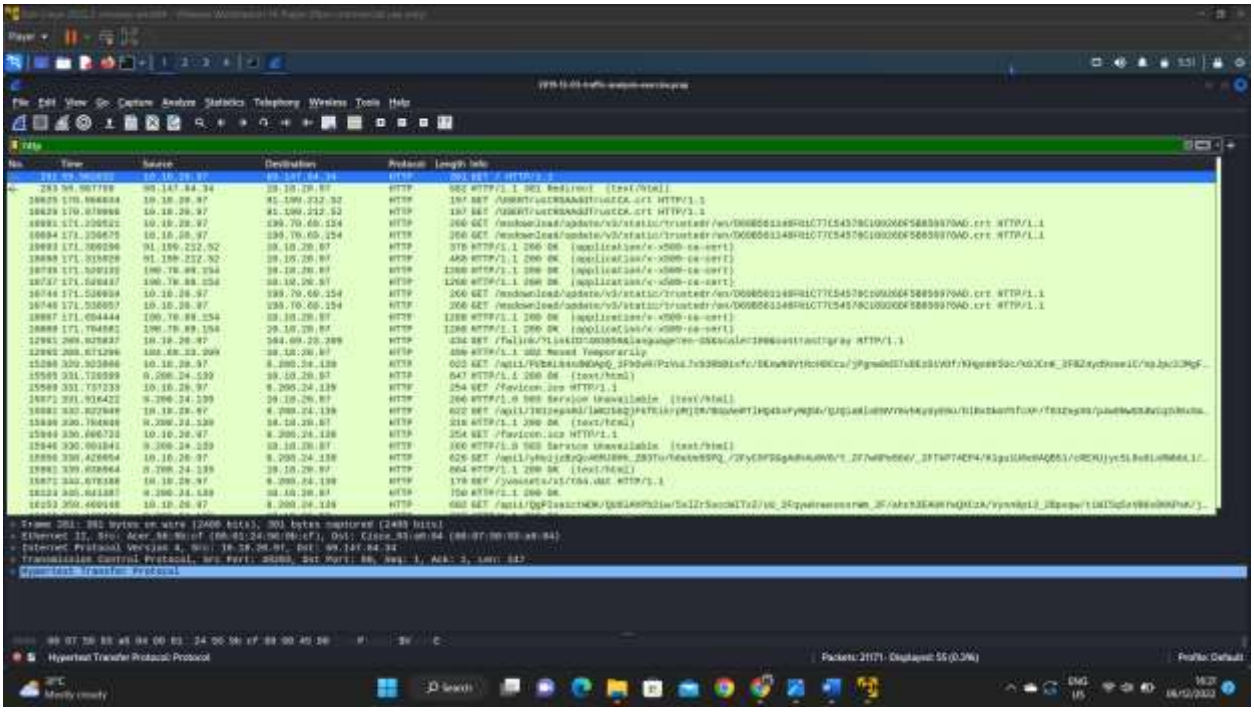
Filtering Packets through HTTP Requests

HTTP

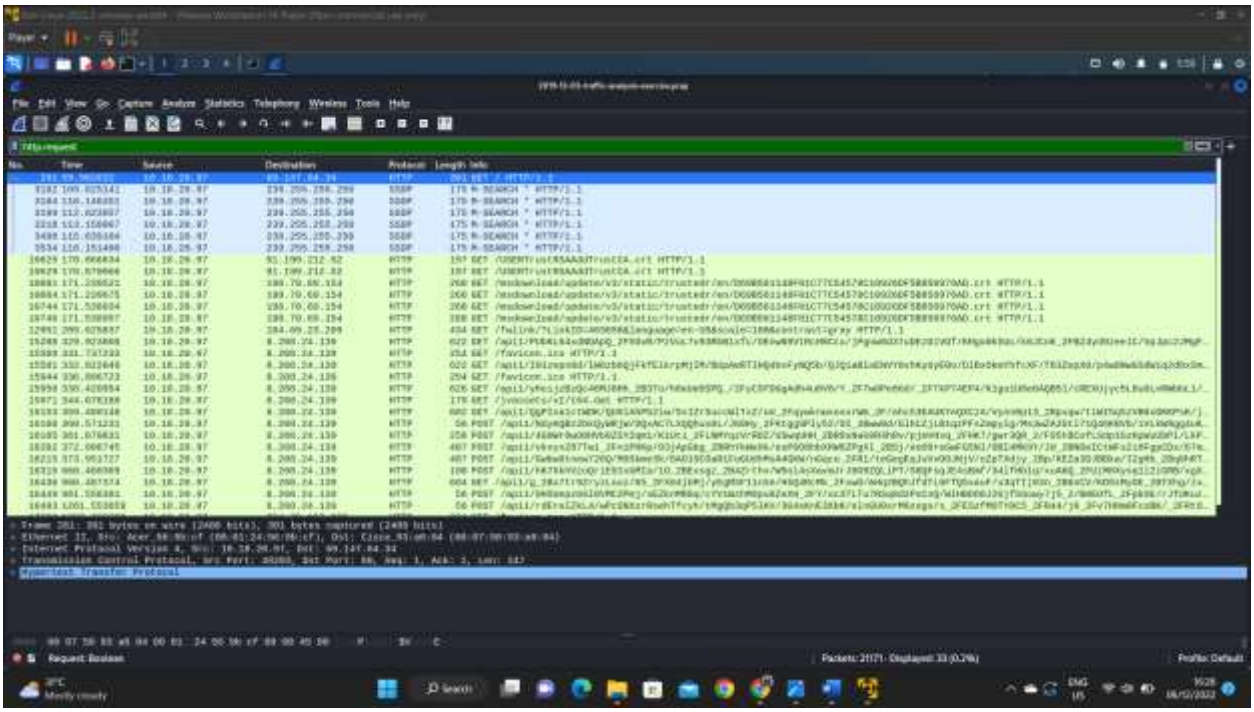
HyperText Transfer Protocol is known as HTTP. It is an access protocol for data on the World Wide Web (www). Data in the form of plain text, hypertext, audio, video, and other formats can all be transferred using the HTTP protocol. Because of its effectiveness in a hypertext context where there are quick jumps from one document to another, this protocol is also known as the "HyperText Transfer Protocol."

Apply the filter HTTP, to get the list of the interfaces with HTTP only and apply the HTTP.REQUEST filter to get the list of GET list of HTTP requests.

Filtering HTTP protocols



Filtering HTTP.request



Question 1

What is the date of the activity?

2019-12-03

Question 2

What is the source IP address of the host that got infected?

10.18.20.97

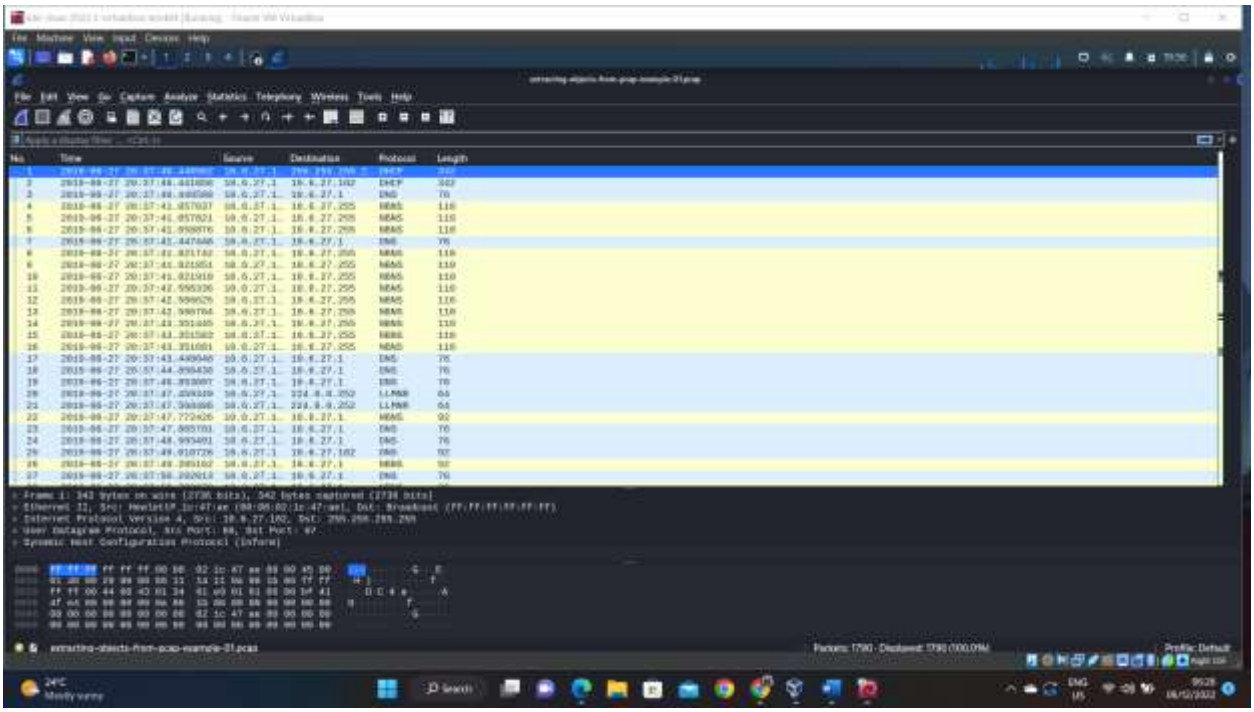
Question 3

What is the MAC address of the host that got infected?

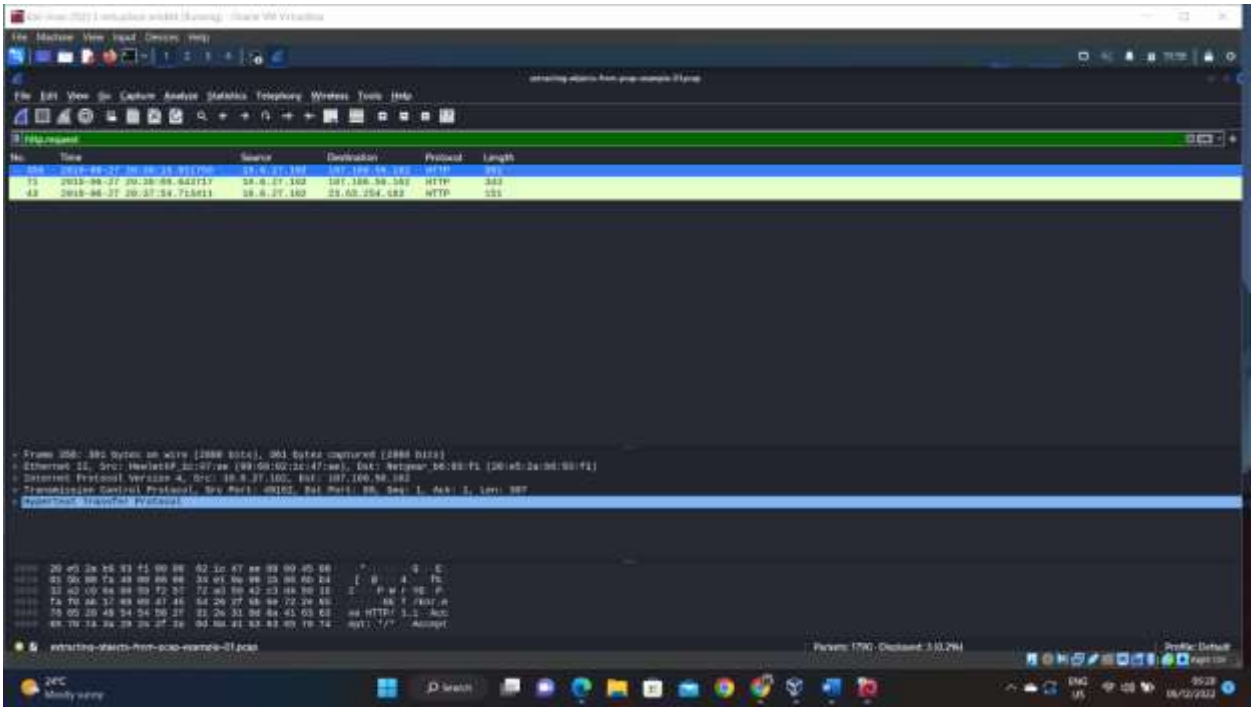
00:01:24:56:9b:cf

Exporting objects from HTTP

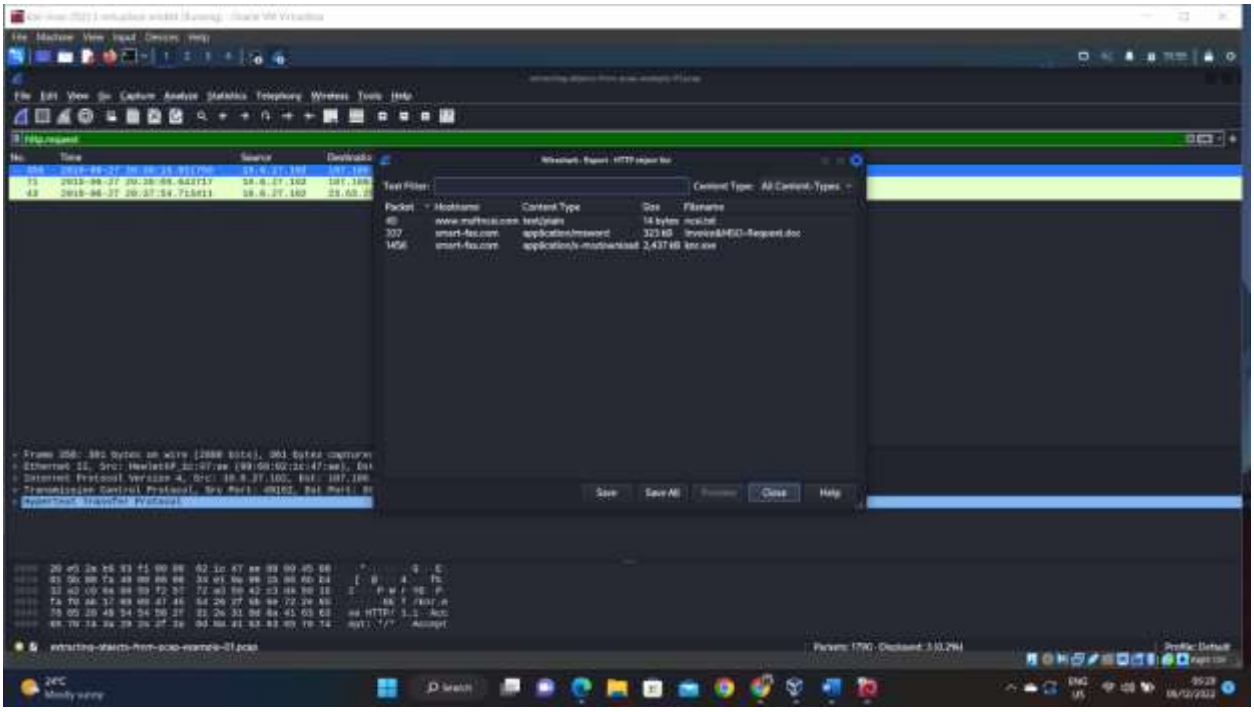
Interface of the pcap file.



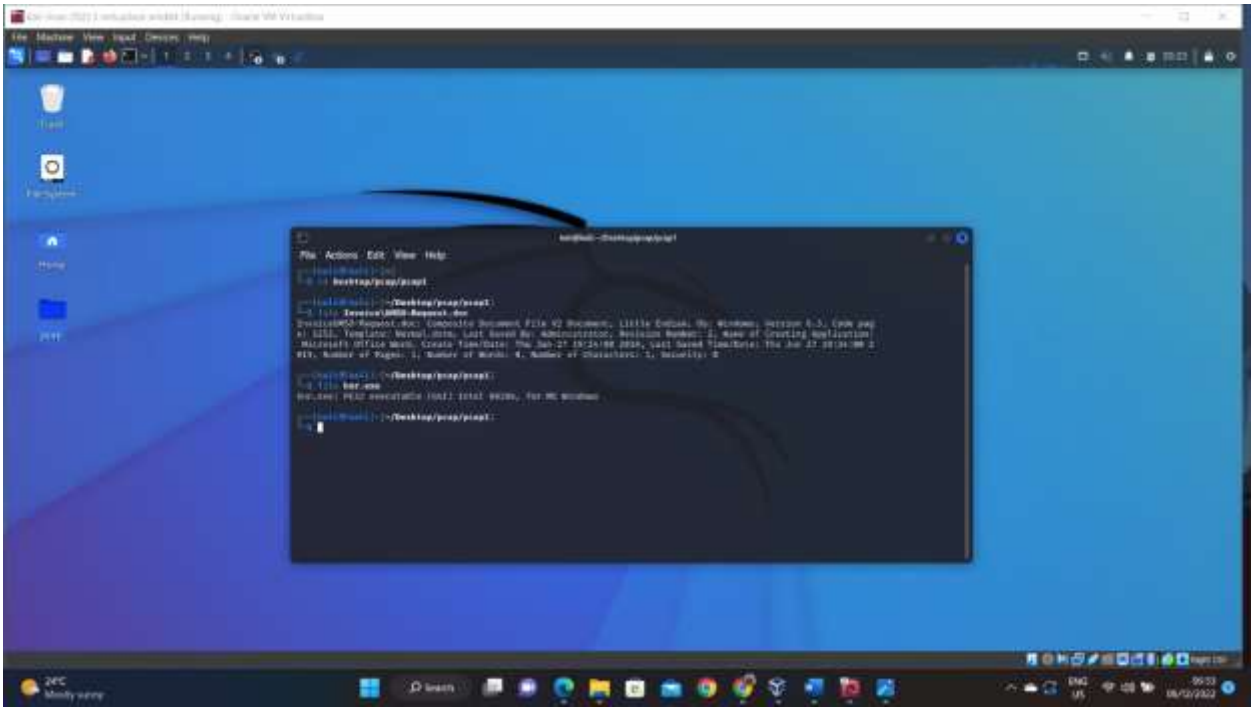
Interface after filtering http.request



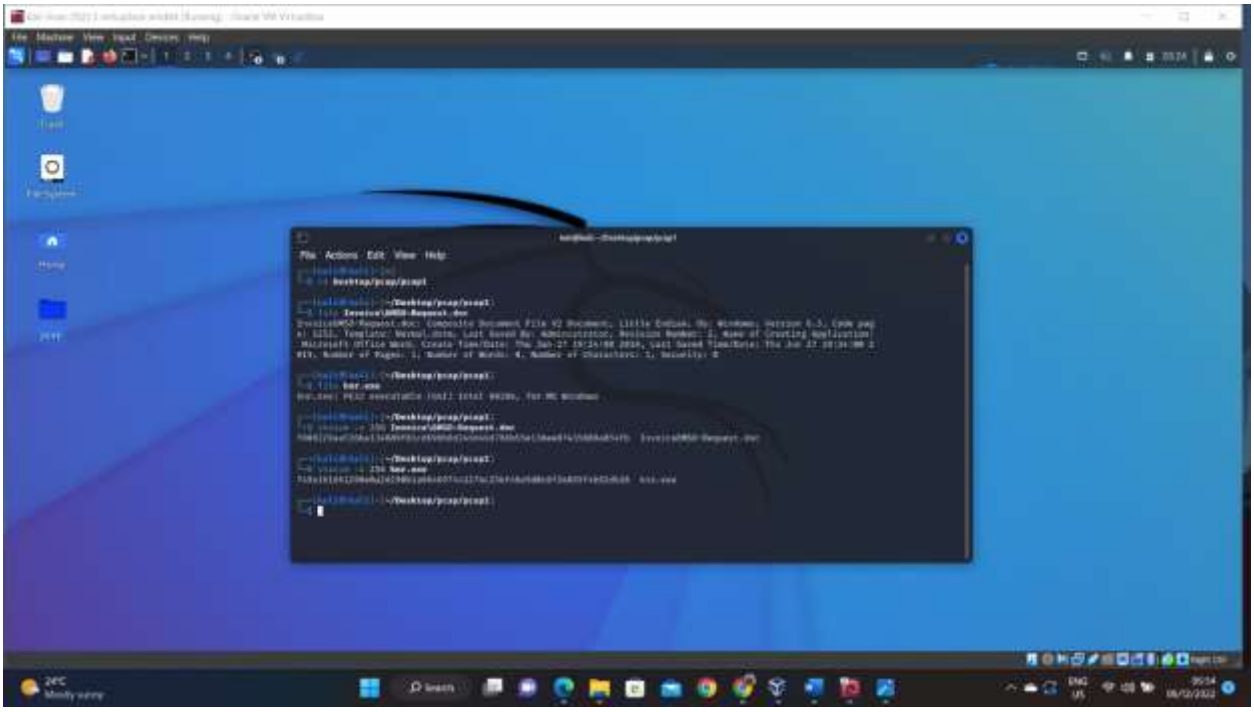
Interface of the http object list



Checking the type of the files



Checking the hash values in the files



Question 1

What is the file type of knr.exe

Executable

Question 2

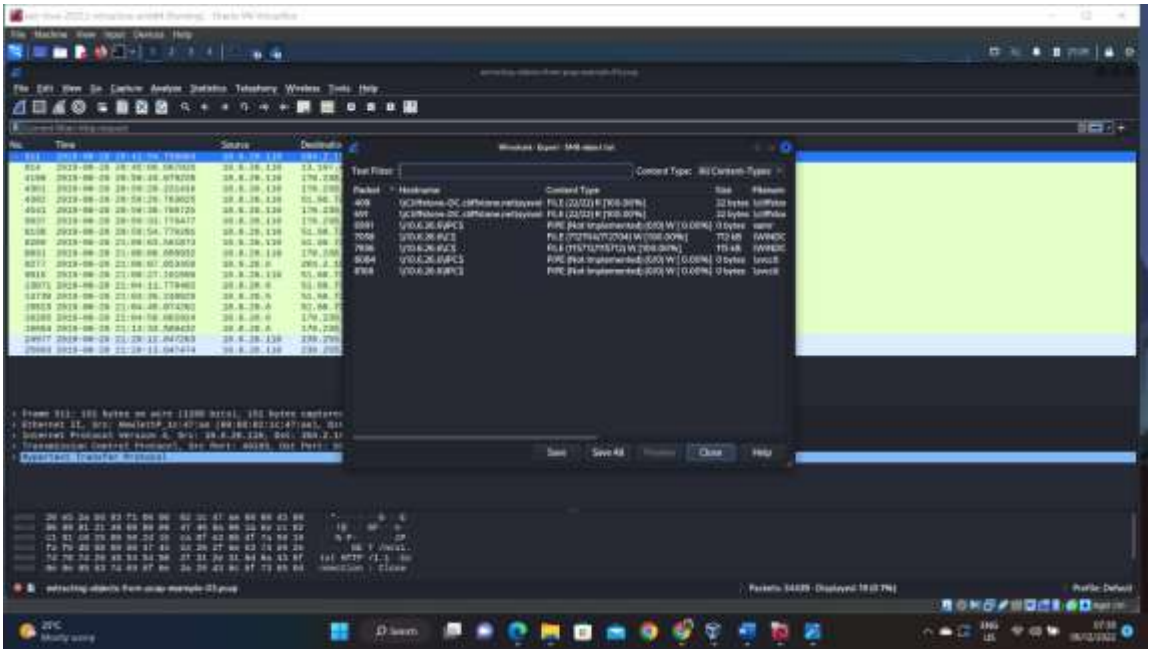
What is the hash value of Invoice&MSO-Request.doc

f808229aa516ba134889f81cd699b8d246d46d796b55e13bee87435889a054fb

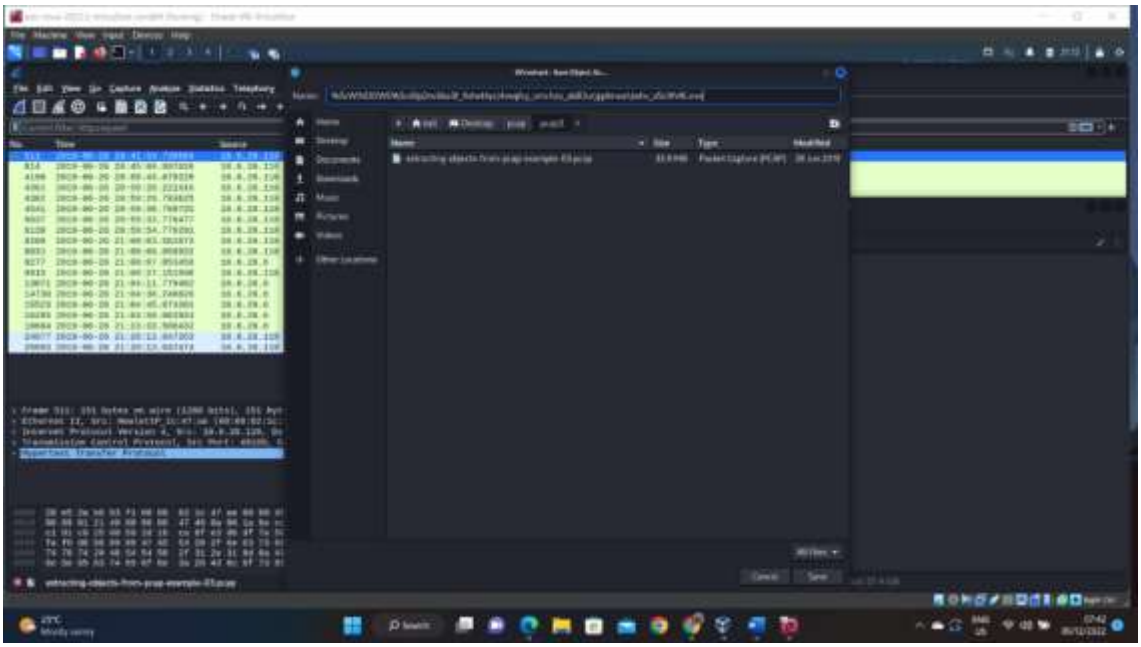
Exporting objects from SMB

To export the objects from the SMB object list use the following menu path:

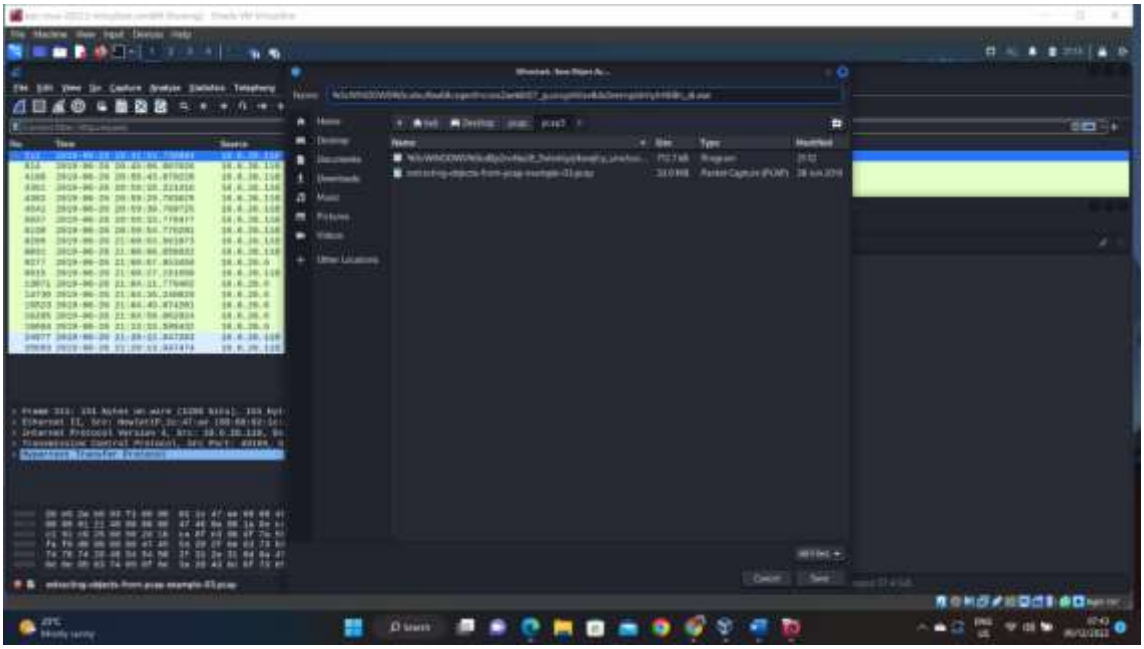
File --> Export Objects --> SMB



Save FILE (712704/712704) W [100.0%] as executable file

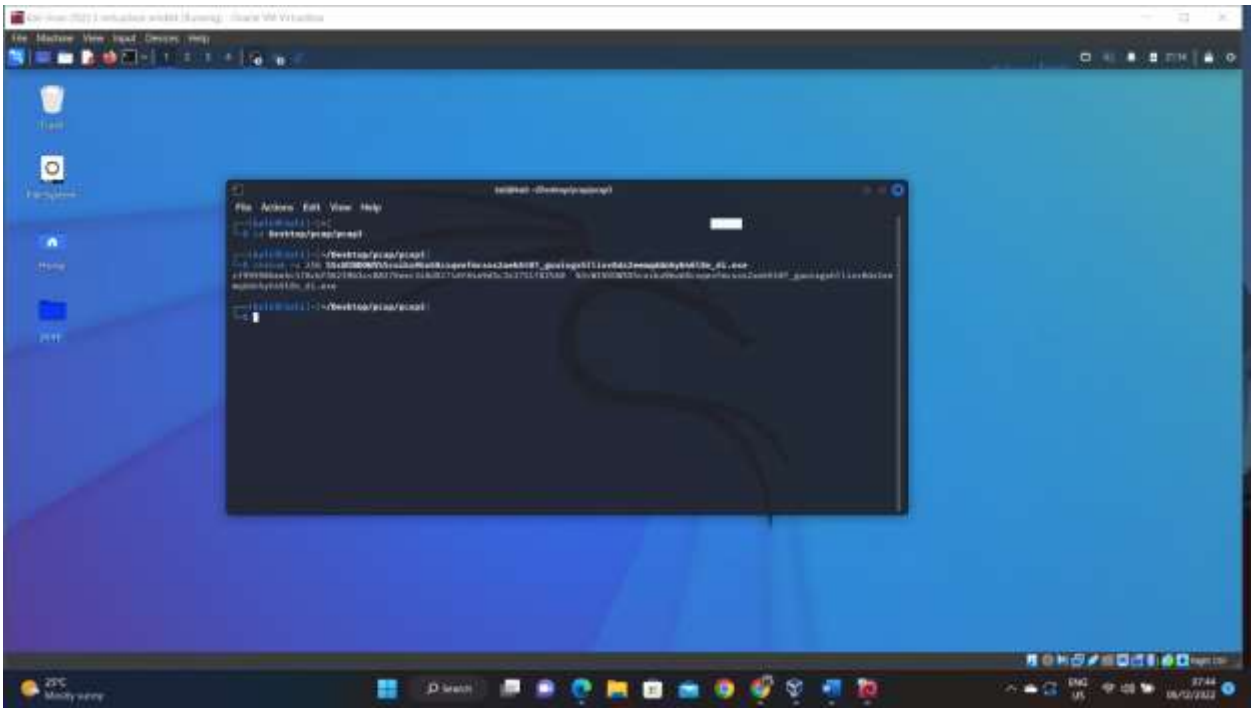


Save FILE (115712/115712) W [100.0%] as executable file.



Run the following command to get the hash of the file

shasum -a 256 {filename}



Question 1

What is the size of the FILE (712704/712704) W [100.0%]?

712 KB

Question 2

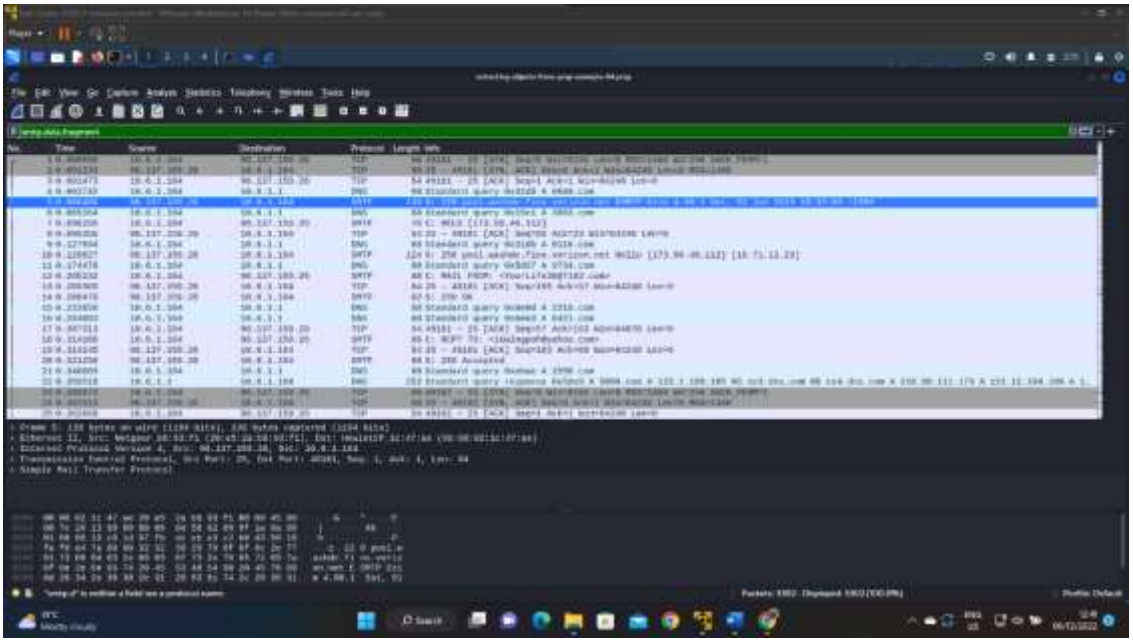
Find the hash value of the FILE (115712/115712) W [100.0%]?

cf99990bee6c378cbf56239b3cc88276eec348d82740f84e9d5c343751f82560

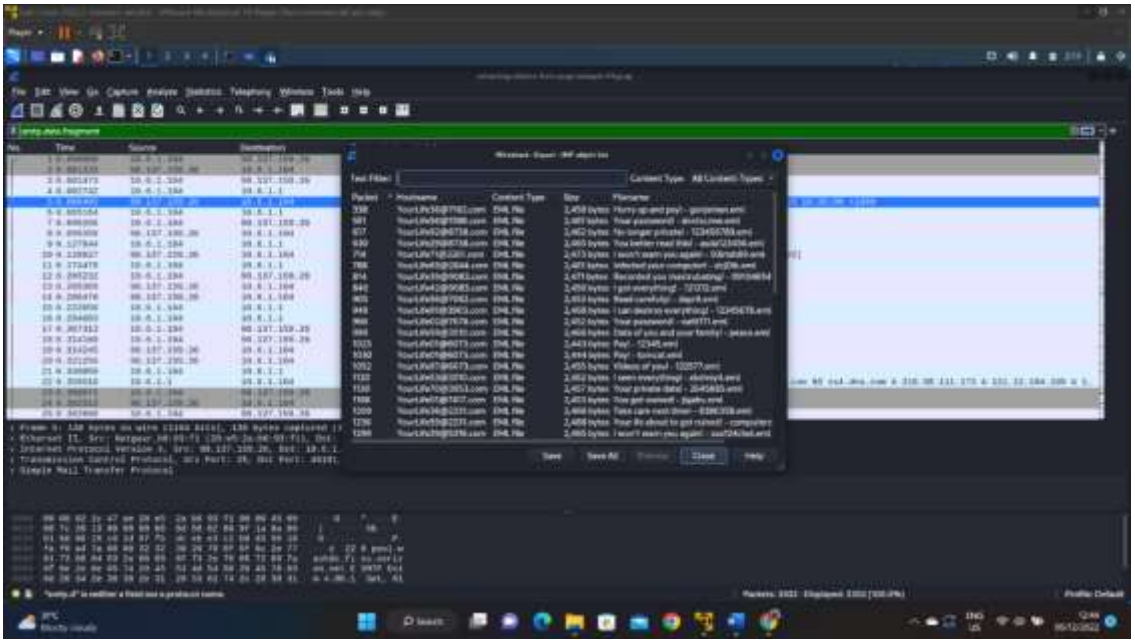
Exporting objects from SMTP

There are certain types of malware that are designed to turn an infected host into a spambot. This is malware that sends hundreds of spam or malicious emails every minute.

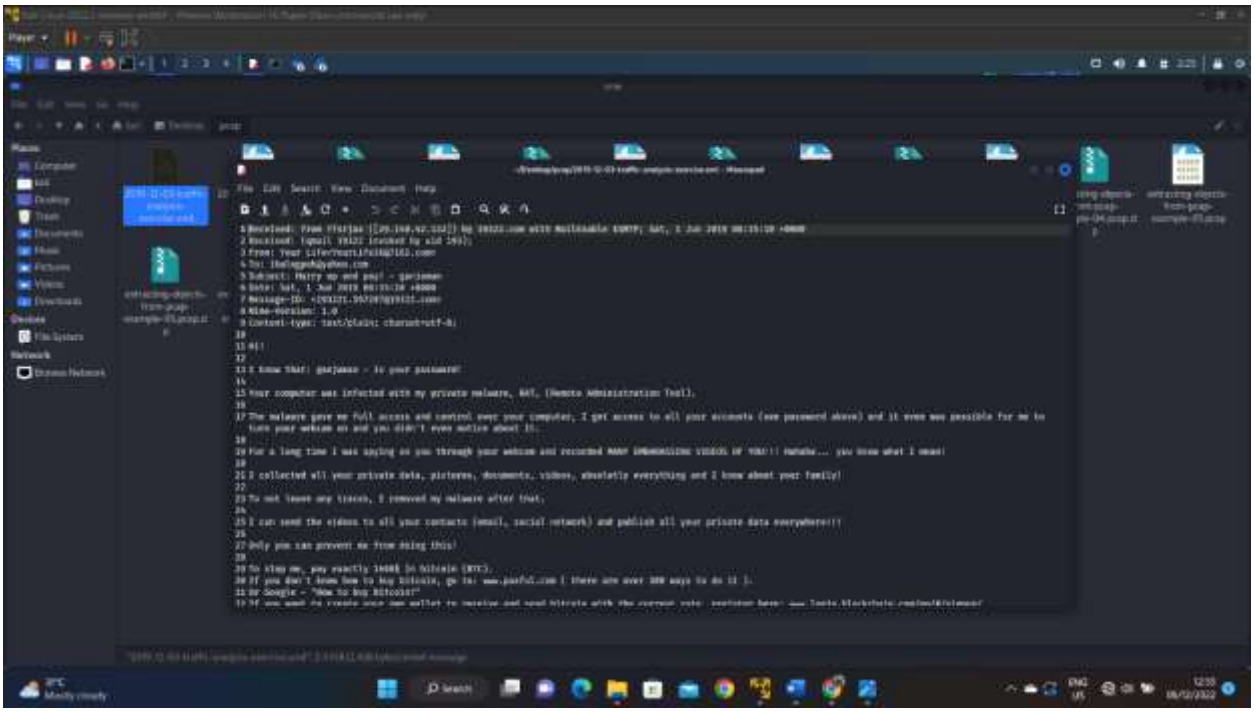
Filtering using smtp.data.fragment



Exporting IMF objects



Opening the file with text editor



Question 1

What is the host name?

YourLife01@7417.com

Question 2

What is the message ID?

93221.597207@19322.com

Question 3

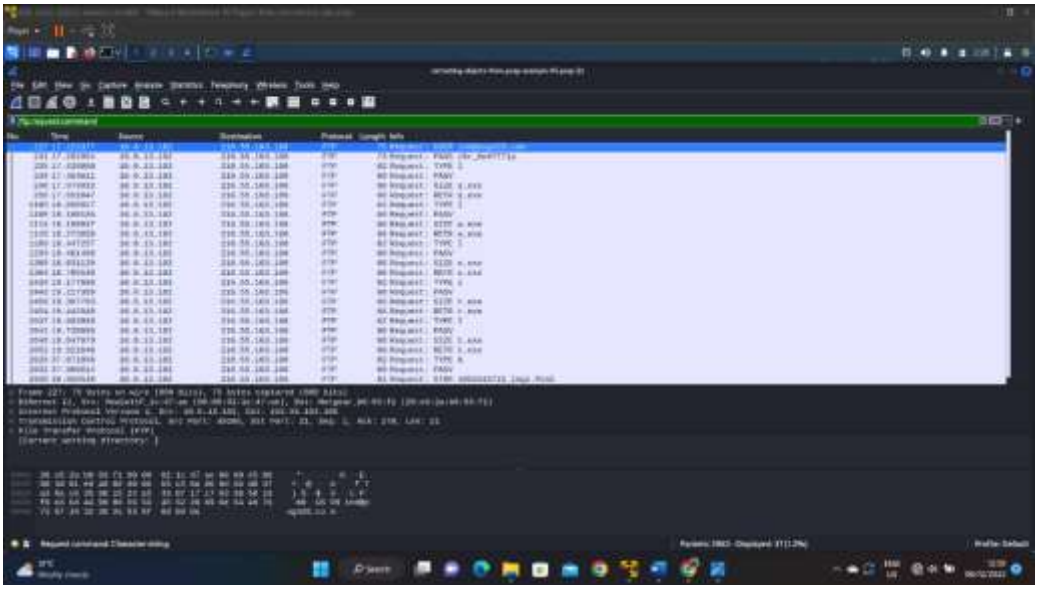
To whom have the emails been sent?

ikwlngpoh@yahoo.com

Exporting objects from FTP

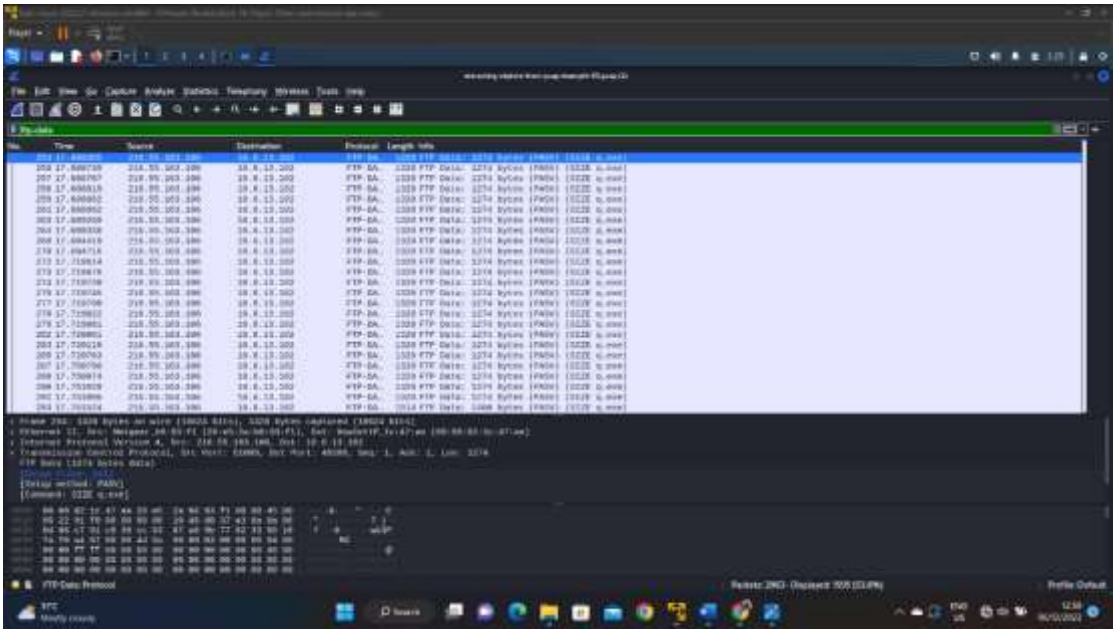
Filter the command

ftp.request.command

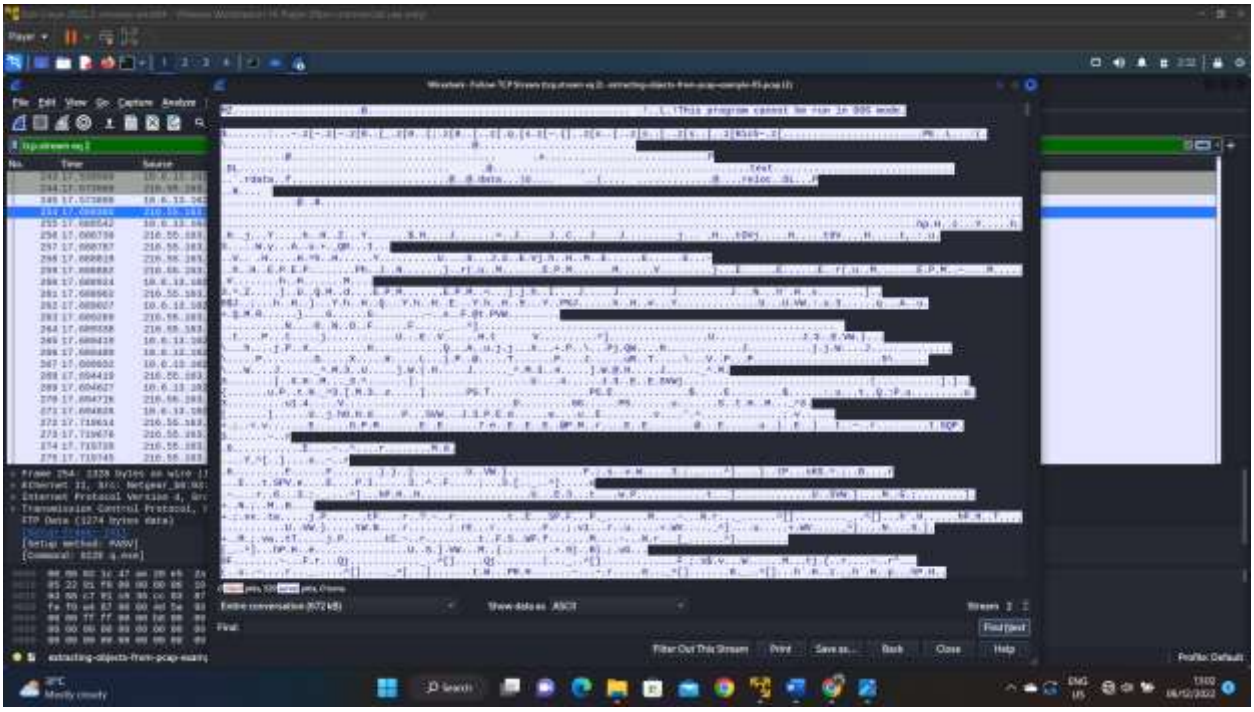


Filter the following command

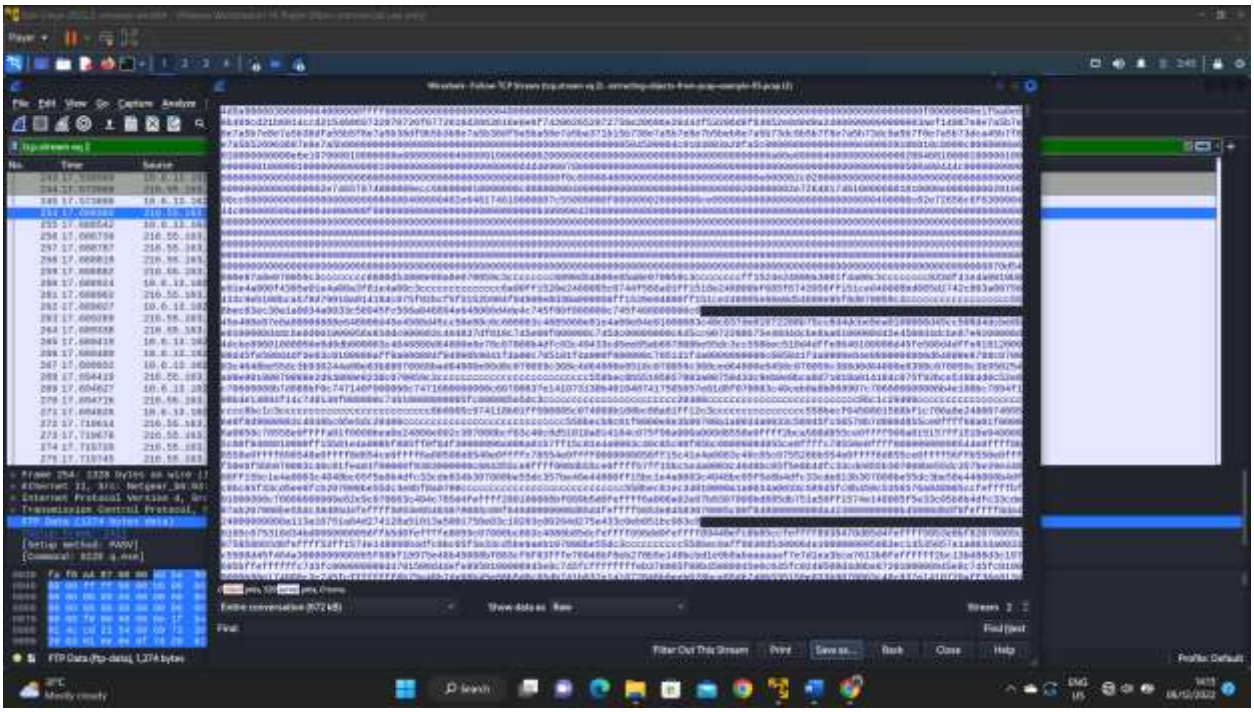
ftp-data



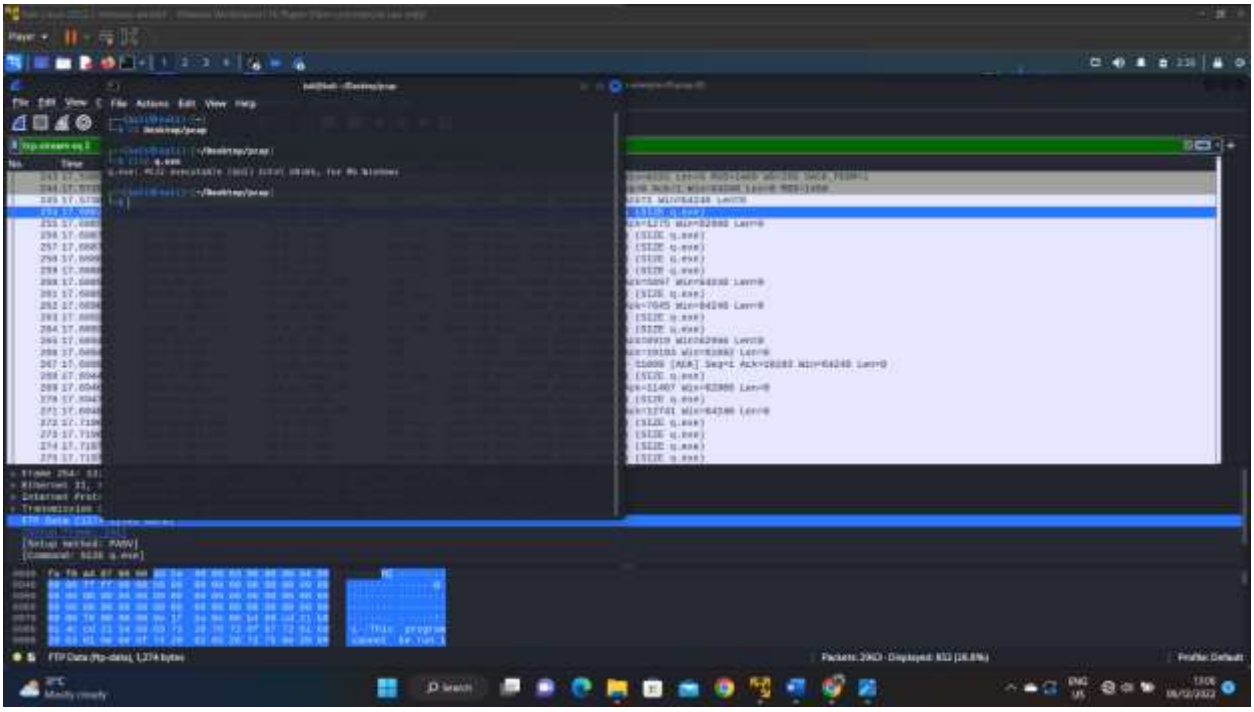
Follow the TCP stream



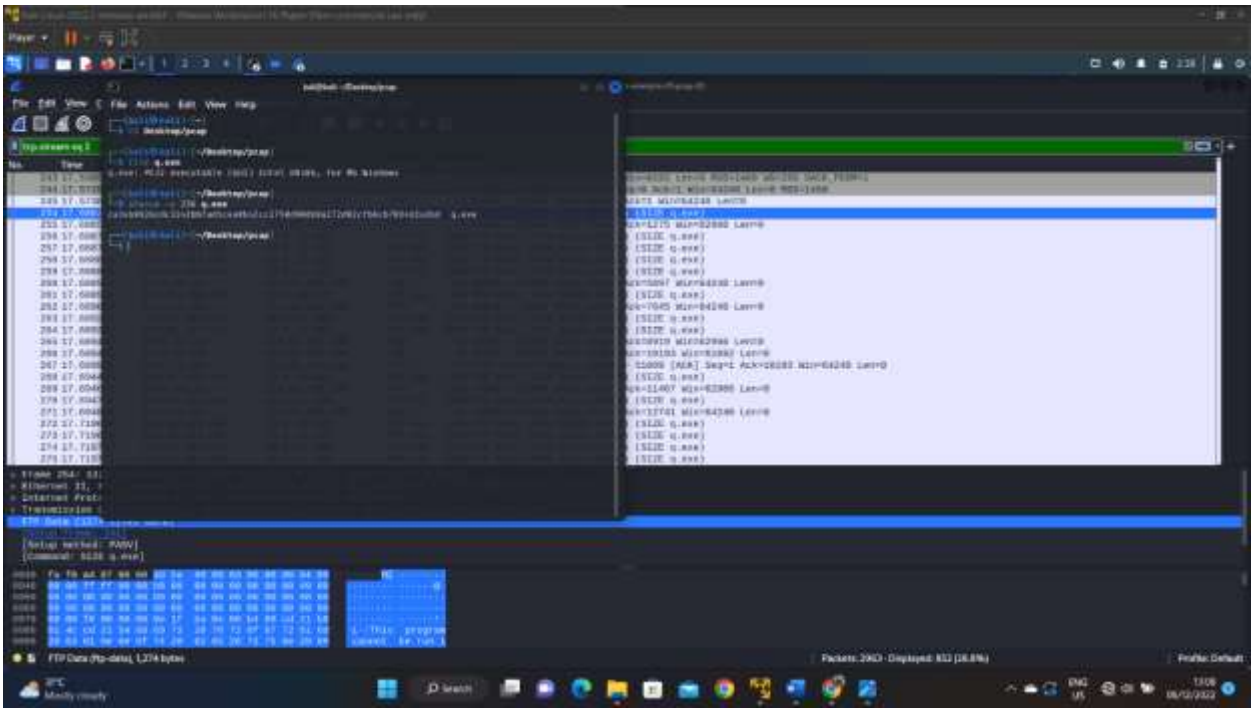
Change ASCII into Raw in the menu labeled as 'show and save data as'.



Finding the type of the file



Finding the hash that is stored in the file



Question 1

What is the source IP of the infected host?

10.6.13.102

Question 2

What is the destination IP of the infected host?

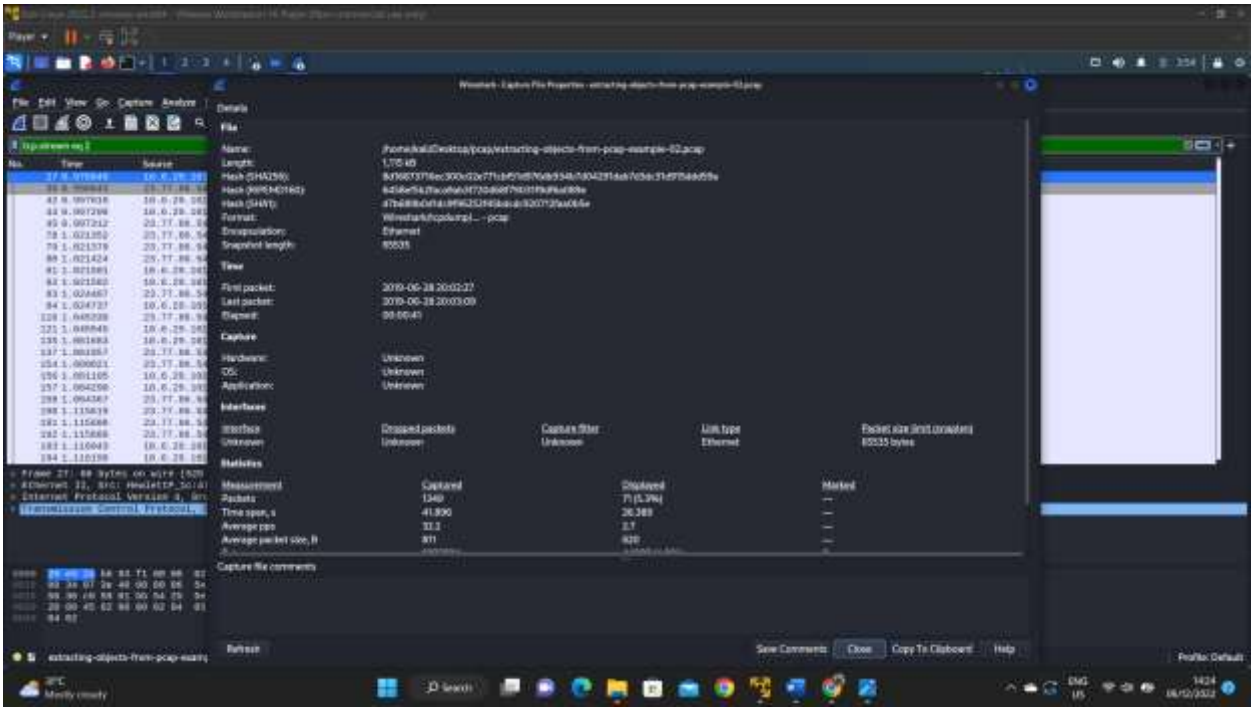
72.52.150.218

Question 3

What is the hash value of q.exe?

ca34b0926cdc3242bbfad1c4a0b42cc2750d90db9a272d92cfb6cb7034d2a3bd

Capturing File Properties



Question 1

What are the number of packets captured?

1349

Question 2

At what time was the first packet captured?

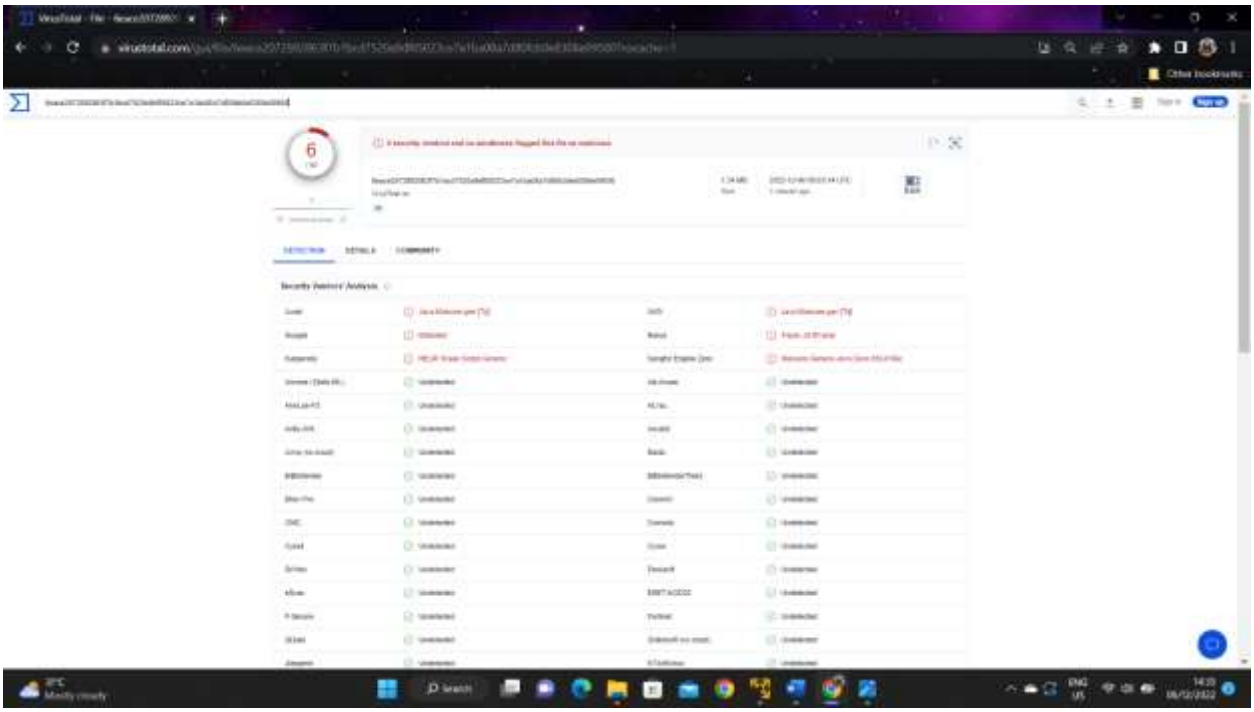
2019-06-28 20:02:27

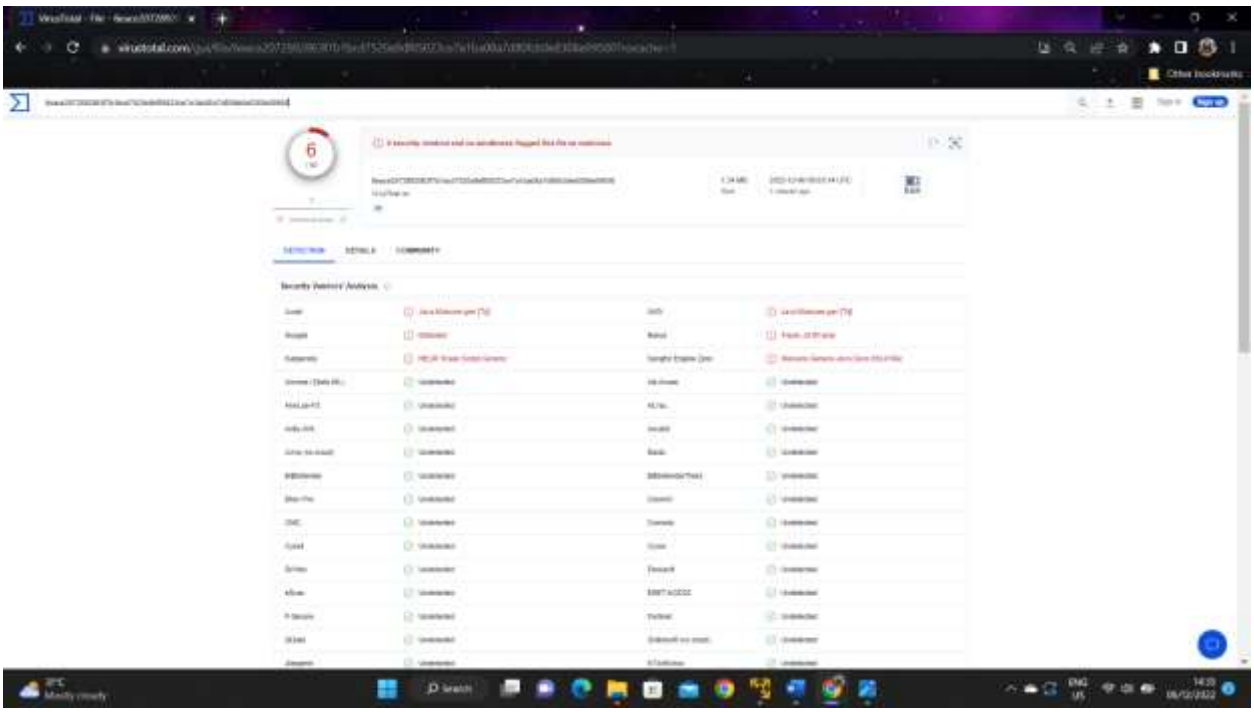
Question 3

At what time was the last packet captured?

2019-06-28 20:03:09

Introduction to Virus Total





Question 1

What is the type of file encapsulation used?

Ethernet

Question 2

What is the snort alert under sensitive data?

(spp_sdf) SDF Combination Alert [1]

Question 3

How many packets have been captured?

3053

Conclusion

This book and the try hack me room along with that provides a great knowledge to the users of the room and the readers of the book. In summary, It gives a basic idea about malware and malware analysis. This report further analyses the operation of Wireshark along with examples and practical solutions.

References

1. www.wireshark.org