

Contents

Scenario	2
Task 1	2
Task 2	2
Task 3	4
Task 4	5
Capstone task	7

Scenario:

- Working for a company that wants to detect certain TCP/IP network traffic on their server
- IT manager wants to be able to capture ethernet network web traffic on the server and be able to detect certain IP addresses as well

Task 1 : Install and set up Wireshark

1. To get the latest stable version of Wireshark on Ubuntu Linux, use the add-apt-repository command: **`sudo add-apt-repository ppa:wireshark-dev/stable`**

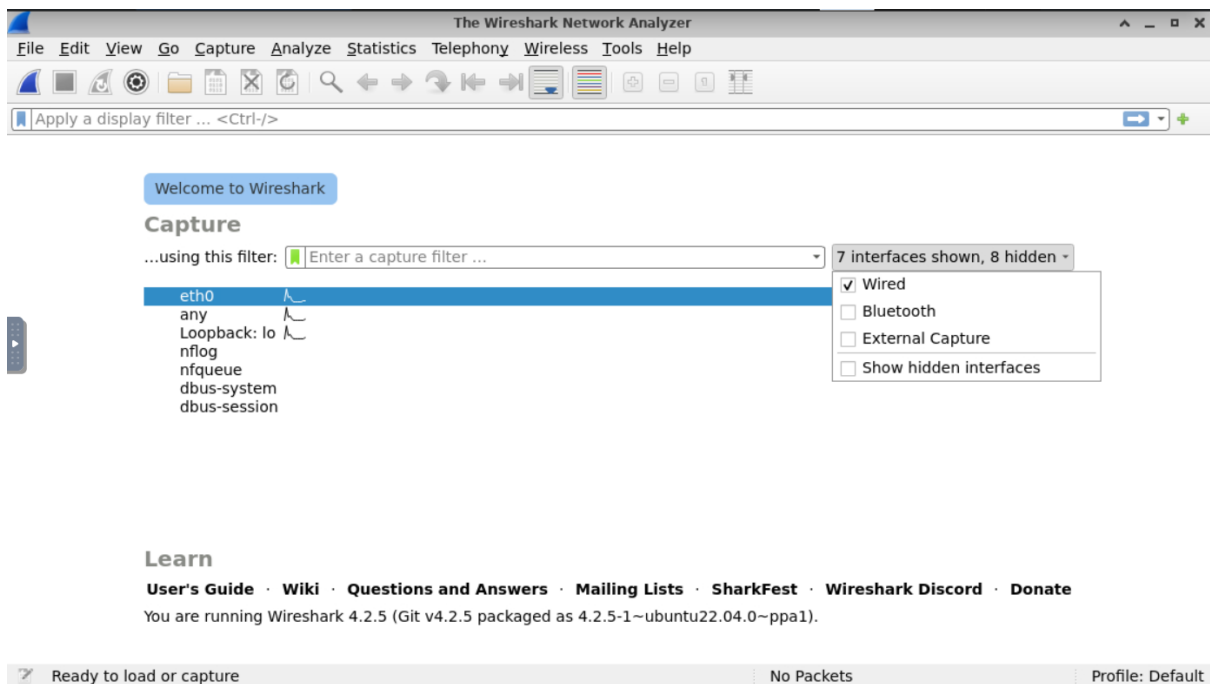
NOTE: Wireshark should not be run as superuser for security reasons.

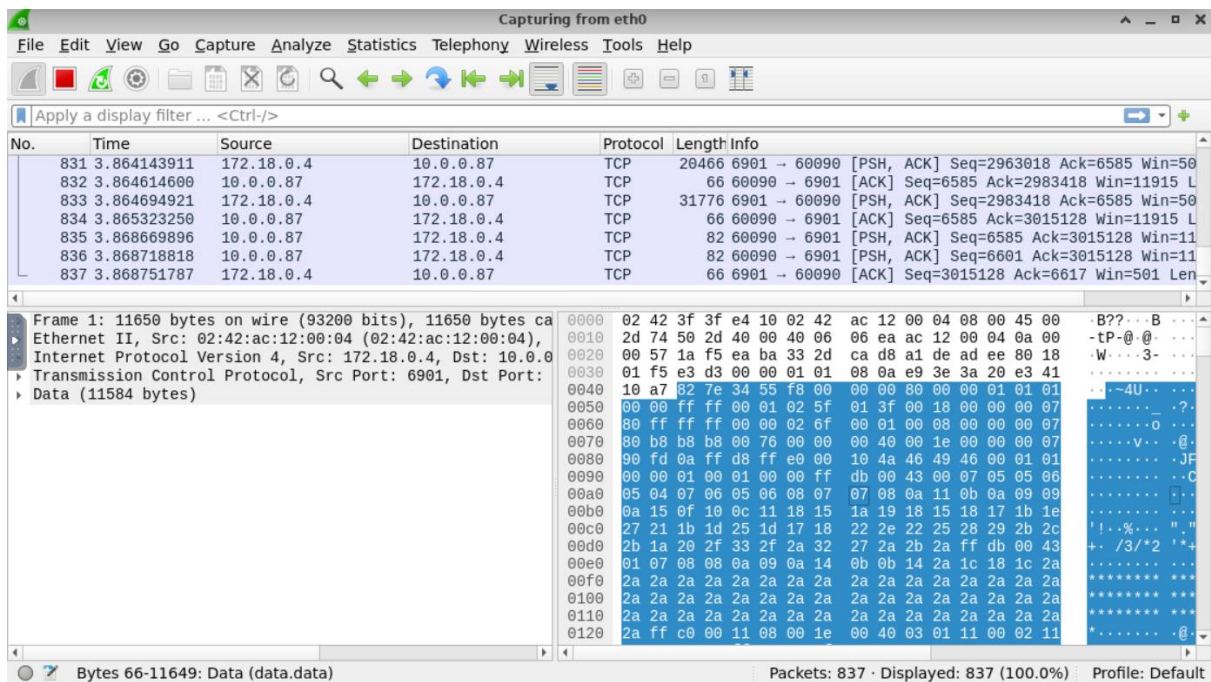
2. The user can be added to the Wireshark group to add packet capture capabilities: **`sudo usermod -aG wireshark $USER`**

NOTE: the -a means to append a user, G is a group

Task 2: Start Packet capture on an ethernet port and save it to a file

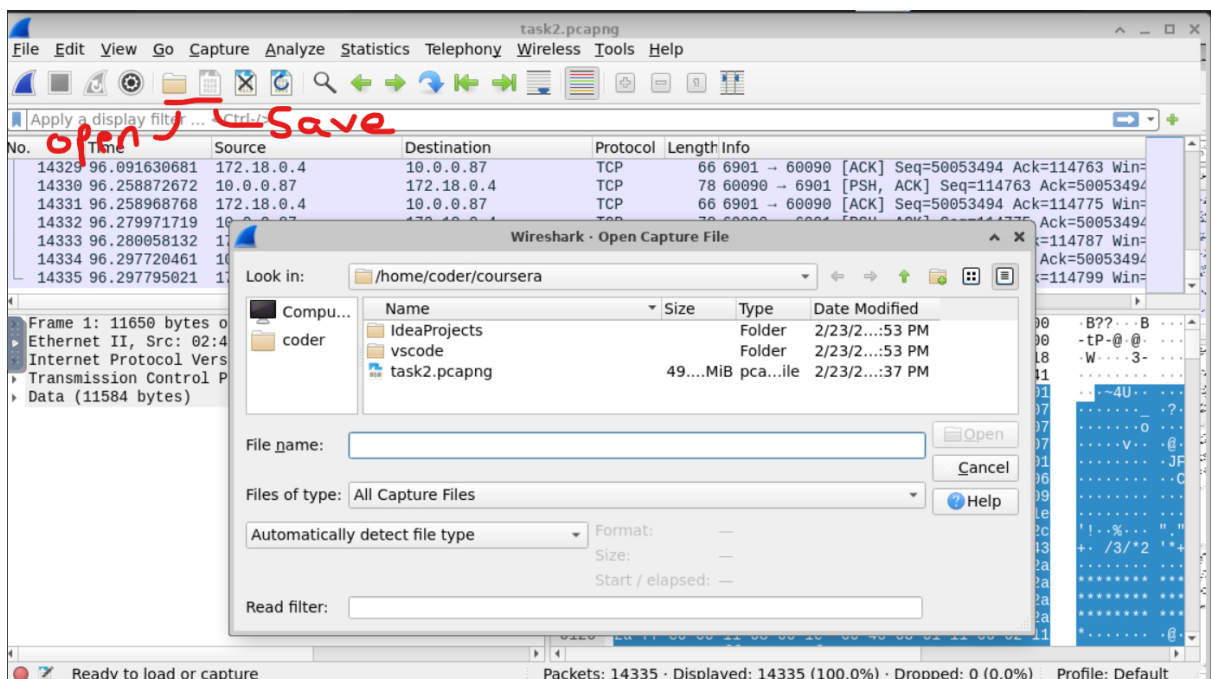
1. Filter to the wired connections and select the ethernet option. Press the blue shark on the top left to start capturing packets





NOTE: Press the stop button to stop capturing packets. If you let it continue you could run out of memory.

2. Save and open the capture file



NOTE: You cannot save a capture if it is running

Task 3: Use a display filter to detect HTTPS packets

1. Start capturing packets, search duckduckgo on the internet, stop capturing packets and save the capture.
2. Use the display filter to find all activity on port 443

The image shows a Wireshark packet capture window titled 'task3.pcapng'. The display filter is set to 'tcp.port == 443'. The packet list shows several packets, with packet 1119 highlighted. The packet details pane shows the following information:

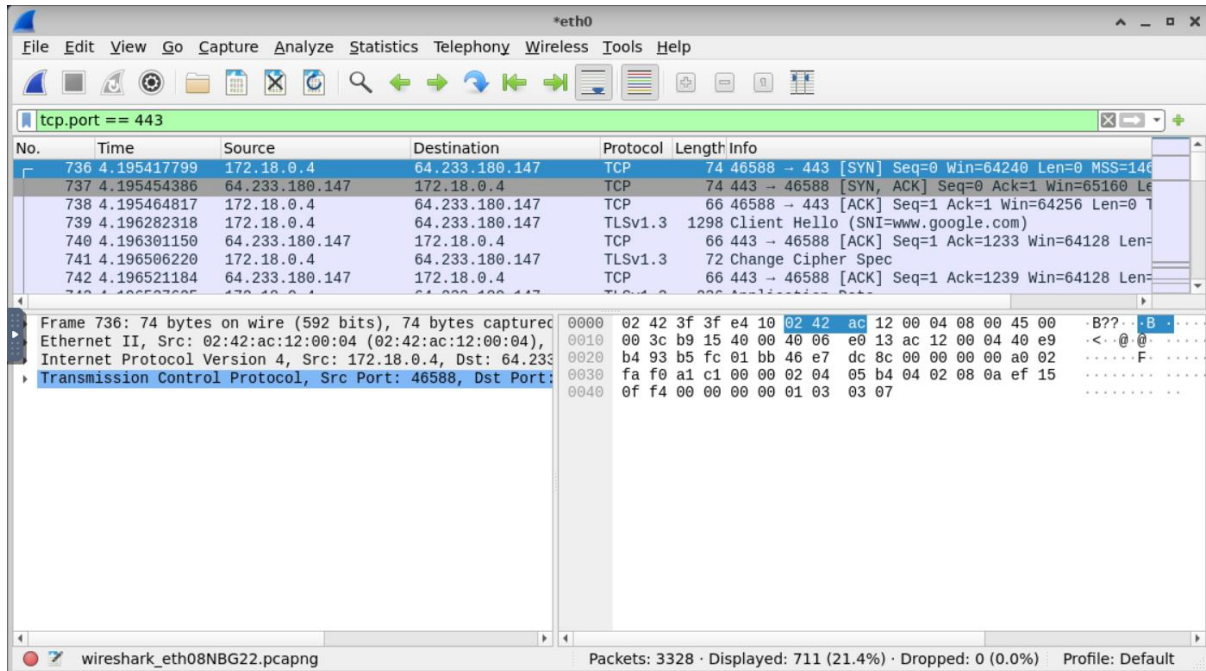
- Frame 1119: 744 bytes on wire (5952 bits), 744 bytes captured (5952 bits) on interface 0
- Ethernet II, Src: 02:42:ac:12:00:04 (02:42:ac:12:00:04), Dst: 34:120:208:123
- Internet Protocol Version 4, Src: 172.18.0.4, Dst: 34.120.208.123
- Transmission Control Protocol, Src Port: 33878, Dst Port: 443
- Transport Layer Security

The packet bytes pane shows the raw data of the TLS Client Hello packet, including the magic bytes '0000 02 42 3f 3f e4 10 02 42'.

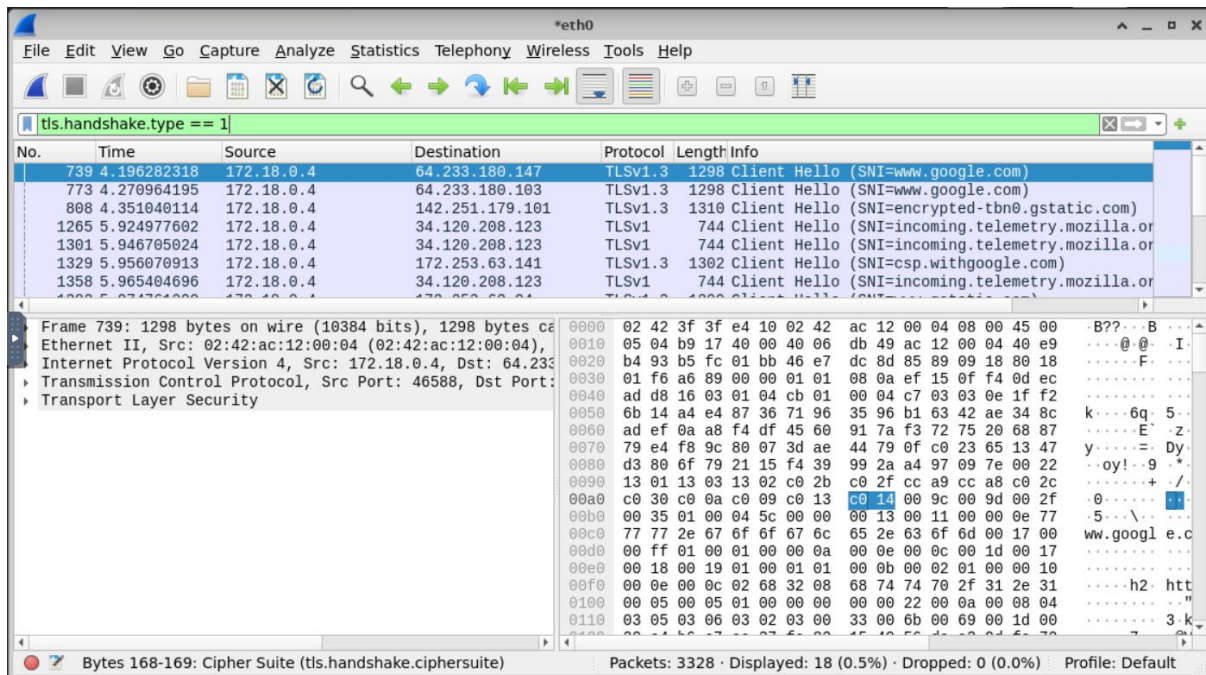
NOTE: the packet with the 'Client Hello' is the search for DuckDuckGo, if you copy the destination IP and paste into your browser, it will take you to DuckDuckGo. You get additional information by double clicking on that packet.

Task 4: Visit webpage and detect its IP address using a display filter

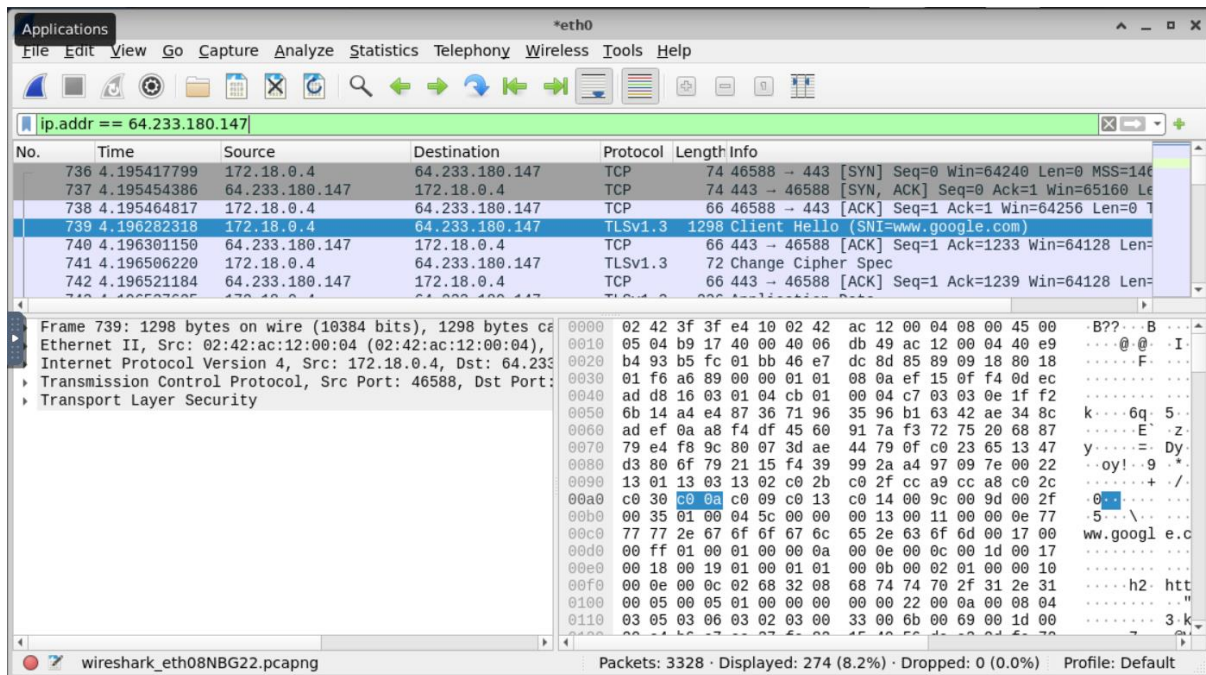
1. Capture packets for a search for google and check port 443 for https packets.



2. Change the display filters to present the first step of the tls handshake



3. We can use another display filter to view all packets associated with the specified IP address

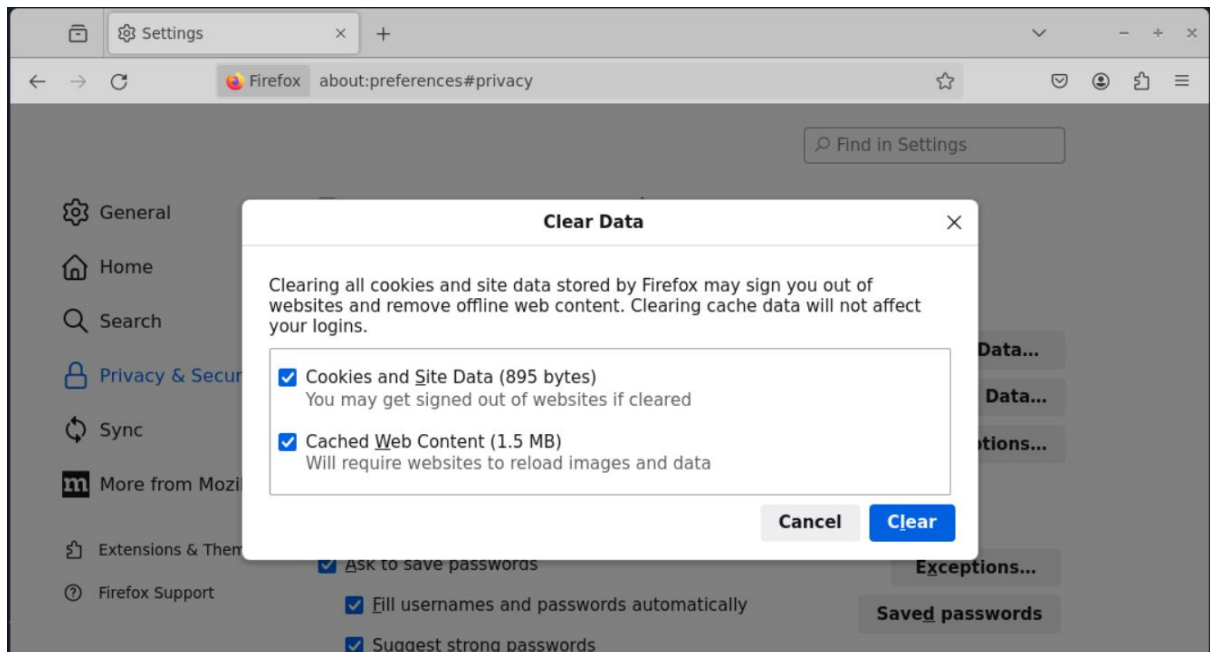


NOTE: There are additional filters like 'ip.src' and 'ip.dst' to view all packets with a source or destination with the IP specified.

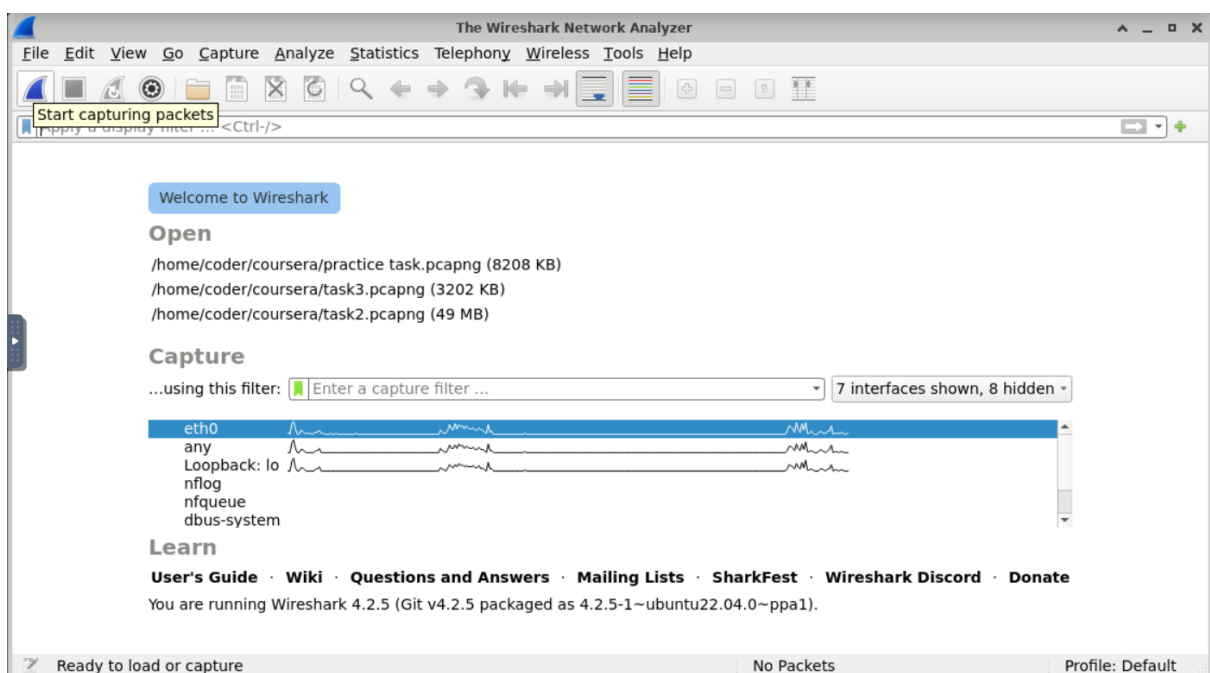
NOTE: We can also use conditional filters using 'and', 'or', and '!(enter filters)' (for NOT).

Capstone task: You are to use Wireshark to create a capture file and then use a display filter to list all https and http packets. You will then eliminate one IP address from the capture using a display filter.

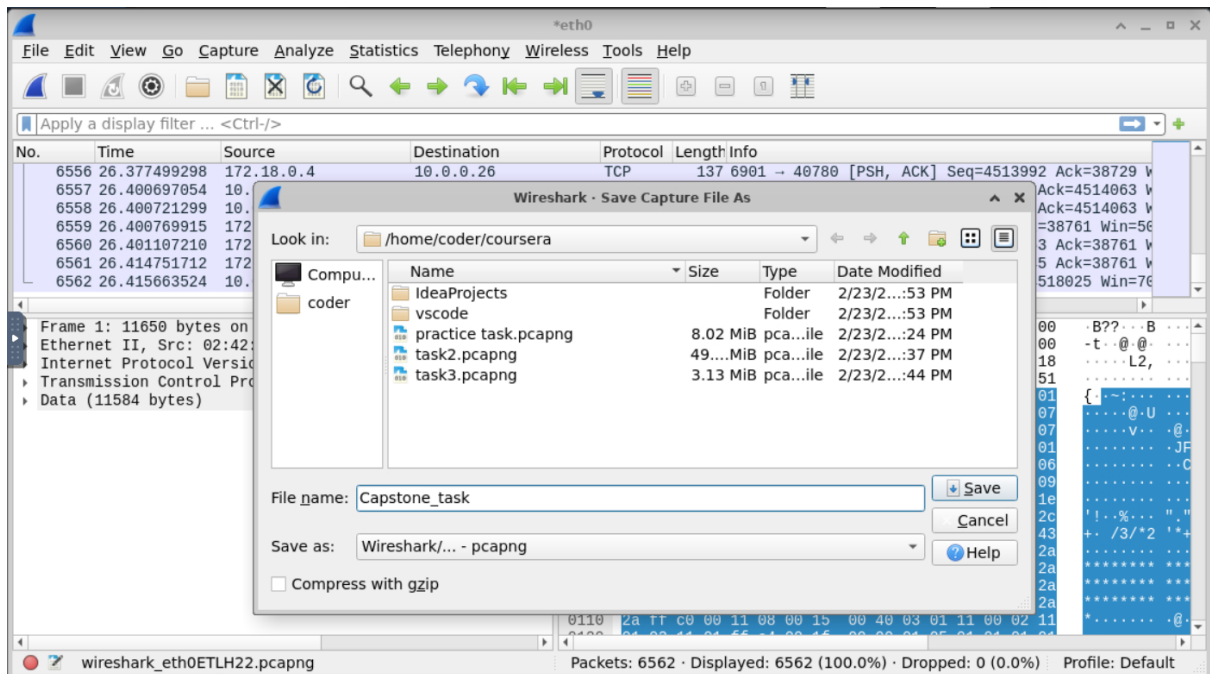
1. Clear the cache in the Firefox browser



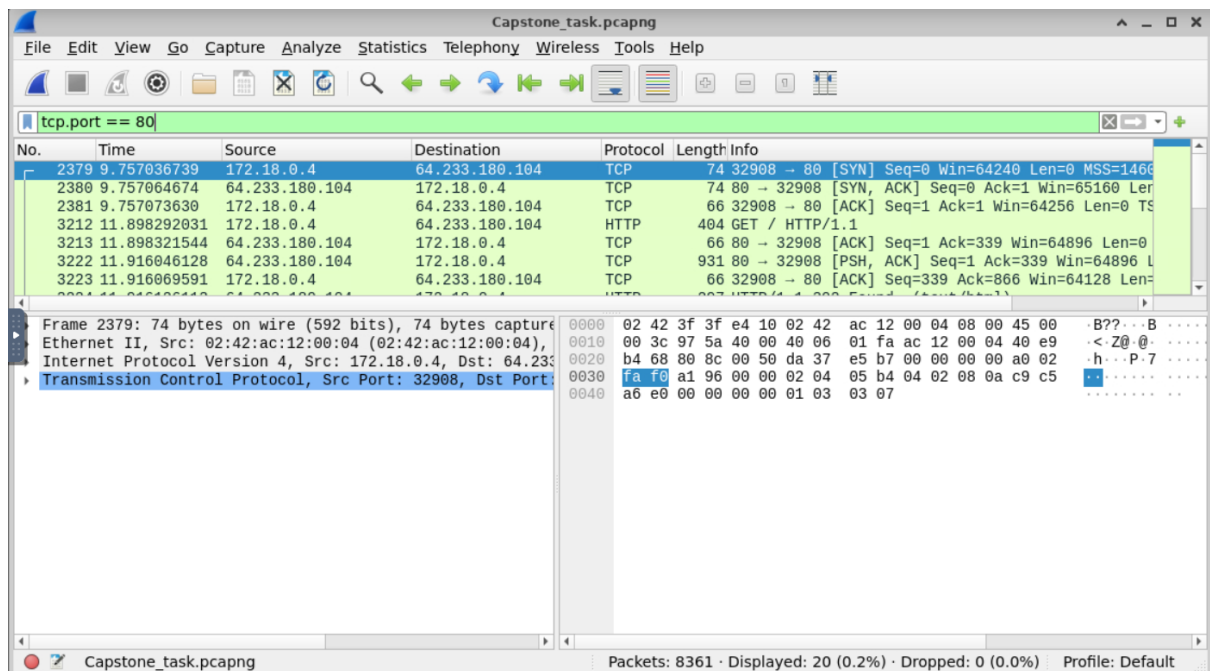
2. Start a packet capture on the ethernet in Wireshark and visit google.com, duckduckgo.com, and <http://cygwin.com> (not https)



3. Stop the packet capture in Wireshark and save the capture to a file



4. Create a filter to just display port 80 TCP data. This should give you the IP address of Cygwin.



5. Create a filter to display only HTTP AND HTTPS packets

Capstone_task.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80 or tcp.port == 443

No.	Time	Source	Destination	Protocol	Length	Info
2379	9.757036739	172.18.0.4	64.233.180.104	TCP	74	32908 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2380	9.757064674	64.233.180.104	172.18.0.4	TCP	74	80 → 32908 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
2381	9.757073630	172.18.0.4	64.233.180.104	TCP	66	32908 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=0
2397	9.800299493	172.18.0.4	64.233.180.105	TCP	74	34392 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2398	9.800326675	64.233.180.105	172.18.0.4	TCP	74	443 → 34392 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
2399	9.800335513	172.18.0.4	64.233.180.105	TCP	66	34392 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=0
2400	9.801021011	172.18.0.4	64.233.180.105	TLSv1.3	1298	Client Hello (SNI=www.google.com)

Frame 2379: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: 02:42:ac:12:00:04 (02:42:ac:12:00:04), Dst: 02:42:ac:12:00:04 (02:42:ac:12:00:04)
Internet Protocol Version 4, Src: 172.18.0.4, Dst: 64.233.180.104
Transmission Control Protocol, Src Port: 32908, Dst Port: 80

Capstone_task.pcapng

Packets: 8361 · Displayed: 1613 (19.3%) · Dropped: 0 (0.0%) · Profile: Default

6. Eliminate the Cygwin site visits from the displayed packets

Capstone_task.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(tcp.port == 80 or tcp.port == 443) and !ip.addr == 64.233.180.104

No.	Time	Source	Destination	Protocol	Length	Info
2397	9.800299493	172.18.0.4	64.233.180.105	TCP	74	34392 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2398	9.800326675	64.233.180.105	172.18.0.4	TCP	74	443 → 34392 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
2399	9.800335513	172.18.0.4	64.233.180.105	TCP	66	34392 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=0
2400	9.801021011	172.18.0.4	64.233.180.105	TLSv1.3	1298	Client Hello (SNI=www.google.com)
2401	9.801033814	64.233.180.105	172.18.0.4	TCP	66	443 → 34392 [ACK] Seq=1 Ack=1233 Win=64128 Len=0
2402	9.801149069	172.18.0.4	64.233.180.105	TLSv1.3	72	Change Cipher Spec
2403	9.801150993	64.233.180.105	172.18.0.4	TCP	66	443 → 34392 [ACK] Seq=1 Ack=1239 Win=64128 Len=0

Frame 2397: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: 02:42:ac:12:00:04 (02:42:ac:12:00:04), Dst: 02:42:ac:12:00:04 (02:42:ac:12:00:04)
Internet Protocol Version 4, Src: 172.18.0.4, Dst: 64.233.180.105
Transmission Control Protocol, Src Port: 34392, Dst Port: 443

Capstone_task.pcapng

Packets: 8361 · Displayed: 1602 (19.2%) · Dropped: 0 (0.0%) · Profile: Default