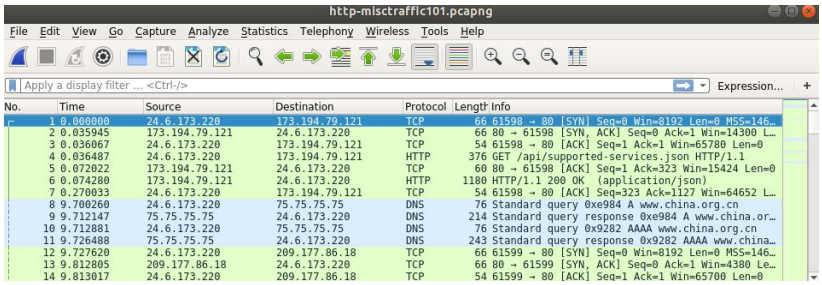
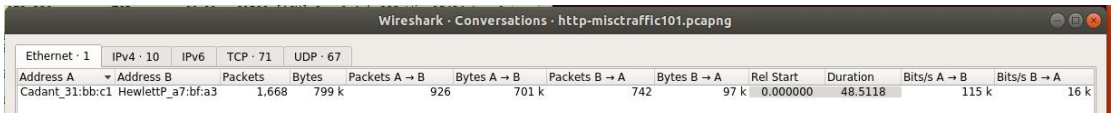
CSI 4139 Lab 10
Aaron Ng (300176901)
Nov 24, 2022

Review of Packet Capture Introspection

Task 1: Find Most Active TCP Flow (15 pts)

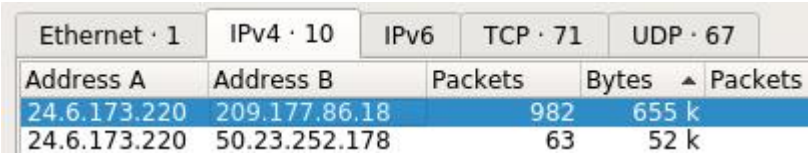


We open pcaps/http-misctraffic101.pcapng in Wireshark



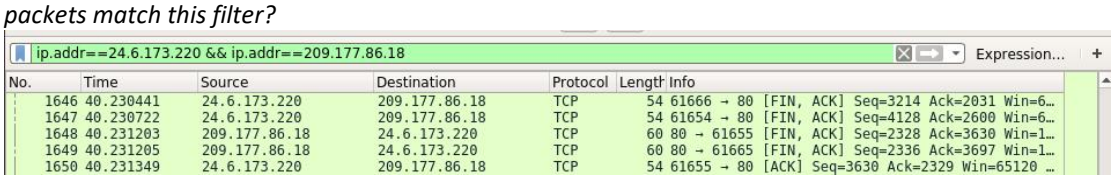
From Statistics > Conversations, we opened a new window.

Q1) Based on the bytes count, what IP addresses participate in the most active IPv4 conversation?

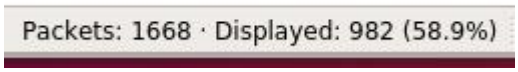


Clicking on the IPv4 tab, and sorting by bytes shows us these two addresses had the most active conversation.

Q2) Right-click on the most active TCP conversation and select Apply as a Filter — Selected — A-B. Wireshark automatically creates and applies a display filter for this TCP conversation. How many packets match this filter?



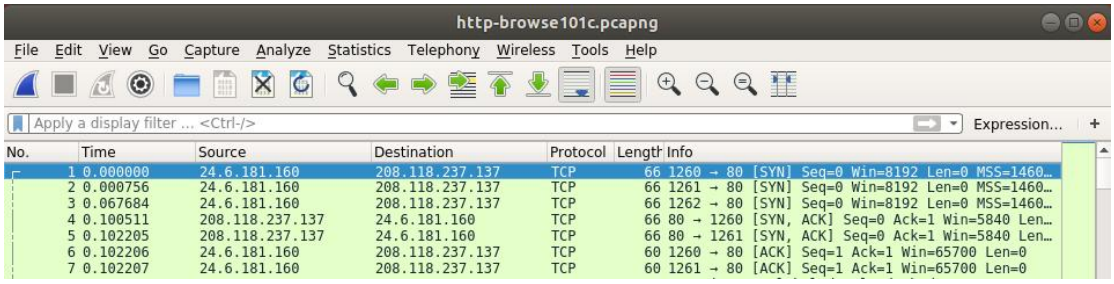
By following the steps above, we have applied this filter as shown.



The summary at the bottom tells us that 982 packets match the filter.

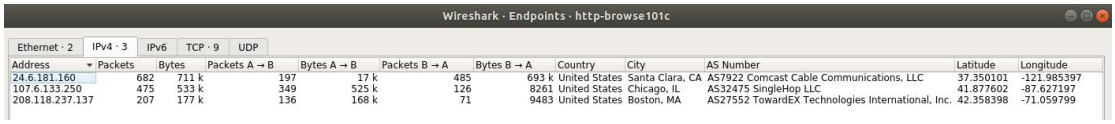
CSI 4139 Lab 10
Aaron Ng (300176901)
Nov 24, 2022

Task 2: Geolocating IP Addresses

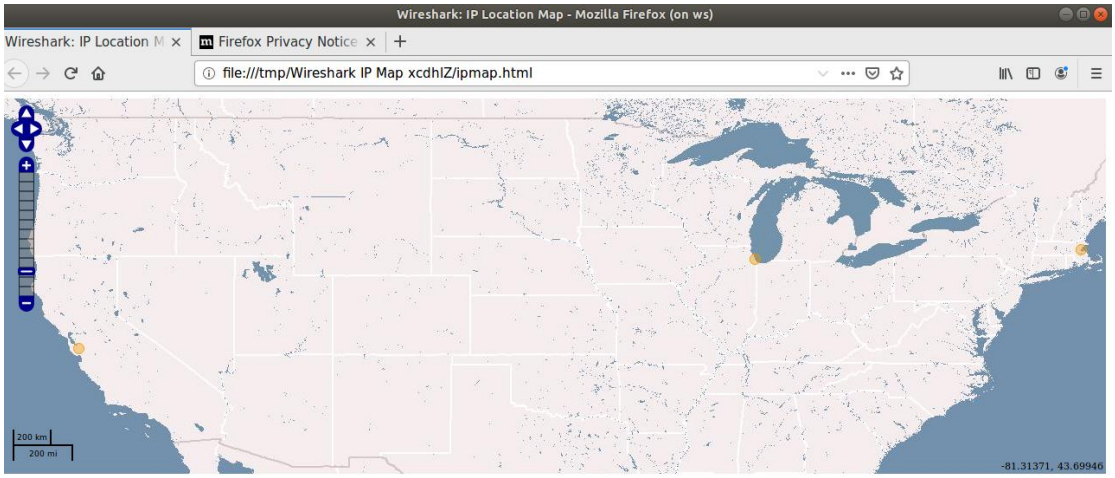


We open pcaps/http-browse101c.pcapng in Wireshark

We add maxmind to the GeoIP database directory.

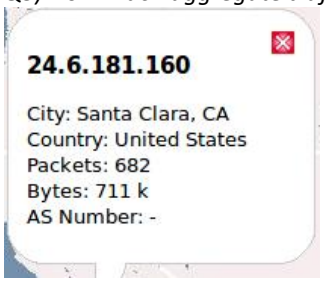


From Statistics > Endpoints, it opens a new window. Since we added the GeoIP database, we are now able to see location details of the IPv4 addresses.



By clicking “Map”, we can visualize all 3 locations of the IP addresses.

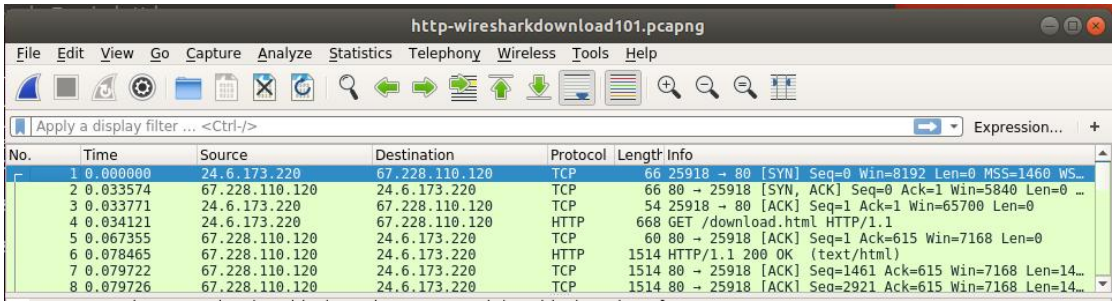
Q3) How much aggregate traffic went to/from Santa Clara, CA?



We can see that 711k bytes of traffic when to/from Santa Clara.

CSI 4139 Lab 10
Aaron Ng (300176901)
Nov 24, 2022

Task 3: Reassemble text from TCP stream

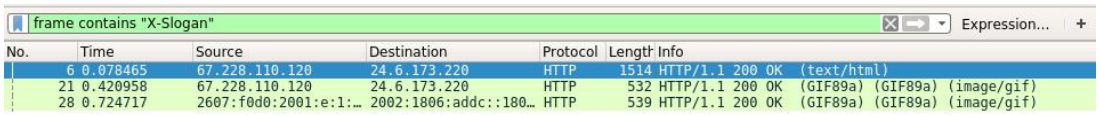


Open pcaps/http-wiresharkdownload101.pcapng in Wireshark.

By Right-clicking on frame 4, and following the TCP stream, we can see the trace file.

Q4) Scroll through the stream to look for the hidden message from Gerald Combs, creator of Wireshark. It is located in the server stream and begins with X-Slogan. What is the message?

From the image above, we see the slogan to be "Sniffing the glue that holds the Internet together."



Applied filter for "X-Slogan" to all packets. 3 Packets found in the search.

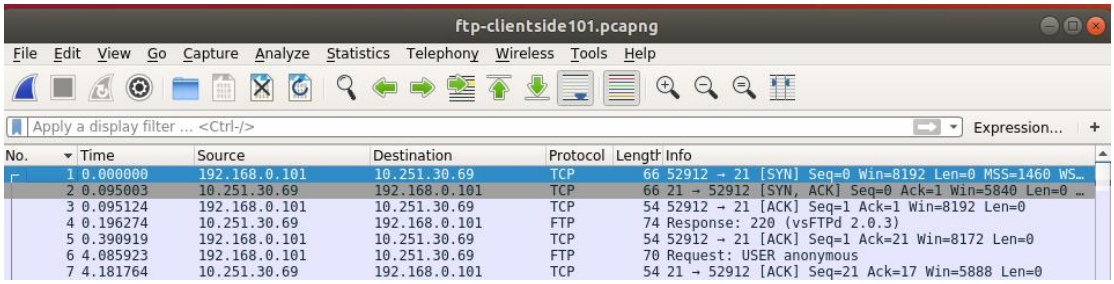
Q5) What other message did you find (different than Q4)?

```
Link: <http://www.wireshark.org/image/ipv6.gif>; rel="canonical"\r\n
X-Slogan: Sniff free or die.\r\n
Cache-control: public, max-age=600\r\n
```

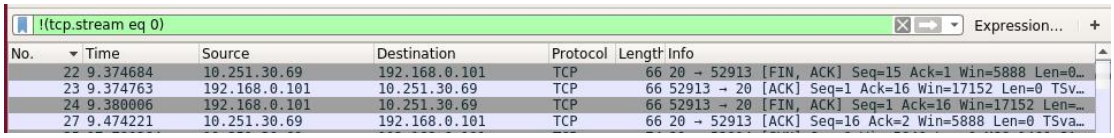
On the 3rd message, it says "Sniff free or die."

CSI 4139 Lab 10
Aaron Ng (300176901)
Nov 24, 2022

Task 4: Extract binary file from FTP session

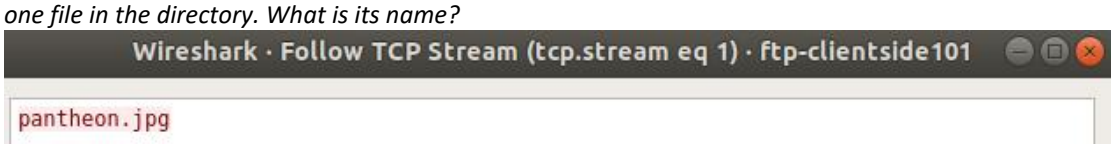


Open pcaps/ftp-clientside101.pcapng in Wireshark.

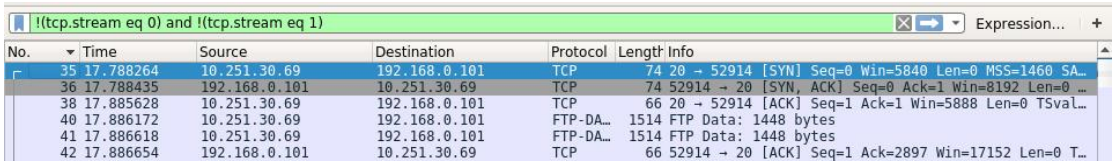


After following command channel stream, we filter it out to find only the data streams.

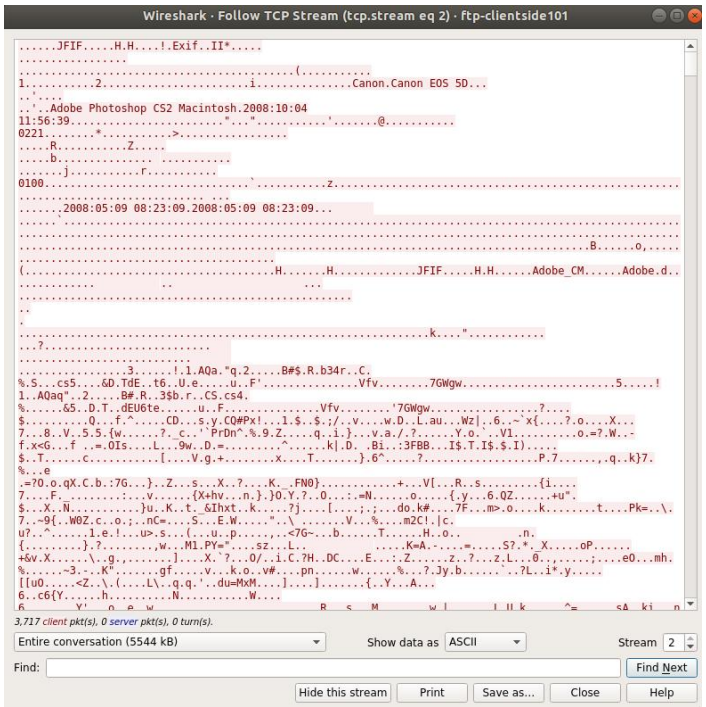
Q6) Right-click on frame 16 and select Follow — TCP Stream. This stream list indicates there is only one file in the directory. What is its name?



One of the data streams reveals the name of the file, “pantheon.jpg”.

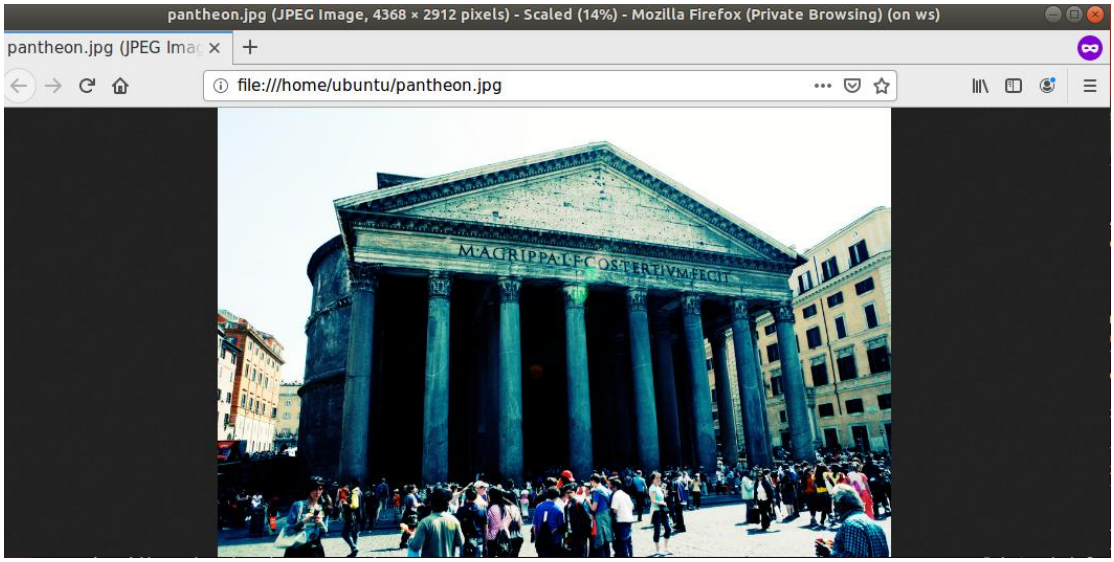


We now filtered out two streams.



Now we follow the final data stream. Here we can see relevant data about the image, camera model, etc.. We will show the data as “Raw” and save the file to our computer.

CSI 4139 Lab 10
Aaron Ng (300176901)
Nov 24, 2022



I ran xdg-open pantheon.jpg which revealed this image.