CSI4139 LAB 4 Report

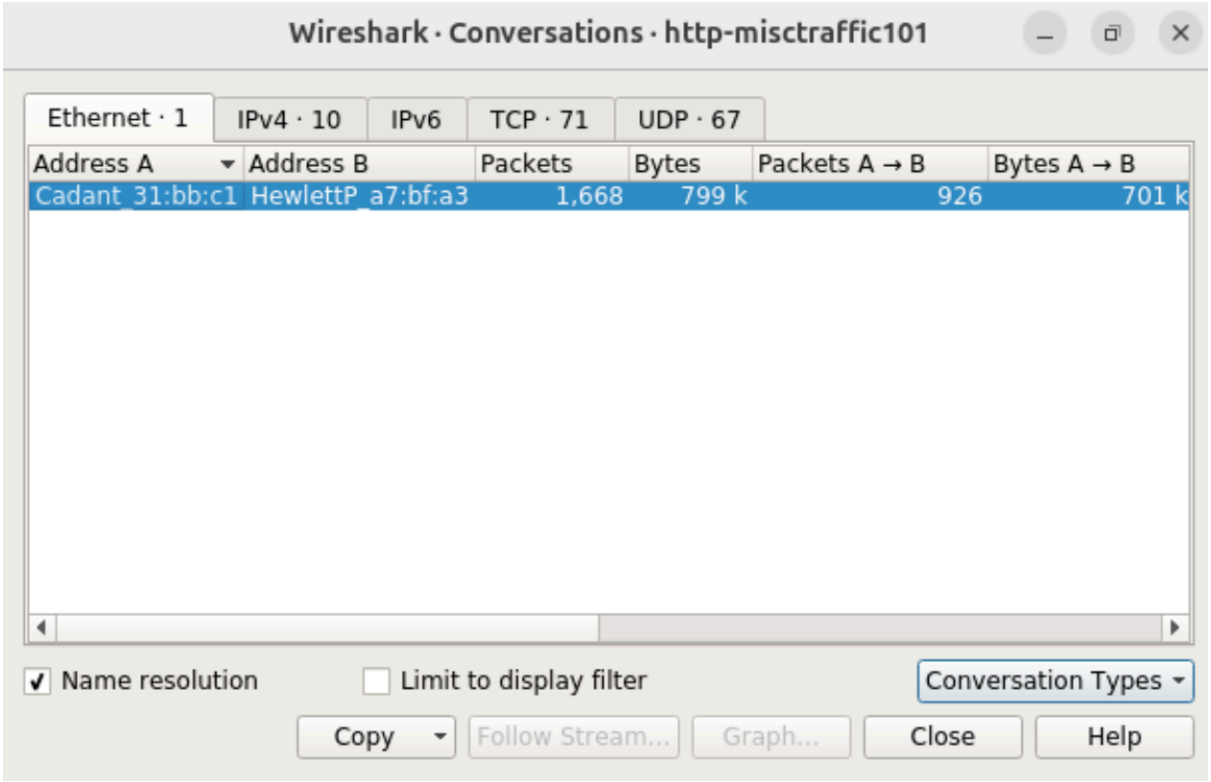
Name: Iyanu Aketepe

Student No: 300170701

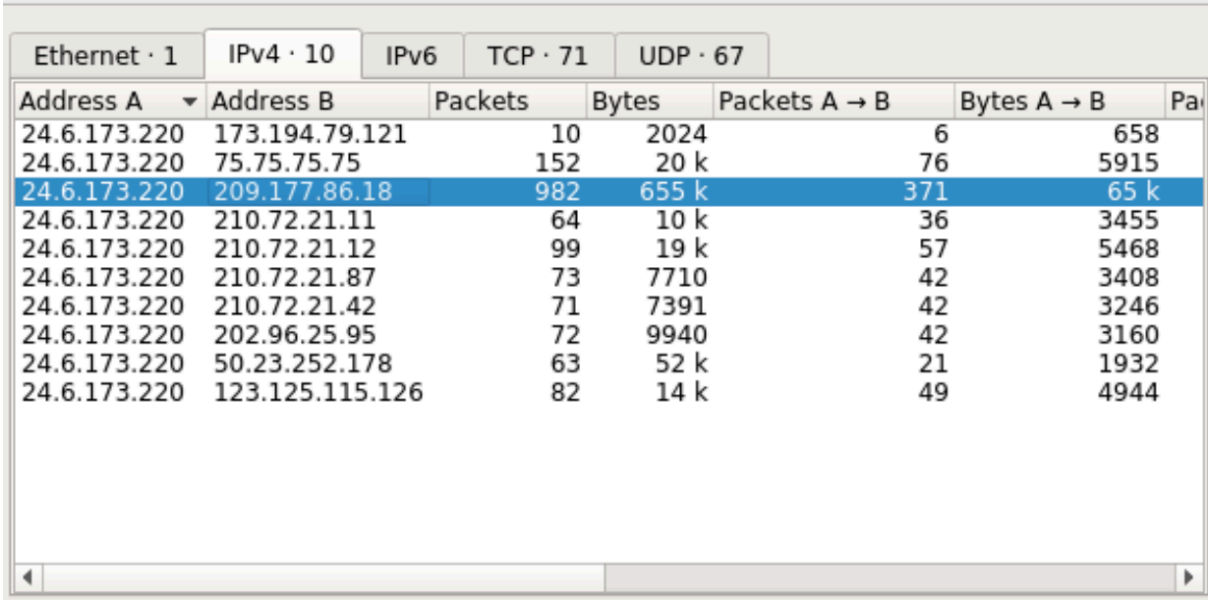
Task 1

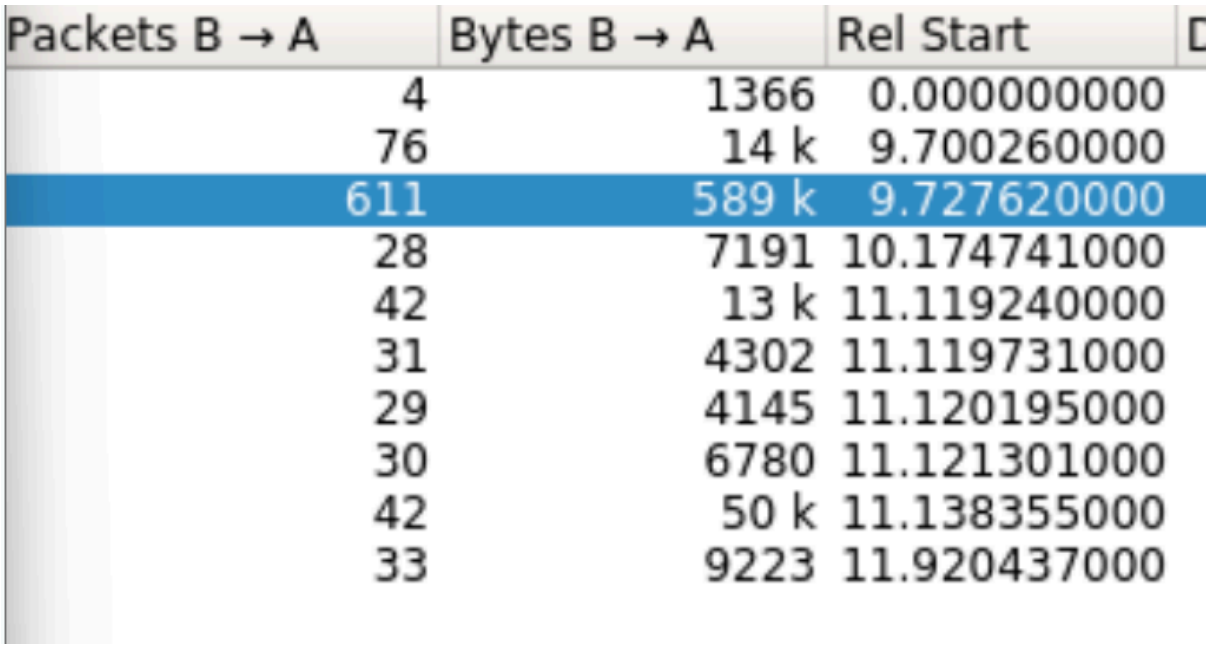
Pt 1

```
-su: http-misctraff8c101.pcapng: command not found
ubuntu@ws:~/pcaps$ wireshark
```

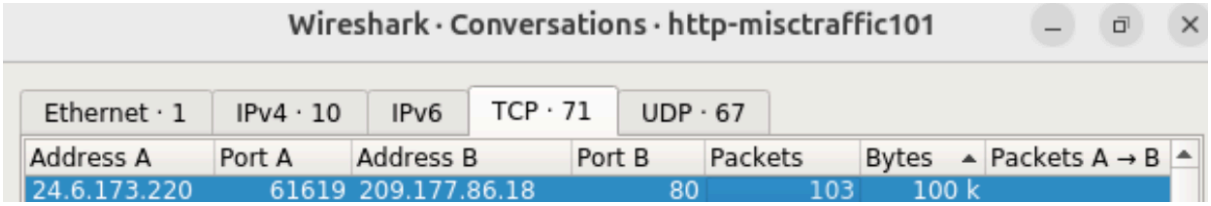


IP Addresses 209.177.86.18 and 24.6.173.220 are the most active with 209.177.86.18 being the most active sending 589k worth of bytes to 24.6.173.220



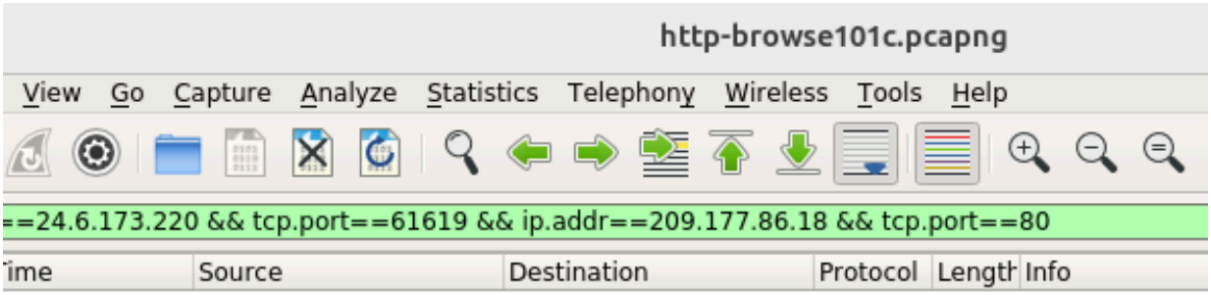


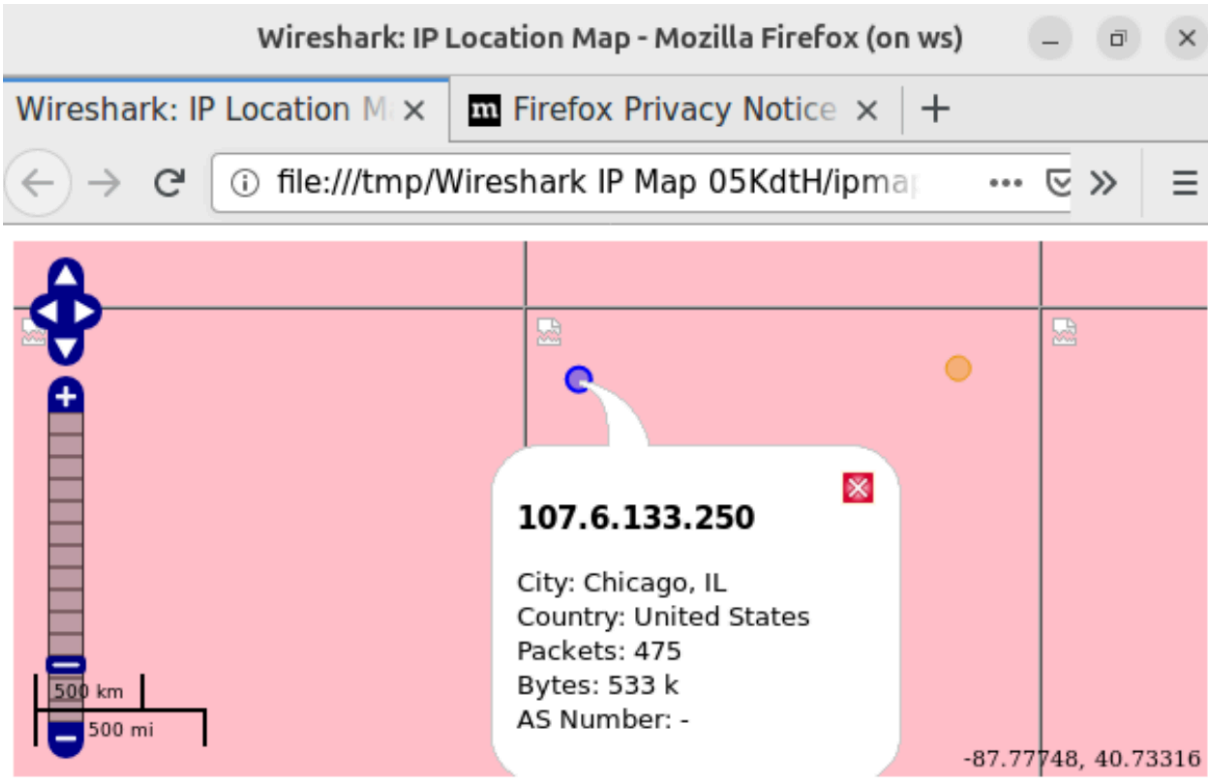
Pt 2

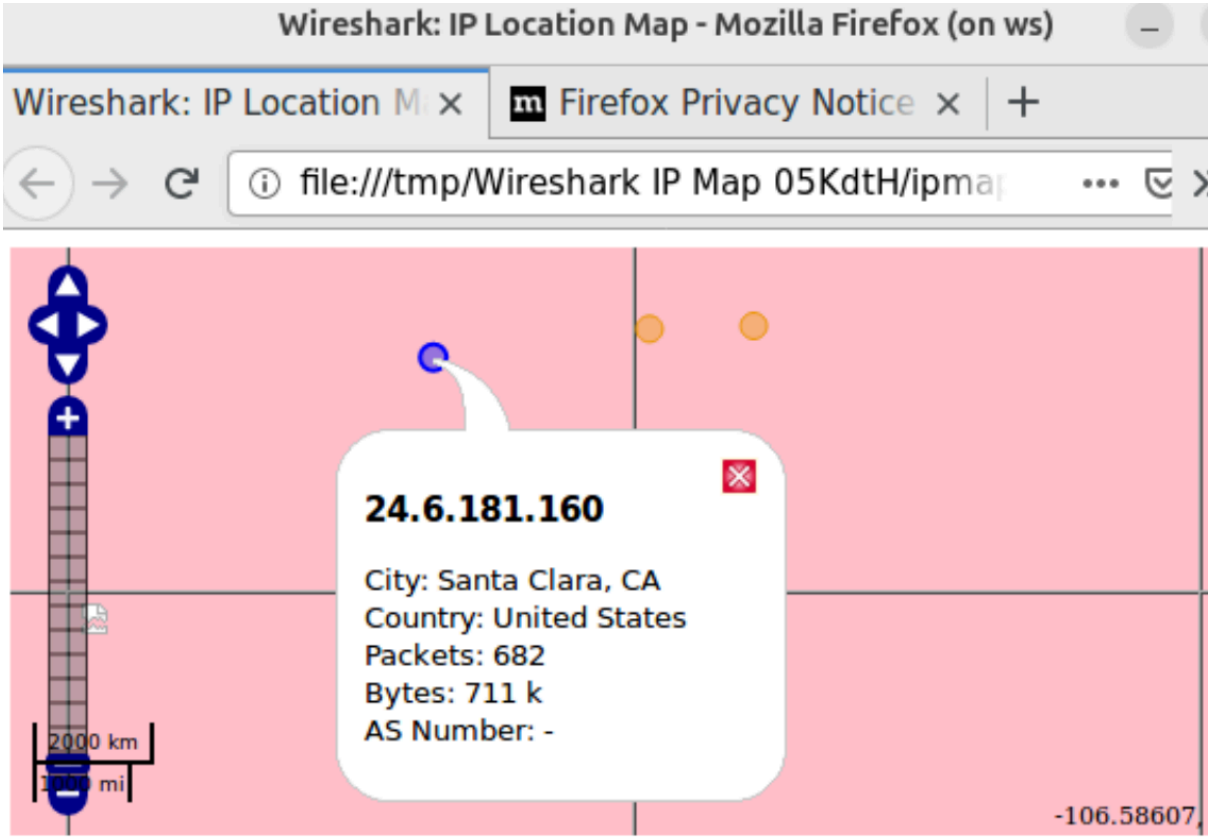


The number of packets is 103.

Task 2


http-browse101c.pcapng
View Go Capture Analyze Statistics Telephony Wireless Tools Help
==24.6.173.220 && tcp.port==61619 && ip.addr==209.177.86.18 && tcp.port==80
ime Source Destination Protocol Length Info

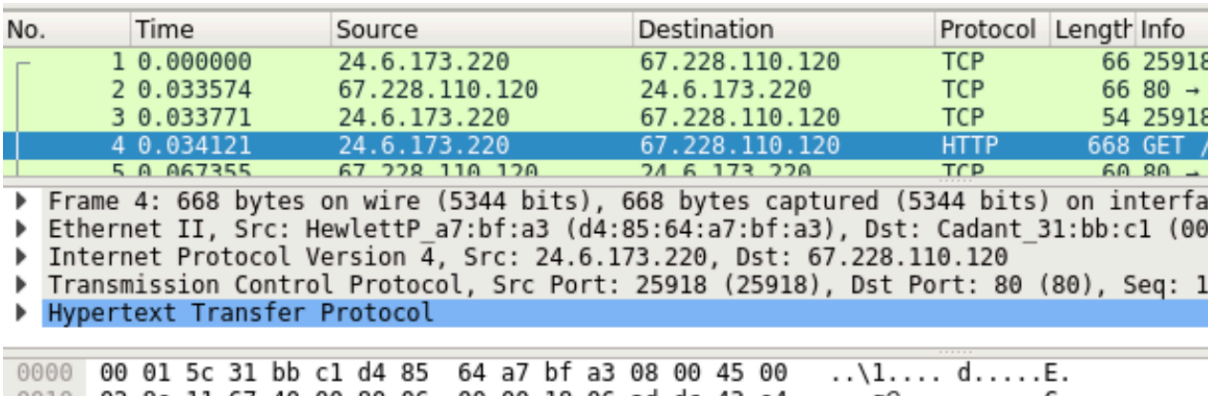

Wireshark: IP Location Map - Mozilla Firefox (on ws)
Wireshark: IP Location M
Firefox Privacy Notice
file:///tmp/Wireshark IP Map 05KdtH/ipma
107.6.133.250
City: Chicago, IL
Country: United States
Packets: 475
Bytes: 533 k
AS Number: -
500 km
500 mi
-87.77748, 40.73316

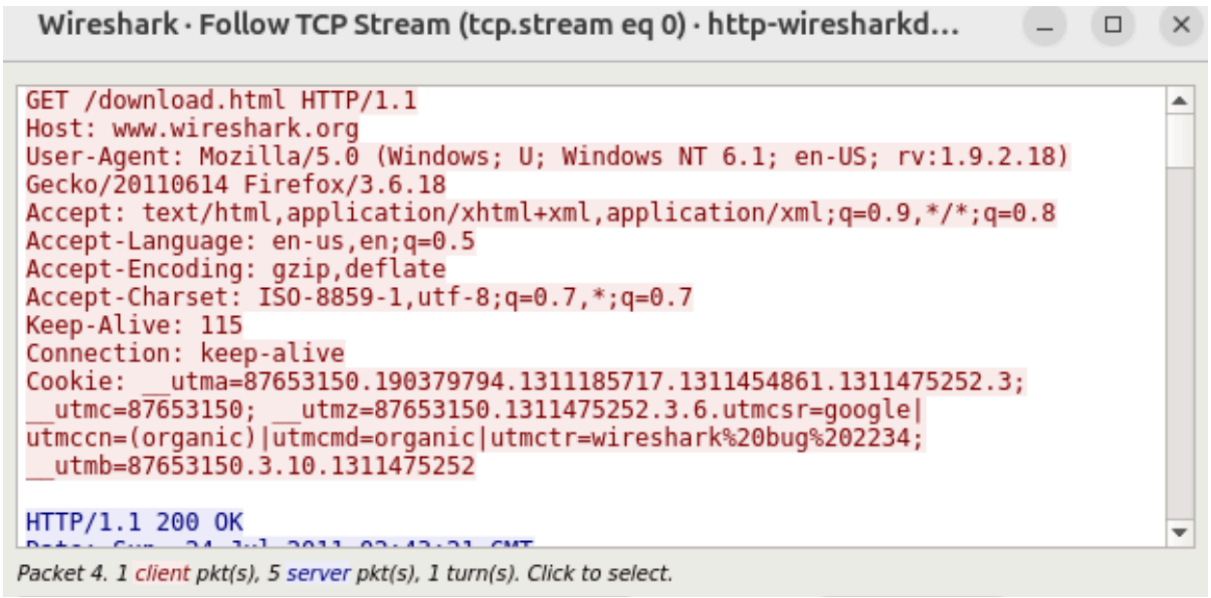


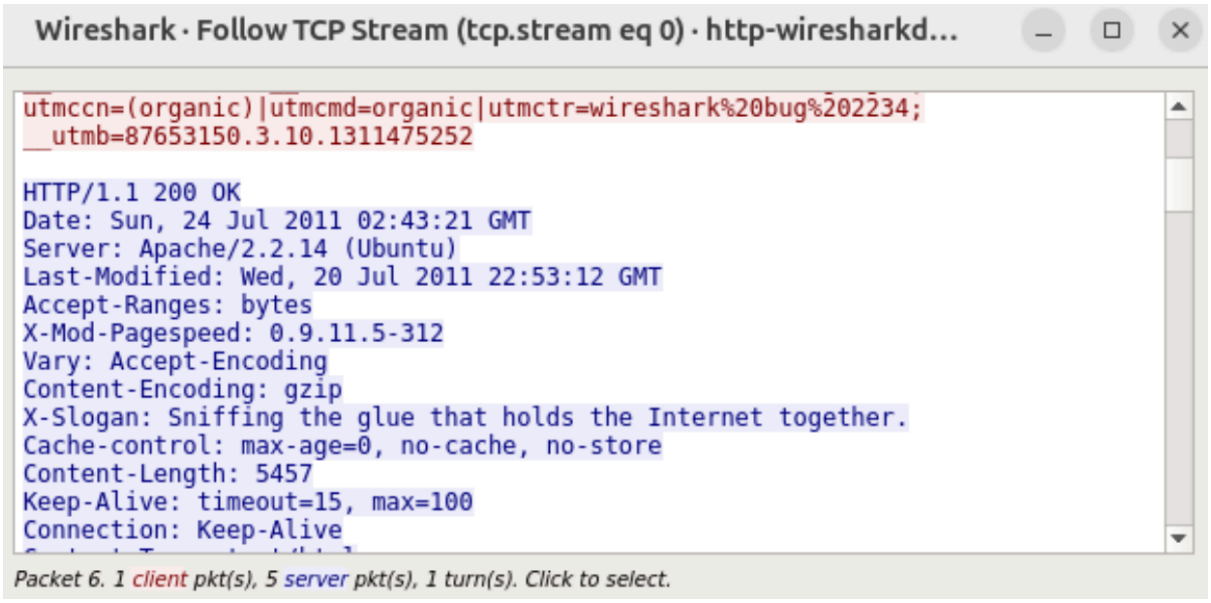
TA NOTE: There is a version mismatch, for this version I need to find the aggregate traffic for Snata Clara not Milpitas.

In terms of aggregate traffic, there were 682 packets in the context of Santa Clara. The total amount of data is 711k for those packets.

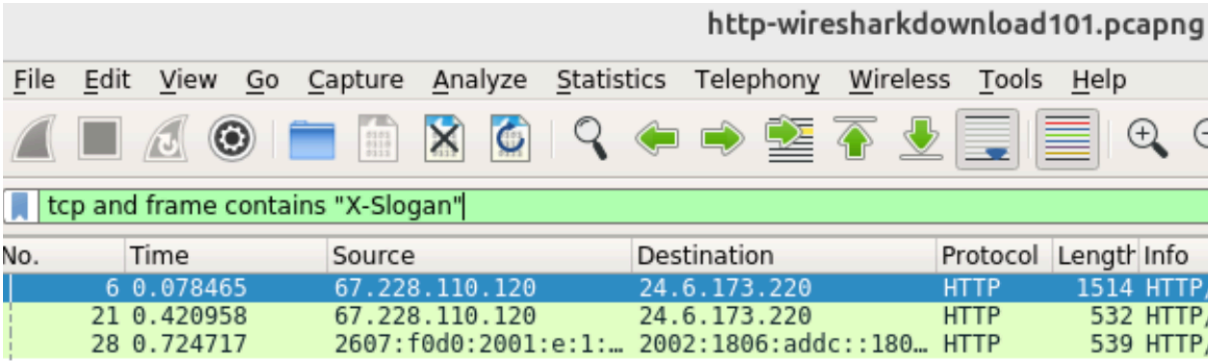
Task 3

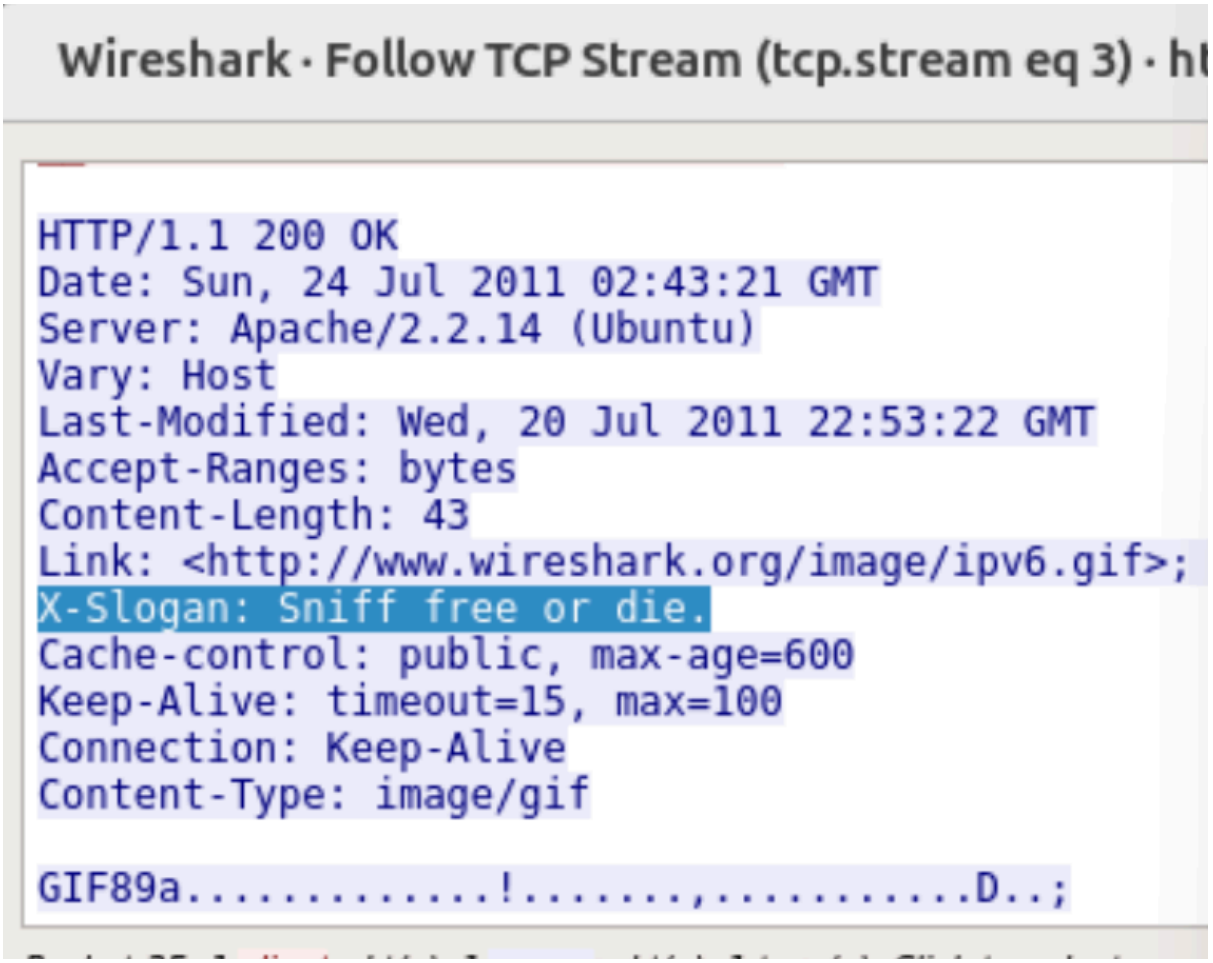






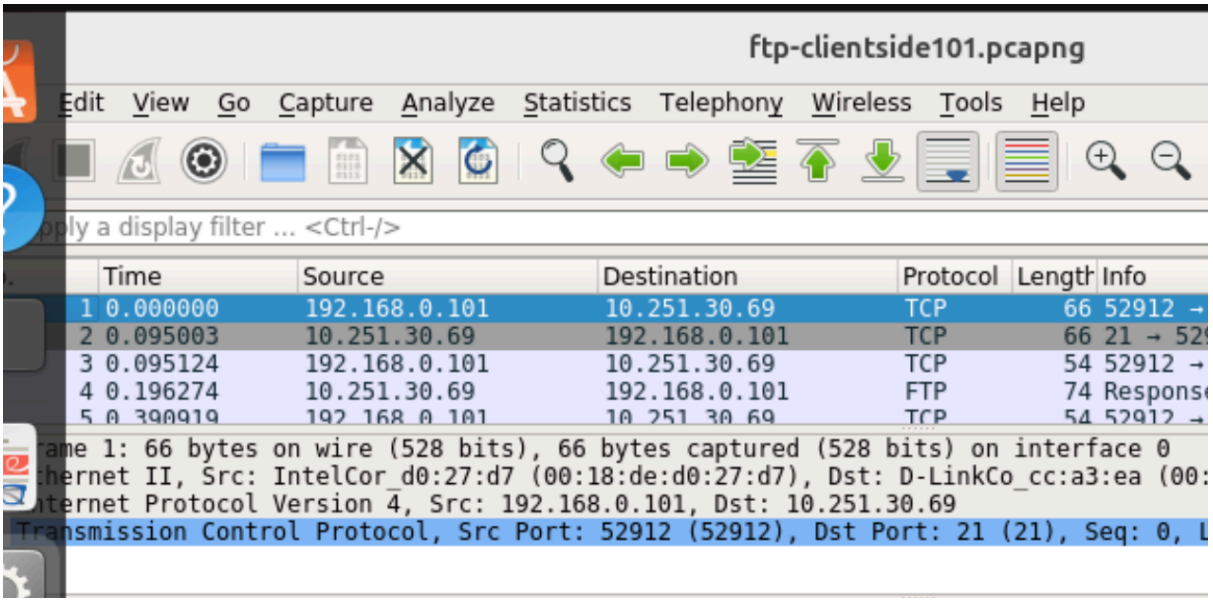
The Message: Sniffing the glue that holds the Internet together.

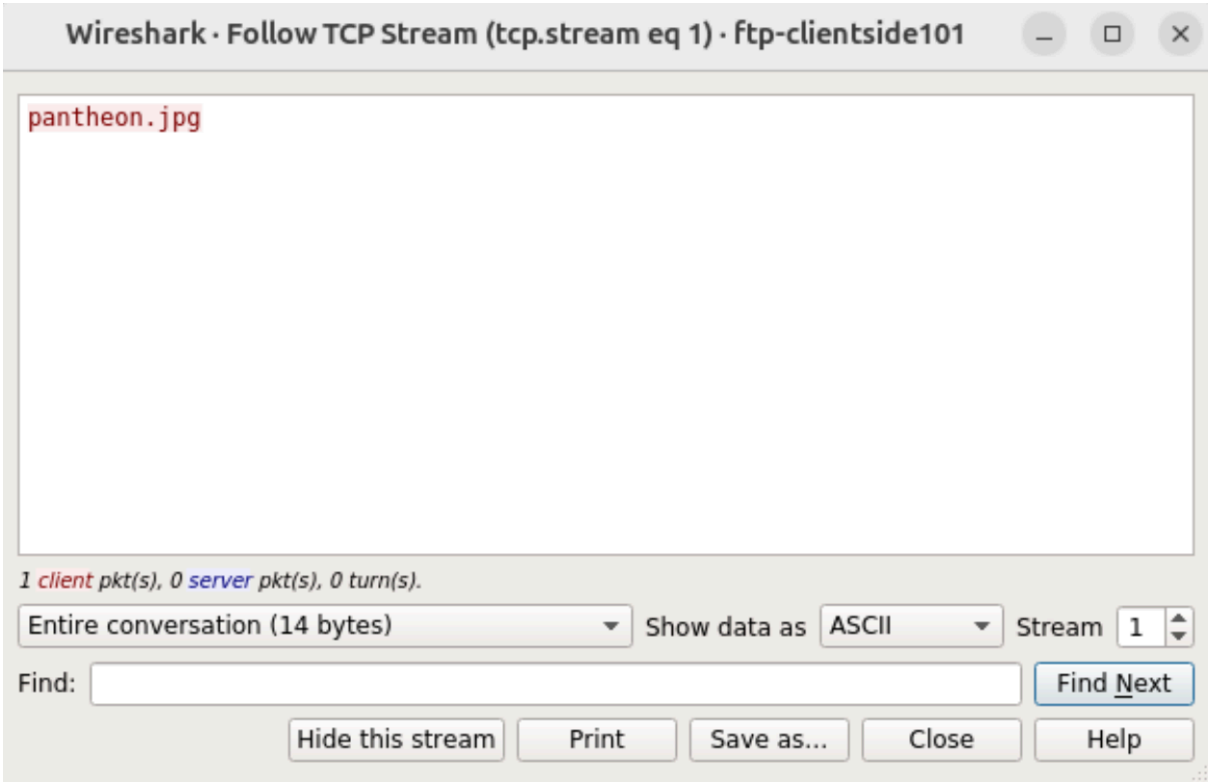


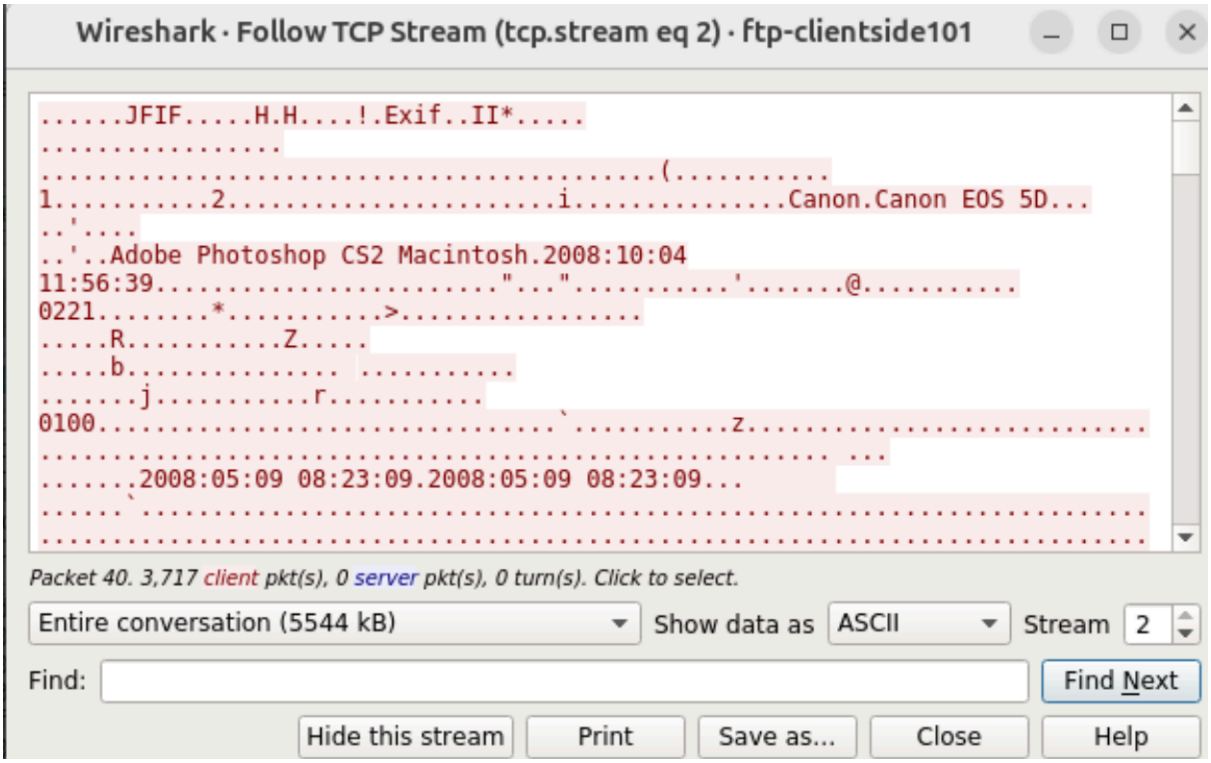


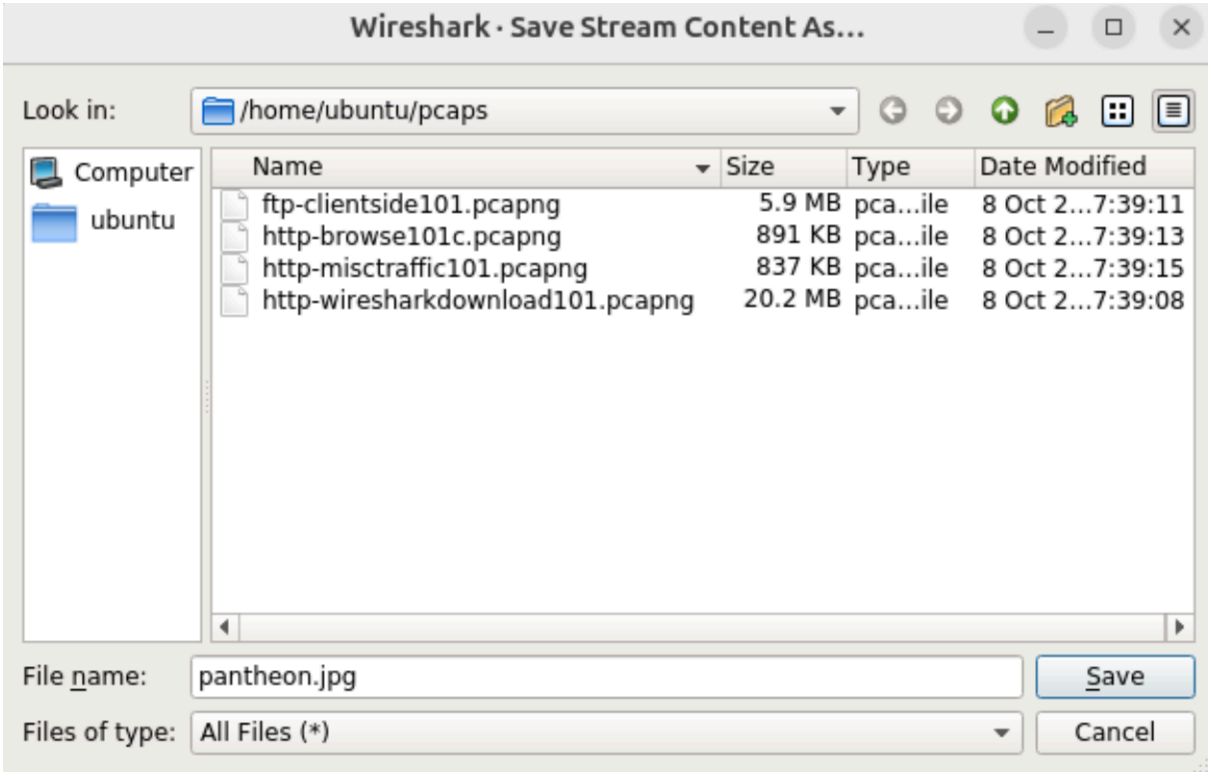
The other message: Sniff free or die.

Task 4




Wireshark · Follow TCP Stream (tcp.stream eq 1) · ftp-clientside101
pantheon.jpg
1 client pkt(s), 0 server pkt(s), 0 turn(s).
Entire conversation (14 bytes)
Show data as
ASCII
Stream
1
Find:
Find Next
Hide this stream
Print
Save as...
Close
Help


Wireshark · Follow TCP Stream (tcp.stream eq 2) · ftp-clientside101
Packet 40. 3,717 client pkt(s), 0 server pkt(s), 0 turn(s). Click to select.
Entire conversation (5544 kB)
Show data as
ASCII
Stream
2
Find:
Find Next
Hide this stream
Print
Save as...
Close
Help




```
ubuntu@ws:~/pcaps$ l
ftp-clientside101.pcapng
http-browse101c.pcapng
http-misctraffic101.pcapng
http-wiresharkdownload101.pcapng
pantheon.jpg
ubuntu@ws:~/pcaps$ xdg-open pantheon.jpg
```

NOTE: xdg-open is the ‘’double-click’’ for images in linux (https://unix.stackexchange.com/questions/35333/what-is-the-fastest-way-to-view-images-from-the-terminal)

```
   file:///home/student/labtainer/trunk/labs/packet-introsp
ection/docs/packet-introspection.pdf

You may open the manual by right clicking
and select "Open Link".


Press <enter> to start the lab
student@Labtainer-VirtualBox:~/labtainer/labtainer-student$
student@Labtainer-VirtualBox:~/labtainer/labtainer-student$
 stoplab
Results stored in directory: /home/student/labtainer_xfer/p
acket-introspection
student@Labtainer-VirtualBox:~/labtainer/labtainer-student$
```