

NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to exercise: <https://www.malware-traffic-analysis.net/2019/11/12/index.html>

Links to some tutorials I've written that should help with this exercise:

- [Customizing Wireshark - Changing Your Column Display](#)
- [Using Wireshark: Identifying Hosts and Users](#)
- [Using Wireshark - Display Filter Expressions](#)
- [Using Wireshark: Exporting Objects from a Pcap](#)

ENVIRONMENT FOR THE PCAP:

- 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

QUESTIONS:

- What operating system and type of device is on 10.11.11.94?
- What operating system and type of device is on 10.11.11.121?
- Based on the MAC address for 10.11.11.145, who is the manufacturer or vendor?
- What operating system and type of device is on 10.11.11.179?
- What version of Windows is being used on the host at 10.11.11.195?
- What is the user account name used to log into the Windows host at 10.11.11.200?
- What operating system and type of device is on 10.11.11.217?

- What IP is a Windows host that downloaded a Windows executable file over HTTP?
- What is the URL that returned the Windows executable file?
- What is the SHA256 file hash for that Windows executable file?
- What is the detection rate for that SHA256 hash on VirusTotal?
- What public IP addresses did that Windows host attempt to connect over TCP after the executable file was downloaded?
- What is the host name and Windows user account name used on that IP address?

NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

ANSWERS:

Q: What operating system and type of device is on 10.11.11.94?

A: **ChromeOS on a Chromebook**

Q: What operating system and type of device is on 10.11.11.121?

A: **Samsung Galaxy Note 8**

Q: Based on the MAC address for 10.11.11.145, who is the manufacturer or vendor?

A: **Motorola**

Q: What operating system and type of device is on 10.11.11.179?

A: **macOS 10.15.1 (Catalina) on a Mac (desktop or Macbook)**

Q: What version of Windows is being used on the host at 10.11.11.195?

A: **Windows 10**

Q: What is the user account name used to log into the Windows host at 10.11.11.200?

A: **brandon.gilbert**

Q: What operating system and type of device is on 10.11.11.217?

A: **iPadOS 13.2.2 on an iPad**

Q: What IP is a Windows host that downloaded a Windows executable file over HTTP?

A: **10.11.11.203**

Q: What is the URL that returned the Windows executable file?

A: **<http://acjabogados.com/40group.tiff>**

Q: What is the SHA256 file hash for that Windows executable file?

A: **8d5d36c8ffb0a9c81b145aa40c1ff3475702fb0b5f9e08e0577bdc405087e635**

Q: What is the detection rate for that SHA256 hash on VirusTotal?

A: **49 of 70**

NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

Q: What public IP addresses did that Windows host attempt to connect over TCP without a response from the server after the above executable file was downloaded?

A: **5.188.108.58 and 138.201.6.195**

Q: What is the host name and Windows user account name used on that IP address?

A: **host name: Tucker-Win7-PC , user account name: candice.tucker**

NOTES:

Q: What operating system and type of device is on 10.11.11.94?

A: **ChromeOS on a Chromebook**

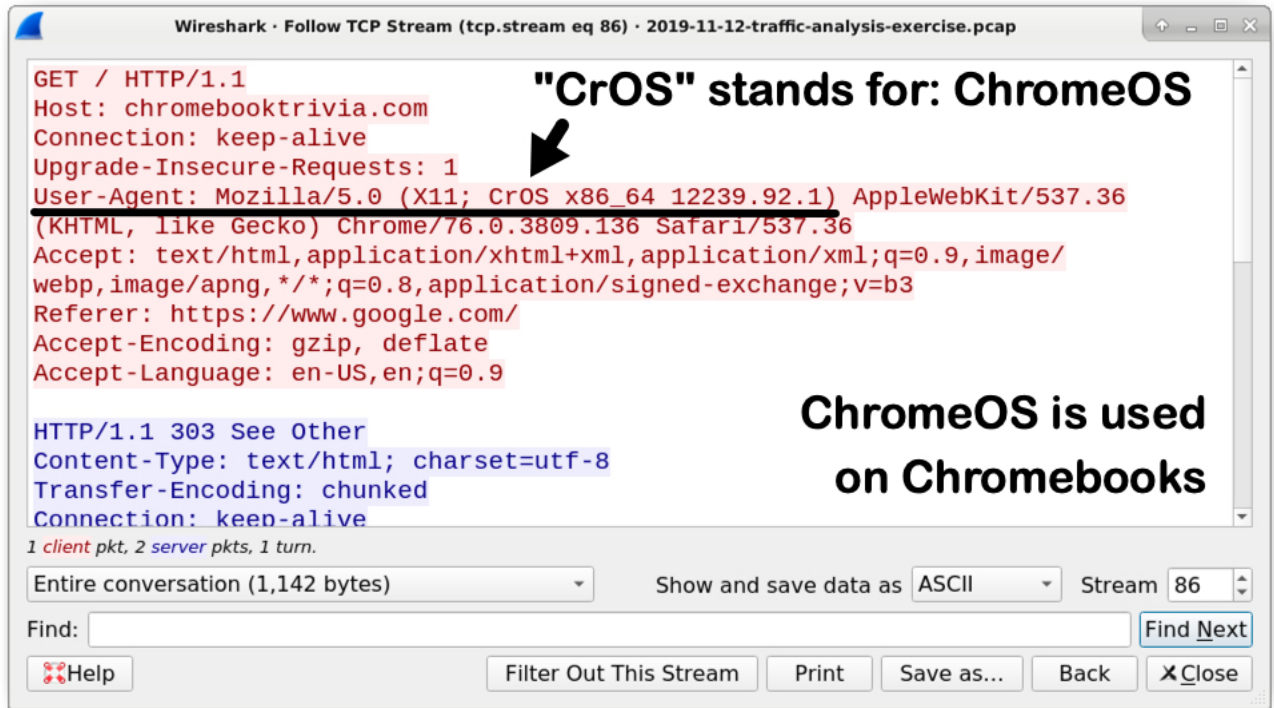
The screenshot shows the Wireshark interface with a capture file named '2019-11-12-traffic-analysis-exercise.pcap'. A filter is applied to the packet list: 'http.request and ip.addr eq 10.11.11.94'. The packet list table is as follows:

Time	Dst	port	Host	Info
2019-11-11 22:21:06	239.255.255...	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2019-11-11 22:21:07	239.255.255...	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2019-11-11 22:21:07	216.58.194...	80	www.gstatic.com	GET /generate_204 HTTP/1.1
2019-11-11 22:21:07	216.58.194...	80	www.gstatic.com	GET /generate_204 HTTP/1.1
2019-11-11 22:21:08	239.255.255...	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2019-11-11 22:21:09	239.255.255...	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2019-11-11 22:21:10	216.58.194...	80	www.gstatic.com	GET /generate_204 HTTP/1.1
2019-11-11 22:21:34	64.98.145.30	80	chromebooktrivia.com	GET / HTTP/1.1
2019-11-11 22:21:35	216.58.194...	80	www.gstatic.com	GET / HTTP/1.1
2019-11-11 22:21:38	52.218.228...	80	www.chromebooktrivia.com	GET /tin-c...
2019-11-11 22:21:38	52.218.228...	80	www.chromebooktrivia.com	GET /friday...
2019-11-11 22:21:38	52.218.228...	80	www.chromebooktrivia.com	GET /friday...
2019-11-11 22:22:04	216.58.194...	80	www.gstatic.com	GET / HTTP/1.1
2019-11-11 22:22:32	216.58.194...	80	www.gstatic.com	GET / HTTP/1.1
2019-11-11 22:23:06	239.255.255...	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2019-11-11 22:23:07	239.255.255...	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2019-11-11 22:23:08	239.255.255...	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2019-11-11 22:23:09	239.255.255...	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2019-11-11 22:23:16	216.58.194...	80	www.gstatic.com	GET / HTTP/1.1

A context menu is open over the selected packet (Time: 2019-11-11 22:21:34). The menu options are:

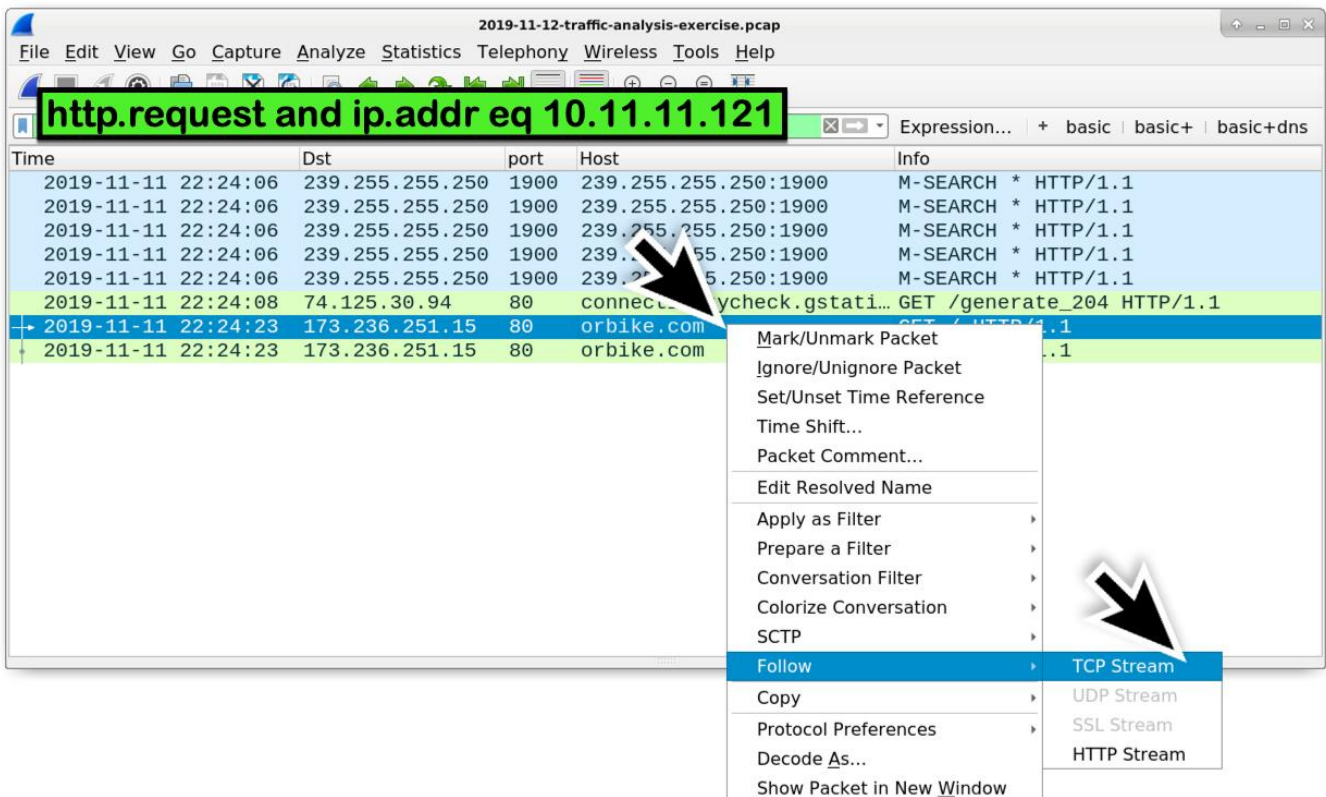
- Mark/Unmark Packet
- Ignore/Unignore Packet
- Set/Unset Time Reference
- Time Shift...
- Packet Comment...
- Edit Resolved Name
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow
 - TCP Stream
 - UDP Stream
 - SSL Stream
 - HTTP Stream
- Copy
- Protocol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

NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS



Q: What operating system and type of device is on 10.11.11.121?

A: **Samsung Galaxy Note 8**



NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

Wireshark · Follow TCP Stream (tcp.stream eq 391) · 2019-11-12-traffic-analysis-exercise.pcap

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

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

2 client pkts, 16 server pkts, 3 turns.

Entire conversation (20 kB) Show and save data as ASCII Stream 391

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close



SM-N950U



All

Shopping

Images

News

Videos

More

Settings

Tools

About 539,000 results (0.54 seconds)

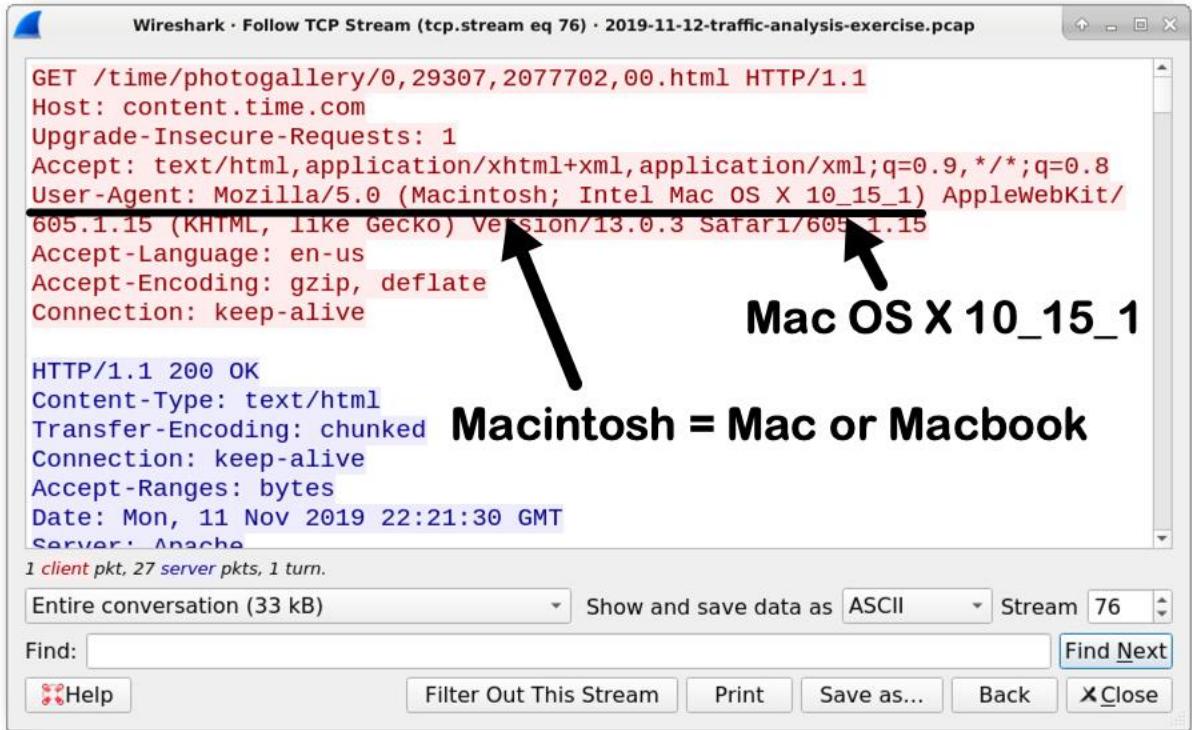
Samsung Galaxy Note 8 (US) SM-N950U full specifications

<https://www.sammobile.com> › Latest Samsung full device specifications ▼

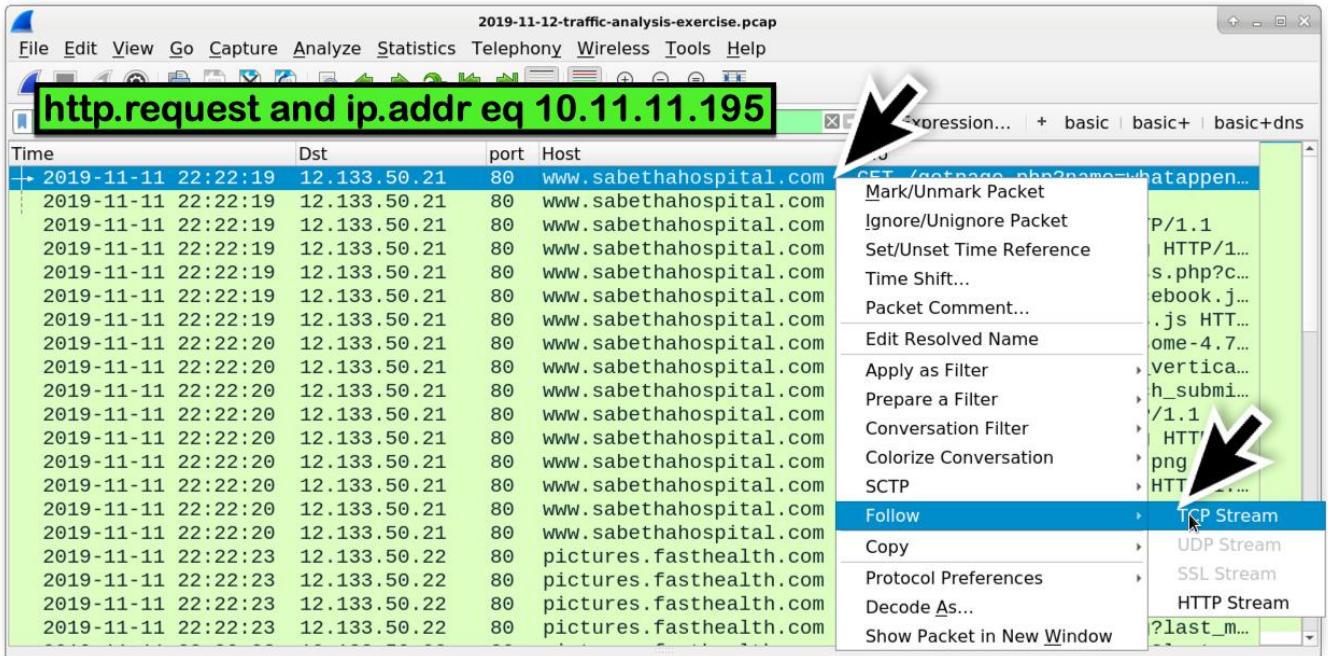
Samsung's **Galaxy Note 8 (US) SM-N950U** specifications and features: this is a 6.3" (160.02mm) device with a QHD 2960x1440 screen resolution. The phone is powered by the Qualcomm Snapdragon 835 soc with a Quad-Core 2.35GHz & Quad-Core 1.9GHz configuration.

People also ask

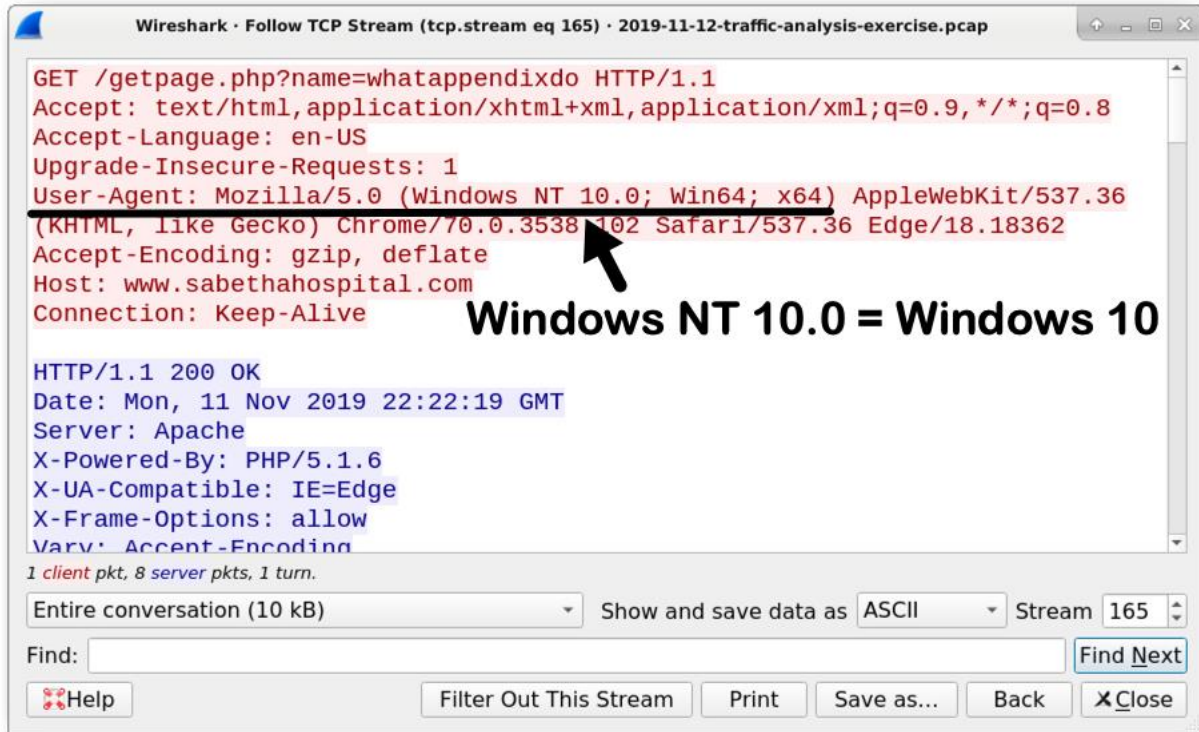
NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS



Q: What version of Windows is being used on the host at 10.11.11.195?
A: **Windows 10**



NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS



Q: What is the user account name used to log into the Windows host at 10.11.11.200?

A: **brandon.gilbert**

NOTE: This assumes you've set your Wireshark column display as noted in the following two tutorials:

- [Customizing Wireshark - Changing Your Column Display](#)
- [Using Wireshark: Identifying Hosts and Users](#)

NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

The screenshot shows the Wireshark interface with a filter expression `kerberos.CNameString and ip.addr eq 10.11.11.200` applied. A context menu is open over the 'Info' column header, and the 'CNameString' option is selected. The main packet list shows various traffic entries with their respective source and destination IP addresses and ports.

Time	Src	port	Dst	port	Info
2019-11-11 22:20:22	10.11.11.200	49159	10.11.11.11	88	AS-RE
2019-11-11 22:20:22	10.11.11.200	49160	10.11.11.11	88	AS-RE
2019-11-11 22:20:22	10.11.11.11	88	10.11.11.200	49160	AS-RE
2019-11-11 22:20:22	10.11.11.11	88	10.11.11.200	49161	TGS-R
2019-11-11 22:20:23	10.11.11.200	49163	10.11.11.11	88	AS-RE
2019-11-11 22:20:23	10.11.11.200	49164	10.11.11.11	88	AS-RE
2019-11-11 22:20:23	10.11.11.11	88	10.11.11.200	49164	AS-RE
2019-11-11 22:20:23	10.11.11.11	88	10.11.11.200	49165	TGS-R
2019-11-11 22:20:24	10.11.11.11	88	10.11.11.200	49167	TGS-R
2019-11-11 22:20:24	10.11.11.11	88	10.11.11.200	49168	TGS-R
2019-11-11 22:20:24	10.11.11.11	88	10.11.11.200	49174	TGS-R
2019-11-11 22:20:24	10.11.11.11	88	10.11.11.200	49175	TGS-R
2019-11-11 22:20:31	10.11.11.200	49179	10.11.11.11	88	AS-RE
2019-11-11 22:20:31	10.11.11.200	49180	10.11.11.11	88	AS-RE
2019-11-11 22:20:31	10.11.11.11	88	10.11.11.200	49180	AS-RE
2019-11-11 22:20:31	10.11.11.11	88	10.11.11.200	49181	TGS-R
2019-11-11 22:21:22	10.11.11.11	88	10.11.11.200	49183	TGS-R
2019-11-11 22:21:22	10.11.11.11	88	10.11.11.200	49184	TGS-R
2019-11-11 22:21:56	10.11.11.200	49185	10.11.11.11	88	AS-RE
2019-11-11 22:21:56	10.11.11.200	49186	10.11.11.11	88	AS-RE

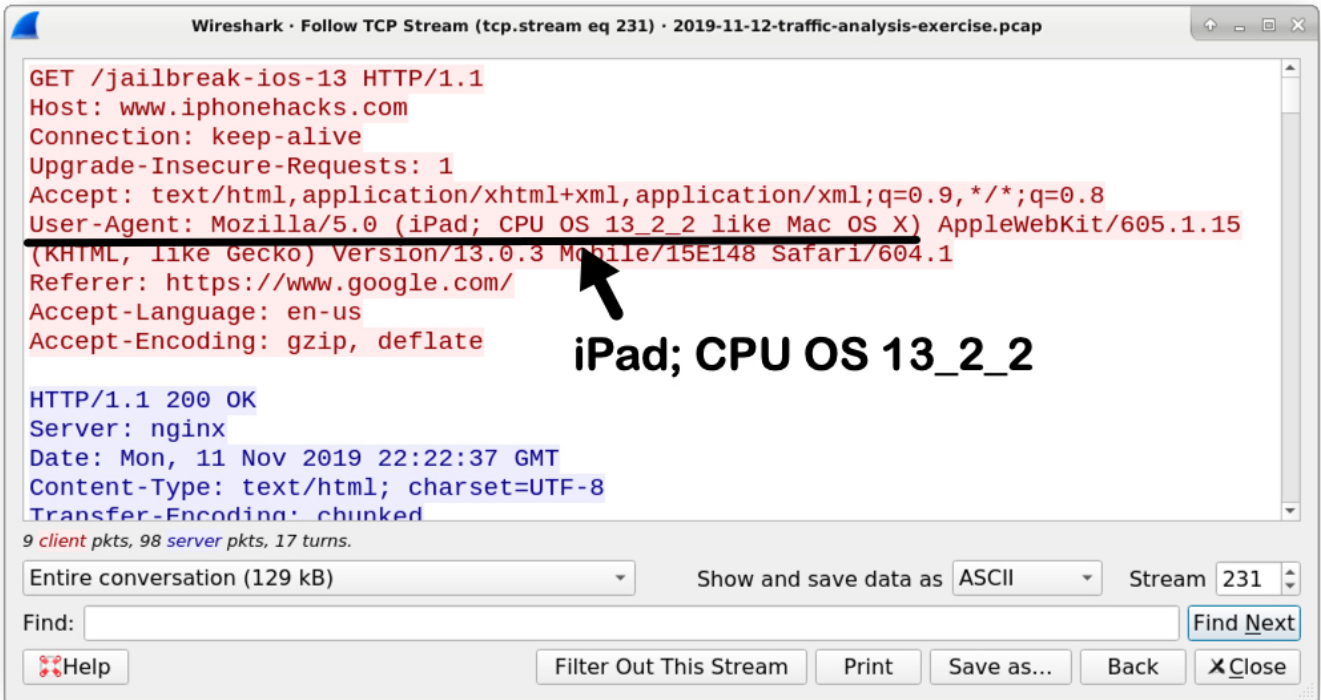
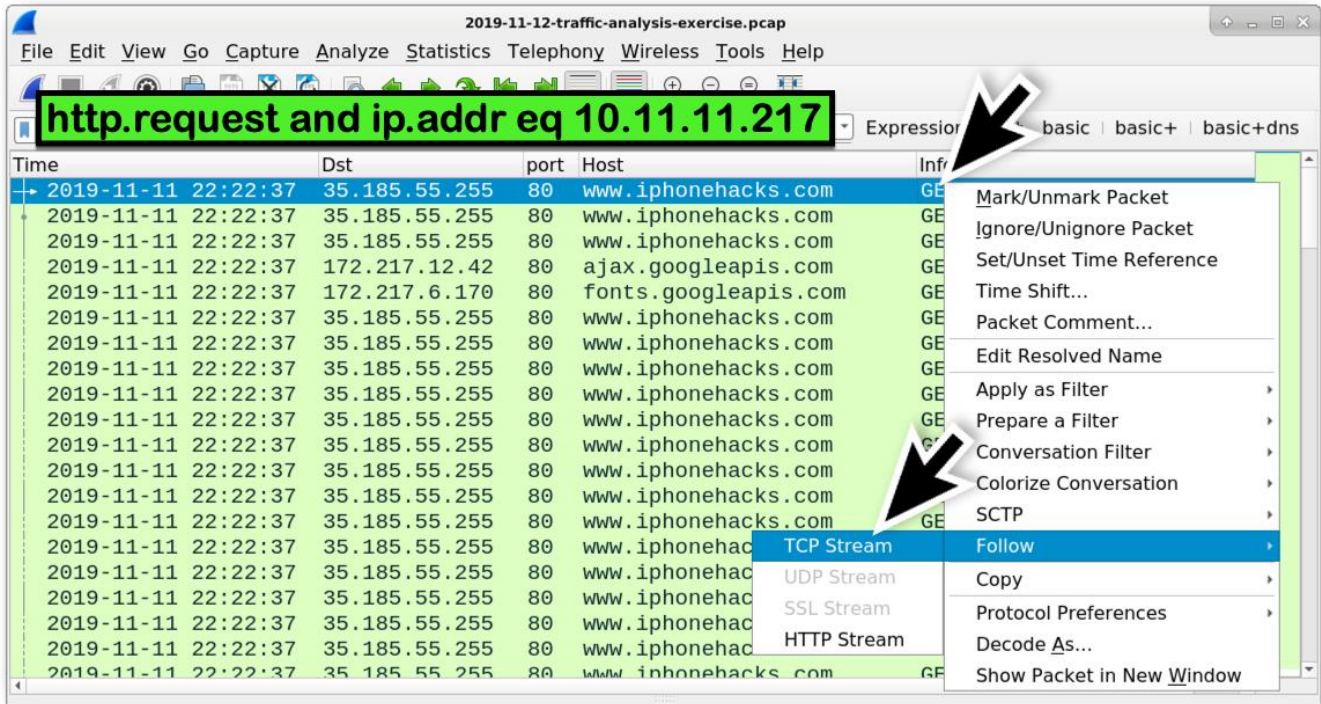
The screenshot shows the filtered traffic results in Wireshark. The filter expression `kerberos.CNameString and ip.addr eq 10.11.11.200` is applied. The 'CNameString' column is now visible, showing the names of the hosts involved in the Kerberos exchange. The 'Info' column shows the type of message (e.g., AS-REQ, TGS-REP).

Time	Src	port	Dst	port	CNameString	Info
2019-11-11 22:20:24	10.11.11.11	88	10.11.11.200	49167	GILBERT-WIN7-PC\$	TGS-REP
2019-11-11 22:20:24	10.11.11.11	88	10.11.11.200	49168	GILBERT-WIN7-PC\$	TGS-REP
2019-11-11 22:20:24	10.11.11.11	88	10.11.11.200	49174	GILBERT-WIN7-PC\$	TGS-REP
2019-11-11 22:20:24	10.11.11.11	88	10.11.11.200	49175	GILBERT-WIN7-PC\$	TGS-REP
2019-11-11 22:20:31	10.11.11.200	49179	10.11.11.11	88	GILBERT-WIN7-PC\$	AS-REQ
2019-11-11 22:20:31	10.11.11.200	49180	10.11.11.11	88	GILBERT-WIN7-PC\$	AS-REQ
2019-11-11 22:20:31	10.11.11.11	88	10.11.11.200	49180	GILBERT-WIN7-PC\$	AS-REP
2019-11-11 22:20:31	10.11.11.11	88	10.11.11.200	49181	GILBERT-WIN7-PC\$	TGS-REP
2019-11-11 22:21:22	10.11.11.11	88	10.11.11.200	49183	GILBERT-WIN7-PC\$	TGS-REP
2019-11-11 22:21:22	10.11.11.11	88	10.11.11.200	49184	GILBERT-WIN7-PC\$	TGS-REP
2019-11-11 22:21:56	10.11.11.200	49185	10.11.11.11	88	brandon.gilbert	AS-REQ
2019-11-11 22:21:56	10.11.11.200	49186	10.11.11.11	88	brandon.gilbert	AS-REQ
2019-11-11 22:21:56	10.11.11.11	88	10.11.11.200	49186	brandon.gilbert	AS-REP
2019-11-11 22:21:56	10.11.11.11	88	10.11.11.200	49187	brandon.gilbert	TGS-REP
2019-11-11 22:21:56	10.11.11.11	88	10.11.11.200	49190	brandon.gilbert	TGS-REP
2019-11-11 22:21:57	10.11.11.11	88	10.11.11.200	49192	brandon.gilbert	TGS-REP
2019-11-11 22:21:57	10.11.11.11	88	10.11.11.200	49195	brandon.gilbert	TGS-REP
2019-11-11 22:21:57	10.11.11.11	88	10.11.11.200	49196	brandon.gilbert	TGS-REP
2019-11-11 22:35:40	10.11.11.11	88	10.11.11.200	49280	GILBERT-WIN7-PC\$	TGS-REP

NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

Q: What operating system and type of device is on 10.11.11.217?

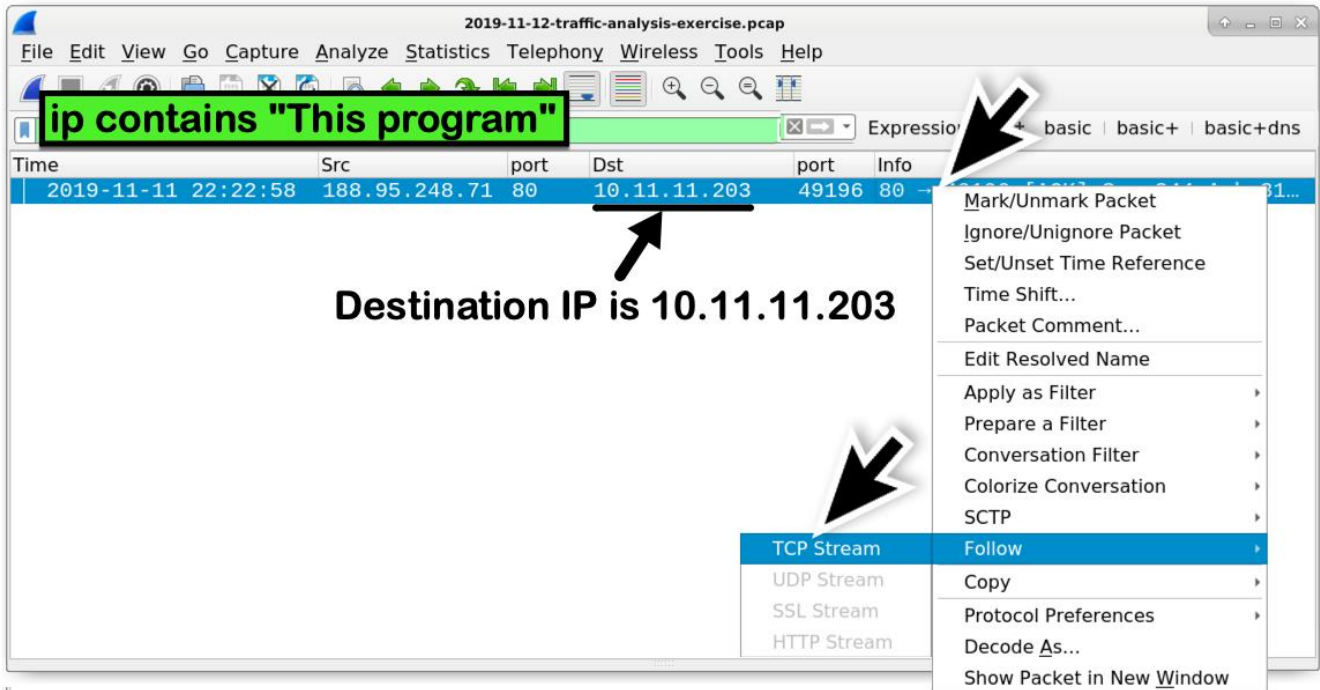
A: **iPadOS 13.2.2 on an iPad**



NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

Q: What IP is the host that downloaded a Windows executable file over HTTP?
A: **10.11.11.203**

Q: What is the URL that returned the Windows executable file?
A: **http://acjabogados.com/40group.tiff**



NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

The screenshot shows a Wireshark window titled "Follow TCP Stream (tcp.stream eq 264) · 2019-11-12-traffic-analysis-exercise.pcap". The main pane displays the following text:

```
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 20:22:59 GMT
Server: LiteSpeed
Strict-Transport-Security: max-age=31536000

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

Annotations in the image include:

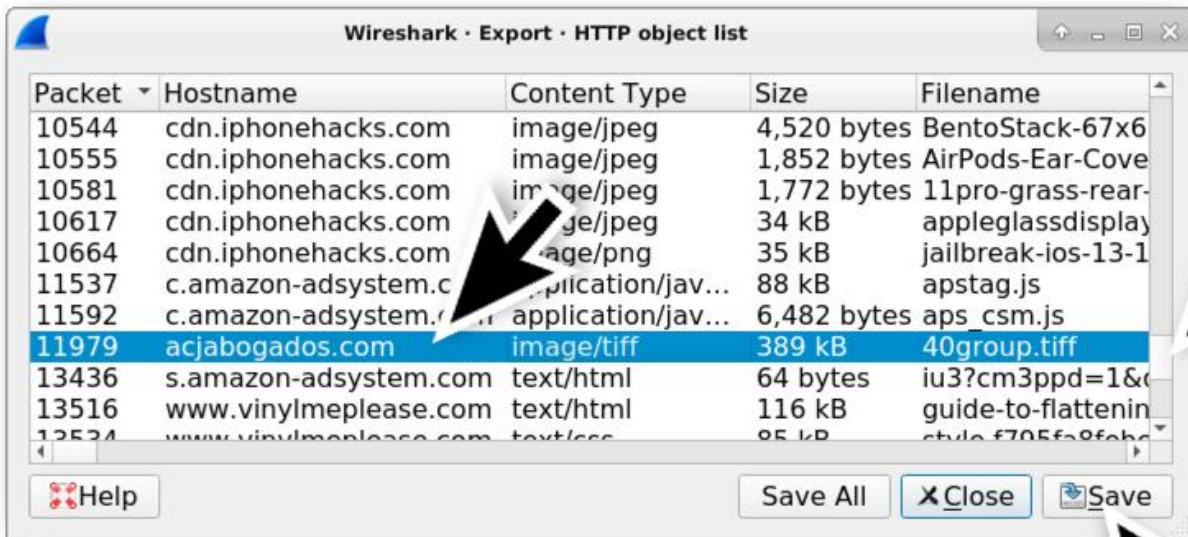
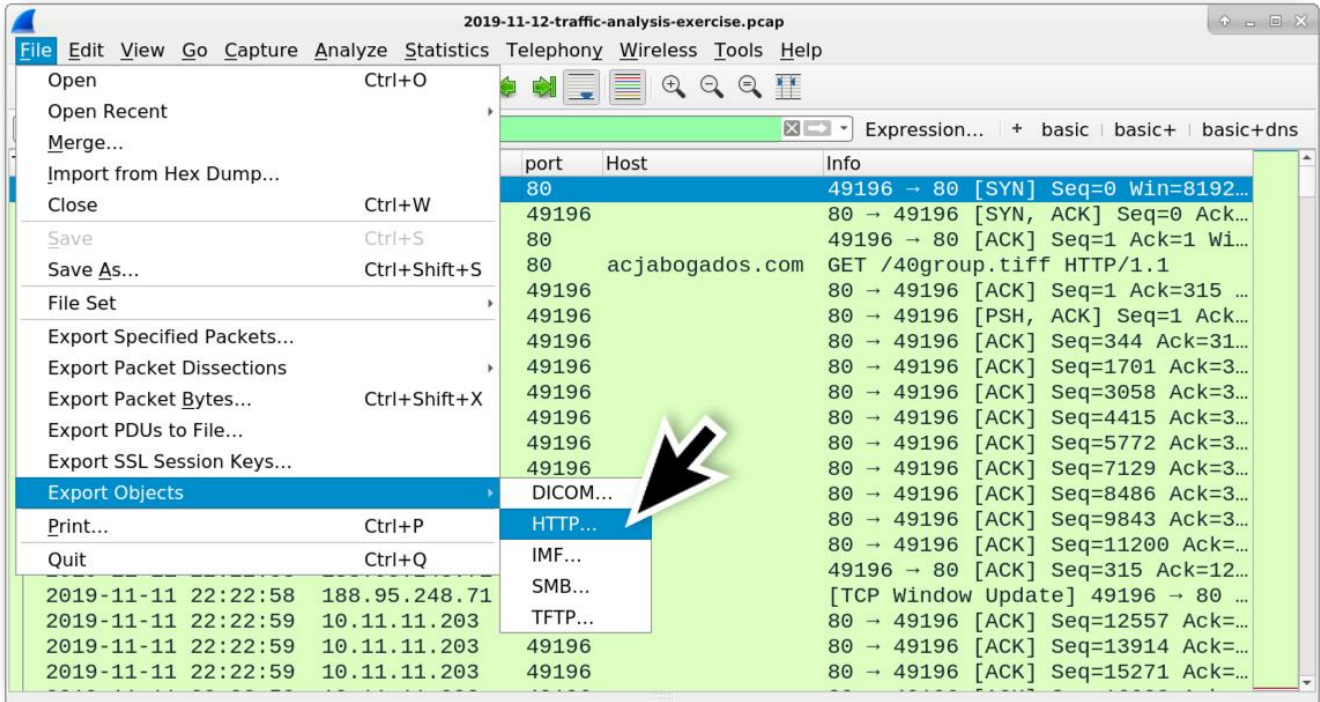
- An arrow pointing to the URL `http://acjabogados.com/40group.tiff` in the request line.
- An arrow pointing to the `MZ` characters in the response body.
- Text annotations: "First two bytes of an EXE or DLL file show as 'MZ'", "This type of line commonly found in EXE or DLL files", and "http://acjabogados.com/40group.tiff".

At the bottom of the window, there are controls for "Entire conversation (389 kB)", "Show and save data as ASCII", "Stream 264", a "Find:" search box, and buttons for "Help", "Filter Out This Stream", "Print", "Save as...", "Back", and "Close".

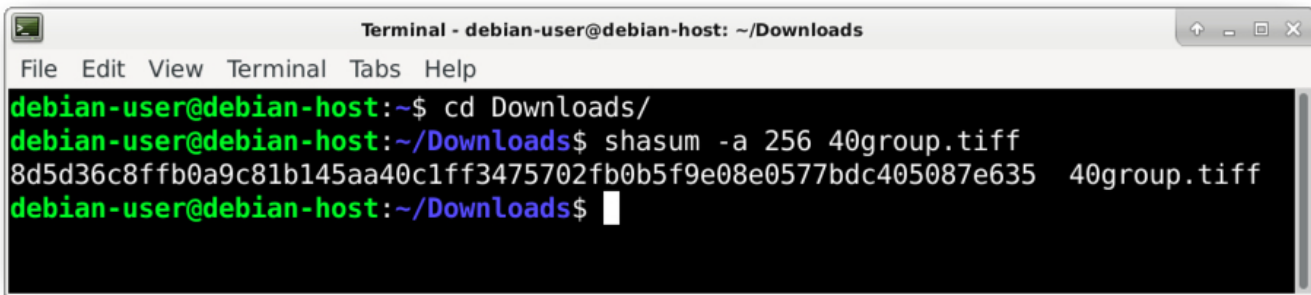
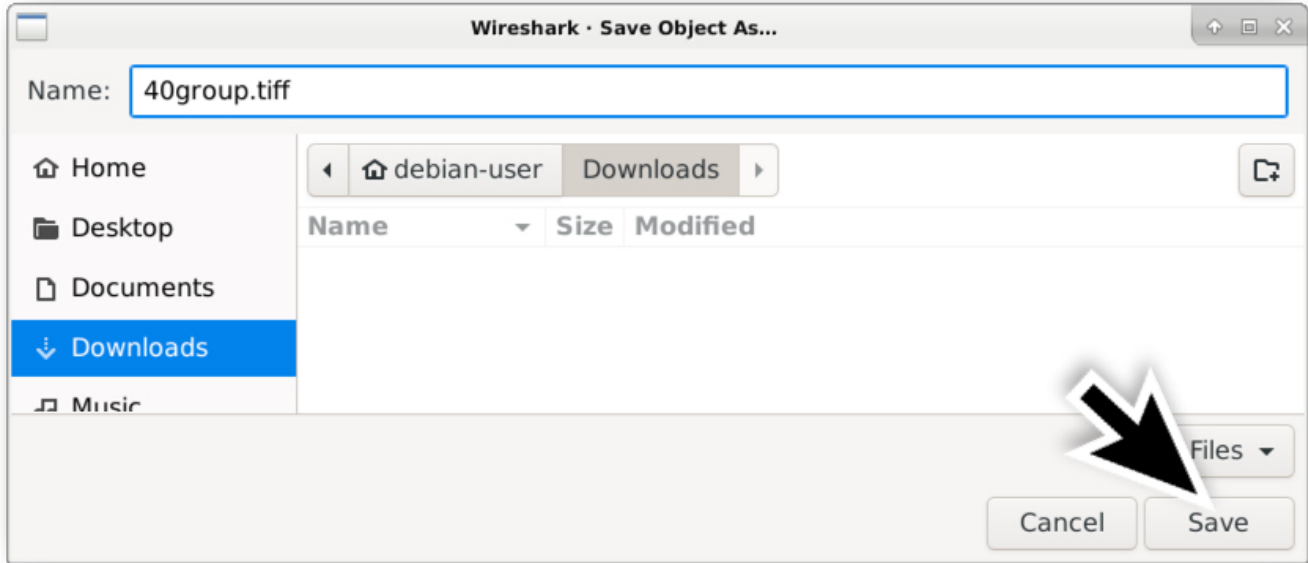
NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

Q: What is the SHA256 file hash for that Windows executable file?

A: **8d5d36c8ffb0a9c81b145aa40c1ff3475702fb0b5f9e08e0577bdc405087e635**



NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS



Q: What is the detection rate for that SHA256 hash on VirusTotal?

A: **49 of 70**

https://www.virustotal.com/gui/file/8d5d36c8ffb0a9c81b145aa40c1f3475702fb0b5f9e08e0577bdc405087e635

8d5d36c8ffb0a9c81b145aa40c1f3475702fb0b5f9e08e0577bdc405087e635

49 / 70

49 engines detected this file

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

Santo Maris Oia

peexe runtime-modules

EXE

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	Trojan.Agent.EHBD	AegisLab	Trojan.Win32.Snojan.4lc	
AhnLab-V3	Trojan/Win32.RL_Inject.R298352	Alibaba	Trojan/Win32/Snojan.c7857a31	
AlYac	Trojan.Agent.EHBD	SecureApp.ABEV	Melissa	

NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

Q: What public IP addresses did that Windows host attempt to connect over TCP without a response from the server after the above executable file was downloaded?

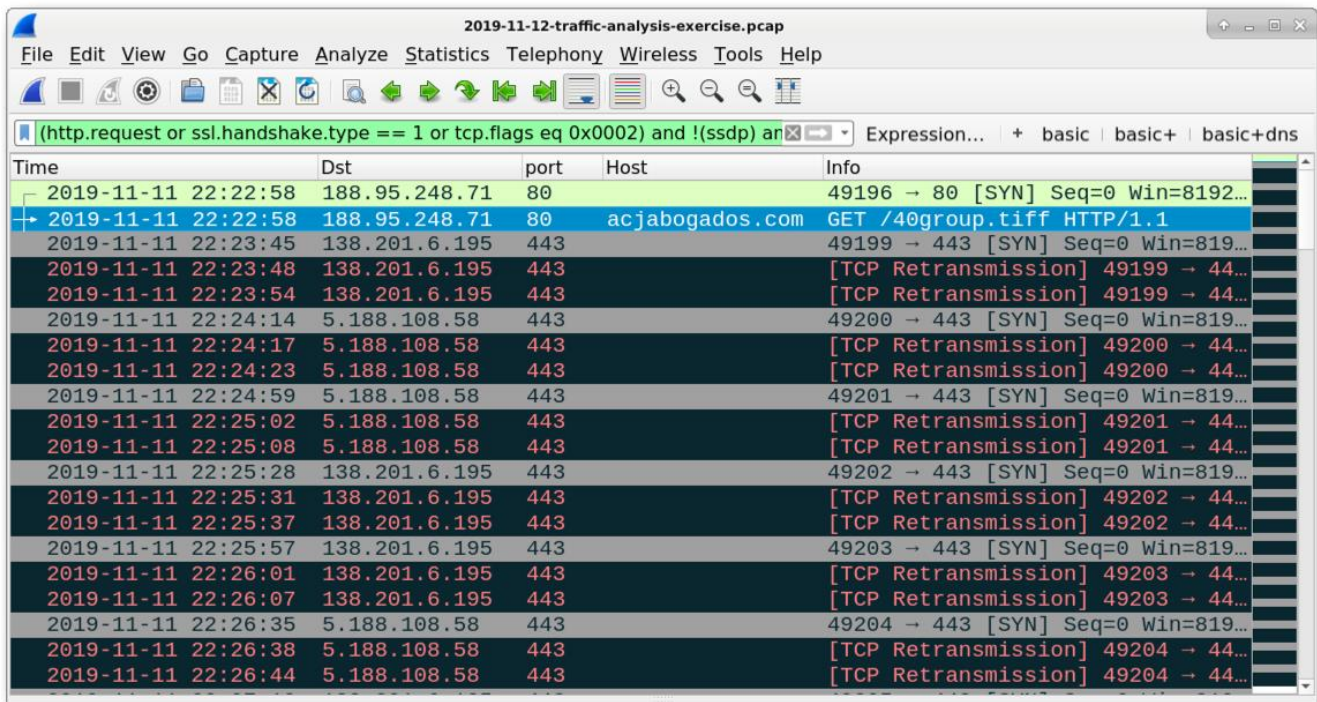
A: **5.188.108.58 and 138.201.6.195**

NOTE: This assumes you've saved Wireshark display filters for web-based traffic as noted in the following tutorial:

- [Using Wireshark - Display Filter Expressions](#)

Use your **basic+** filter and add:

and ip.addr eq 10.11.11.203 and !(ip.dst eq 10.11.11.11)



Q: What is the host name & Windows user account name used on that IP address?

A: **host name: Tucker-Win7-PC , user account name: candice.tucker**

NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

NOTE: This assumes you've set your Wireshark column display as noted in the following two tutorials:

- [Customizing Wireshark - Changing Your Column Display](#)
- [Using Wireshark: Identifying Hosts and Users](#)

