

[Open in app](#)[Sign up](#)[Sign in](#)**Medium**

Search

Write



Pcap Analysis using Wireshark — 1



Abhijit Kamath

[Follow](#)

5 min read · Sep 12, 2022

28

1



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!!!!

10/6/25, 8:38 PM

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.

10/6/25, 8:38 PM

Pcap Analysis using Wireshark — 1 | by Abhiljit Kamath | Medium

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request and ip.addr eq 10.11.11.94

Time	Dst	port	Host
2019-11-11 22:21:06	239.255.255.1900	1900	239.255.255.250:1900
2019-11-11 22:21:07	239.255.255.1900	1900	239.255.255.250:1900
2019-11-11 22:21:07	216.58.194... 80	80	www.gstatic.com
2019-11-11 22:21:07	216.58.194... 80	80	www.gstatic.com
2019-11-11 22:21:08	239.255.255.1900	1900	239.255.255.250:1900
2019-11-11 22:21:09	239.255.255.1900	1900	239.255.255.250:1900
2019-11-11 22:21:10	216.58.194... 80	80	www.gstatic.com
2019-11-11 22:21:34	64.98.145.30:80	80	chromebooktrivia.com
2019-11-11 22:21:35	216.58.194... 80	80	www.gstatic.com
2019-11-11 22:21:38	52.218.228... 80	80	www.chromebooktrivia.
2019-11-11 22:21:38	52.218.228... 80	80	www.chromebooktrivia.
2019-11-11 22:21:38	52.218.228... 80	80	www.chromebooktrivia.
2019-11-11 22:22:04	216.58.194... 80	80	www.gstatic.com
2019-11-11 22:22:32	216.58.194... 80	80	www.gstatic.com
2019-11-11 22:23:06	239.255.255.1900	1900	239.255.255.250:1900
2019-11-11 22:23:07	239.255.255.1900	1900	239.255.255.250:1900
2019-11-11 22:23:08	239.255.255.1900	1900	239.255.255.250:1900
2019-11-11 22:23:09	239.255.255.1900	1900	239.255.255.250:1900
2019-11-11 22:23:16	216.58.194... 80	80	www.gstatic.com

Expression... + basic basic+ Info
M-SEARCH * HTTP/1.1
M-SEARCH * HTTP/1.1
GET /generate_204 HTTP/1.1
GET /generate_204 HTTP/1.1
M-SEARCH * HTTP/1.1
M-SEARCH * HTTP/1.1
GET /generate_204 HTTP/1.1

Mark/Unmark Packet IP/1.1
Ignore/Unignore Packet /tin-c...
Set/Unset Time Reference .friday-
Time Shift... .friday-
Packet Comment... IP/1.1
Edit Resolved Name IP/1.1
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Copy UDP Stream
Protocol Preferences SSL Stream
Decode As... HTTP Stream
Show Packet in New Window

Filtering

GET / HTTP/1.1
Host: chromebooktrivia.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; CrOS x86_64 12239.92.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.136 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

"CrOS" stands for: ChromeOS

HTTP/1.1 303 See Other
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
I client pkt. 2 server pkts. 1 turn.

Entire conversation (1,142 bytes) Show and save data as ASCII Stream 86 Find Next
Find: Filter Out This Stream Print Save as... Back X Close
Help

ChromeOS is used on Chromebooks

Finding the header

Question 2

4/21

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

A screenshot of the Wireshark interface. A right-click context menu is open over a selected packet. The menu path 'TCP Stream' is highlighted in green, with a green arrow pointing towards it from the bottom right. Other options in the menu include 'Mark/Unmark Packet', 'Ignore/Unignore Packet', 'Set/Unset Time Reference', 'Time Shift...', 'Packet Comment...', 'Edit Resolved Name', 'Apply as Filter', 'Prepare a Filter', 'Conversation Filter', 'Colorize Conversation', 'SCTP', 'Follow', 'Copy', 'Protocol Preferences', 'Decode As...', and 'Show Packet in New Window'. The main window shows a list of network packets with columns for Time, Dst, port, Host, Info, and a detailed pane below.

A screenshot of the Wireshark TCP Stream details view. The stream is identified as 'Android 9 SM-N950U'. The request message is displayed in yellow, showing the following headers:

```

GET / HTTP/1.1
Host: orbike.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-N950U) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/10.1 Chrome/71.0.3578.99 Mobile Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ko-KR;q=0.8,ko;q=0.7
Cookie: _ga=GA1.2.2905005.1573510360; _gid=GA1.2.1395558662.1573510360

```

The response message is displayed in orange, showing:

```

HTTP/1.1 200 OK
Server: openresty
Date: Mon, 11 Nov 2019 22:24:23 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

```

At the bottom, there are buttons for 'Entire conversation (20 KB)', 'Show and save data as ASCII', 'Stream 391', 'Find Next', 'Help', 'Filter Out This Stream', 'Print', 'Save as...', 'Back', and 'Close'.

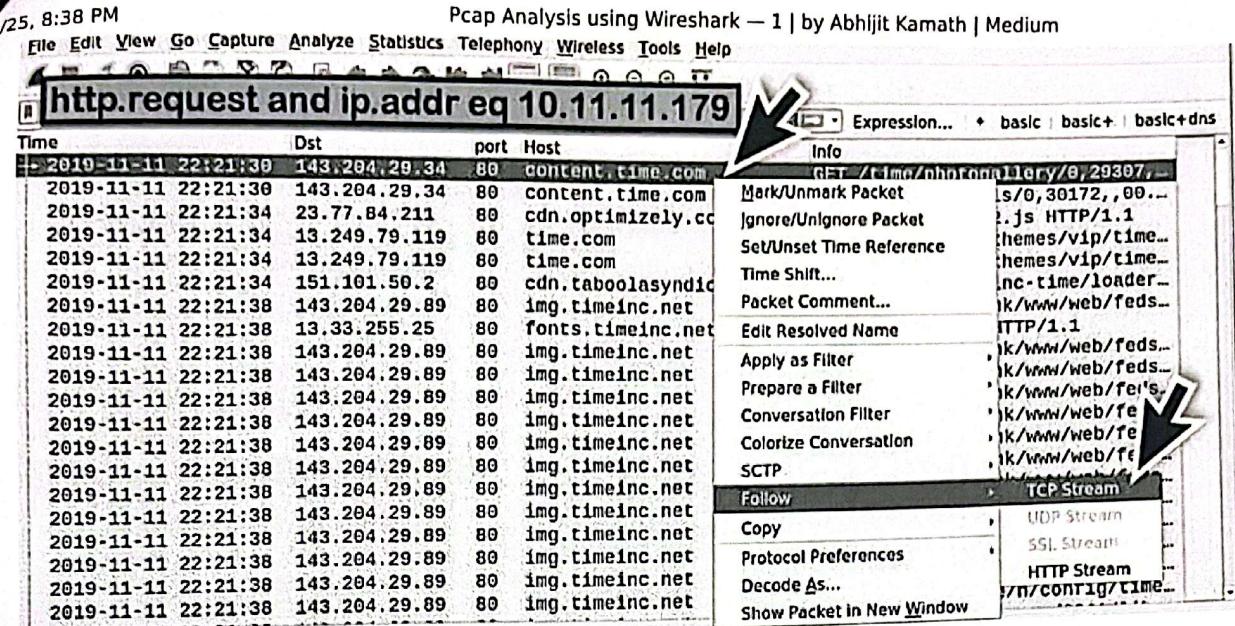
Question 3

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).

The screenshot shows the Wireshark interface with a search bar at the top containing the expression "ip.src eq 10.11.11.145". Below the search bar is a table of network traffic. The columns are labeled Time, Src, port, Dst, port, and Info. The table lists five network frames captured on November 11, 2019, between 22:22:01 and 22:23:00. The source IP address for all frames is 10.11.11.145. The destination IP addresses are 8.8.8.8, 173.194.67.188, 127.0.0.1, and Cisco_97:4b:f0. The destination port numbers are 53, 5228, 53, and 33656 respectively. The protocol information section below the table provides a detailed breakdown of the selected frame, identifying it as an Ethernet II frame with source address Motorola_bc:2d:98 and destination Cisco_97:4b:f0, containing an Internet Protocol Version 4 header with source 10.11.11.145 and destination 8.8.8.8, and a User Datagram Protocol header with source port 33656 and destination port 53, which is identified as a Domain Name System (query) request.

Question 4

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



GET /time/photogallery/0,29307,2077702,00.html HTTP/1.1
Host: content.time.com
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Safari/605.1.15
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 200 OK
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Accept-Ranges: bytes
Date: Mon, 11 Nov 2019 22:21:30 GMT
Server: Apache

1 client pkt, 27 server pkts, 1 turn.

Entire conversation (33 kB)

Show and save data as Stream

Find:

Filter Out This Stream Save as...

Question 5

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

```
GET /getpage.php?name=whatappendixdo HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362
Accept-Encoding: gzip, deflate
Host: www.sabethahospital.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 11 Nov 2019 22:22:19 GMT
Server: Apache
X-Powered-By: PHP/5.1.6
X-UA-Compatible: IE=Edge
X-Frame-Options: allow
Vary: Accept-Encoding
1 client pkt, 8 server pkts, 1 turn.

Entire conversation (10 kB) ▾ Show and save data as ASCII Stream 165
Find: 
Help  Filter Out This Stream  Print  Save as...  Back  Find Next  X Close 
```

Question 6

5/6/25, 8:38 PM

Pcap Analysis using Wireshark — 1 | by Abhijit Kamath | Medium

Time	Source	Dest	Protocol	Length	Time to live	Checksum	Info
1684	50.045550	50.045550	10.11.11.200	10.11.11.11	KRBS	254	128 TGS-REQ
1687	0.001578	0.001578	10.11.11.11	10.11.11.200	KRBS	234	128 GILBERT-WIN7-PCS TGS-REP
1695	0.040902	0.040902	10.11.11.200	10.11.11.11	KRBS	88	128 TGS-REQ
1699	0.000594	0.000594	10.11.11.11	10.11.11.200	KRBS	100	128 GILBERT-WIN7-PCS TGS-REP
1707	0.034637	0.034637	10.11.11.200	10.11.11.11	SMB2	403	128 Session Setup Request
1709	0.026308	0.026308	10.11.11.11	10.11.11.200	SMB2	314	128 Session Setup Response
3749	34.134264	34.134264	10.11.11.200	10.11.11.11	KRBS	291	128 brandon.gilbert AS-REQ
3750	0.000686	0.000686	10.11.11.11	10.11.11.200	KRBS	300	128 KRB Error: KRBSKDC_ERR_PRE
3756	0.044425	0.044425	10.11.11.200	10.11.11.11	KRBS	371	128 brandon.gilbert AS-REQ
3758	0.001060	0.001060	10.11.11.11	10.11.11.200	KRBS	230	128 brandon.gilbert AS-REP
3766	0.034712	0.034712	10.11.11.200	10.11.11.11	KRBS	114	128 TGS-REQ
3769	0.001211	0.001211	10.11.11.11	10.11.11.200	KRBS	144	128 brandon.gilbert TGS-REP

- req-body
 Padding: 0
 • kdc-options: 40810010
 • cname
 name-type: KRBS-NT-PRINCIPAL (1)
 • cname-string: 1 item
 CNameString: brandon.gilbert
 realm: OKAY-BOOMER
 - sname

0000	00 14 22 80 a3 66 84 8f	69 8a 50 a9 88
0010	01 15 01 10 40 00 80 06	cd ea 0a 0b 0b
0020	0b 0e c0 21 00 58 85 e6	6d fa 47 a9 dc
0030	01 00 9c 9c 00 00 00 00	00 e9 6a 81 e6
0040	a1 03 02 01 05 a2 03 02	01 0a a3 15 30
0050	a1 04 02 02 00 80 a2 09	04 07 30 05 a0
0060	ff a4 81 bf 30 81 bc a0	07 03 05 00 40
0070	a1 1c 30 1a a0 03 02 01	01 a1 13 30 11
0080	72 61 6e 64 6f 6e 2e 67	69 6c 62 65 72

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

Get Abhijit Kamath's stories in your inbox

Join Medium for free to get updates from this writer.

Enter your email

Subscribe

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

<https://medium.com/@DaRkrAl69/pcap-analysis-using-wireshark-1-d69d0e107367>

9/21

```
GET /jailbreak-ios-13 HTTP/1.1
Host: www.iphonehacks.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (iPad; CPU OS 13_2_2 like Mac OS X) AppleWebKit/605.1.15
(KHTML, like Gecko) Version/13.0.3 Mobile/15E148 Safari/604.1
Referer: https://www.google.com/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
```

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"

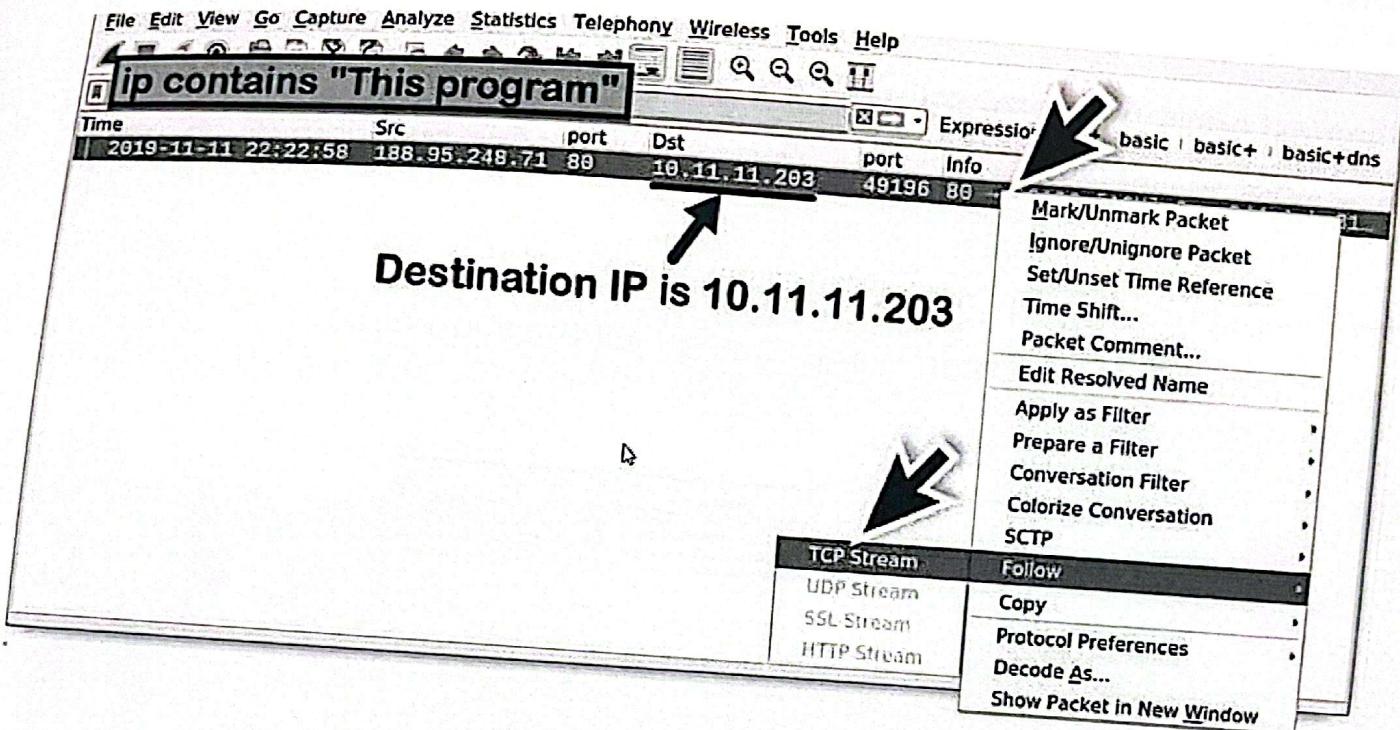
Frame 11419: 1411 bytes on wire (1118 bits), 1411 bytes captured (1118 bits) on interface Intel PRO/100 MT Desktop
 Ethernet II, Src: Cisco_97:4b:f0 (00:0c:cb:97:4b:f0), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
 Internet Protocol Version 4, Src: 188.95.248.71 (188.95.248.71), Dst: 10.11.11.203 (10.11.11.203)
 Transmission Control Protocol, Src Port: 80 (80), Dest Port: 49196 (49196)
 Sequence Number: 344 (relative), Sequence Number (raw): 3859588737
 [Next Sequence Number: 1701 (relative), Acknowledgment Number: 49234 (relative)]
 [TCP Segment Len: 1357]
 [Stream index: 264]
 [Conversation completeness: Complete]
 [TCP Segment Len: 1357]
 [Raw data length: 1357]

Hex	Dec	Text
0020	32	00 cb 00 56 c0 2c e6 0c
0030	48	a6 81 01 10 7f 31 50 10
0040	64	90 00 03 00 00 00 00 04 00
0050	80	00 00 00 00 00 00 00 00 00
0060	96	00 00 00 00 00 00 00 00 00
0070	112	00 00 b8 00 00 00 0e 1f
0080	128	ba 0e 00 b4 09 cd 21 b8
0090	144	20 70 72 6f 67 72 51 6d
00a0	160	01 4c cd 21 54 68 69 73
00b0	176	20 63 61 6e 6e 6f 74 20
00c0	192	62 65 20 72 75 6e 20 69
00d0	208	6e 20 44 4f 53 20 6d 6f
00e0	224	64 65 2e 0d 0d 0a 24 00
00f0	240	ab 31 40 af c5 62 40 af
0100	256	c5 62 40 af c5 62 c3 b3
0110	272	cb 62 41 af c5 62 29 b0
0120	288	c8 62 41 af c5 62 52 69
0130	304	ch@... b... bA.. bRi
0140	320	b@... b... bA.. bRi
0150	336	ch@... b... bA.. bRi
0160	352	ch@... b... bA.. bRi
0170	368	ch@... b... bA.. bRi
0180	384	ch@... b... bA.. bRi
0190	400	ch@... b... bA.. bRi
01a0	416	ch@... b... bA.. bRi
01b0	432	ch@... b... bA.. bRi
01c0	448	ch@... b... bA.. bRi
01d0	464	ch@... b... bA.. bRi
01e0	480	ch@... b... bA.. bRi
01f0	496	ch@... b... bA.. bRi
0200	512	ch@... b... bA.. bRi
0210	528	ch@... b... bA.. bRi
0220	544	ch@... b... bA.. bRi
0230	560	ch@... b... bA.. bRi
0240	576	ch@... b... bA.. bRi
0250	592	ch@... b... bA.. bRi
0260	608	ch@... b... bA.. bRi
0270	624	ch@... b... bA.. bRi
0280	640	ch@... b... bA.. bRi
0290	656	ch@... b... bA.. bRi
02a0	672	ch@... b... bA.. bRi
02b0	688	ch@... b... bA.. bRi
02c0	704	ch@... b... bA.. bRi
02d0	720	ch@... b... bA.. bRi
02e0	736	ch@... b... bA.. bRi
02f0	752	ch@... b... bA.. bRi
0300	768	ch@... b... bA.. bRi
0310	784	ch@... b... bA.. bRi
0320	800	ch@... b... bA.. bRi
0330	816	ch@... b... bA.. bRi
0340	832	ch@... b... bA.. bRi
0350	848	ch@... b... bA.. bRi
0360	864	ch@... b... bA.. bRi
0370	880	ch@... b... bA.. bRi
0380	896	ch@... b... bA.. bRi
0390	912	ch@... b... bA.. bRi
03a0	928	ch@... b... bA.. bRi
03b0	944	ch@... b... bA.. bRi
03c0	960	ch@... b... bA.. bRi
03d0	976	ch@... b... bA.. bRi
03e0	992	ch@... b... bA.. bRi
03f0	1008	ch@... b... bA.. bRi
0400	1024	ch@... b... bA.. bRi
0410	1040	ch@... b... bA.. bRi
0420	1056	ch@... b... bA.. bRi
0430	1072	ch@... b... bA.. bRi
0440	1088	ch@... b... bA.. bRi
0450	1104	ch@... b... bA.. bRi
0460	1120	ch@... b... bA.. bRi
0470	1136	ch@... b... bA.. bRi
0480	1152	ch@... b... bA.. bRi
0490	1168	ch@... b... bA.. bRi
04a0	1184	ch@... b... bA.. bRi
04b0	1200	ch@... b... bA.. bRi
04c0	1216	ch@... b... bA.. bRi
04d0	1232	ch@... b... bA.. bRi
04e0	1248	ch@... b... bA.. bRi
04f0	1264	ch@... b... bA.. bRi
0500	1280	ch@... b... bA.. bRi
0510	1296	ch@... b... bA.. bRi
0520	1312	ch@... b... bA.. bRi
0530	1328	ch@... b... bA.. bRi
0540	1344	ch@... b... bA.. bRi
0550	1360	ch@... b... bA.. bRi
0560	1376	ch@... b... bA.. bRi
0570	1392	ch@... b... bA.. bRi
0580	1408	ch@... b... bA.. bRi
0590	1424	ch@... b... bA.. bRi
05a0	1440	ch@... b... bA.. bRi
05b0	1456	ch@... b... bA.. bRi
05c0	1472	ch@... b... bA.. bRi
05d0	1488	ch@... b... bA.. bRi
05e0	1504	ch@... b... bA.. bRi
05f0	1520	ch@... b... bA.. bRi
0600	1536	ch@... b... bA.. bRi
0610	1552	ch@... b... bA.. bRi
0620	1568	ch@... b... bA.. bRi
0630	1584	ch@... b... bA.. bRi
0640	1600	ch@... b... bA.. bRi
0650	1616	ch@... b... bA.. bRi
0660	1632	ch@... b... bA.. bRi
0670	1648	ch@... b... bA.. bRi
0680	1664	ch@... b... bA.. bRi
0690	1680	ch@... b... bA.. bRi
06a0	1696	ch@... b... bA.. bRi
06b0	1712	ch@... b... bA.. bRi
06c0	1728	ch@... b... bA.. bRi
06d0	1744	ch@... b... bA.. bRi
06e0	1760	ch@... b... bA.. bRi
06f0	1776	ch@... b... bA.. bRi
0700	1792	ch@... b... bA.. bRi
0710	1808	ch@... b... bA.. bRi
0720	1824	ch@... b... bA.. bRi
0730	1840	ch@... b... bA.. bRi
0740	1856	ch@... b... bA.. bRi
0750	1872	ch@... b... bA.. bRi
0760	1888	ch@... b... bA.. bRi
0770	1904	ch@... b... bA.. bRi
0780	1920	ch@... b... bA.. bRi
0790	1936	ch@... b... bA.. bRi
07a0	1952	ch@... b... bA.. bRi
07b0	1968	ch@... b... bA.. bRi
07c0	1984	ch@... b... bA.. bRi
07d0	2000	ch@... b... bA.. bRi
07e0	2016	ch@... b... bA.. bRi
07f0	2032	ch@... b... bA.. bRi
0800	2048	ch@... b... bA.. bRi
0810	2064	ch@... b... bA.. bRi
0820	2080	ch@... b... bA.. bRi
0830	2096	ch@... b... bA.. bRi
0840	2112	ch@... b... bA.. bRi
0850	2128	ch@... b... bA.. bRi
0860	2144	ch@... b... bA.. bRi
0870	2160	ch@... b... bA.. bRi
0880	2176	ch@... b... bA.. bRi
0890	2192	ch@... b... bA.. bRi
08a0	2208	ch@... b... bA.. bRi
08b0	2224	ch@... b... bA.. bRi
08c0	2240	ch@... b... bA.. bRi
08d0	2256	ch@... b... bA.. bRi
08e0	2272	ch@... b... bA.. bRi
08f0	2288	ch@... b... bA.. bRi
0900	2304	ch@... b... bA.. bRi
0910	2320	ch@... b... bA.. bRi
0920	2336	ch@... b... bA.. bRi
0930	2352	ch@... b... bA.. bRi
0940	2368	ch@... b... bA.. bRi
0950	2384	ch@... b... bA.. bRi
0960	2400	ch@... b... bA.. bRi
0970	2416	ch@... b... bA.. bRi
0980	2432	ch@... b... bA.. bRi
0990	2448	ch@... b... bA.. bRi
09a0	2464	ch@... b... bA.. bRi
09b0	2480	ch@... b... bA.. bRi
09c0	2496	ch@... b... bA.. bRi
09d0	2512	ch@... b... bA.. bRi
09e0	2528	ch@... b... bA.. bRi
09f0	2544	ch@... b... bA.. bRi
0a00	2560	ch@... b... bA.. bRi
0a10	2576	ch@... b... bA.. bRi
0a20	2592	ch@... b... bA.. bRi
0a30	2608	ch@... b... bA.. bRi
0a40	2624	ch@... b... bA.. bRi
0a50	2640	ch@... b... bA.. bRi
0a60	2656	ch@... b... bA.. bRi
0a70	2672	ch@... b... bA.. bRi
0a80	2688	ch@... b... bA.. bRi
0a90	2704	ch@... b... bA.. bRi
0aa0	2720	ch@... b... bA.. bRi
0ab0	2736	ch@... b... bA.. bRi
0ac0	2752	ch@... b... bA.. bRi
0ad0	2768	ch@... b... bA.. bRi
0ae0	2784	ch@... b... bA.. bRi
0af0	2800	ch@... b... bA.. bRi
0b00	2816	ch@... b... bA.. bRi
0b10	2832	ch@... b... bA.. bRi
0b20	2848	ch@... b... bA.. bRi
0b30	2864	ch@... b... bA.. bRi
0b40	2880	ch@... b... bA.. bRi
0b50	2896	ch@... b... bA.. bRi
0b60	2912	ch@... b... bA.. bRi
0b70	2928	ch@... b... bA.. bRi
0b80	2944	ch@... b... bA.. bRi
0b90	2960	ch@... b... bA.. bRi
0ba0	2976	ch@... b... bA.. bRi
0bb0	2992	ch@... b... bA.. bRi
0bc0	3008	ch@... b... bA.. bRi
0bd0	3024	ch@... b... bA.. bRi
0be0	3040	ch@... b... bA.. bRi
0bf0	3056	ch@... b... bA.. bRi
0c00	3072	ch@... b... bA.. bRi
0c10	3088	ch@... b... bA.. bRi
0c20	3104	ch@... b... bA.. bRi
0c30	3120	ch@... b... bA.. bRi
0c40	3136	ch@... b... bA.. bRi
0c50	3152	ch@... b... bA.. bRi
0c60	3168	ch@... b... bA.. bRi
0c70	3184	ch@... b... bA.. bRi
0c80	3200	ch@... b... bA.. bRi
0c90	3216	ch@... b... bA.. bRi
0ca0	3232	ch@... b... bA.. bRi
0cb0	3248	ch@... b... bA.. bRi
0cc0	3264	ch@... b... bA.. bRi
0cd0	3280	ch@... b... bA.. bRi
0ce0	3296	ch@... b... bA.. bRi
0cf0	3312	ch@... b... bA.. bRi
0d00	3328	ch@... b... bA.. bRi
0d10	3344	ch@... b... bA.. bRi
0d20	3360	ch@... b... bA.. bRi
0d30	3376	ch@... b... bA.. bRi
0d40	3392	ch@... b... bA.. bRi
0d50	3408	ch@... b... bA.. bRi
0d60	3424	ch@... b... bA.. bRi
0d70	3440	ch@... b... bA.. bRi
0d80	3456	ch@... b... bA.. bRi
0d90	3472	ch@... b... bA.. bRi
0da0	3488	ch@... b... bA.. bRi
0db0	3504	ch@... b... bA.. bRi
0dc0	3520	ch@... b... bA.. bRi
0dd0	3536	ch@... b... bA.. bRi
0de0	3552	ch@... b... bA.. bRi
0df0	3568	ch@... b... bA.. bRi
0e00	3584	ch@... b... bA.. bRi
0e10	3600	ch@... b... bA.. bRi
0e20	3616	ch@... b... bA.. bRi
0e30	3632	ch@... b... bA.. bRi
0e40	3648	ch@... b... bA.. bRi
0e50	3664	ch@... b... bA.. bRi
0e60	3680	ch@... b... bA.. bRi
0e70	3696	ch@... b... bA.. bRi
0e80	3712	ch@... b... bA.. bRi
0e90	3728	ch@... b... bA.. bRi
0ea0	3744	ch@... b... bA.. bRi
0eb0	3760	ch@... b... bA.. bRi
0ec0	3776	ch@... b... bA.. bRi
0ed0	3792	ch@... b... bA.. bRi
0ef0	3808	ch@... b... bA.. bRi
0f00	3824	ch@... b... bA.. bRi
0f10	3840	ch@... b... bA.. bRi
0f20	3856	ch@... b... bA.. bRi
0f30	3872	ch@... b... bA.. bRi
0f40	3888	ch@... b... bA.. bRi
0f50	3904	ch@... b... bA.. bRi
0f60	3920	ch@... b... bA.. bRi
0f70	3936	ch@... b... bA.. bRi
0f80	3952	ch@... b... bA.. bRi
0f90	3968	ch@... b... bA.. bRi
0fa0	3984	ch@... b... bA.. bRi
0fb0	4000	ch@... b... bA.. bRi
0fc0	4016	ch@... b... bA.. bRi
0fd0	4032	ch@... b... bA.. bRi
0fe0	4048	ch@... b... bA.. bRi
0ff0	4064	ch@... b... bA.. bRi
1000	4080	ch@... b... bA.. bRi
1010	4096	ch@... b... bA.. bRi
1020	4112	ch@... b... bA.. bRi
1030	4128	ch@... b... bA.. bRi
1040	4144	ch@... b... bA.. bRi
1050	4160	ch@... b... bA.. bRi
1060	4176	ch@... b... bA.. bRi
1070	4192	ch@... b... bA.. bRi
1080	4208	ch@... b... bA.. bRi
1090	4224	ch@... b... bA.. bRi
10a0	4240	ch@... b... bA.. bRi
10b0	4256	ch@... b... bA.. bRi
10c0	4272	ch@... b... bA.. bRi
10d0	4288	ch@... b... bA.. bRi
10e0	4304	ch@... b... bA.. bRi
10f0	4320	ch@... b...

10/6/25, 8:38 PM

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.



6/25, 8:38 PM

Pcap Analysis using Wireshark — 1 | by Abhijit Kamath | Medium

```
GET /40group.tiff HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/
7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media
Center PC 6.0; .NET4.0C; .NET4.0E)
Host: acjabogados.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Connection: Keep-Alive
Cache-Control: public, max-age=31557600
Expires: Wed, 11 Nov 2020 04:22:59 GMT
Content-Type: image/tiff
Last-Modified: Tue, 05 Nov 2019 13:19:00 GMT
Accept-Ranges: bytes
Content-Length: 389120
Date: Mon, 11 Nov 2019 04:22:59 GMT
Server: LiteSpeed
Strict-Transport-Security: max-age=31536000

MZ.....@.....!
This program cannot be run in DOS mode.

$.....
```

1 client pkt. 288 server pkts. 1 turn.

Entire conversation (389 kB)

Show and save data as **ASCII** Stream **264** Find Next

Find:

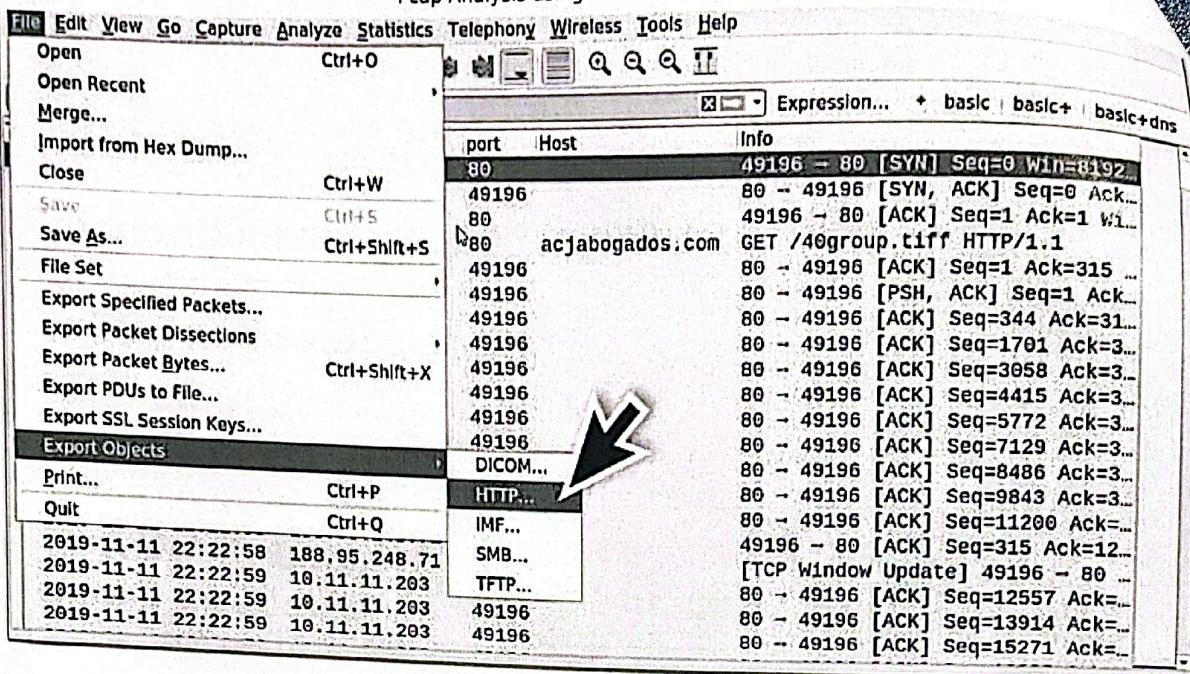
First two bytes of an EXE or DLL file show as "MZ"

This type of line commonly found in EXE or DLL files

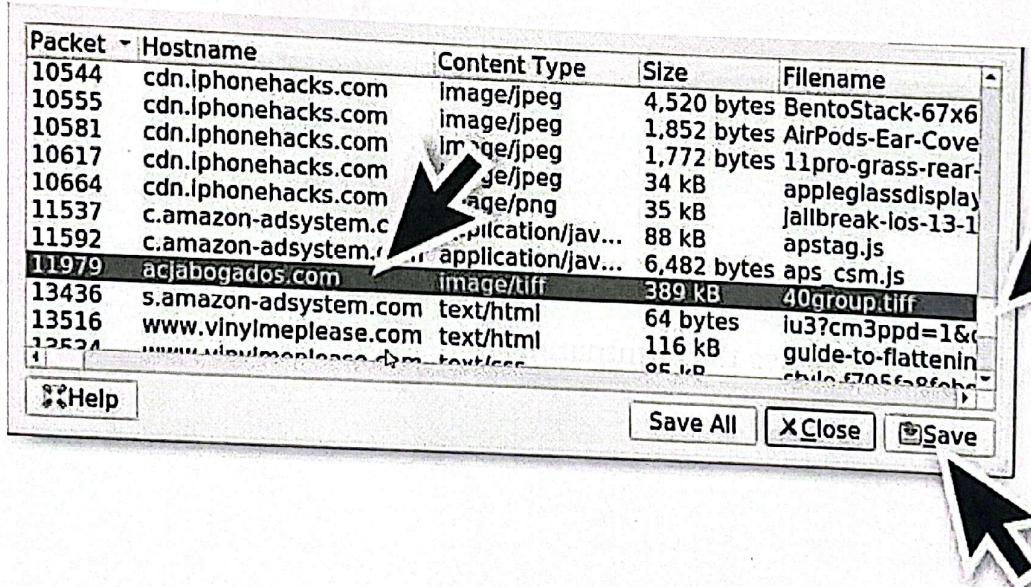
http://acjabogados.com/40group.tiff

Question 10

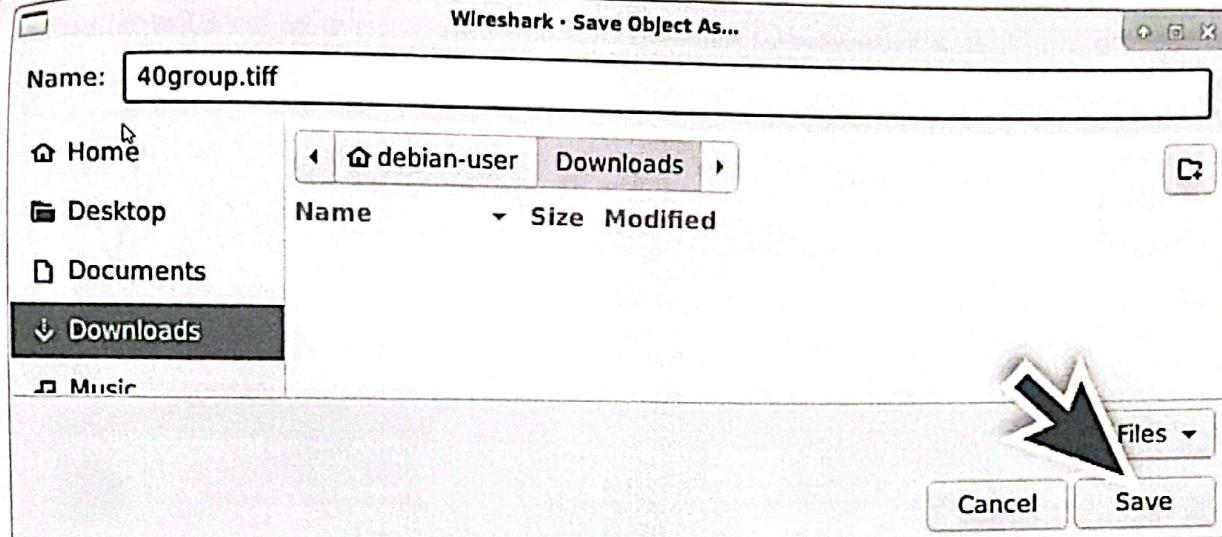
To find the SHA value use the Linux command **shasum**. So, here save the file on your device (kali) and use the command.



Finding the Object in Wireshark



Saving the file on to your host machine



Saving it

```
Terminal - debian-user@debian-host: ~/Downloads
File Edit View Terminal Tabs Help
debian-user@debian-host:~$ cd Downloads/
debian-user@debian-host:~/Downloads$ shasum -a 256 40group.tif
8d5d36c8fb0a9c81b145aa40c1ff3475702fb0b5f9e08e0577bdc405087e635 40group.tif
debian-user@debian-host:~/Downloads$
```

Find the SHA value

Question 11

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

49 / 70
Community Score

① 49 engines detected this file

8d5d36c8fffb0a9c81b145aa40c1f3475702fb0b5f0e08e0577bdc405087e635
Santo Maris Ola

380 KB 2019-11-12 16:01:33 UTC
Size 5 hours ago

① Trojan.VBS!Win32.Snejan.4'e
① Trojan.Win32.Snejan.c7857a31

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	① Trojan.Agent.EHBD		AegisLab	① Trojan.VBS!Win32.Snejan.4'e
AhnLab-V3	① Trojan.Win32.RL.Inject.R29B352		Alibaba	① Trojan.Win32.Snejan.c7857a31
Alfa	① Trojan.Agent.EHBD		Comptech.ANOV	① Trojan.VBS!Win32.Snejan.4'e

Question 12

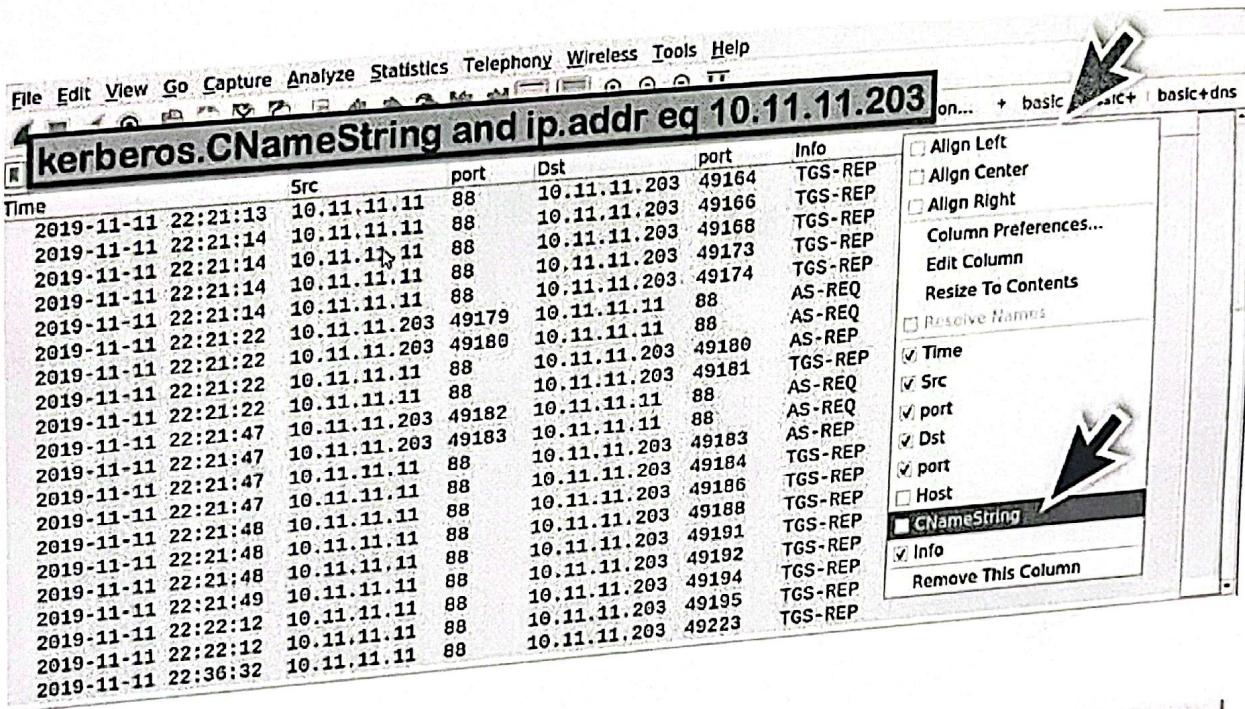
Time	Src	Dst	port	Host	Info
2019-11-11 22:22:58	188.95.248.71	80			49196 → 80 [SYN] Seq=0 Win=819...
2019-11-11 22:22:58	188.95.248.71	80		acjabogados.com	GET /40group.tif HTTP/1.1
2019-11-11 22:23:45	138.201.6.195	443			49199 → 443 [SYN] Seq=0 Win=819...
2019-11-11 22:23:48	138.201.6.195	443			[TCP Retransmission] 49199 → 44...
2019-11-11 22:23:54	138.201.6.195	443			[TCP Retransmission] 49199 → 44...
2019-11-11 22:24:14	5.188.108.58	443			49200 → 443 [SYN] Seq=0 Win=819...
2019-11-11 22:24:17	5.188.108.58	443			[TCP Retransmission] 49200 → 44...
2019-11-11 22:24:23	5.188.108.58	443			[TCP Retransmission] 49200 → 44...
2019-11-11 22:24:59	5.188.108.58	443			49201 → 443 [SYN] Seq=0 Win=819...
2019-11-11 22:25:02	5.188.108.58	443			[TCP Retransmission] 49201 → 44...
2019-11-11 22:25:08	5.188.108.58	443			[TCP Retransmission] 49201 → 44...
2019-11-11 22:25:28	138.201.6.195	443			49202 → 443 [SYN] Seq=0 Win=819...
2019-11-11 22:25:31	138.201.6.195	443			[TCP Retransmission] 49202 → 44...
2019-11-11 22:25:37	138.201.6.195	443			[TCP Retransmission] 49202 → 44...
2019-11-11 22:25:57	138.201.6.195	443			49203 → 443 [SYN] Seq=0 Win=819...
2019-11-11 22:26:01	138.201.6.195	443			[TCP Retransmission] 49203 → 44...
2019-11-11 22:26:07	138.201.6.195	443			[TCP Retransmission] 49203 → 44...
2019-11-11 22:26:35	5.188.108.58	443			49204 → 443 [SYN] Seq=0 Win=819...
2019-11-11 22:26:38	5.188.108.58	443			[TCP Retransmission] 49204 → 44...
2019-11-11 22:26:44	5.188.108.58	443			[TCP Retransmission] 49204 → 44...

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.

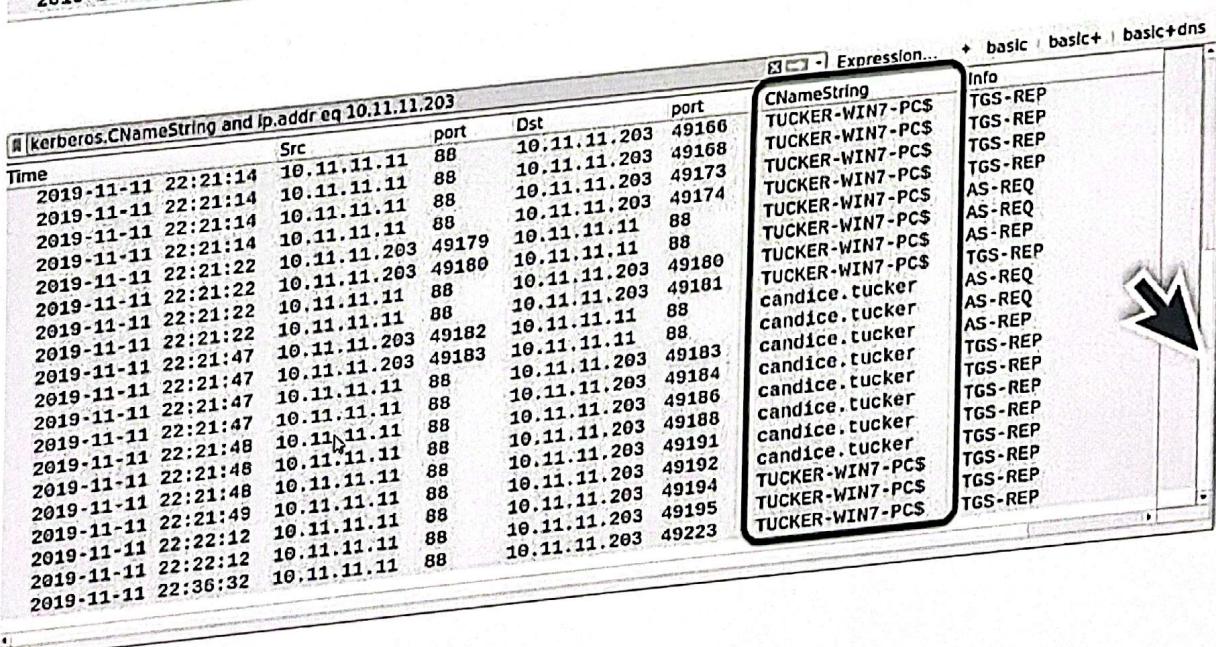
Question 13

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



Wireshark screenshot showing a list of Kerberos CNameString requests. The list includes:

Time	Src	port	Dst	port	Info
2019-11-11 22:21:13	10.11.11.11	88	10.11.11.203	49164	TGS-REP
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49166	TGS-REP
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49168	TGS-REP
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49173	TGS-REP
2019-11-11 22:21:14	10.11.11.203	49179	10.11.11.11	88	TGS-REP
2019-11-11 22:21:22	10.11.11.203	49180	10.11.11.203	49180	AS-REQ
2019-11-11 22:21:22	10.11.11.11	88	10.11.11.203	49181	AS-REQ
2019-11-11 22:21:22	10.11.11.203	49182	10.11.11.11	88	TGS-REP
2019-11-11 22:21:47	10.11.11.203	49183	10.11.11.11	88	AS-REQ
2019-11-11 22:21:47	10.11.11.11	88	10.11.11.203	49183	AS-REQ
2019-11-11 22:21:47	10.11.11.11	88	10.11.11.203	49184	TGS-REP
2019-11-11 22:21:48	10.11.11.11	88	10.11.11.203	49186	TGS-REP
2019-11-11 22:21:48	10.11.11.11	88	10.11.11.203	49188	TGS-REP
2019-11-11 22:21:49	10.11.11.11	88	10.11.11.203	49191	TGS-REP
2019-11-11 22:22:12	10.11.11.11	88	10.11.11.203	49192	TGS-REP
2019-11-11 22:22:12	10.11.11.11	88	10.11.11.203	49194	TGS-REP
2019-11-11 22:36:32	10.11.11.11	88	10.11.11.203	49195	TGS-REP
			10.11.11.203	49223	TGS-REP



Wireshark screenshot showing a list of Kerberos CNameString responses. The list includes:

Time	Src	port	Dst	port	Info
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49166	TGS-REP
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49168	TGS-REP
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49173	TGS-REP
2019-11-11 22:21:14	10.11.11.203	49179	10.11.11.11	88	TGS-REP
2019-11-11 22:21:22	10.11.11.203	49180	10.11.11.11	88	AS-REQ
2019-11-11 22:21:22	10.11.11.11	88	10.11.11.203	49180	AS-REQ
2019-11-11 22:21:22	10.11.11.11	88	10.11.11.203	49181	TGS-REP
2019-11-11 22:21:47	10.11.11.203	49182	10.11.11.11	88	AS-REQ
2019-11-11 22:21:47	10.11.11.11	88	10.11.11.203	49183	AS-REQ
2019-11-11 22:21:47	10.11.11.11	88	10.11.11.203	49184	TGS-REP
2019-11-11 22:21:47	10.11.11.11	88	10.11.11.203	49186	TGS-REP
2019-11-11 22:21:48	10.11.11.11	88	10.11.11.203	49188	TGS-REP
2019-11-11 22:21:48	10.11.11.11	88	10.11.11.203	49191	TGS-REP
2019-11-11 22:21:49	10.11.11.11	88	10.11.11.203	49192	TGS-REP
2019-11-11 22:22:12	10.11.11.11	88	10.11.11.203	49194	TGS-REP
2019-11-11 22:22:12	10.11.11.11	88	10.11.11.203	49195	TGS-REP
2019-11-11 22:36:32	10.11.11.11	88	10.11.11.203	49223	TGS-REP