Pcap Analysis using Wireshark — 1

 Abhijit Kamath Follow 5 min read · Sep 12, 2022

This would be a series of **pcap analyses** using **Wireshark.** This would be the 1st article of the series. So, before we get on to the main stuff, let me explain the prerequisites for getting the maximum out of this series. Let me give you a little heads up, this series, or maybe the initial part of the series will be for beginners who wish to be a SOC analyst or any blue side.

1. Basis Understanding of Networking
2. Basic Understanding of Linux
3. Wireshark installed and it's working (Basics)
4. pcap files to start analyzing.

So, without any further ado, let's start analyzing!!!!

I will be providing the pcap files that we are going to analyze here in my google drive, you can simply download it from there and start doing it. Let's get started!!!

Click here to download the pcap file:

So here are the scenario and the things that you need to find out using the "pcap" file.

ENVIRONMENT:

- LAN segment range: 10.11.11.0/24 (10.11.11.0 through 10.11.11.255)
- Domain: okay-boomer.info
- Domain controller: 10.11.11.11 - Okay-Boomer-DC
- LAN segment gateway: 10.11.11.1
- LAN segment broadcast address: 10.11.11.255

ENVIRONMENT/SENARIO

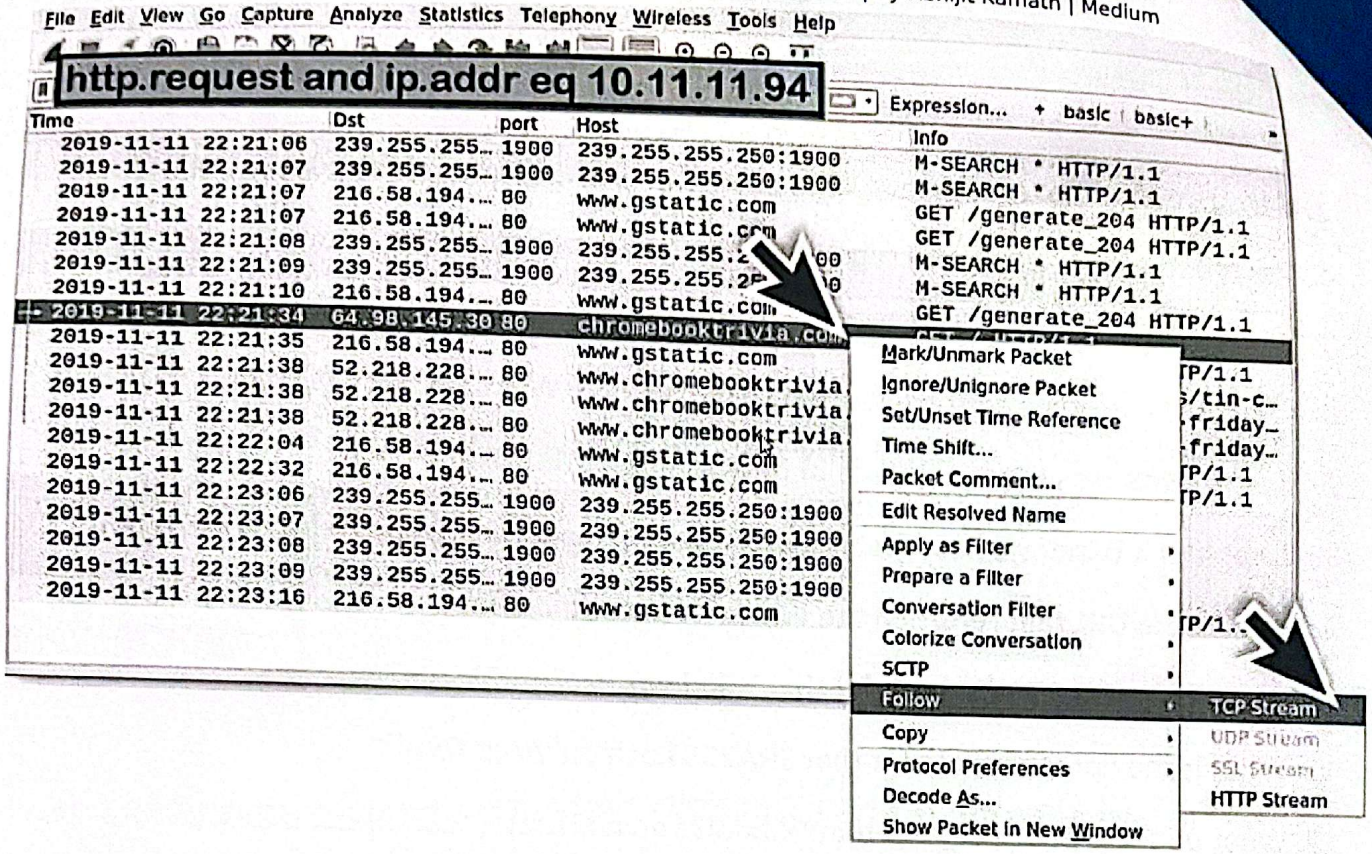
QUESTIONS: -

1. What operating system and type of device is on 10.11.11.94?
2. What operating system and type of device is on 10.11.11.121?
3. Based on the MAC address for 10.11.11.145, who is the manufacturer or vendor?
4. What operating system and type of device is on 10.11.11.179?
5. What version of Windows is being used on the host at 10.11.11.195?
6. What is the user account name used to log into the Windows host at 10.11.11.200?
7. What operating system and type of device is on 10.11.11.217?
8. What IP is a Windows host that downloaded a Windows executable file over HTTP?
9. What is the URL that returned the Windows executable file?
10. What is the SHA256 file hash for that Windows executable file?
11. What is the detection rate for that SHA256 hash on Virus Total?
12. What public IP addresses did that Windows host attempt to connect over TCP after the executable file was downloaded?
13. What are the hostname and Windows user account name used on that IP address?

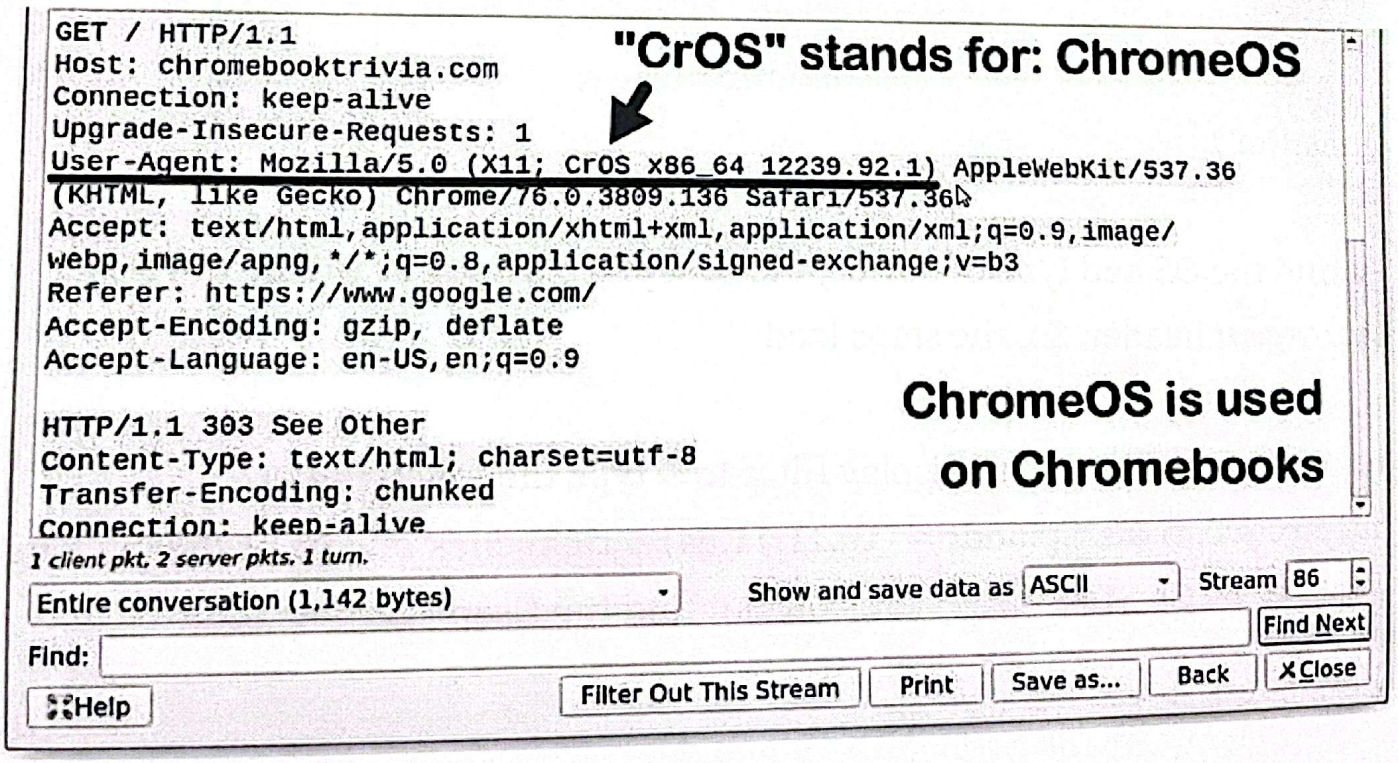
Question 1

To find the OS and type of device, the best place to look at will be the HTTP *User-Agent* header. So, the steps load

load the pcap file → go to display filter to → type the following → **(http.request) && (ip.addr == 10.11.11.94)** → right click on any of the packets → follow → TCP STREAM → here you can find the User-Agent header.



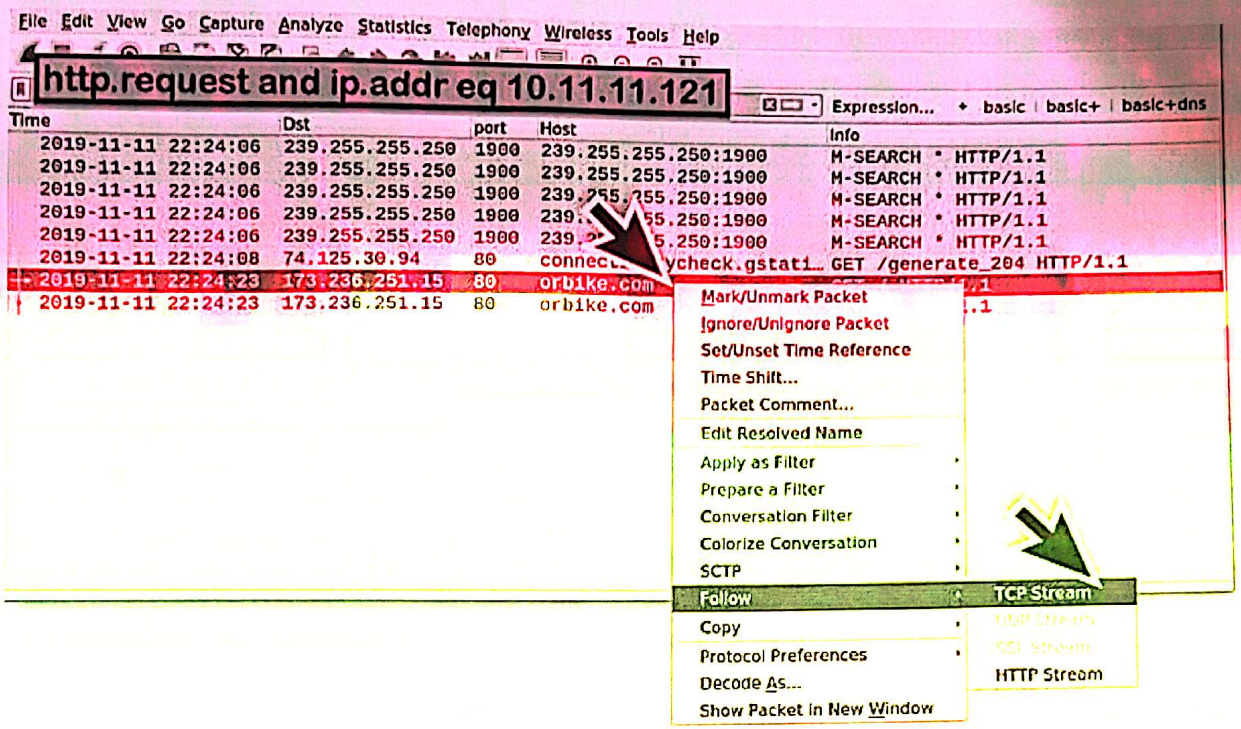
Filtering

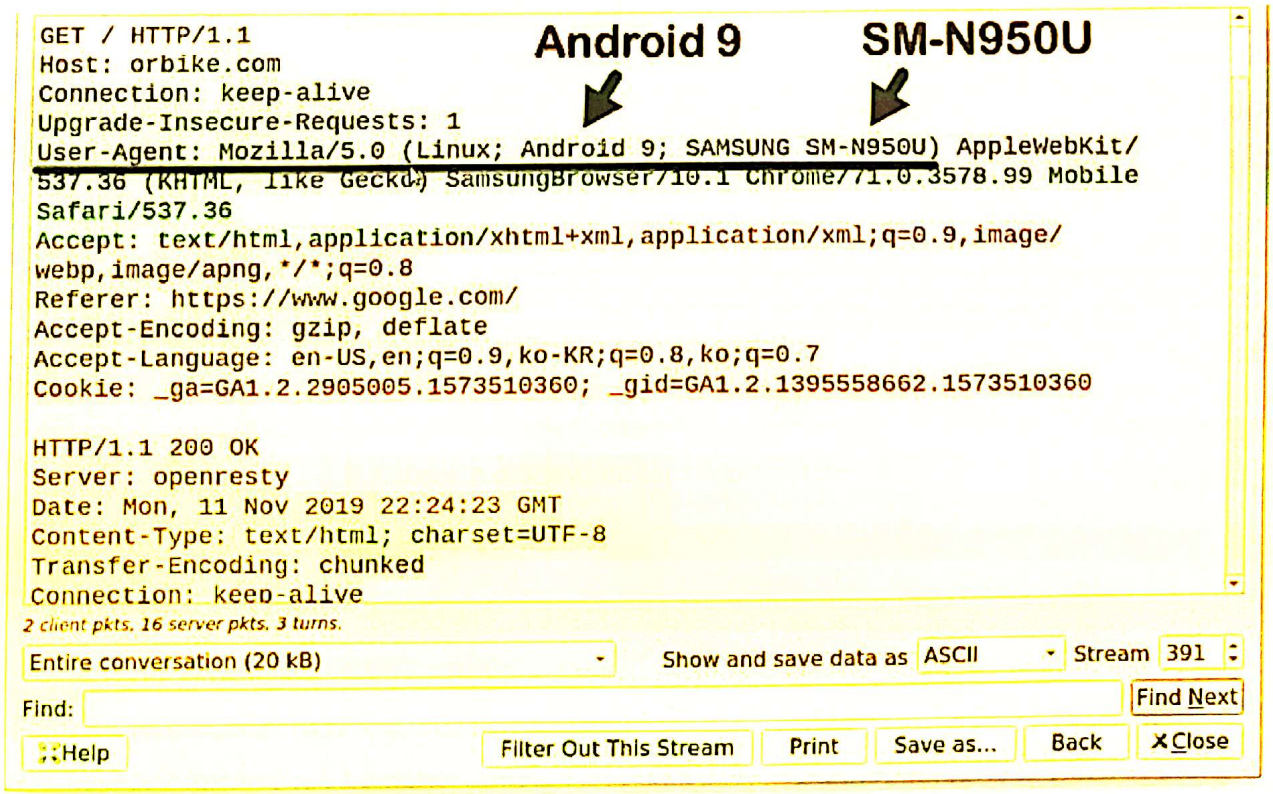


Finding the header

Question 2

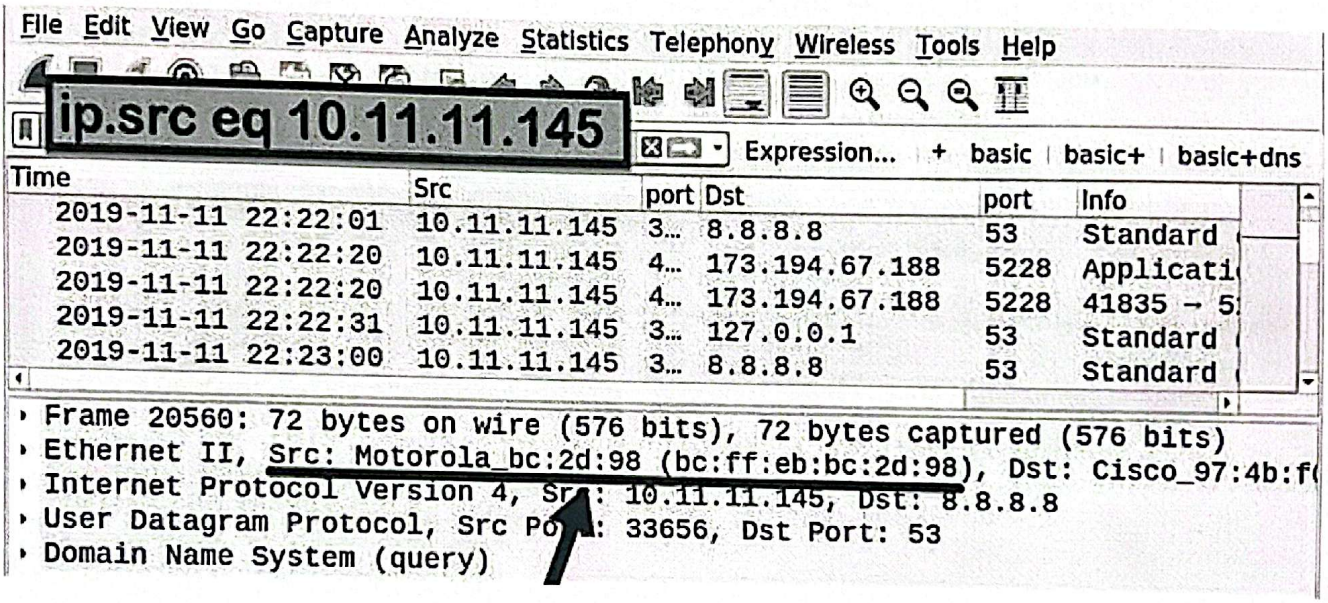
Follow the same process as **question 1** with the difference in IP address





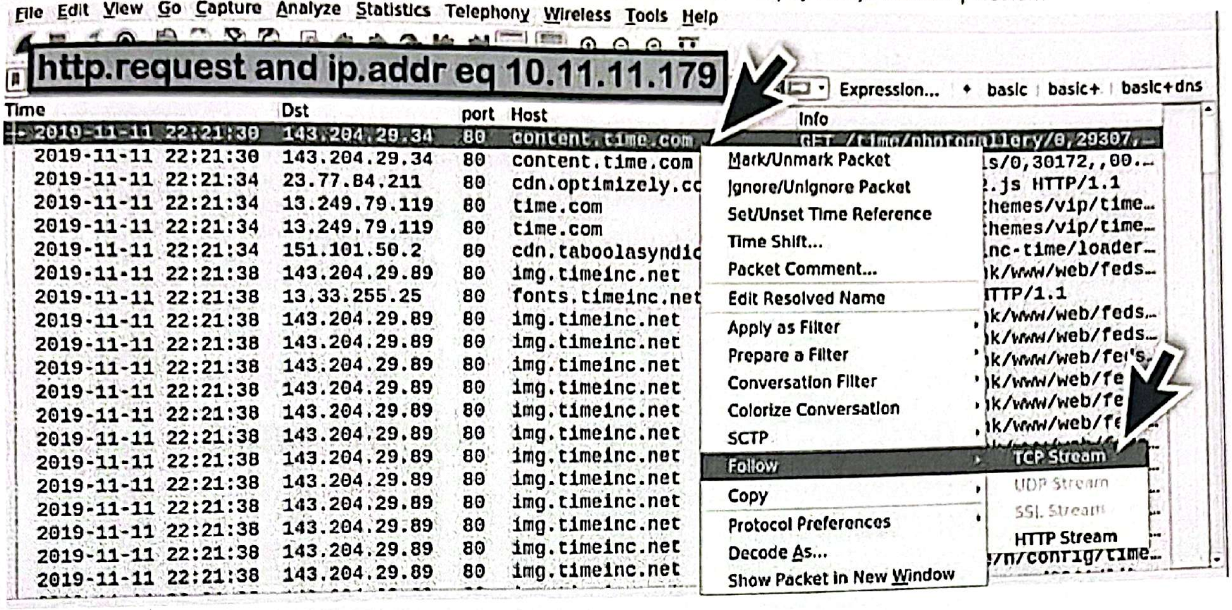
Question 3

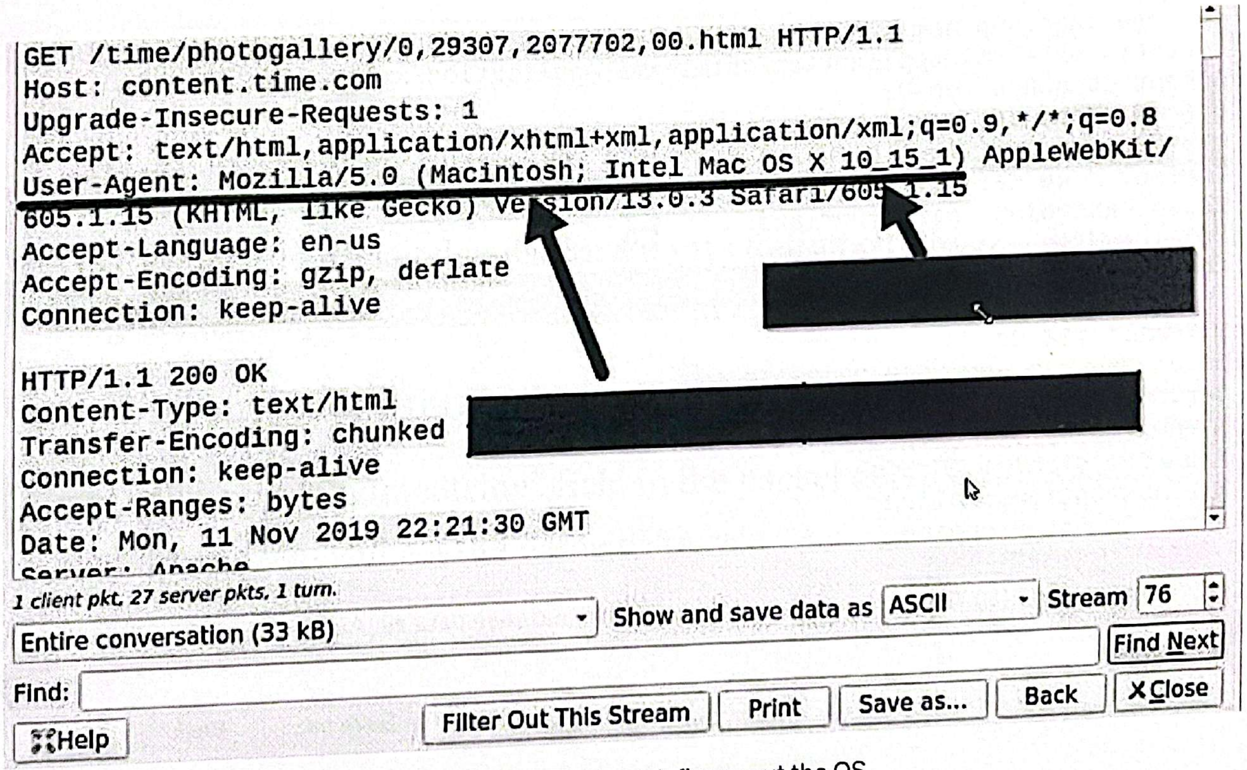
For the MAC address, since it's a layer 2 thing, you need to go to the link layer packet details of the required packet, i.e., the packet that contains the required IP address (either as src or dest).



Question 4

Follow the same process as question 1 with the difference in IP address

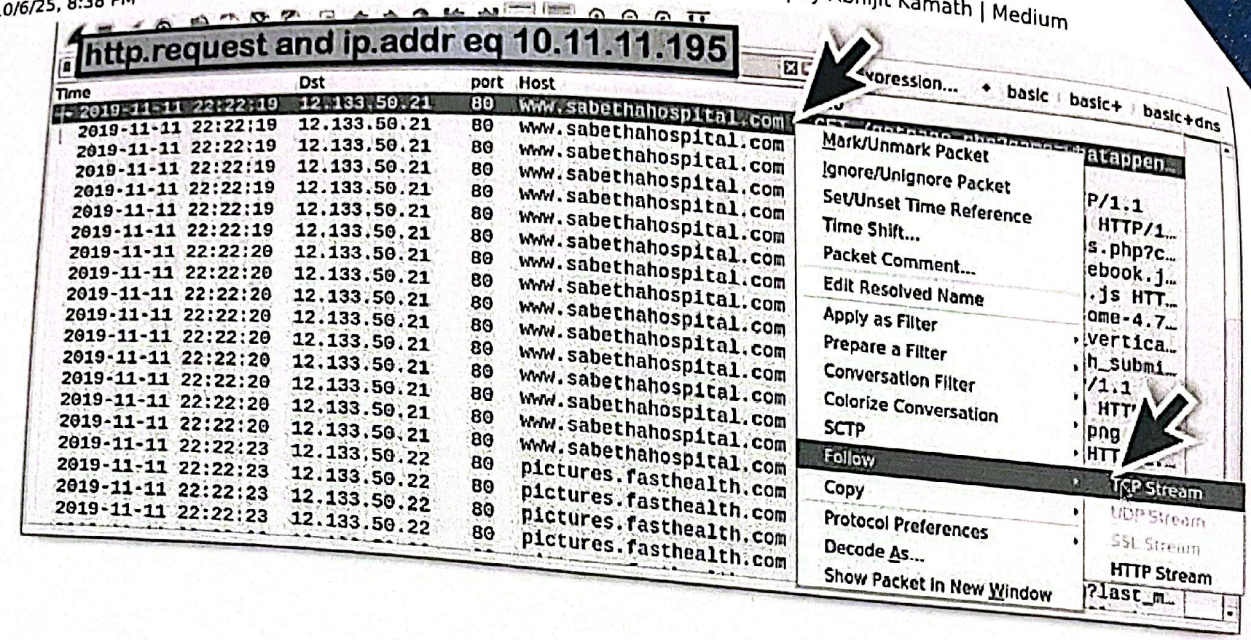


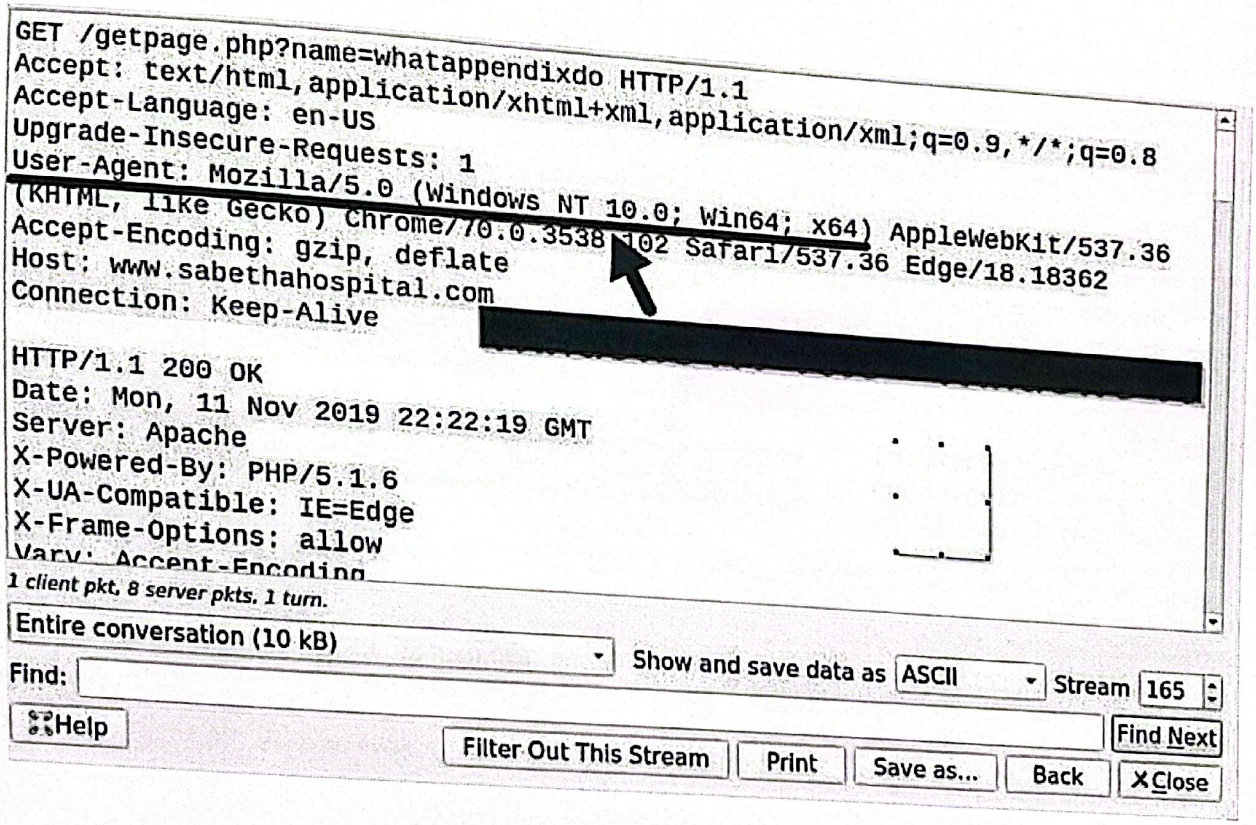


Search online if you can't figure out the OS

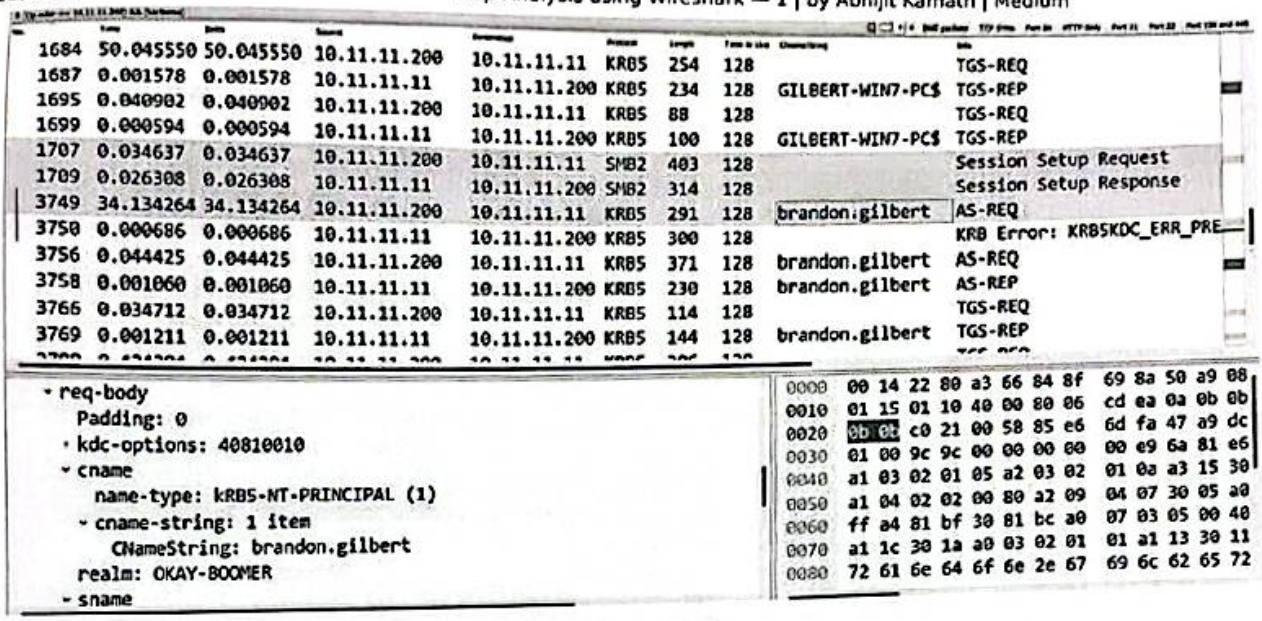
Question 5

Follow the same process as question 1 with the difference in IP address





Question 6

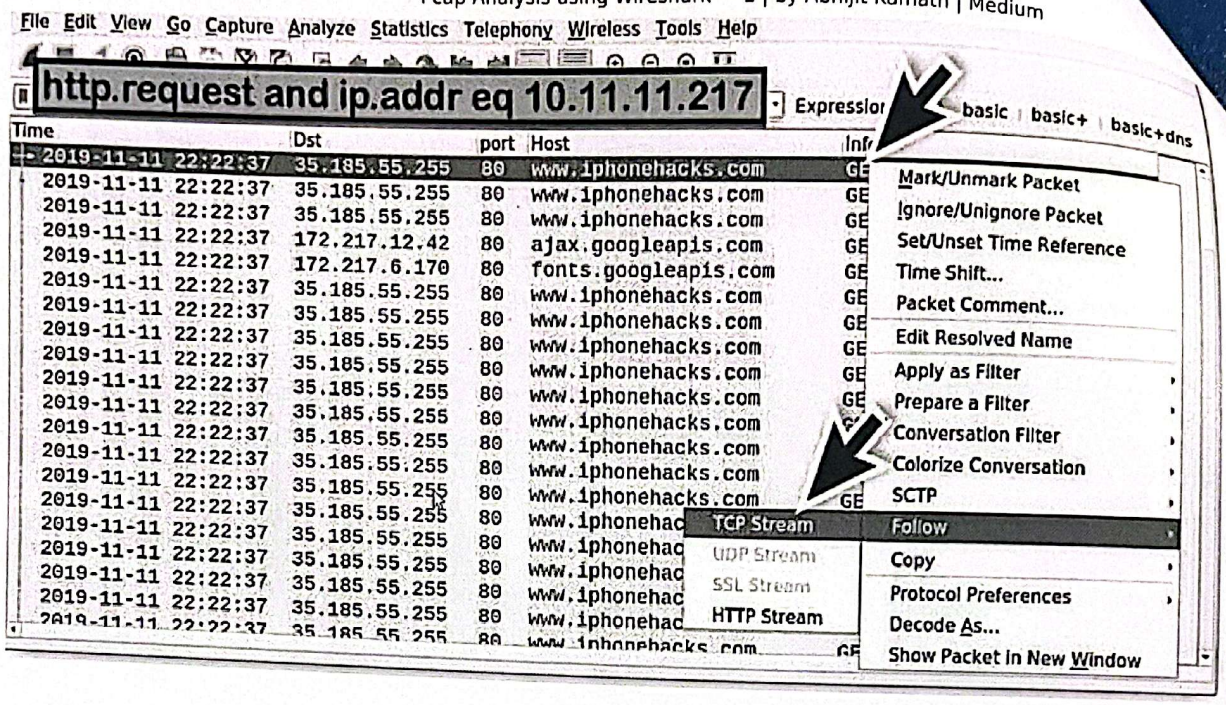


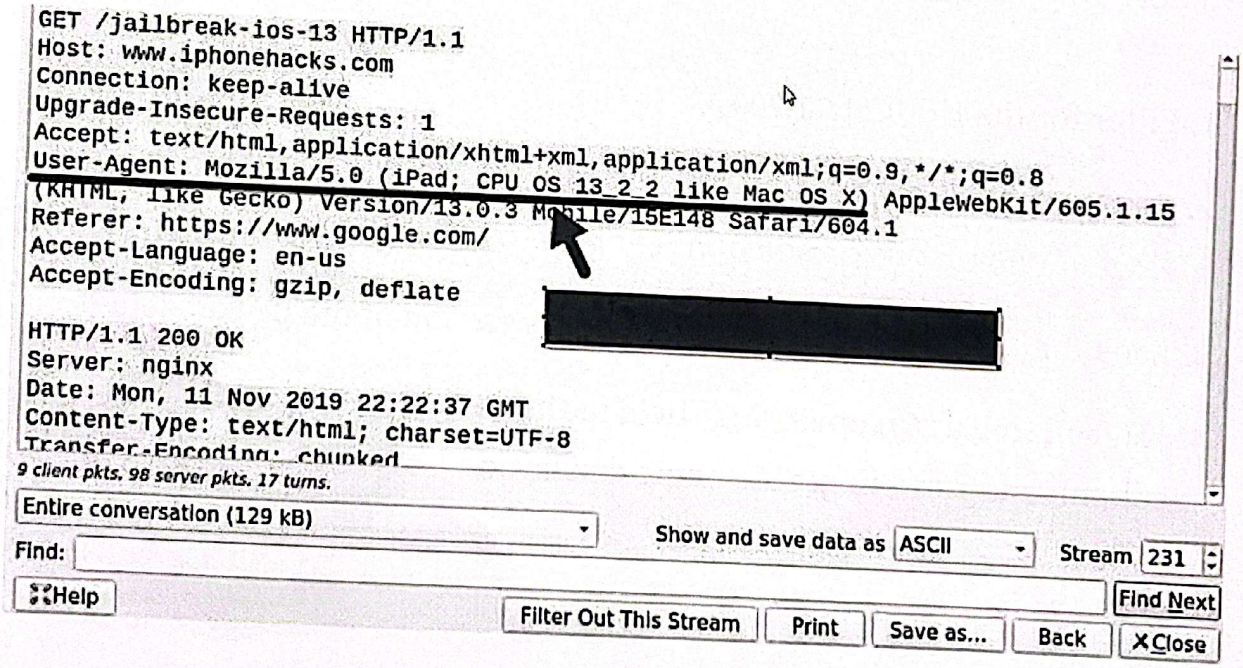
So here what you do is: -

1. Filter for the IP 10.11.11.200.
2. Go through the packet details since it says to find out the name used to "log in", the required content might be in the "**AS-REQ**" packets.
3. Look for any name string in the Kerberos section of the packet details.
4. you will find a "**CnameString**" field in the packet details, add that as a column and you will get the name displayed

Question 7

Follow the same process as question 1 with the difference in IP address





Question 8

Here this is a bit tricky, so in windows, the executables are called **PE files**, (portable executable) but the host won't download an executable file from a random IP address, so it might be in another format, like an image or audio or something, most probably an image.

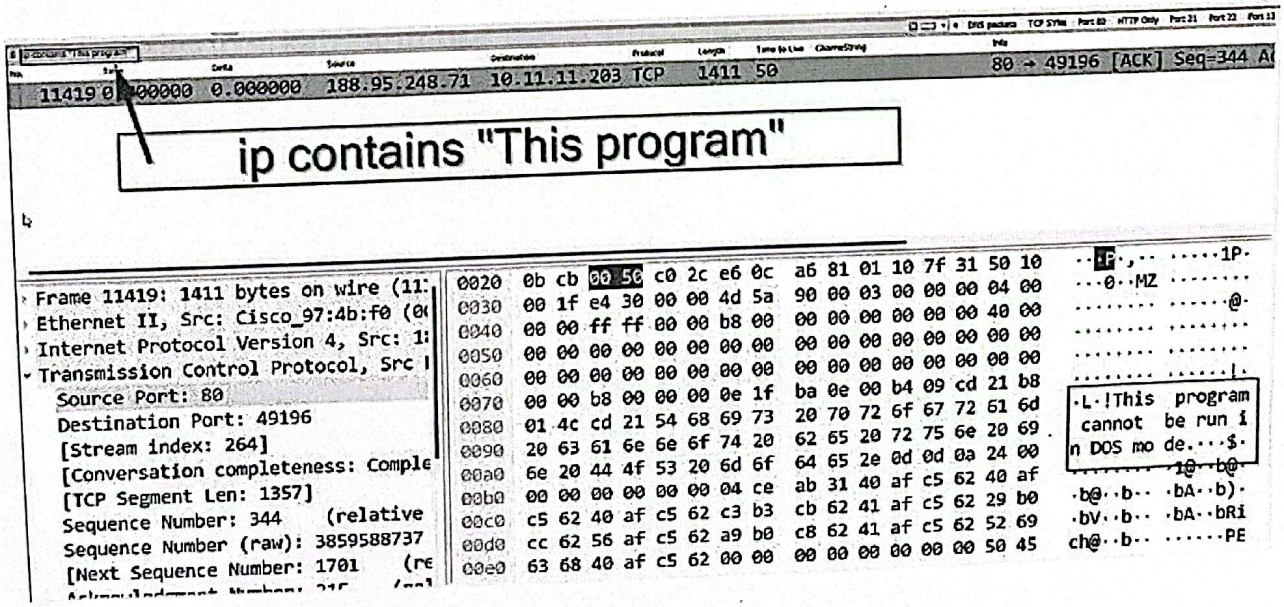
So, the trick is to try to search for some kind of string in the packet that might probably be in a PE file. and that is "*This program cannot be run in DOS mode*". This will be the error that comes when we try to execute the file, and windows updates the software architecture and older format will throw in errors like this one, because of compatibility.

The next question is a continuation of this one so, take a look at that to get more insight

frame contains "**This program**" or
ip contains "**This program**" → and you will get the source IP

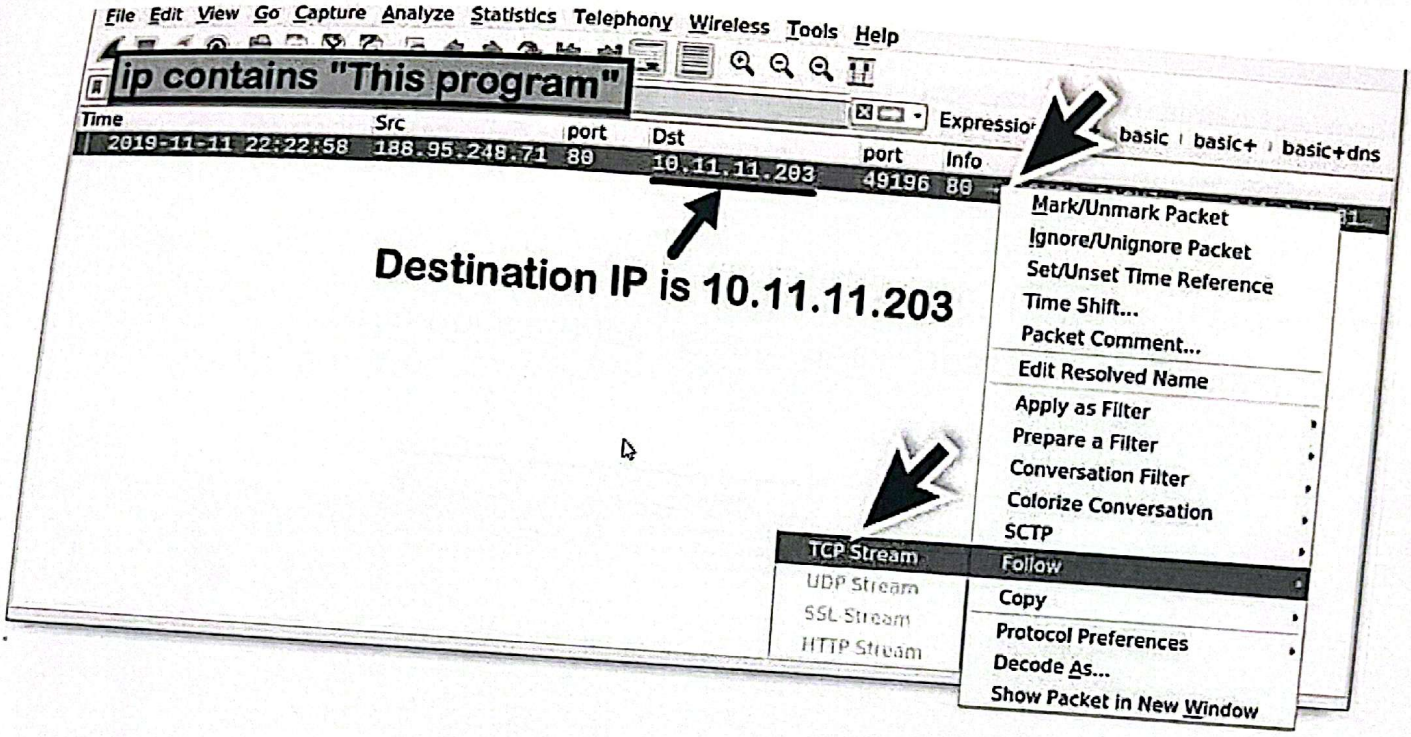
ip contains "This program"

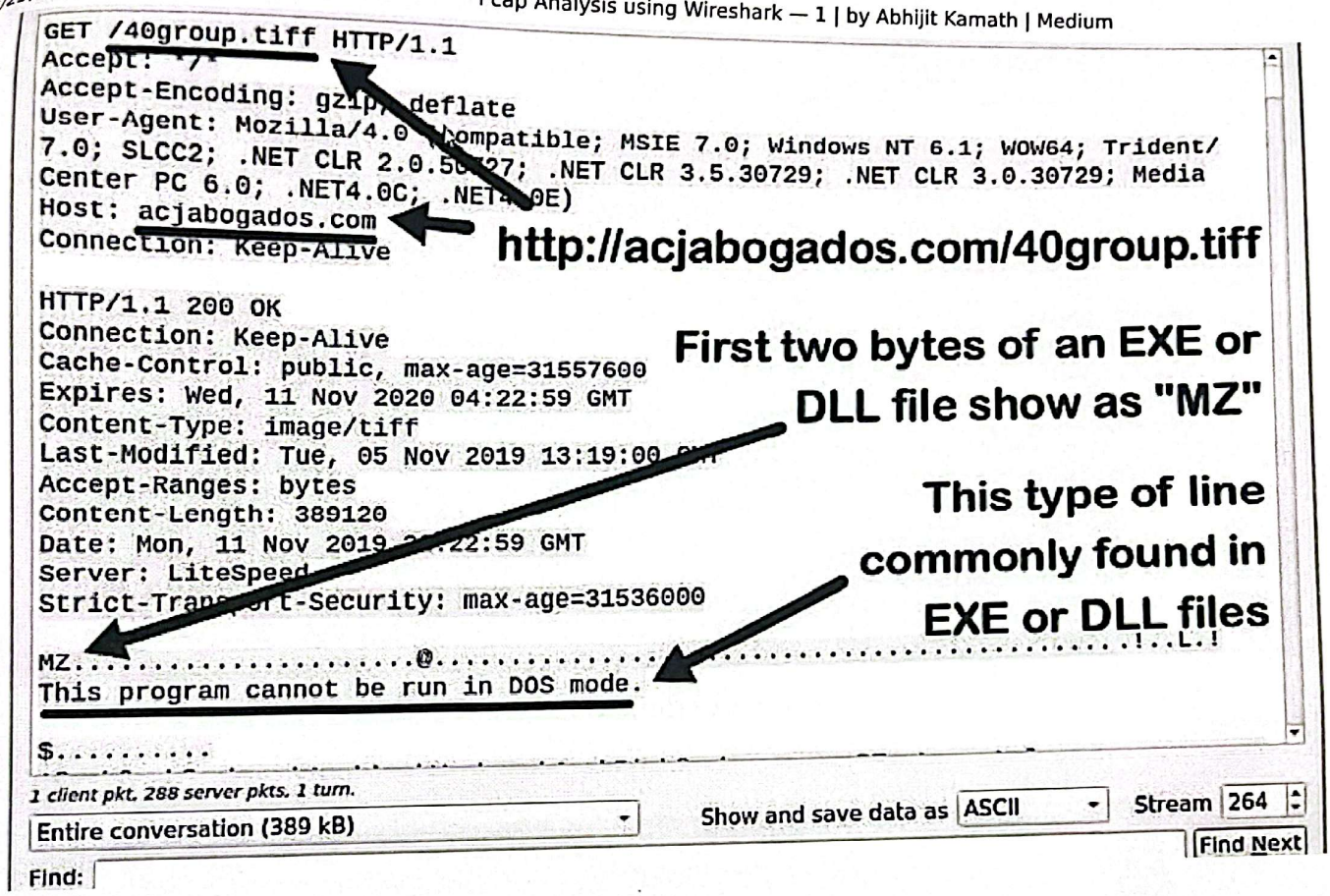
frame contains "This program"



Question 9

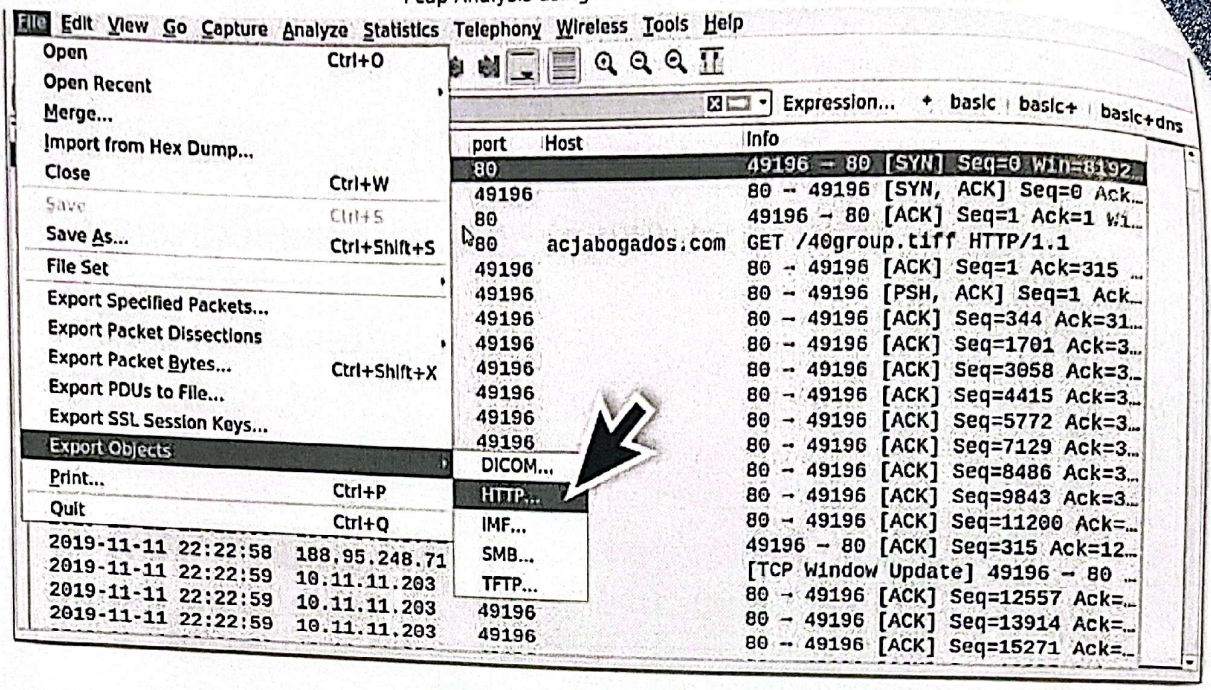
This question is like a continuation of the last question and to find the URL just follow the TCP stream and you will get all the information.



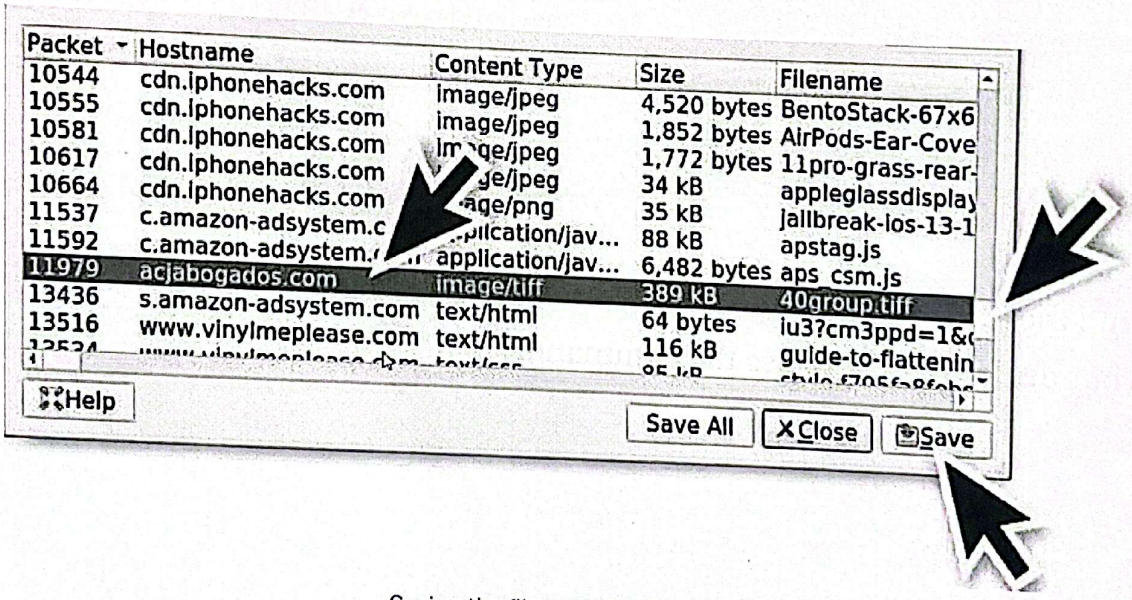


Question 10

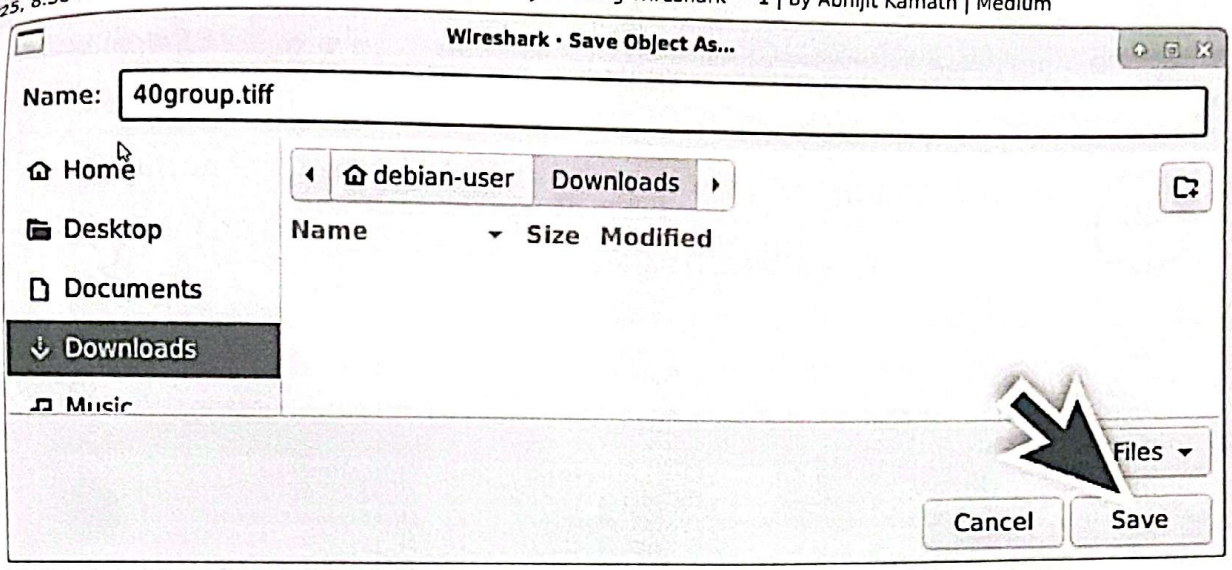
To find the SHA value use the Linux command **shasum.** So, her save the file on your device (kali) and use the command.



Finding the Object in Wireshark



Saving the file on to your host machine

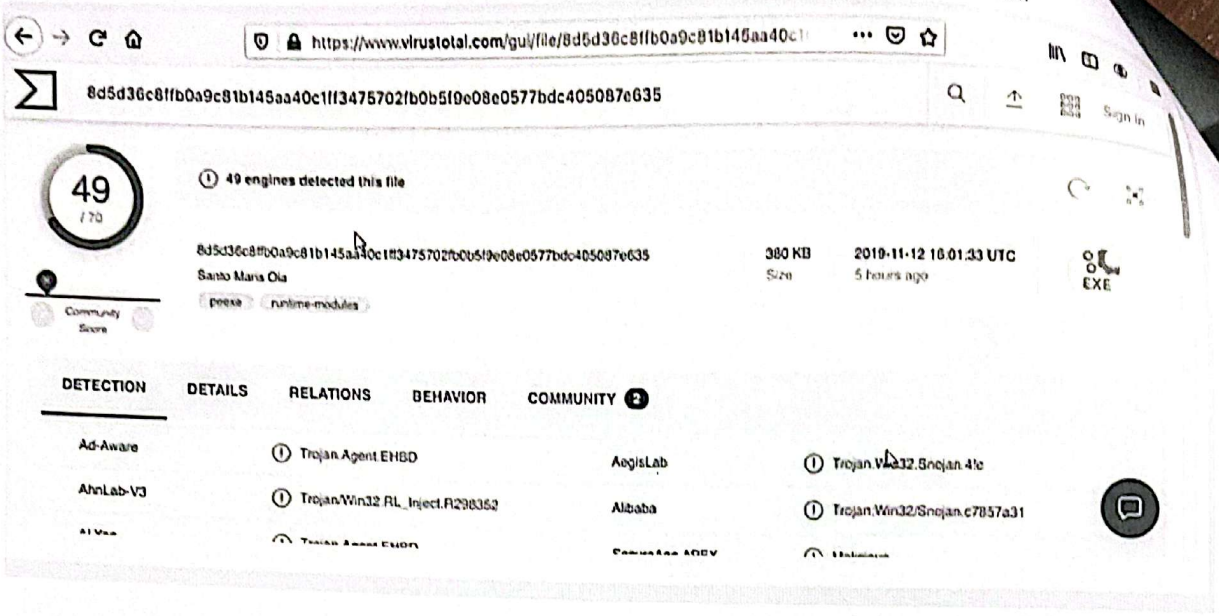


Saving it

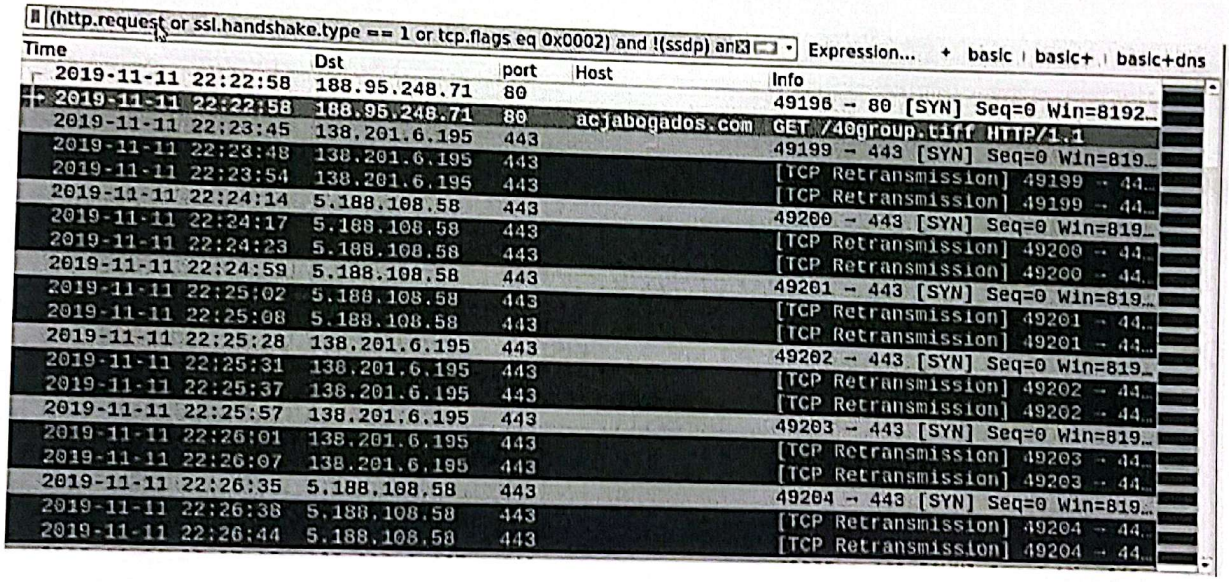
Find the SHA value

Question 11

Load that file into the “virus total” website and that's it.



Question 12

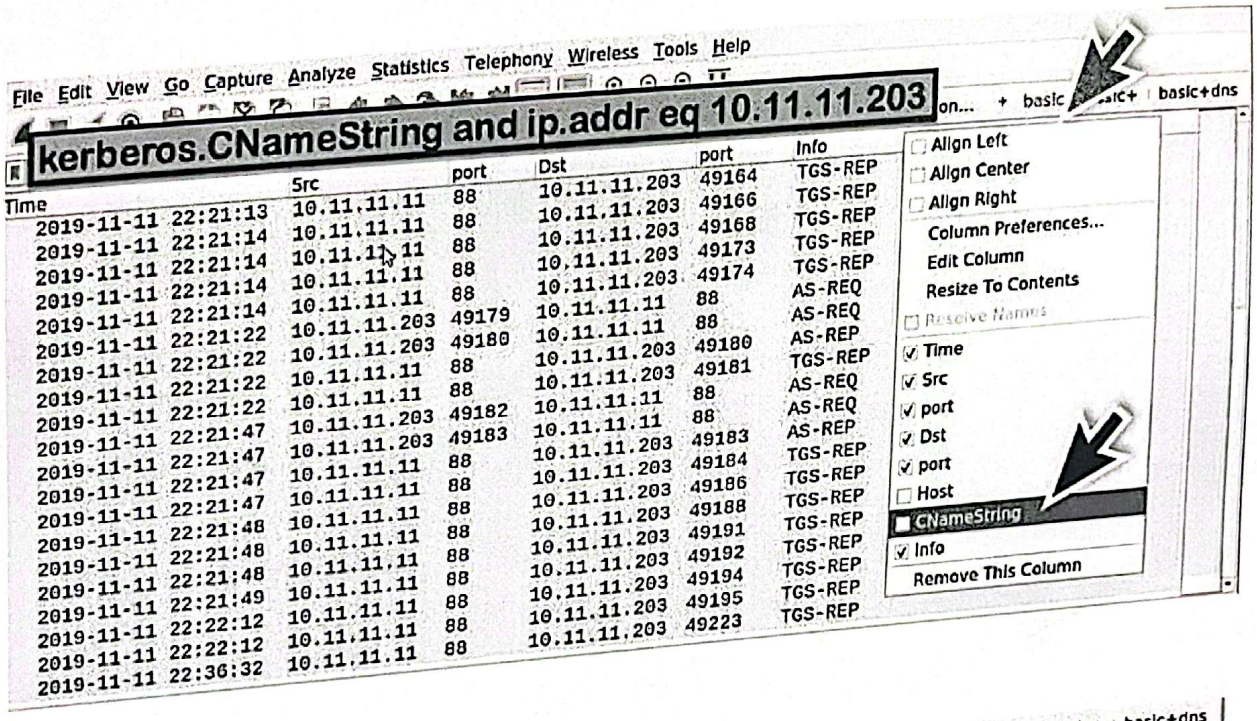


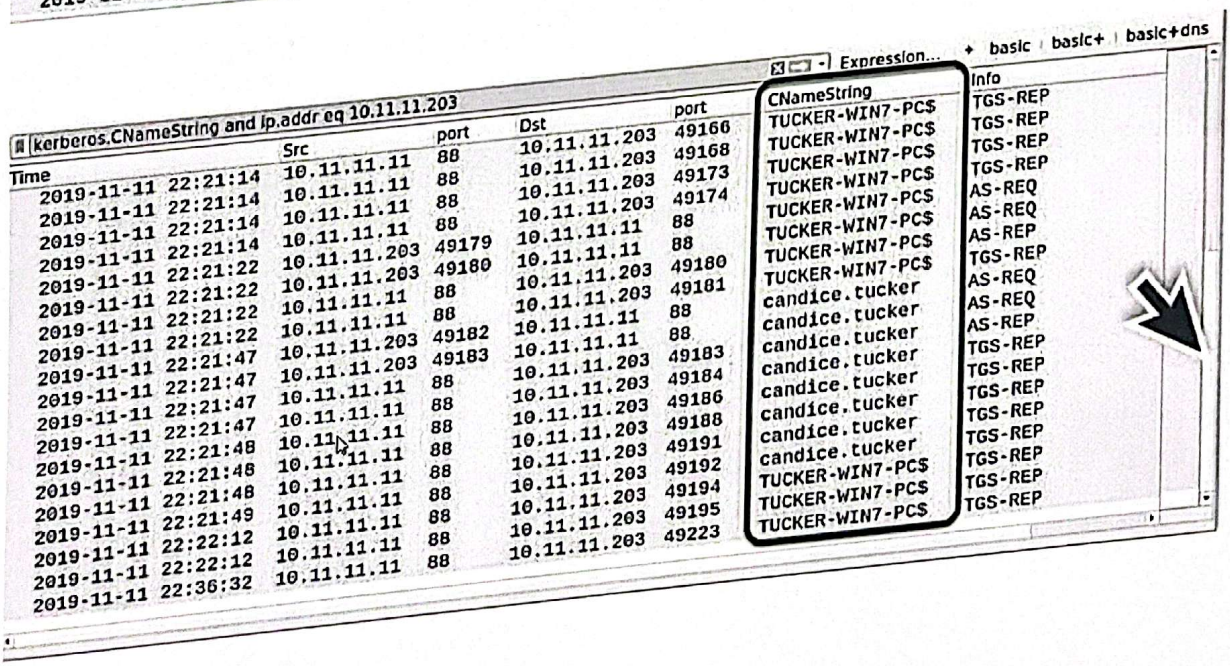
filter: (http.request or ssl.handshake.type == 1 or tcp.flags eq 0x0002) and !(udp.port eq 1900) and ip.addr eq 10.11.11.203 and !(ip.dst eq 10.11.11.11)

The full idea about this filter can be found in this **link**. this is an awesome article that explains a lot about using display filters to the full use.

Question 13

The solution is the same as that in **Question 6.** Just follow the same sequence. The IP address is linked with **Question 8**





. . .