

CSI4139 LAB 4 Report

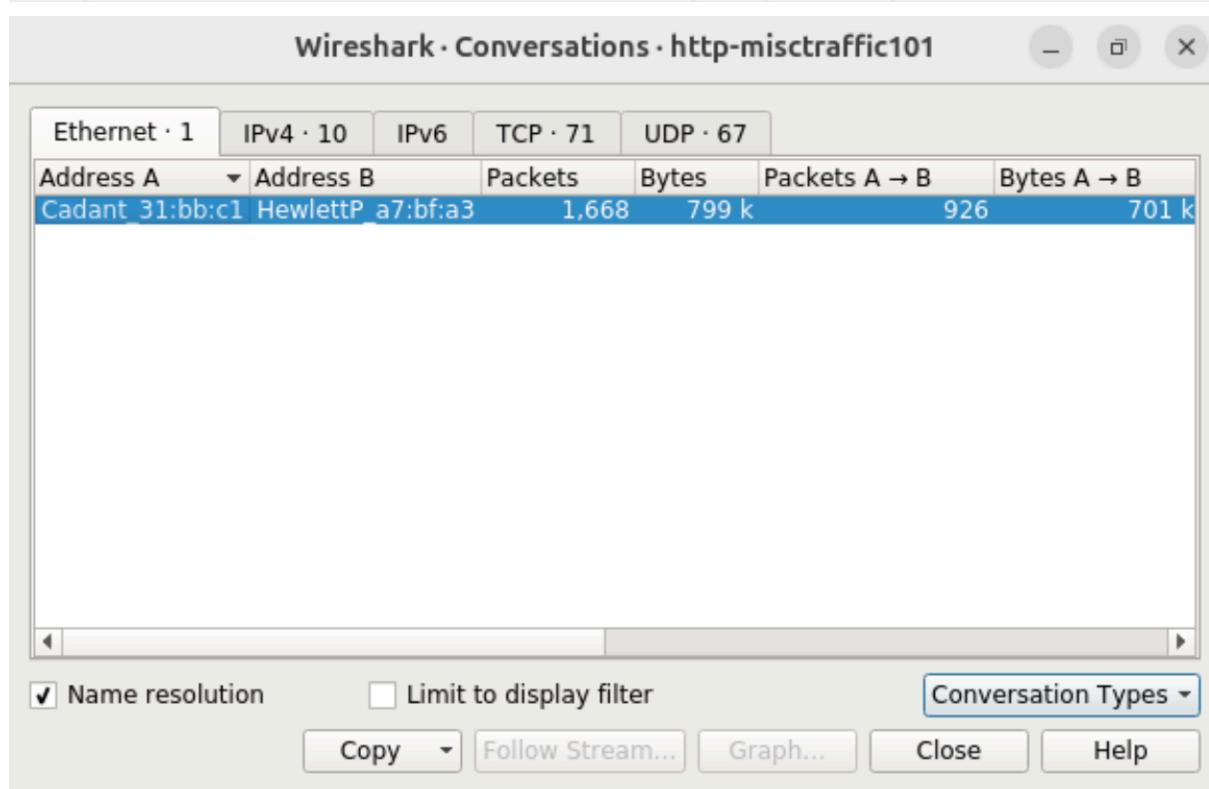
Name: Iyanu Aketepe

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

Ethernet · 1		IPv4 · 10	IPv6	TCP · 71	UDP · 67		
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Pa	
24.6.173.220	173.194.79.121	10	2024	6	658		
24.6.173.220	75.75.75.75	152	20 k	76	5915		
24.6.173.220	209.177.86.18	982	655 k	371	65 k		
24.6.173.220	210.72.21.11	64	10 k	36	3455		
24.6.173.220	210.72.21.12	99	19 k	57	5468		
24.6.173.220	210.72.21.87	73	7710	42	3408		
24.6.173.220	210.72.21.42	71	7391	42	3246		
24.6.173.220	202.96.25.95	72	9940	42	3160		
24.6.173.220	50.23.252.178	63	52 k	21	1932		
24.6.173.220	123.125.115.126	82	14 k	49	4944		

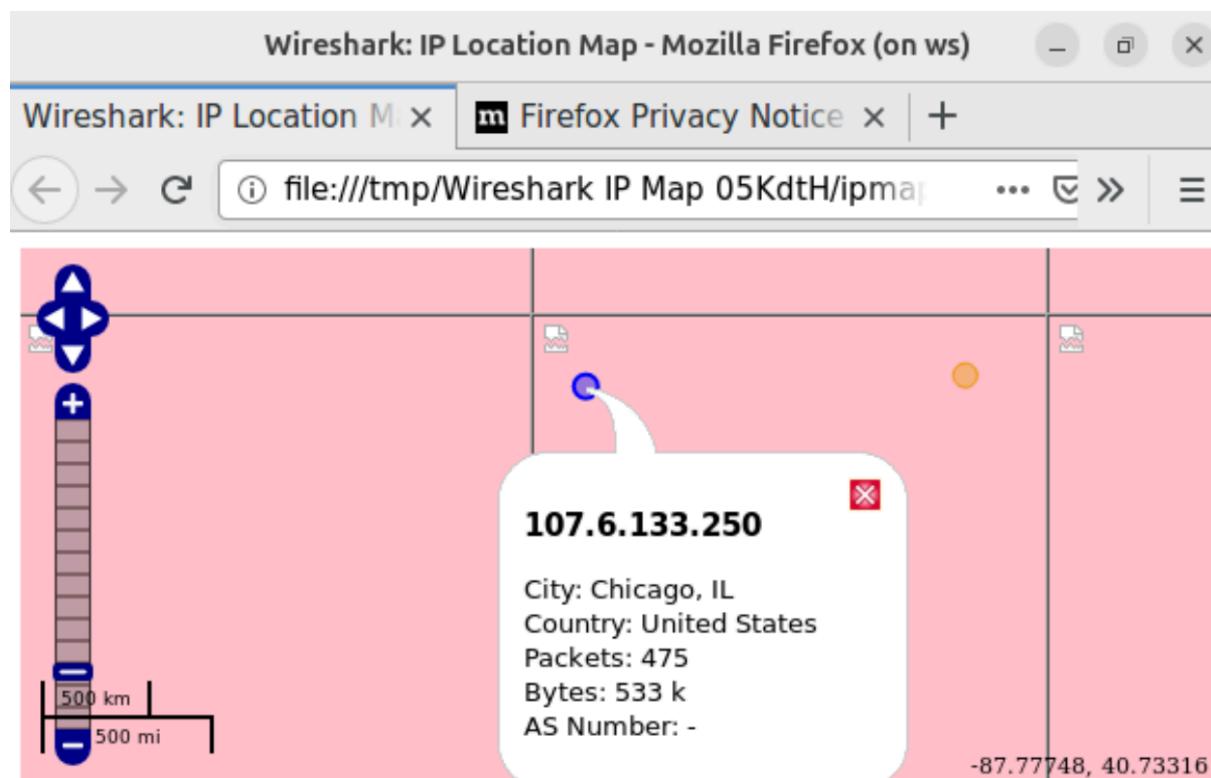
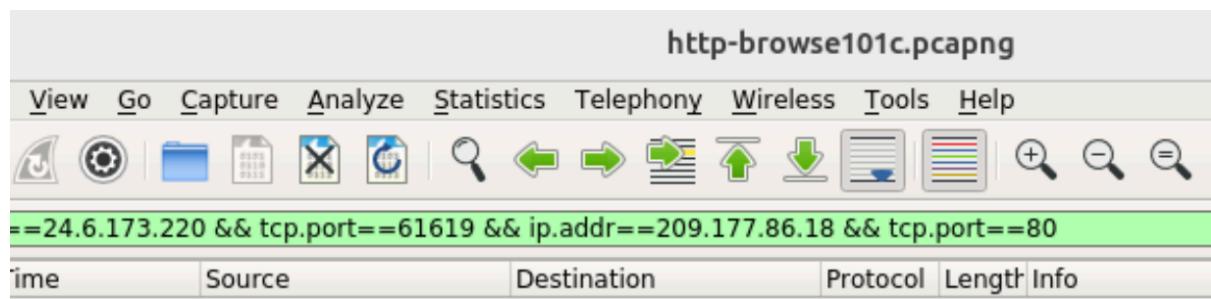
Packets B → A	Bytes B → A	Rel Start	End
4	1366	0.0000000000	
76	14 k	9.7002600000	
611	589 k	9.7276200000	
28	7191	10.1747410000	
42	13 k	11.1192400000	
31	4302	11.1197310000	
29	4145	11.1201950000	
30	6780	11.1213010000	
42	50 k	11.1383550000	
33	9223	11.9204370000	

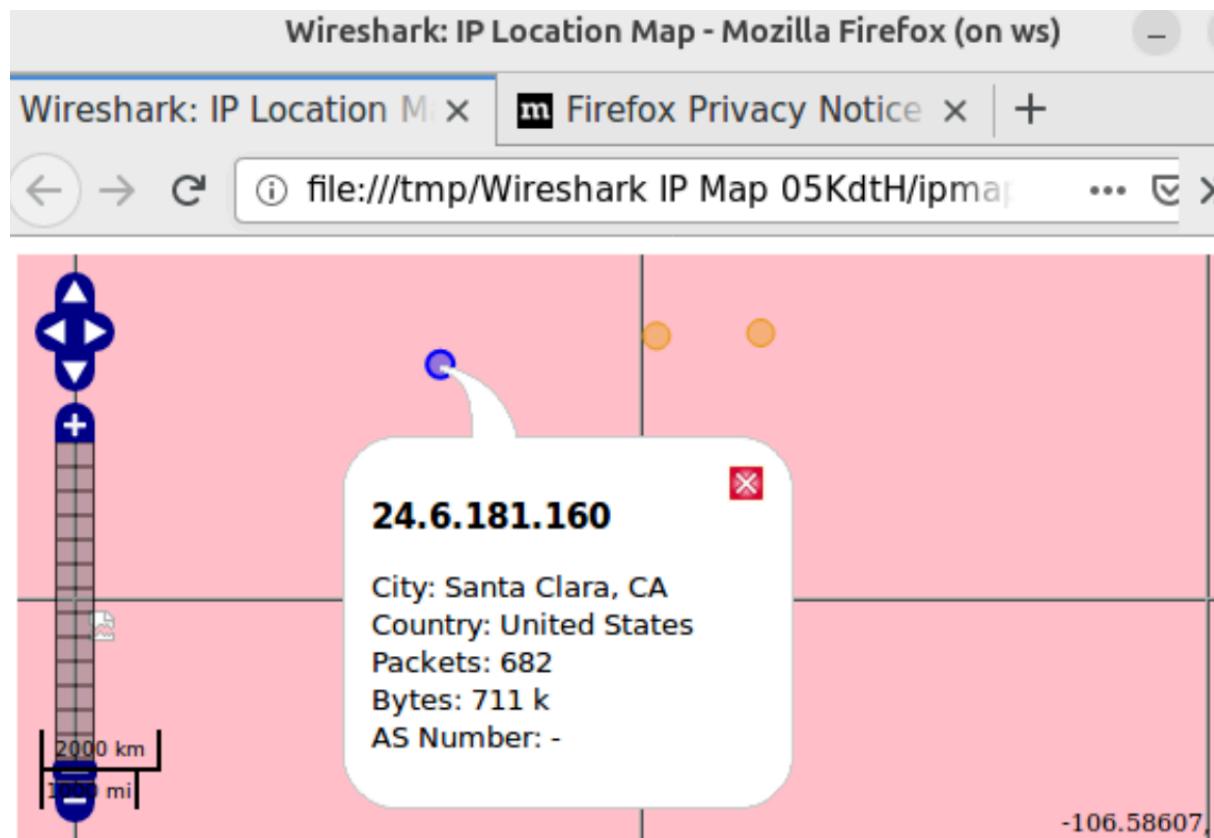
Pt 2

Wireshark · Conversations · http-misctraffic101							
Ethernet · 1		IPv4 · 10	IPv6	TCP · 71	UDP · 67		
Address A	Port A	Address B	Port B	Packets	Bytes	▲ Packets A → B	▲ Packets B → A
24.6.173.220	61619	209.177.86.18	80	103	100 k		

The number of packets is 103.

Task 2





TA NOTE: There is a version mismatch, for this version I need to find the aggregate traffic for Santa 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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	24.6.173.220	67.228.110.120	TCP	66	25918
2	0.033574	67.228.110.120	24.6.173.220	TCP	66	80 →
3	0.033771	24.6.173.220	67.228.110.120	TCP	54	25918
4	0.034121	24.6.173.220	67.228.110.120	HTTP	668	GET /
5	0.067355	67.228.110.120	24.6.173.220	TCP	60	80 →

► Frame 4: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits) on interface
 ► Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:0c:29:31:bb:c1)
 ► Internet Protocol Version 4, Src: 24.6.173.220, Dst: 67.228.110.120
 ► Transmission Control Protocol, Src Port: 25918 (25918), Dst Port: 80 (80), Seq: 1
 ► Hypertext Transfer Protocol

```
0000  00 01 5c 31 bb c1 d4 85  64 a7 bf a3 08 00 45 00  ..\1.... d....E.
```

Wireshark · Follow TCP Stream (tcp.stream eq 0) · http-wiresharkd...

```

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

```

Packet 4. 1 client pkt(s), 5 server pkt(s), 1 turn(s). Click to select.

Wireshark · Follow TCP Stream (tcp.stream eq 0) · http-wiresharkd...

```

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

```

Packet 6. 1 client pkt(s), 5 server pkt(s), 1 turn(s). Click to select.

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

http-wiresharkdownload101.pcapng

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
21	0.420958	67.228.110.120	24.6.173.220	HTTP	532	
28	0.724717	2607:f0d0:2001:e:1:...	2002:1806:adcc::180...	HTTP	539	

HTTP/1.1 200 OK
Date: Sun, 24 Jul 2011 02:43:21 GMT
Server: Apache/2.2.14 (Ubuntu)
Vary: Host
Last-Modified: Wed, 20 Jul 2011 22:53:22 GMT
Accept-Ranges: bytes
Content-Length: 43
Link: <http://www.wireshark.org/image/ipv6.gif>;
X-Slogan: Sniff free or die.
Cache-control: public, max-age=600
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: image/gif

GIF89a.....!.....,.....D...;

The other message: Sniff free or die.

Task 4

ftp-clientside101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.101	10.251.30.69	TCP	66	52912 →
2	0.095003	10.251.30.69	192.168.0.101	TCP	66	21 → 52912
3	0.095124	192.168.0.101	10.251.30.69	TCP	54	52912 →
4	0.196274	10.251.30.69	192.168.0.101	FTP	74	Response
5	0.390919	192.168.0.101	10.251.30.69	TCP	54	52912 →

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: IntelCor_d0:27:d7 (00:18:de:d0:27:d7), Dst: D-LinkCo_cc:a3:ea (00:
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 10.251.30.69
Transmission Control Protocol, Src Port: 52912 (52912), Dst Port: 21 (21), Seq: 0, Len:

Wireshark · Follow TCP Stream (tcp.stream eq 1) · ftp-clientside101

pantheon.jpg

1 client pkt(s), 0 server pkt(s), 0 turn(s).

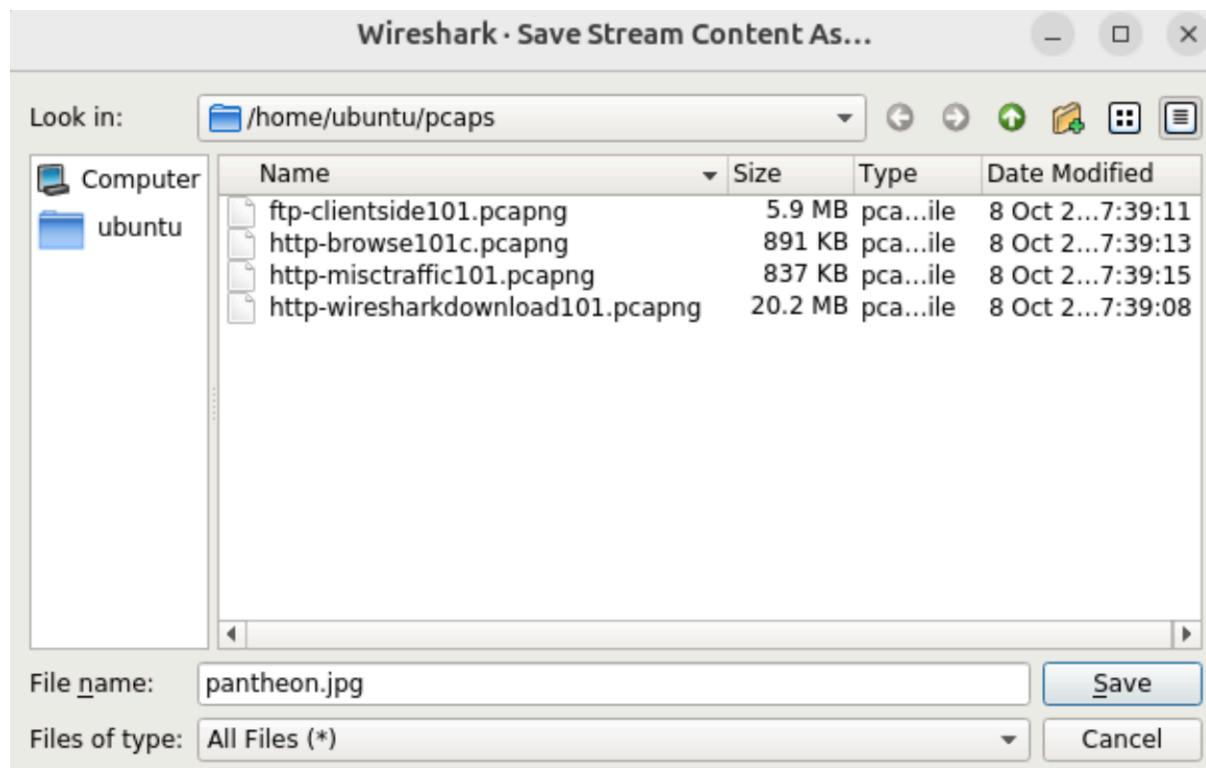
Entire conversation (14 bytes) Show data as ASCII Stream 1

Find: Find Next

Hide this stream Print Save as... Close Help

Wireshark · Follow TCP Stream (tcp.stream eq 2) · ftp-clientside101

```
....JFIF....H.H....!.Exif..II*....  
.....(.....  
1.....2.....i.....Canon.Canon EOS 5D...  
'.....  
..'.Adobe Photoshop CS2 Macintosh.2008:10:04  
11:56:39....."...".....@.....  
0221.....*.....>.....  
R.....Z.....  
b.....  
j.....r.....  
0100.....`.....z.....  
.....2008:05:09 08:23:09.2008:05:09 08:23:09.....  
.....
```



```
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-introspection/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/packet-introspection

```
student@Labtainer-VirtualBox:~/labtainer/labtainer-student$
```

