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**

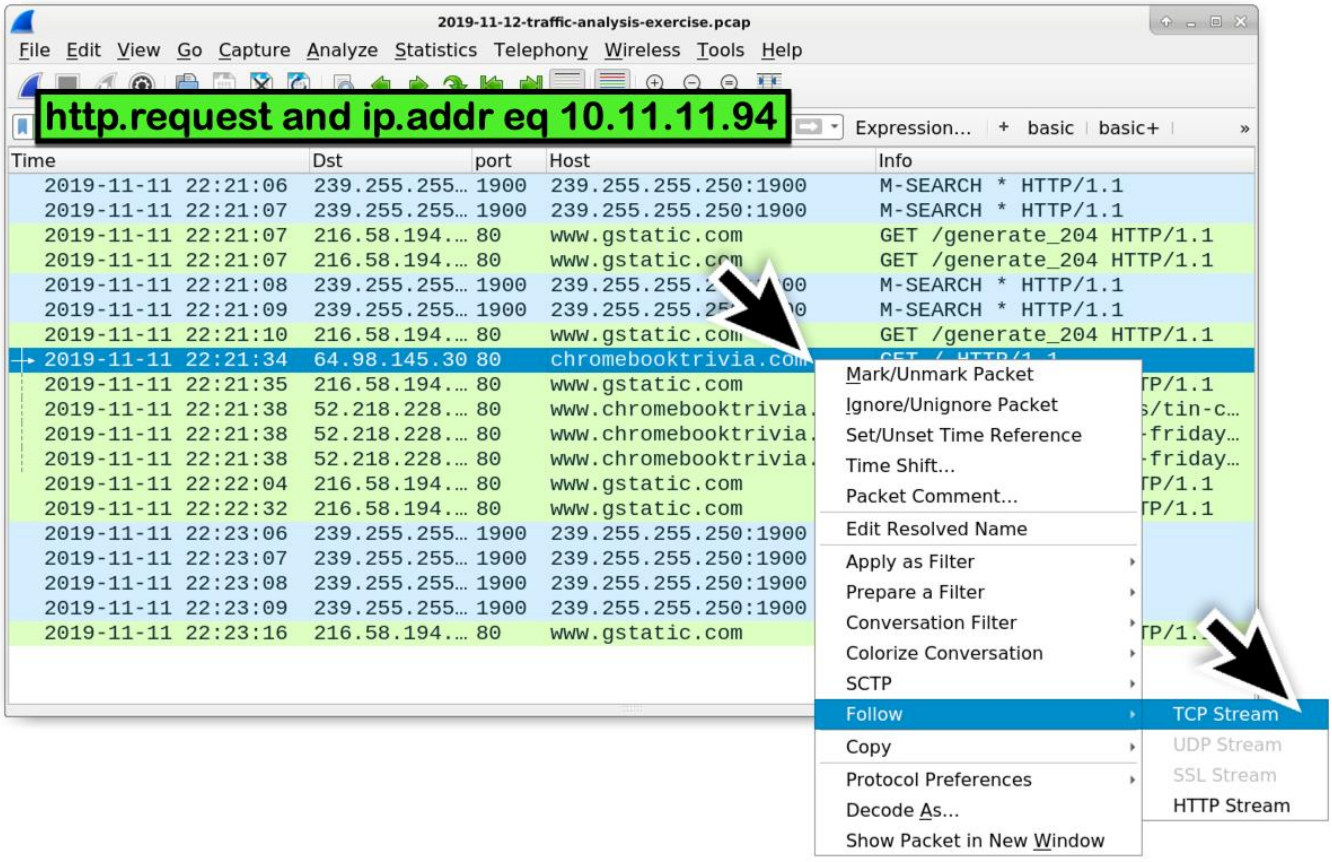
NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

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**

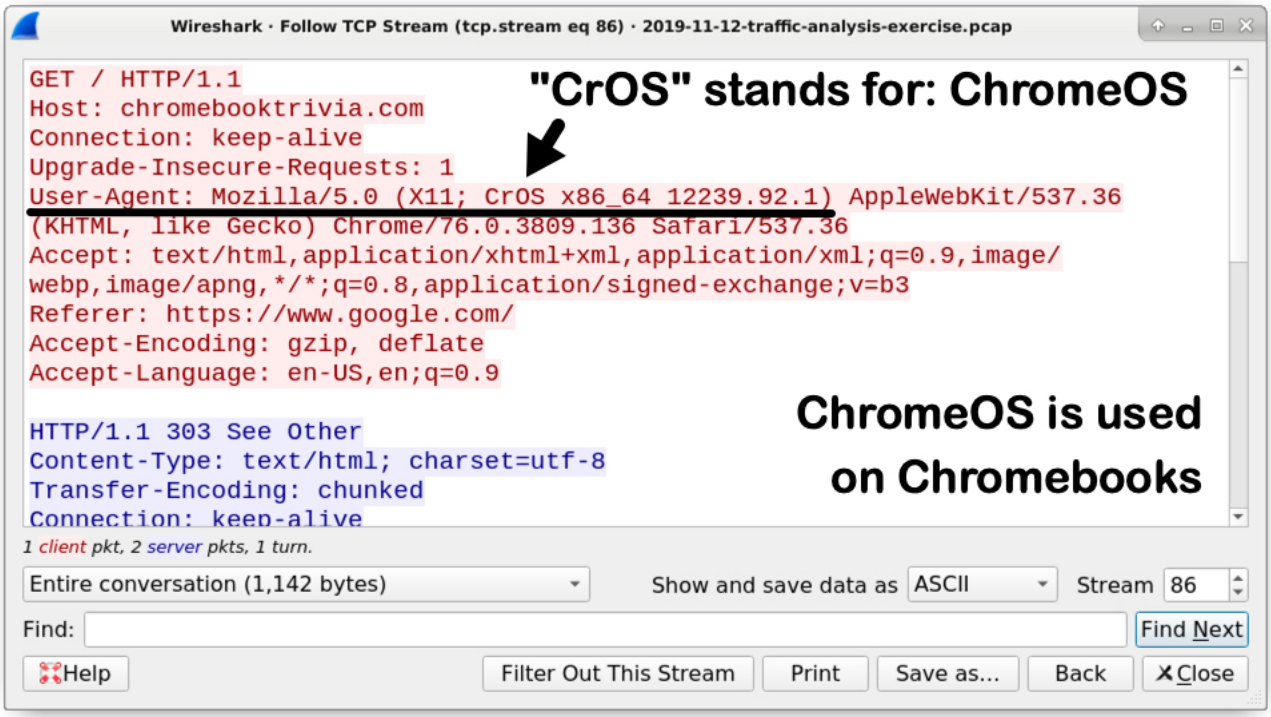
Q: What is the host name and Windows user account name used on that IP address?
A: **host name: Tucker-Win7-PC , user account name: candice.tucker**

NOTES:

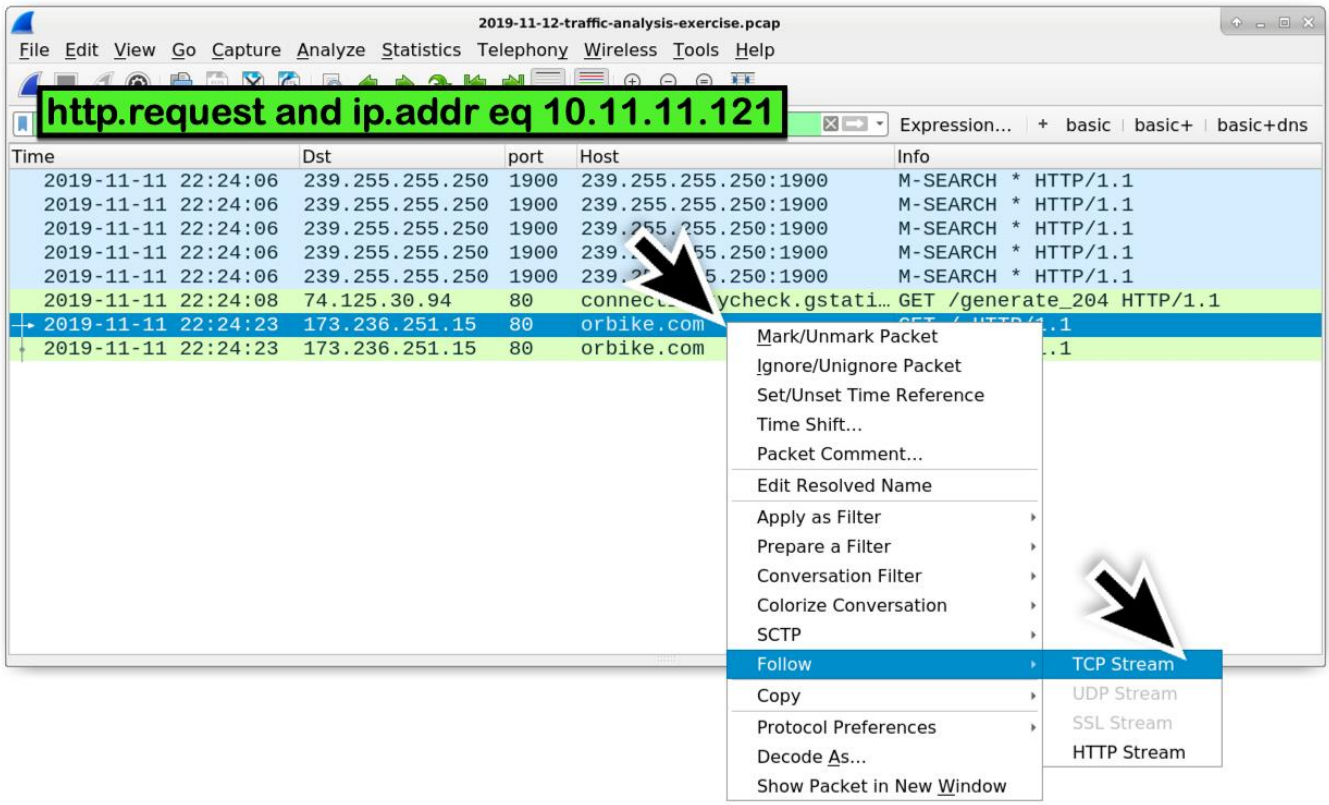
Q: What operating system and type of device is on 10.11.11.94?
A: **ChromeOS on a Chromebook**



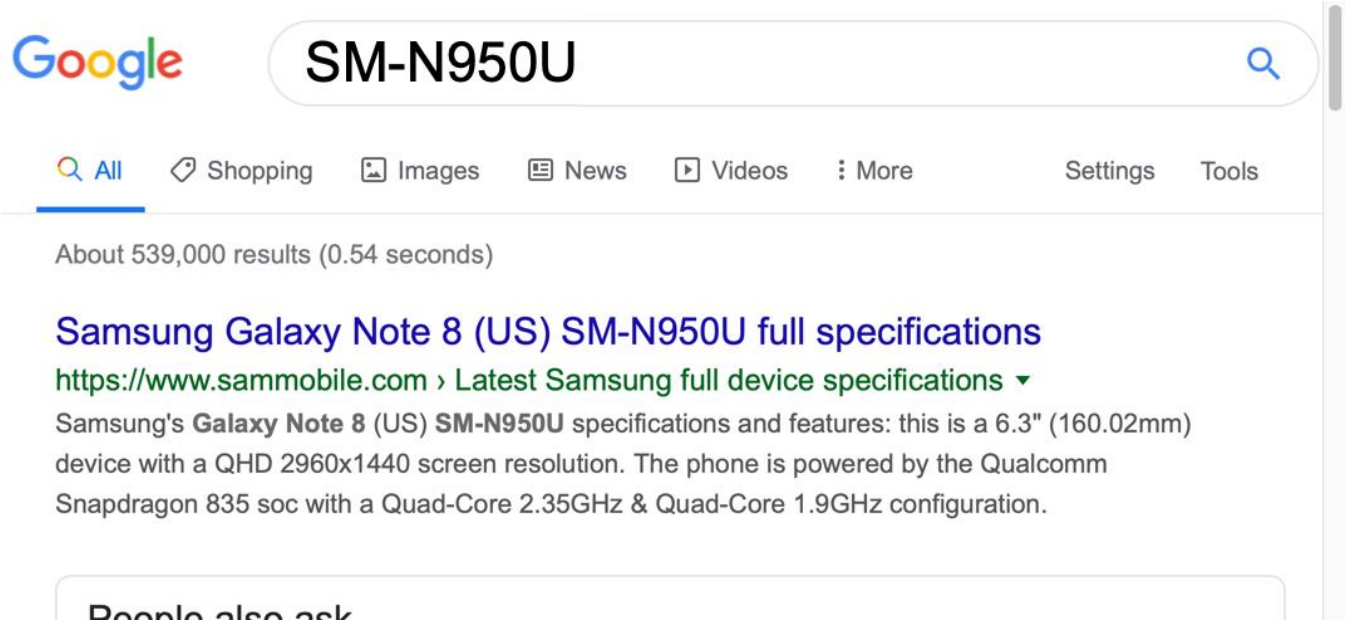
NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS



Q: What operating system and type of device is on 10.11.11.121?
A: **Samsung Galaxy Note 8**

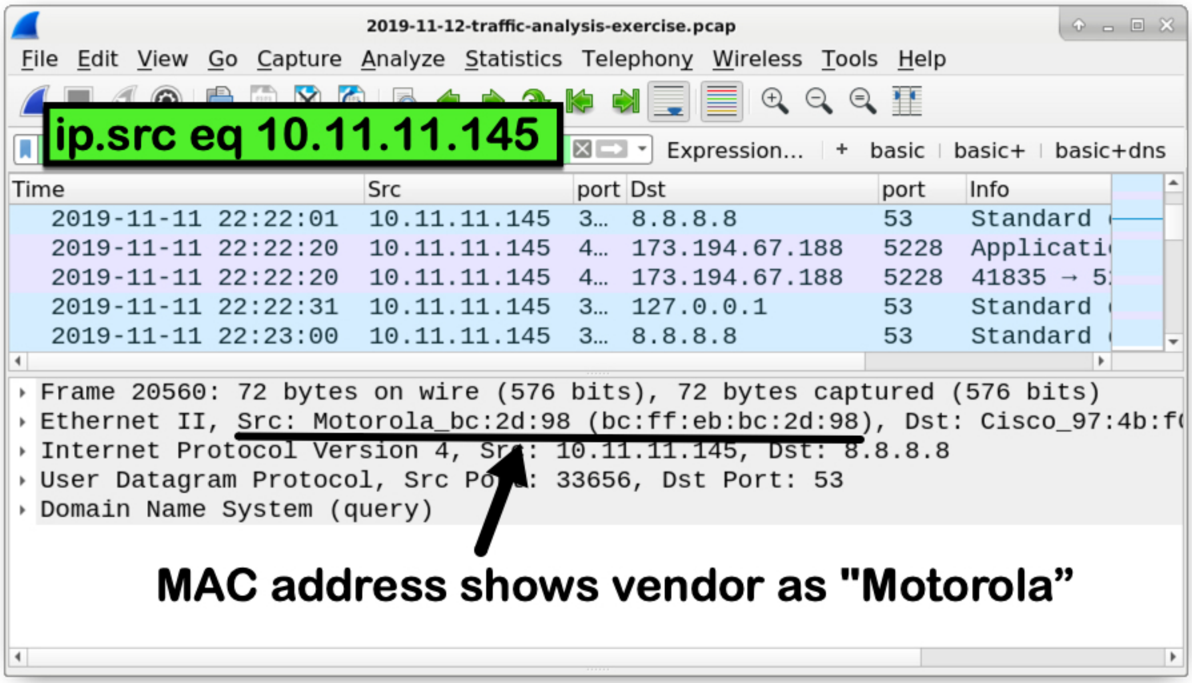


NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

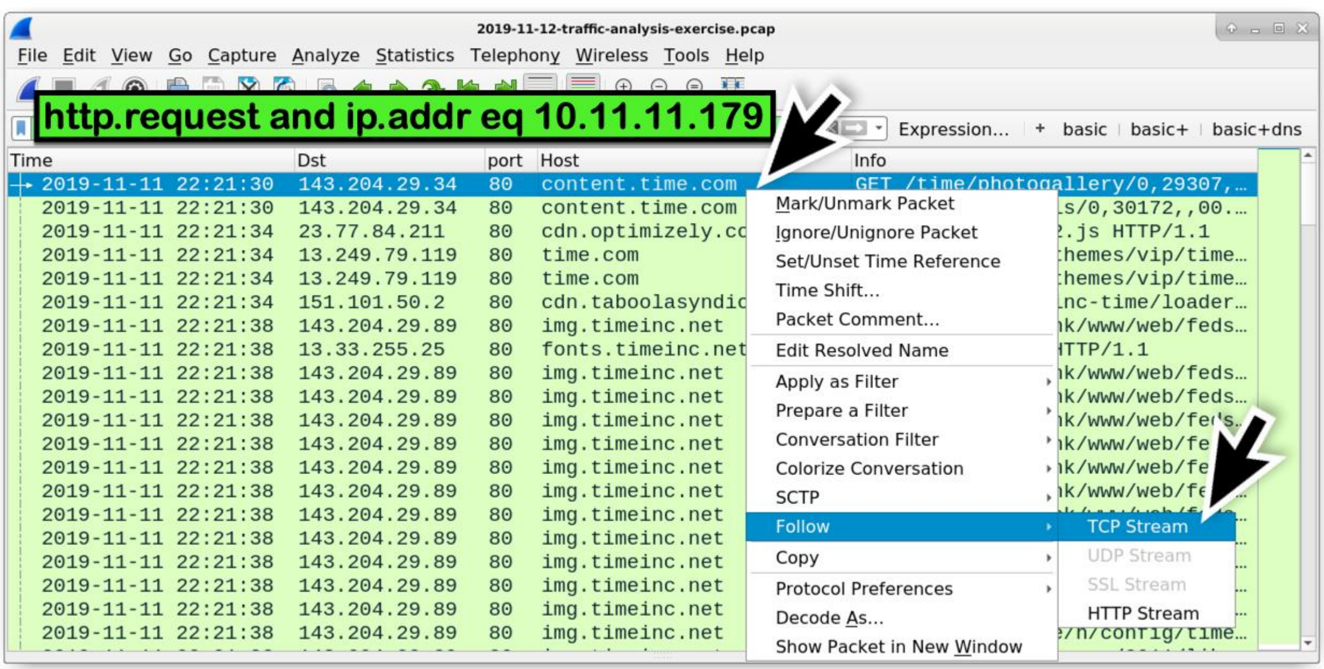


NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

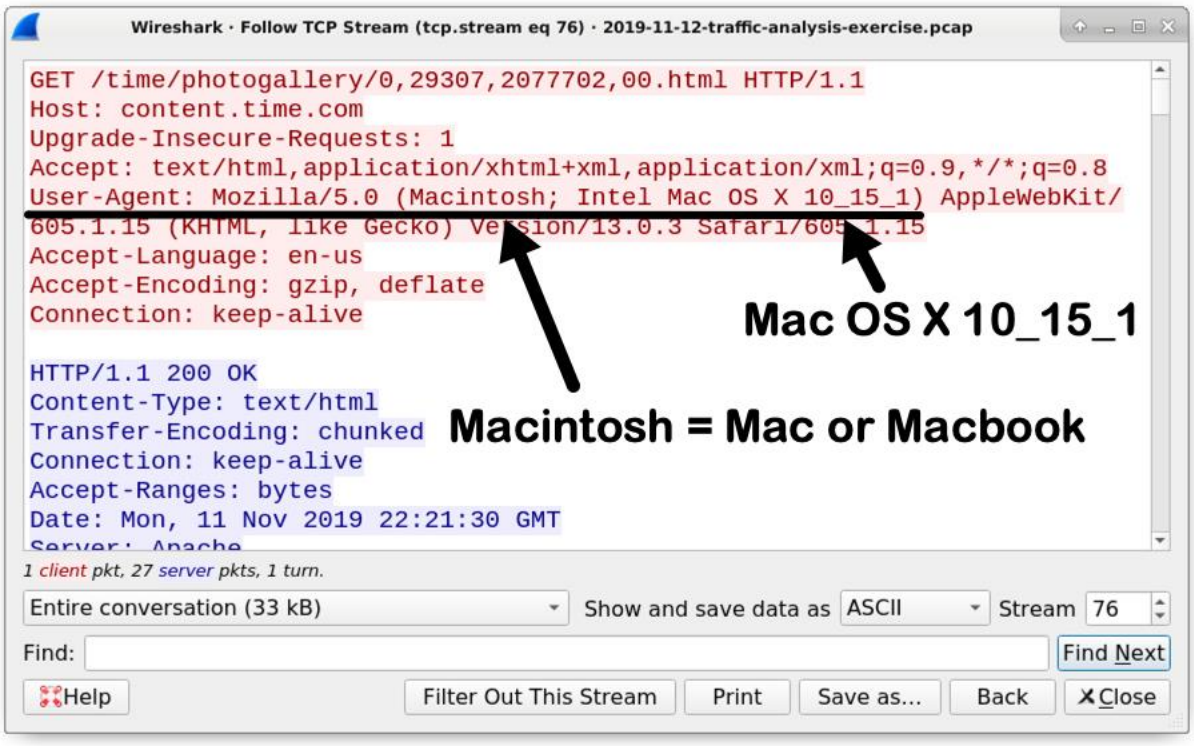
Q: Based on the MAC address for 10.11.11.145, who is the manufacturer or vendor?
A: **Motorola**



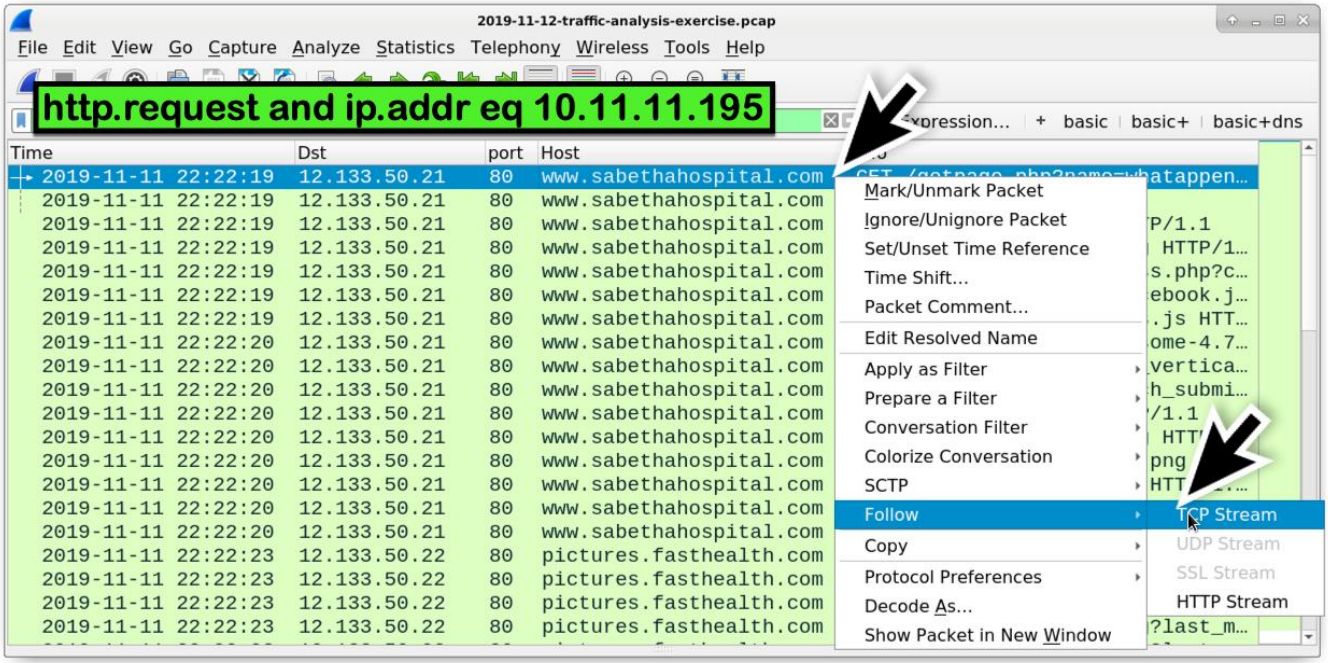
Q: What operating system and type of device is on 10.11.11.179?
A: **macOS 10.15.1 (Catalina) on a Mac (desktop or Macbook)**



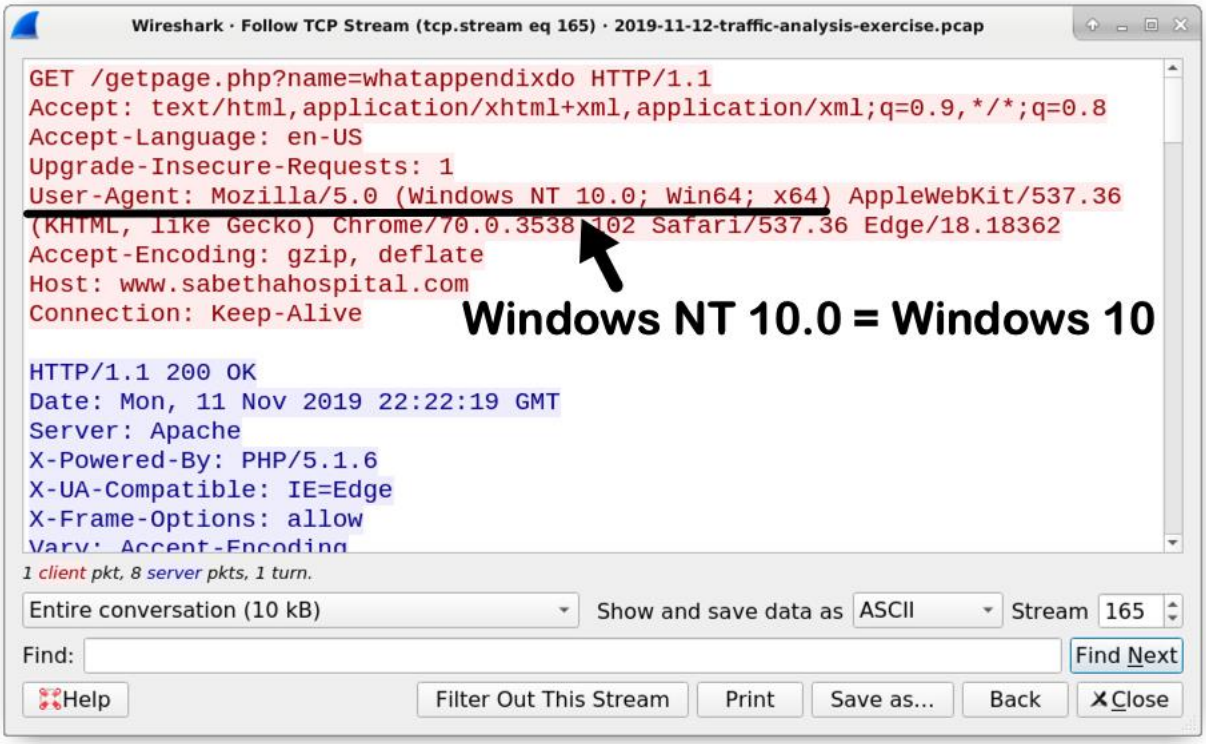
NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS



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

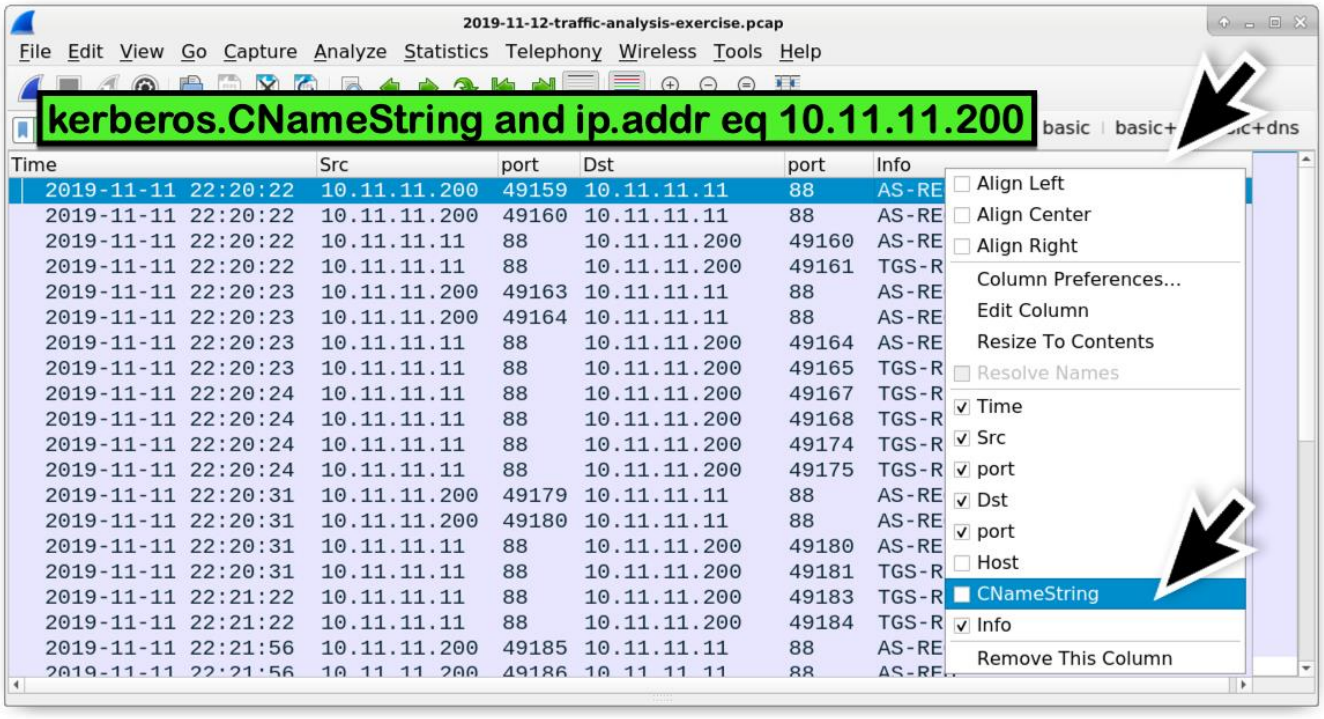


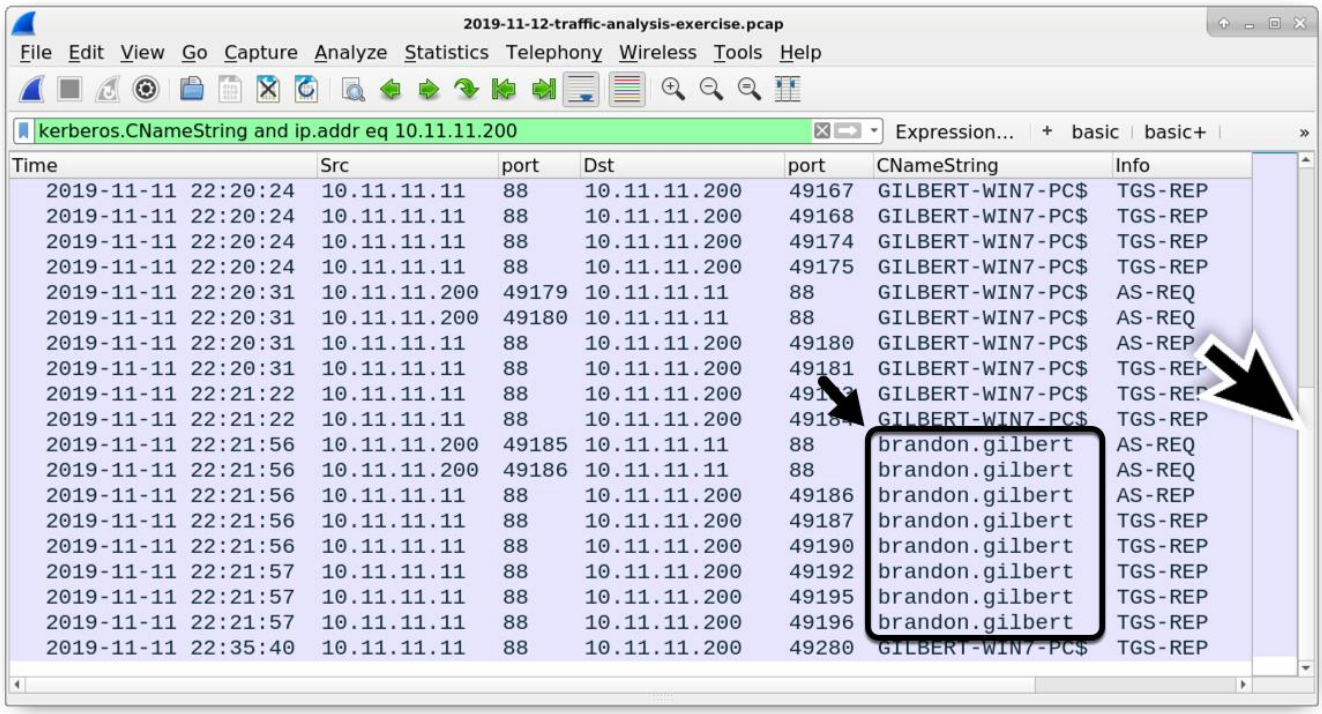
Q: What is the user account name used to log into the Windows host at 10.11.11.200?
A: **brandon.gilbert**

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

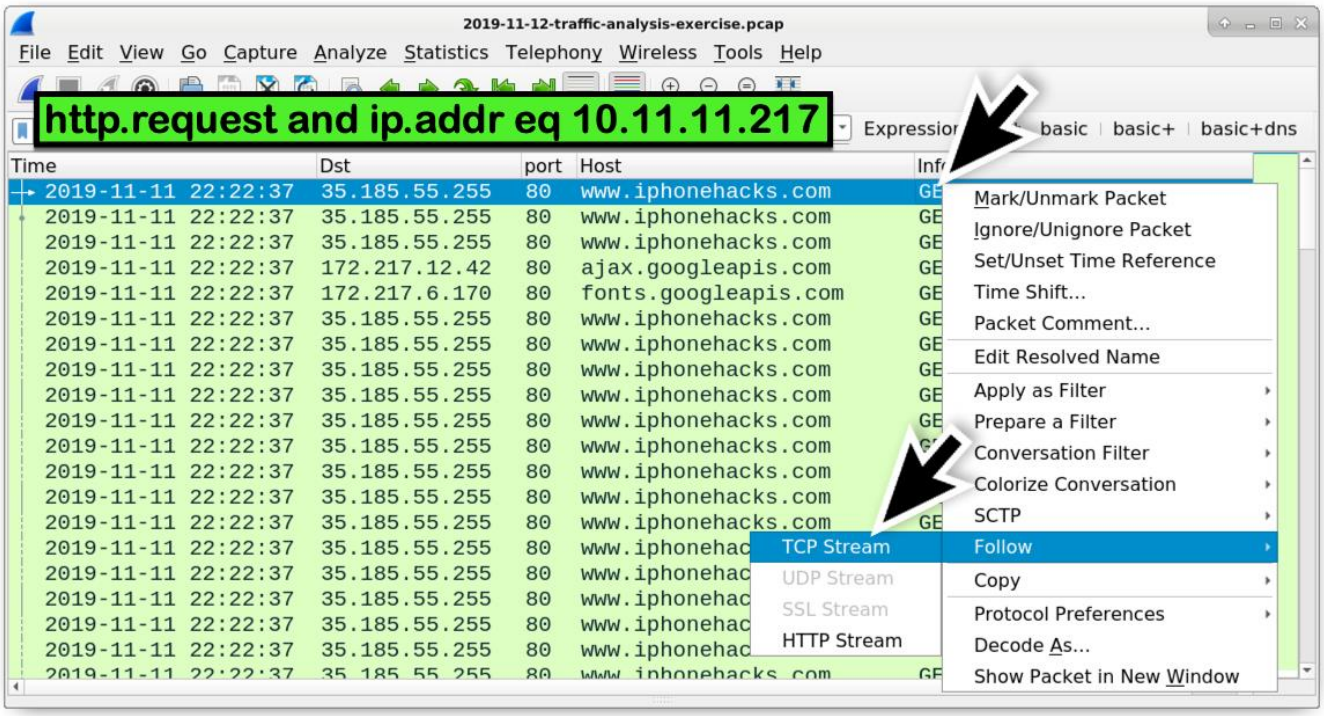
NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS





NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

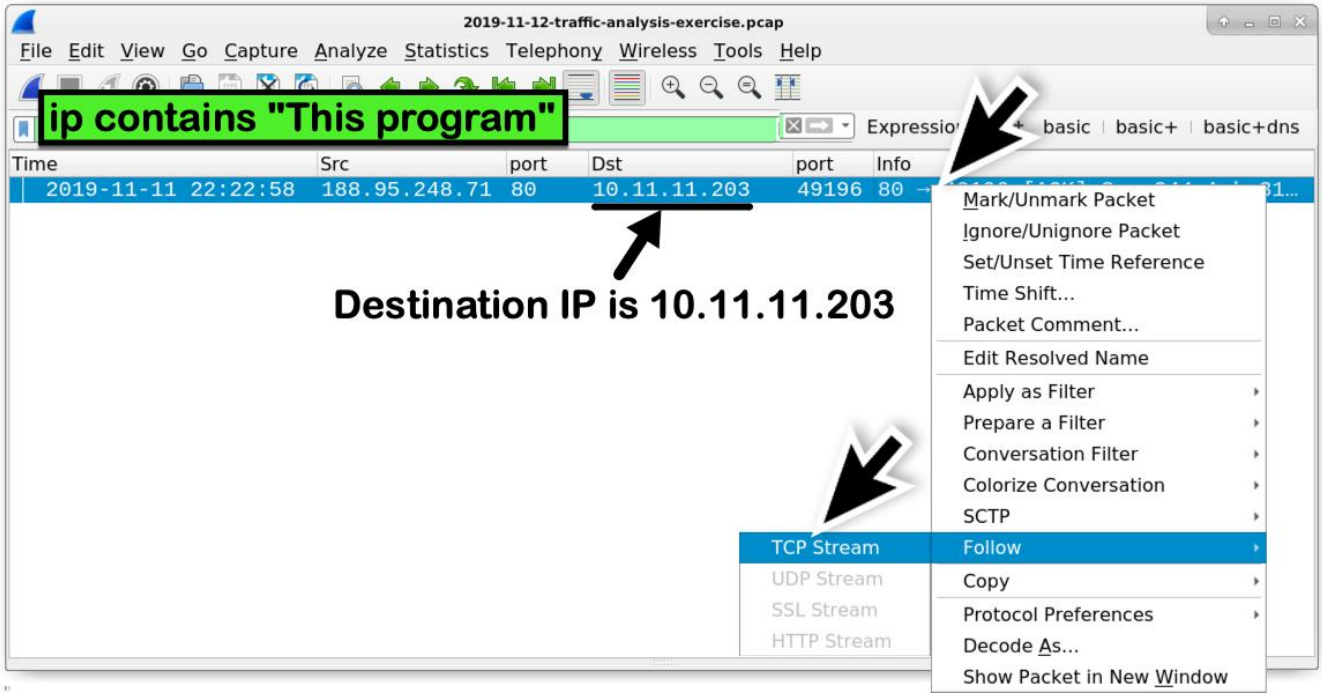
Q: What operating system and type of device is on 10.11.11.217?
A: **iPadOS 13.2.2 on an iPad**



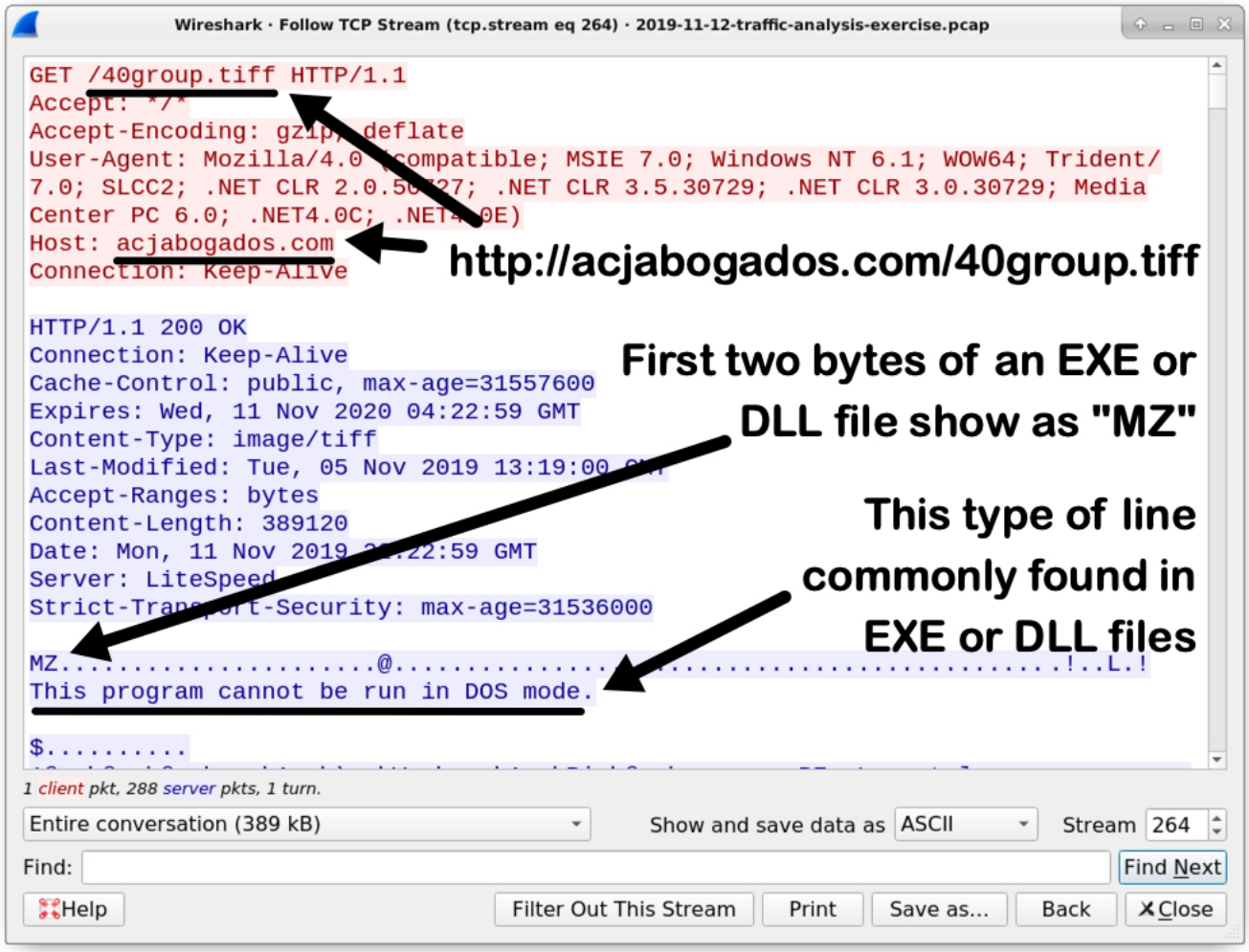
NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

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**

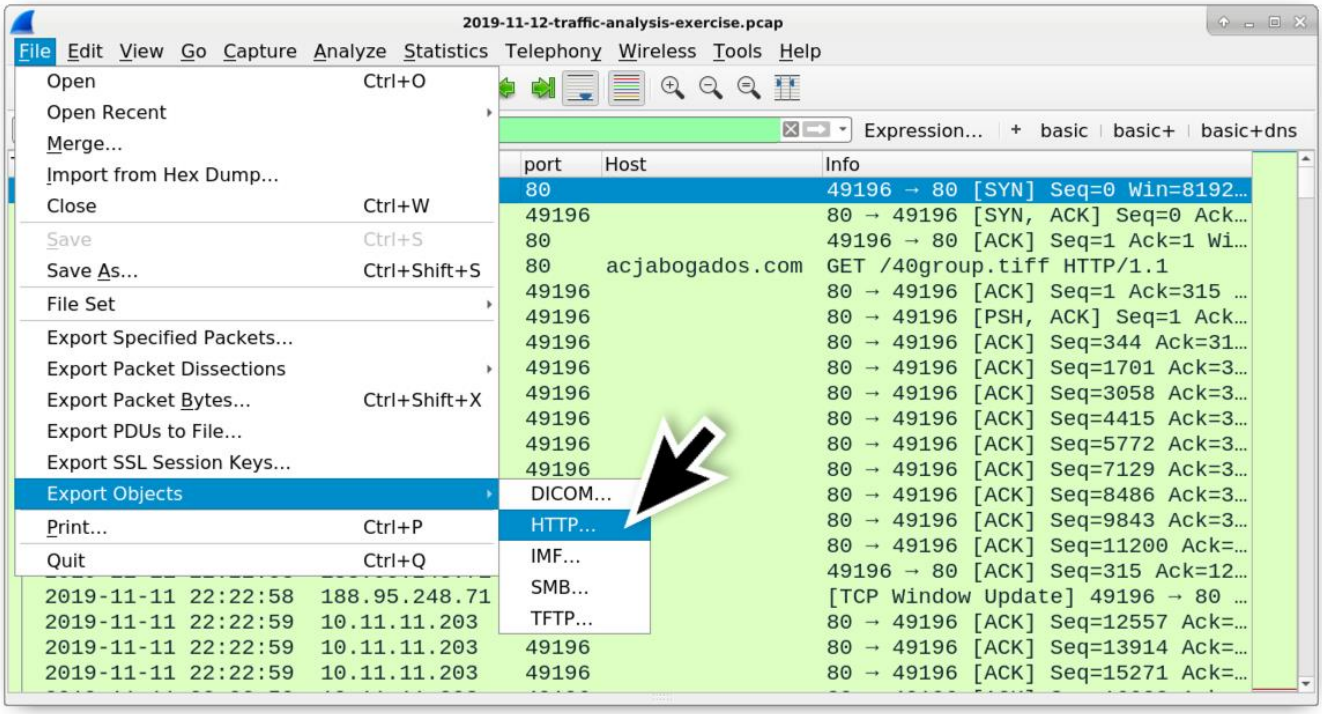


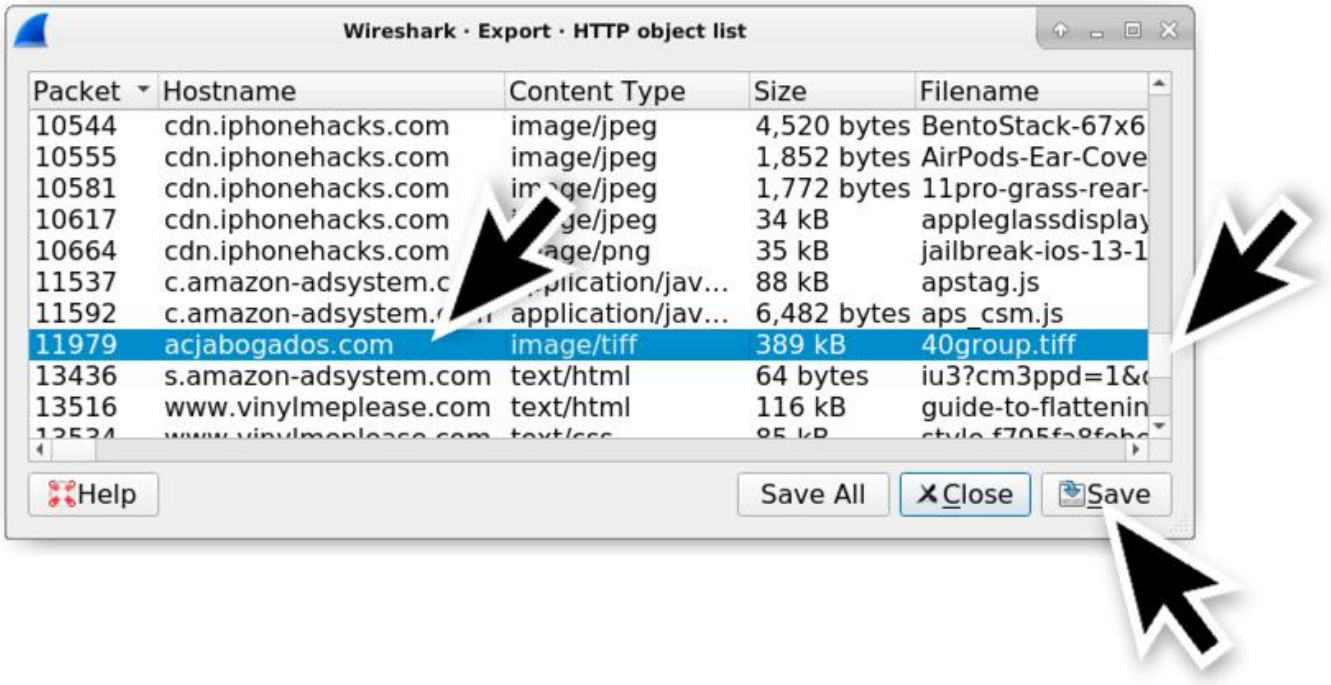
NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

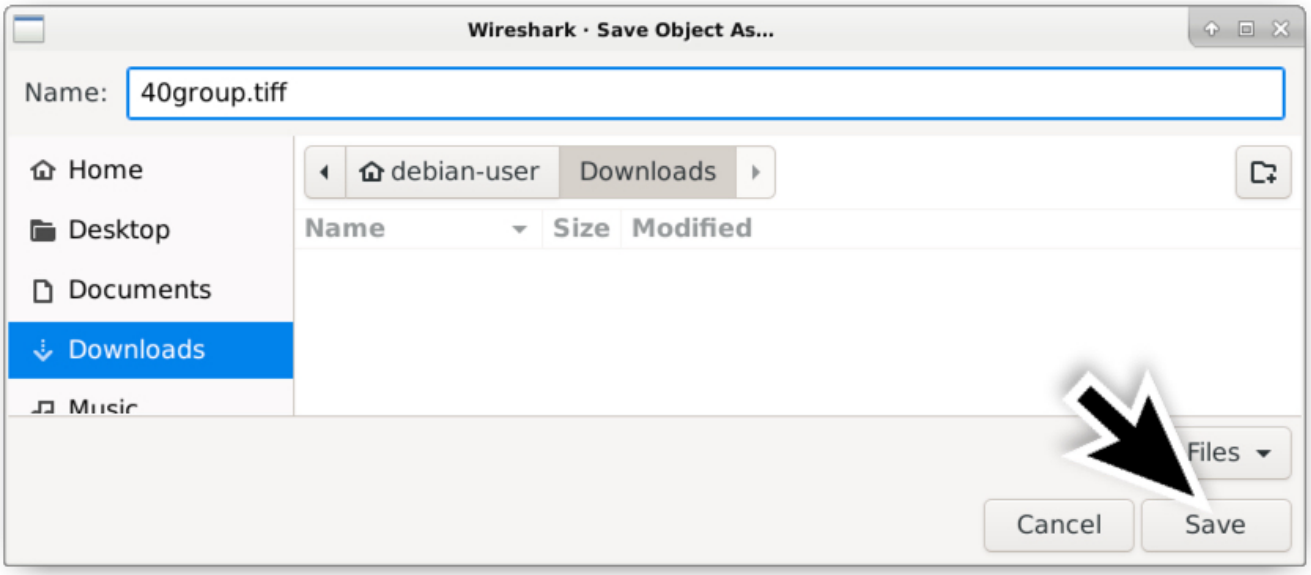


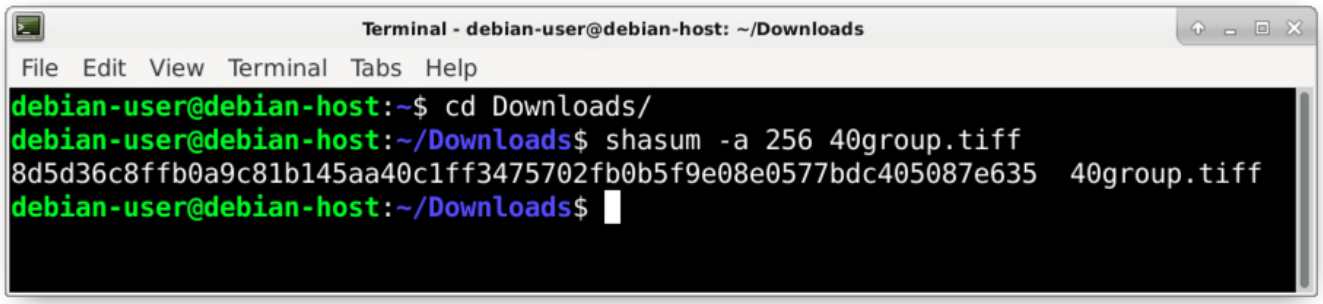
NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

Q: What is the SHA256 file hash for that Windows executable file?
A: **8d5d36c8ffb0a9c81b145aa40c1ff3475702fb0b5f9e08e0577bdc405087e635**

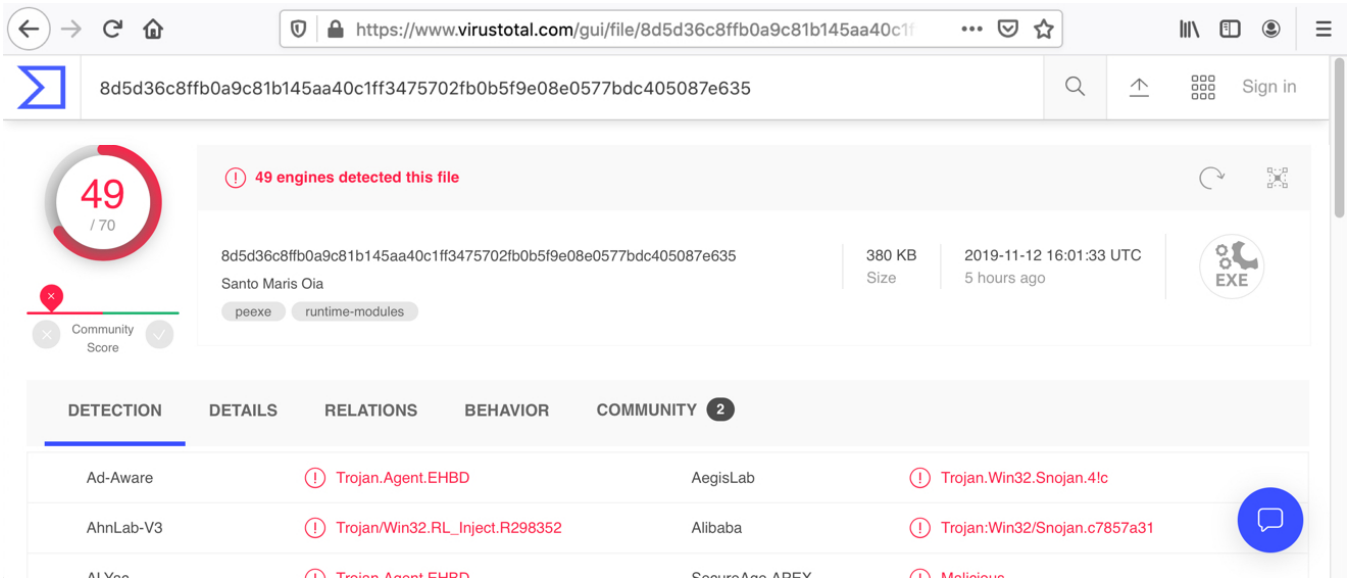








Q: What is the detection rate for that SHA256 hash on VirusTotal?
A: **49 of 70**



NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

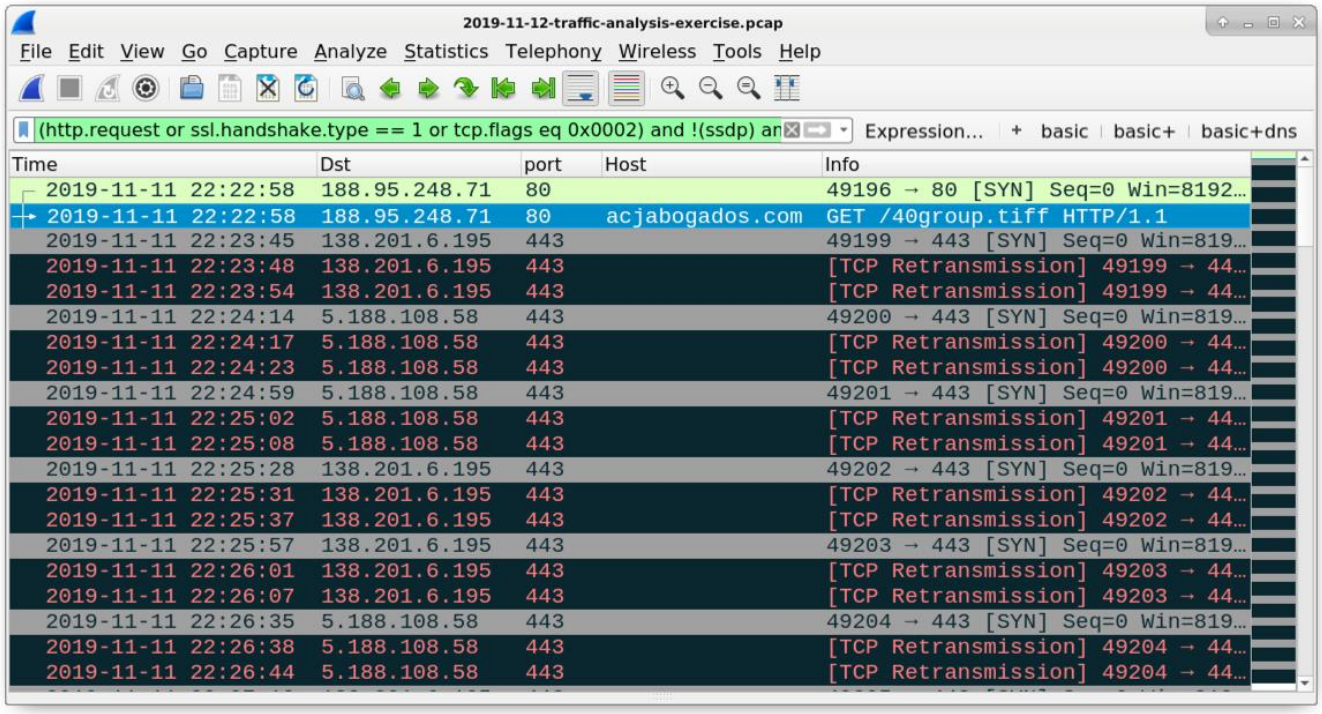
Q: What public IP addresses did that Windows host attempt to connect over TCP without a response from the server after the above executable file was downloaded?
A: **5.188.108.58 and 138.201.6.195**

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