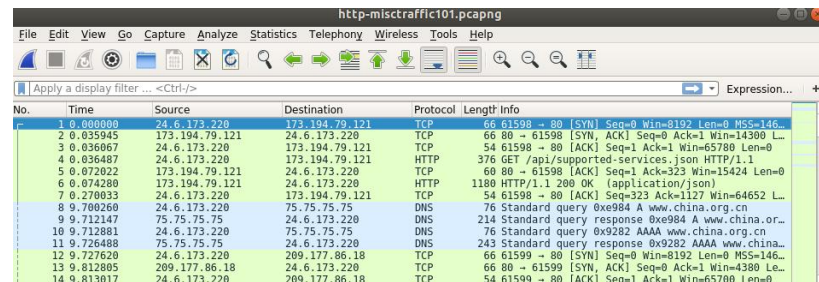
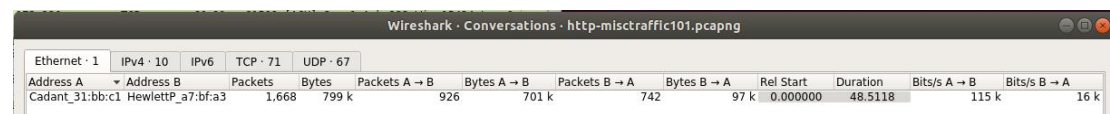


Review of Packet Capture Introspection

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



We open pcaps/http-misstraffic101.pcapng in Wireshark



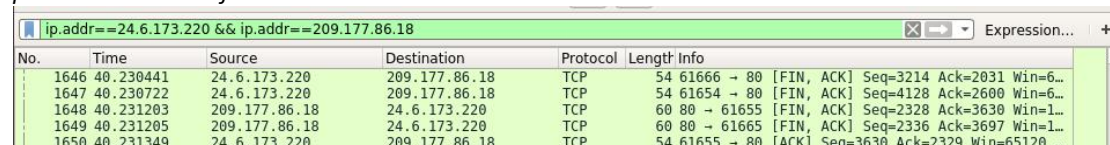
From Statistics > Conversations, we opened a new window.

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

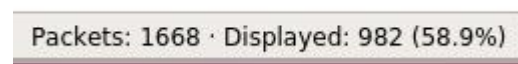
Ethernet · 1	IPv4 · 10	IPv6	TCP · 71	UDP · 67
Address A	Address B	Packets	Bytes	Packets
24.6.173.220	209.177.86.18	982	655 k	
24.6.173.220	50.23.252.178	63	52 k	

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?



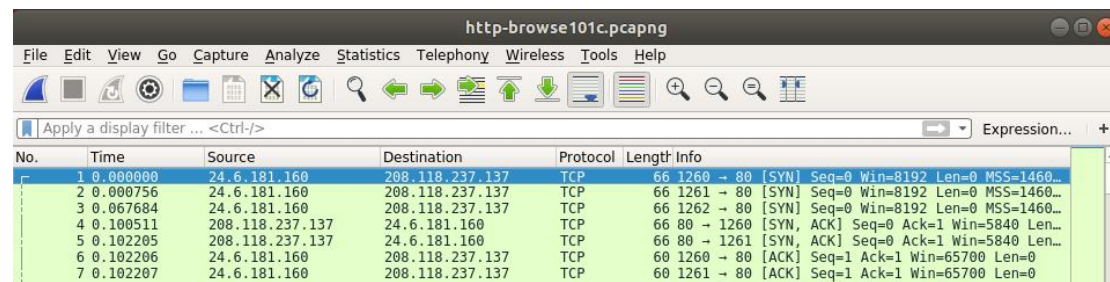
By following the steps above, we have applied this filter as shown.



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

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

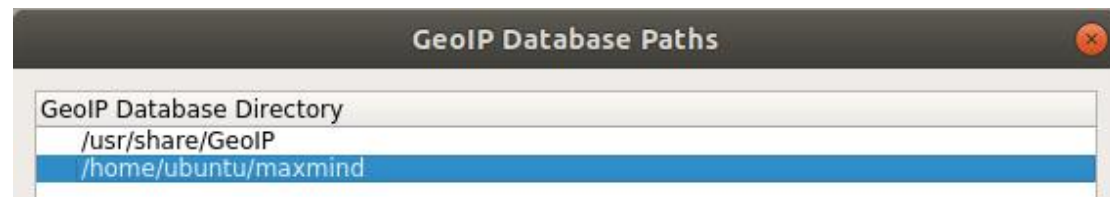
Task 2: Geolocating IP Addresses



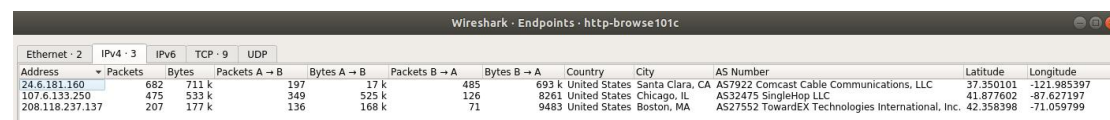
The screenshot shows a Wireshark packet capture window titled 'http-browse101c.pcapng'. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	24.6.181.160	208.118.237.137	TCP	66	1260 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460...
2	0.000756	24.6.181.160	208.118.237.137	TCP	66	1261 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460...
3	0.067684	24.6.181.160	208.118.237.137	TCP	66	1262 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460...
4	0.100511	208.118.237.137	24.6.181.160	TCP	66	80 → 1260 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=...
5	0.102205	208.118.237.137	24.6.181.160	TCP	66	80 → 1261 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=...
6	0.102206	24.6.181.160	208.118.237.137	TCP	60	1260 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
7	0.102207	24.6.181.160	208.118.237.137	TCP	60	1261 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0

We open pcaps/http-browse101c.pcapng in Wireshark



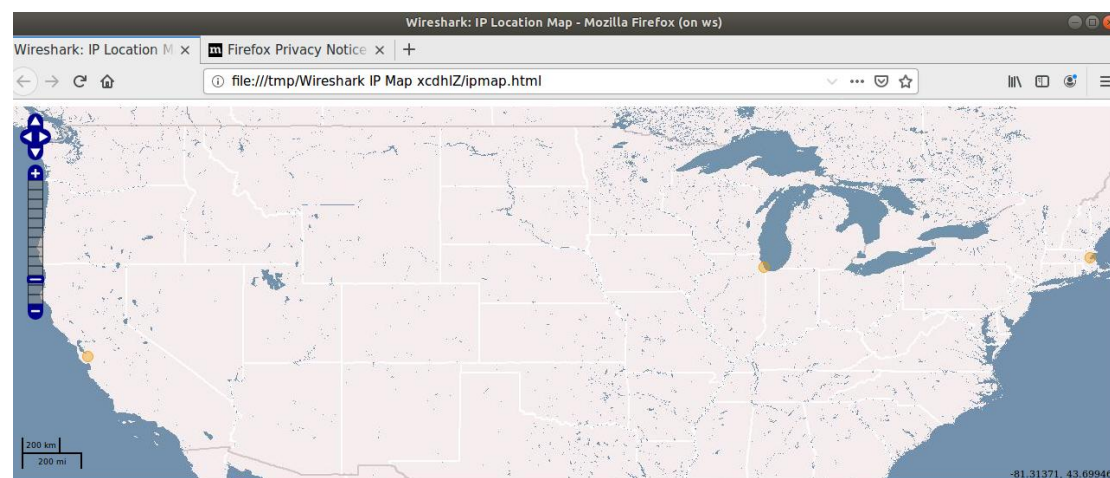
We add maxmind to the GeoIP database directory.



The screenshot shows the 'Wireshark - Endpoints - http-browse101c' window. It displays a table with location details for the IP addresses in the capture:

Address	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Country	City	AS Number	Latitude	Longitude
24.6.181.160	682	711 k	197	17 k	485	693 k	United States	Santa Clara, CA	AS7922 Comcast Cable Communications, LLC	37.350101	-121.985397
107.6.133.250	475	633 k	349	525 k	126	8261	United States	Chicago, IL	AS32475 SingleHop LLC	41.877602	-87.627197
208.118.237.137	207	177 k	136	168 k	71	9483	United States	Boston, MA	AS27552 TwardEX Technologies International, Inc.	42.358398	-71.059799

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?

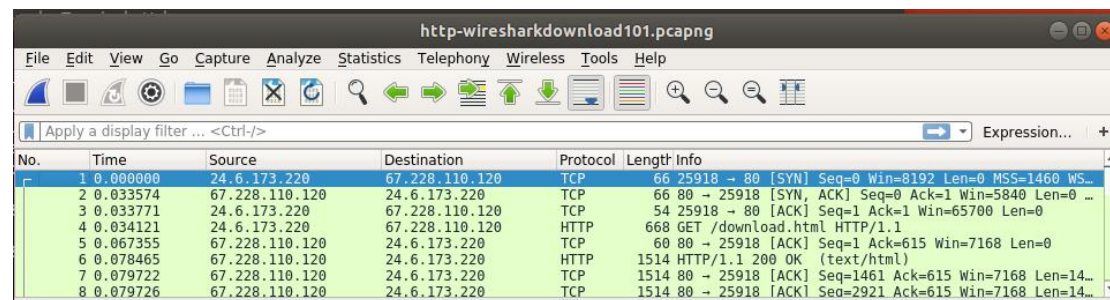


The screenshot shows a popup window for the IP address 24.6.181.160. It displays the following information:

- City: Santa Clara, CA
- Country: United States
- Packets: 682
- Bytes: 711 k
- AS Number: -

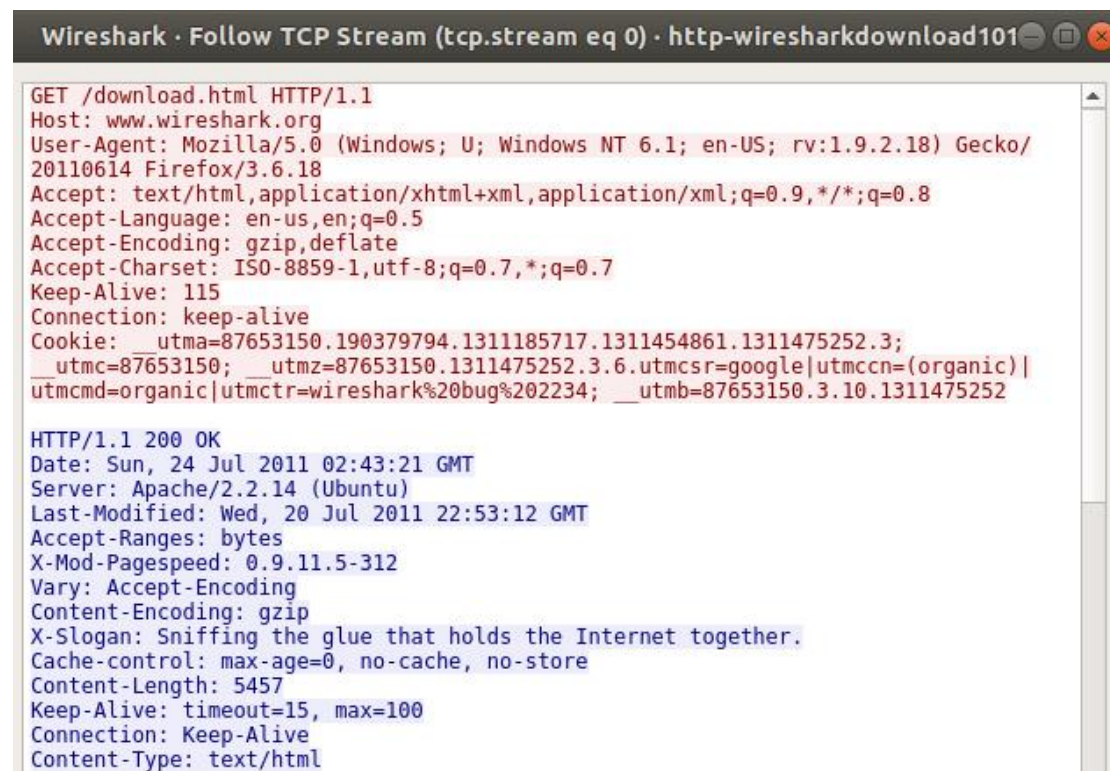
We can see that 711k bytes of traffic when to/from Santa Clara.

Task 3: Reassemble text from TCP stream



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	24.6.173.220	67.228.110.120	TCP	66	25918 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS...
2	0.033574	67.228.110.120	24.6.173.220	TCP	66	80 → 25918 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 ...
3	0.033771	24.6.173.220	67.228.110.120	TCP	54	25918 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0 ...
4	0.034121	24.6.173.220	67.228.110.120	HTTP	668	GET /download.html HTTP/1.1
5	0.067355	67.228.110.120	24.6.173.220	TCP	60	80 → 25918 [ACK] Seq=1 Ack=615 Win=7168 Len=0 ...
6	0.078465	67.228.110.120	24.6.173.220	HTTP	1514	HTTP/1.1 200 OK (text/html)
7	0.079722	67.228.110.120	24.6.173.220	TCP	1514	80 → 25918 [ACK] Seq=1461 Ack=615 Win=7168 Len=14...
8	0.079726	67.228.110.120	24.6.173.220	TCP	1514	80 → 25918 [ACK] Seq=2921 Ack=615 Win=7168 Len=14...

Open pcaps/http-wiresharkdownload101.pcapng in Wireshark.



```

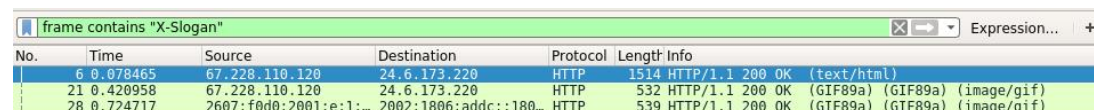
GET /download.html HTTP/1.1
Host: www.wireshark.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.18) Gecko/20110614 Firefox/3.6.18
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie: __utma=87653150.190379794.1311185717.1311454861.1311475252.3;
__utmc=87653150; __utmz=87653150.1311475252.3.6.utmcsr=google|utmccn=(organic)|
utmcmd=organic|utmctr=wireshark%20bug%202234; __utmb=87653150.3.10.1311475252

HTTP/1.1 200 OK
Date: Sun, 24 Jul 2011 02:43:21 GMT
Server: Apache/2.2.14 (Ubuntu)
Last-Modified: Wed, 20 Jul 2011 22:53:12 GMT
Accept-Ranges: bytes
X-Mod-Pagespeed: 0.9.11.5-312
Vary: Accept-Encoding
Content-Encoding: gzip
X-Slogan: Sniffing the glue that holds the Internet together.
Cache-control: max-age=0, no-cache, no-store
Content-Length: 5457
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
  
```

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."



No.	Time	Source	Destination	Protocol	Length	Info
6	0.078465	67.228.110.120	24.6.173.220	HTTP	1514	HTTP/1.1 200 OK (text/html)
21	0.420958	67.228.110.120	24.6.173.220	HTTP	532	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
28	0.724717	2607:f0d0:2001:e:1::...	2002:1806:adcc::180...	HTTP	539	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)

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

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

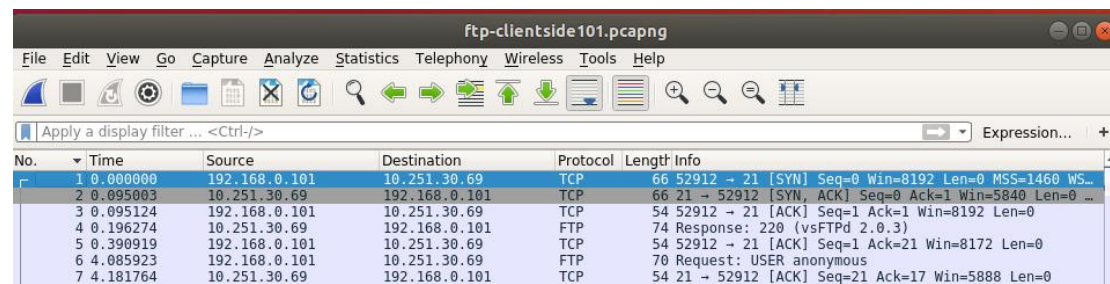
```

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

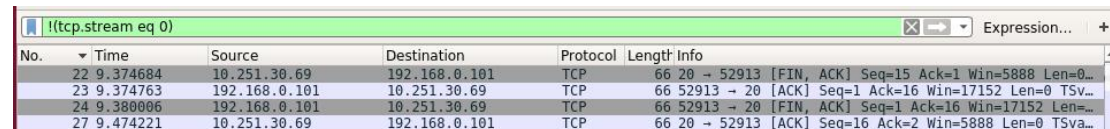
Task 4: Extract binary file from FTP session



Wireshark packet capture for ftp-clientside101.pcapng. The table shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.101	10.251.30.69	TCP	66	52912 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS...
2	0.095003	10.251.30.69	192.168.0.101	TCP	66	21 → 52912 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 ...
3	0.095124	192.168.0.101	10.251.30.69	TCP	54	52912 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4	0.196274	10.251.30.69	192.168.0.101	FTP	74	Response: 220 (vsFTPD 2.0.3)
5	0.390919	192.168.0.101	10.251.30.69	TCP	54	52912 → 21 [ACK] Seq=1 Ack=21 Win=8172 Len=0
6	4.085923	192.168.0.101	10.251.30.69	FTP	70	Request: USER anonymous
7	4.181764	10.251.30.69	192.168.0.101	TCP	54	21 → 52912 [ACK] Seq=21 Ack=17 Win=5888 Len=0

Open pcaps/ftp-clientside101.pcapng in Wireshark.

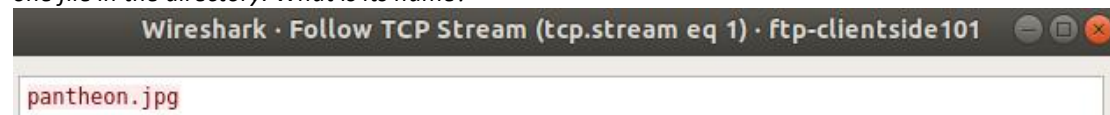


Wireshark packet capture filtered for TCP stream eq 0. The table shows the following packets:

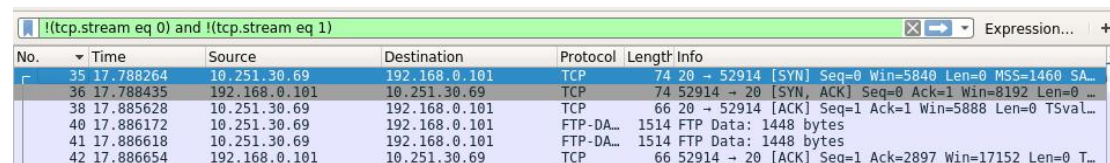
No.	Time	Source	Destination	Protocol	Length	Info
22	9.374684	10.251.30.69	192.168.0.101	TCP	66	20 → 52913 [FIN, ACK] Seq=15 Ack=1 Win=5888 Len=0...
23	9.374763	192.168.0.101	10.251.30.69	TCP	66	52913 → 20 [ACK] Seq=1 Ack=16 Win=17152 Len=0 TSv...
24	9.380006	192.168.0.101	10.251.30.69	TCP	66	52913 → 20 [FIN, ACK] Seq=1 Ack=16 Win=17152 Len=...
27	9.474221	10.251.30.69	192.168.0.101	TCP	66	20 → 52913 [ACK] Seq=16 Ack=2 Win=5888 Len=0 TSva...

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?



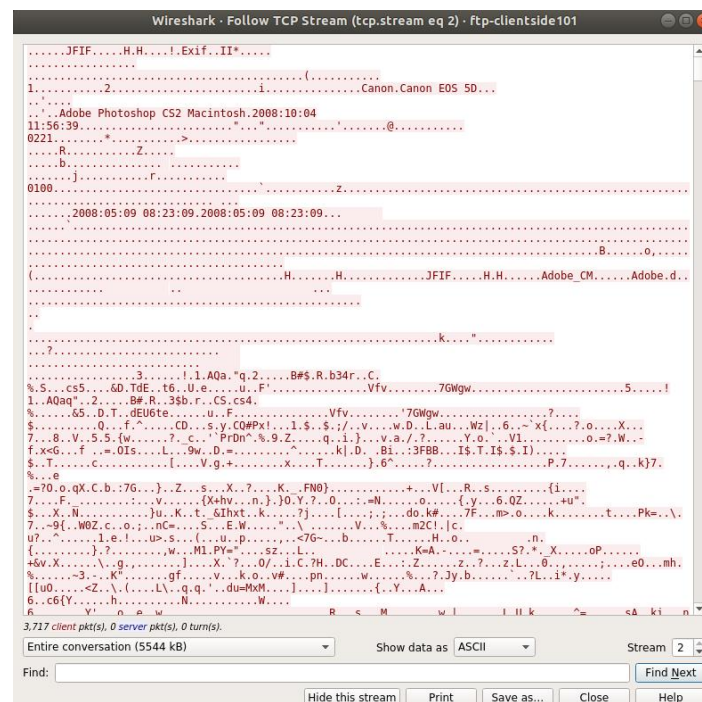
One of the data streams reveals the name of the file, “pantheon.jpg”.



Wireshark packet capture filtered for TCP streams eq 0 and eq 1. The table shows the following packets:

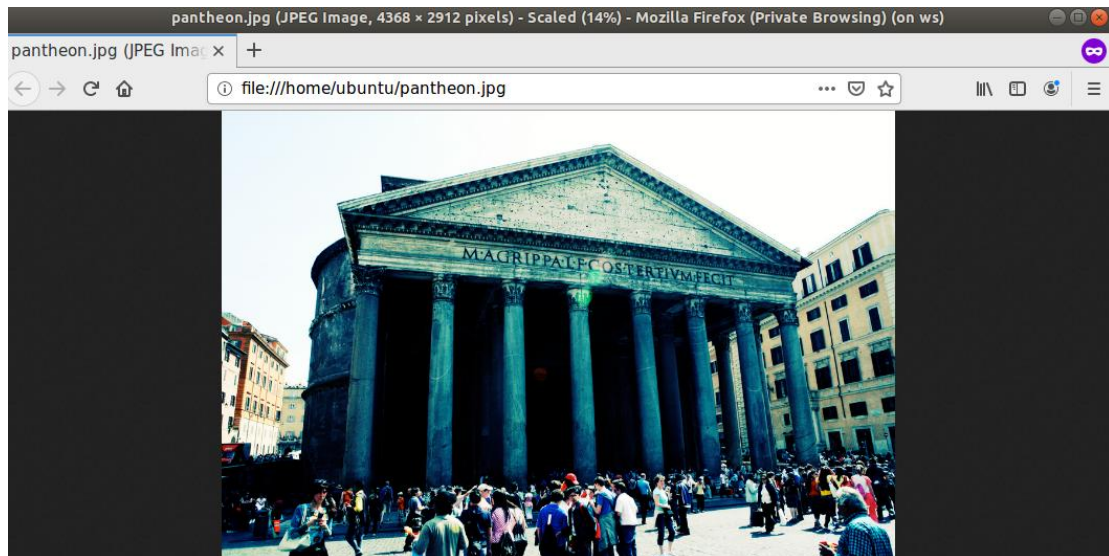
No.	Time	Source	Destination	Protocol	Length	Info
35	17.788264	10.251.30.69	192.168.0.101	TCP	74	20 → 52914 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SA...
36	17.788435	192.168.0.101	10.251.30.69	TCP	74	52914 → 20 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 ...
38	17.885628	10.251.30.69	192.168.0.101	TCP	66	20 → 52914 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval...
40	17.886172	10.251.30.69	192.168.0.101	FTP-DA..	1514	FTP Data: 1448 bytes
41	17.886618	10.251.30.69	192.168.0.101	FTP-DA..	1514	FTP Data: 1448 bytes
42	17.886654	192.168.0.101	10.251.30.69	TCP	66	52914 → 20 [ACK] Seq=1 Ack=2897 Win=17152 Len=0 T...

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.