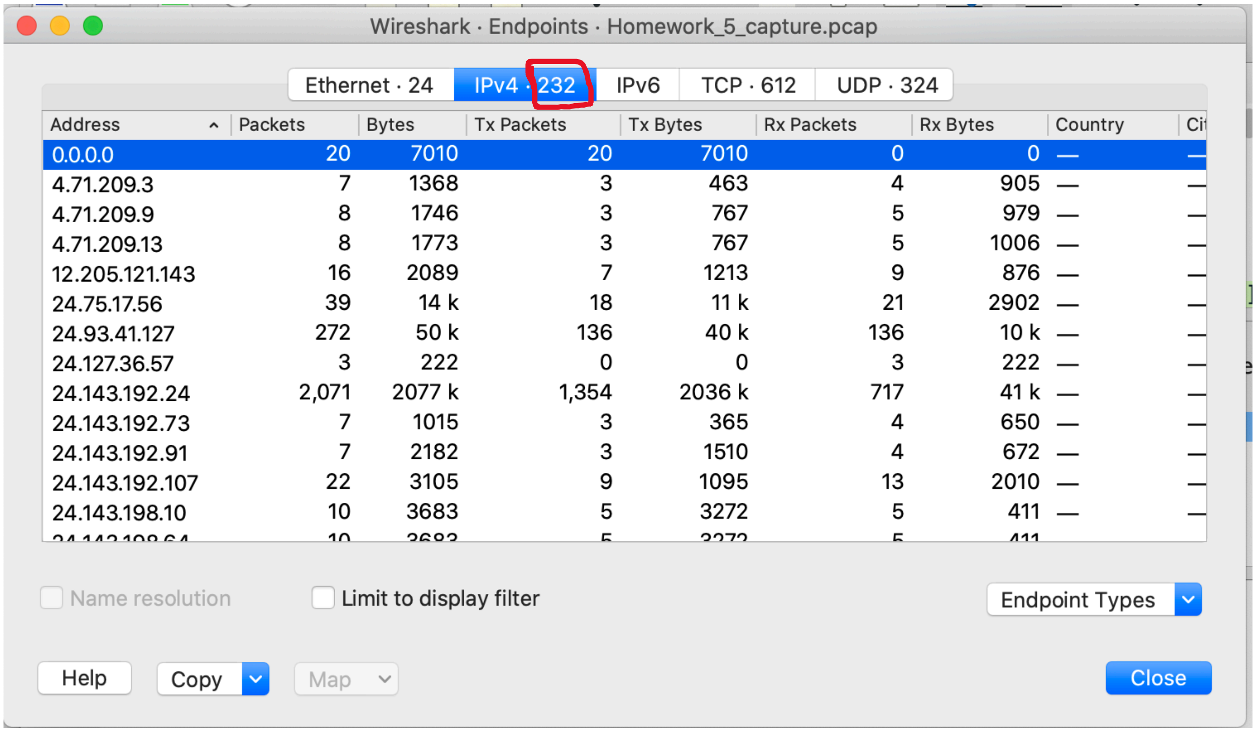
Hunter Donald
Hzd0011
COMP 5370
Homework 5

1) There are 232 unique IP addresses. This is found by going to statistics, then endpoints, then the IPv4 tab.

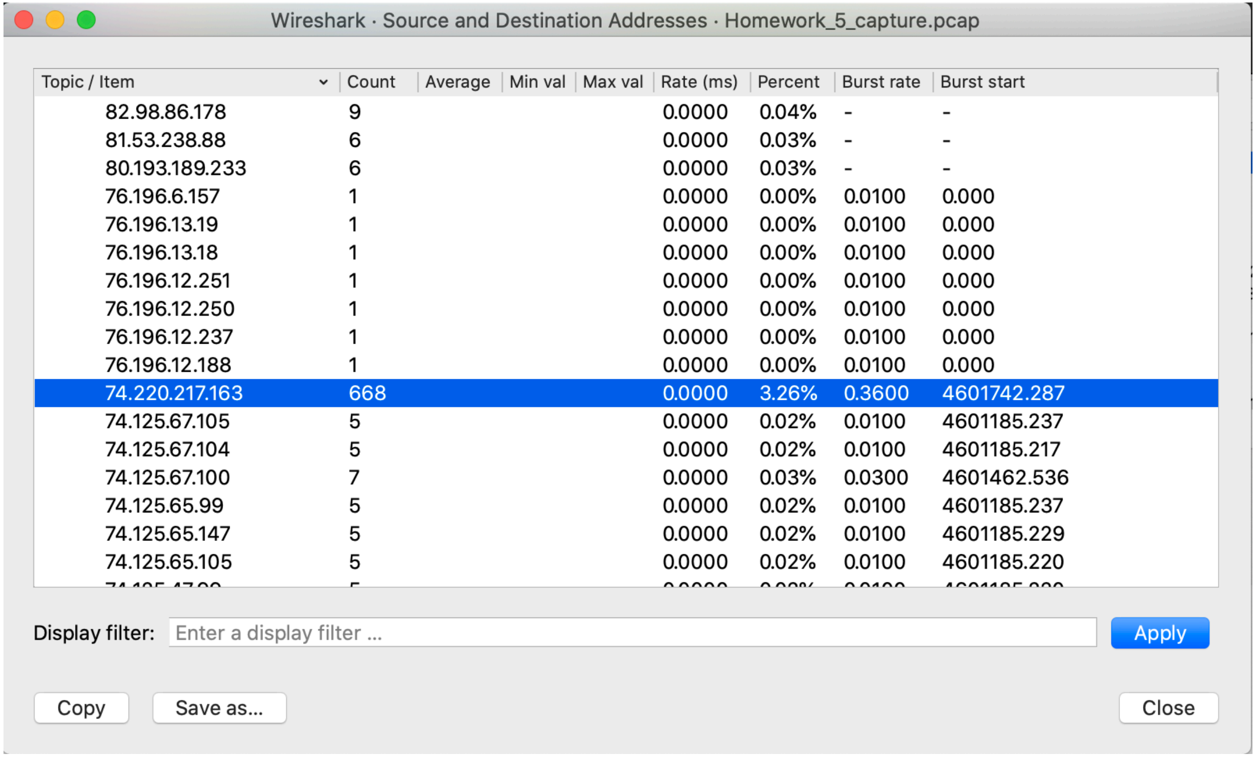


Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	Ci
0.0.0.0	20	7010	20	7010	0	0	—	—
4.71.209.3	7	1368	3	463	4	905	—	—
4.71.209.9	8	1746	3	767	5	979	—	—
4.71.209.13	8	1773	3	767	5	1006	—	—
12.205.121.143	16	2089	7	1213	9	876	—	—
24.75.17.56	39	14 k	18	11 k	21	2902	—	—
24.93.41.127	272	50 k	136	40 k	136	10 k	—	—
24.127.36.57	3	222	0	0	3	222	—	—
24.143.192.24	2,071	2077 k	1,354	2036 k	717	41 k	—	—
24.143.192.73	7	1015	3	365	4	650	—	—
24.143.192.91	7	2182	3	1510	4	672	—	—
24.143.192.107	22	3105	9	1095	13	2010	—	—
24.143.198.10	10	3683	5	3272	5	411	—	—
24.143.198.64	10	3683	5	3272	5	411		

☐ Name resolution
☐ Limit to display filter

Hunter Donald
Hzd0011
COMP 5370
Homework 5

2) For 74.220.217.163 as a source, there are 668 packets.



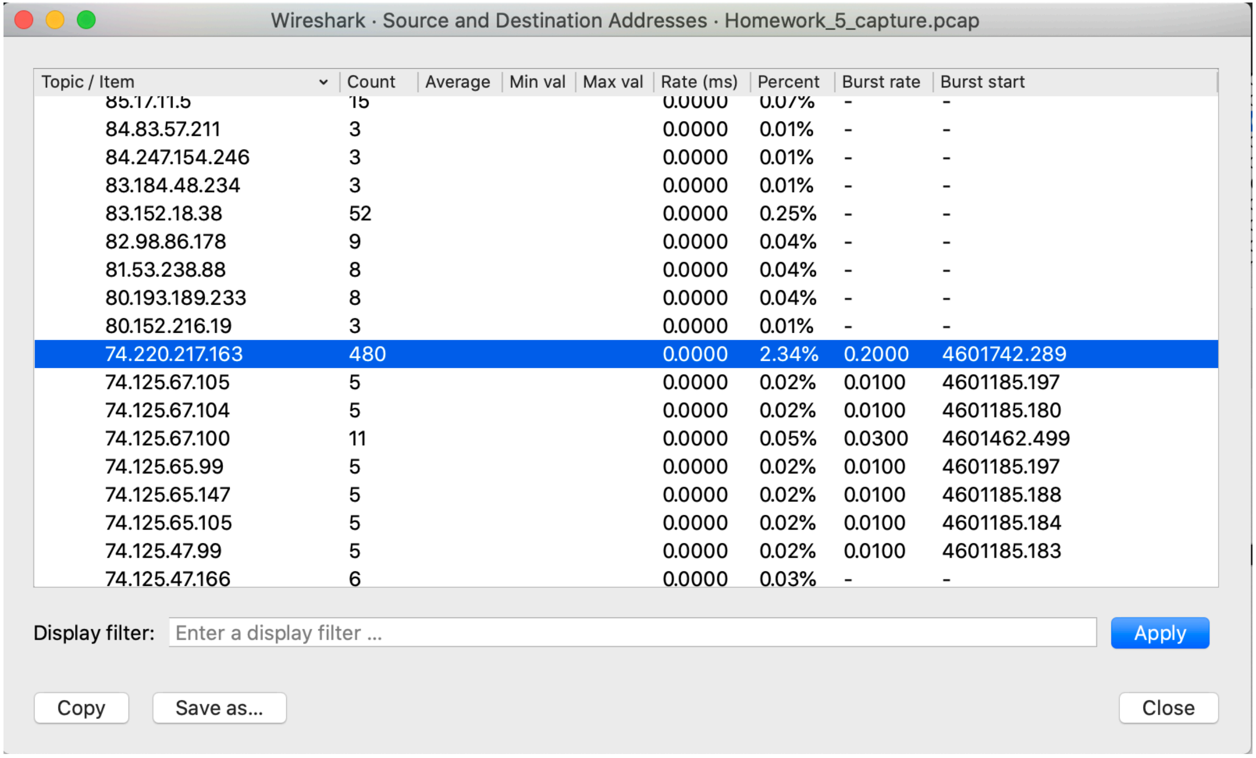
Wireshark · Source and Destination Addresses · Homework_5_capture.pcap

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
82.98.86.178	9				0.0000	0.04%	-	-
81.53.238.88	6				0.0000	0.03%	-	-
80.193.189.233	6				0.0000	0.03%	-	-
76.196.6.157	1				0.0000	0.00%	0.0100	0.000
76.196.13.19	1				0.0000	0.00%	0.0100	0.000
76.196.13.18	1				0.0000	0.00%	0.0100	0.000
76.196.12.251	1				0.0000	0.00%	0.0100	0.000
76.196.12.250	1				0.0000	0.00%	0.0100	0.000
76.196.12.237	1				0.0000	0.00%	0.0100	0.000
76.196.12.188	1				0.0000	0.00%	0.0100	0.000
74.220.217.163	668				0.0000	3.26%	0.3600	4601742.287
74.125.67.105	5				0.0000	0.02%	0.0100	4601185.237
74.125.67.104	5				0.0000	0.02%	0.0100	4601185.217
74.125.67.100	7				0.0000	0.03%	0.0300	4601462.536
74.125.65.99	5				0.0000	0.02%	0.0100	4601185.237
74.125.65.147	5				0.0000	0.02%	0.0100	4601185.229
74.125.65.105	5				0.0000	0.02%	0.0100	4601185.220

Display filter: Enter a display filter ...

Hunter Donald
Hzd0011
COMP 5370
Homework 5

For 74.220.217.163 as a destination, there are 480 packets.


Wireshark · Source and Destination Addresses · Homework_5_capture.pcap
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close

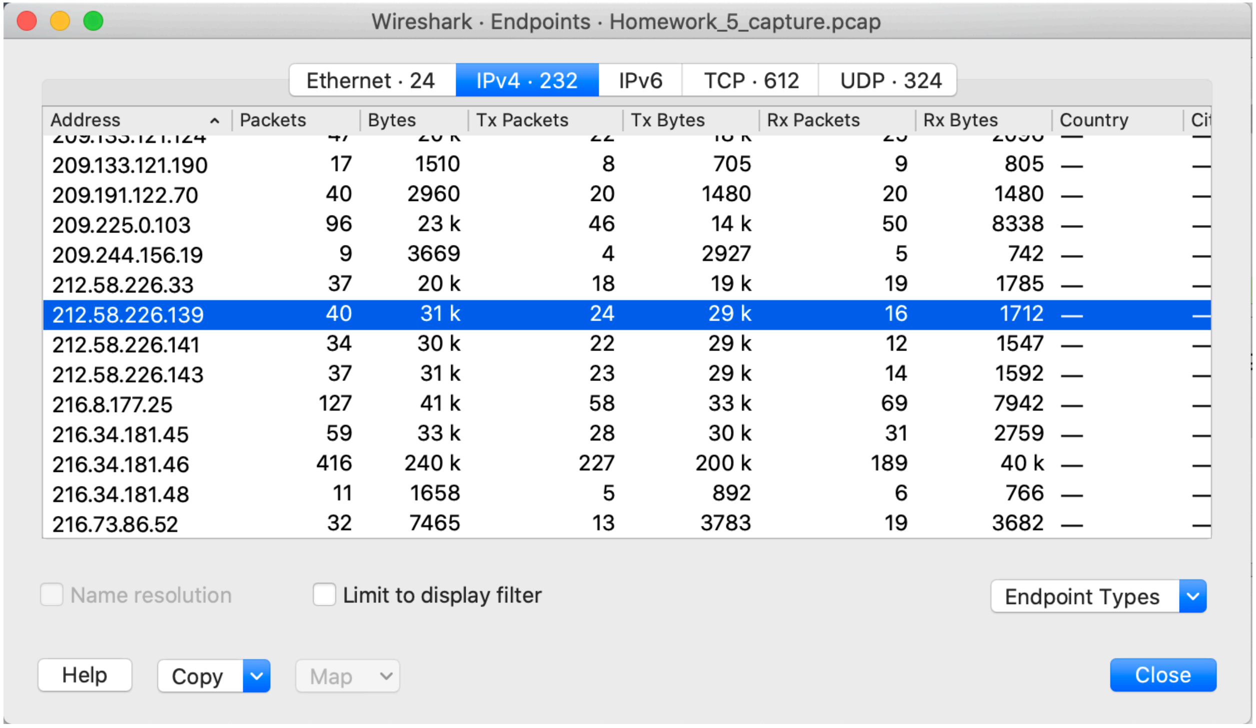
Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
85.17.11.5	15				0.0000	0.07%	-	-
84.83.57.211	3				0.0000	0.01%	-	-
84.247.154.246	3				0.0000	0.01%	-	-
83.184.48.234	3				0.0000	0.01%	-	-
83.152.18.38	52				0.0000	0.25%	-	-
82.98.86.178	9				0.0000	0.04%	-	-
81.53.238.88	8				0.0000	0.04%	-	-
80.193.189.233	8				0.0000	0.04%	-	-
80.152.216.19	3				0.0000	0.01%	-	-
74.220.217.163	480				0.0000	2.34%	0.2000	4601742.289
74.125.67.105	5				0.0000	0.02%	0.0100	4601185.197
74.125.67.104	5				0.0000	0.02%	0.0100	4601185.180
74.125.67.100	11				0.0000	0.05%	0.0300	4601462.499
74.125.65.99	5				0.0000	0.02%	0.0100	4601185.197
74.125.65.147	5				0.0000	0.02%	0.0100	4601185.188
74.125.65.105	5				0.0000	0.02%	0.0100	4601185.184
74.125.47.99	5				0.0000	0.02%	0.0100	4601185.183
74.125.47.166	6				0.0000	0.03%	-	-

This is found by going to statistics, then IPv4 statistics, then Source and Destination Addresses.

Hunter Donald
Hzd0011
COMP 5370
Homework 5

3)

There are 40 packets captured from 212.58.226.139. This was found by going to Statistics, then Endpoints, and find the IP address in question.



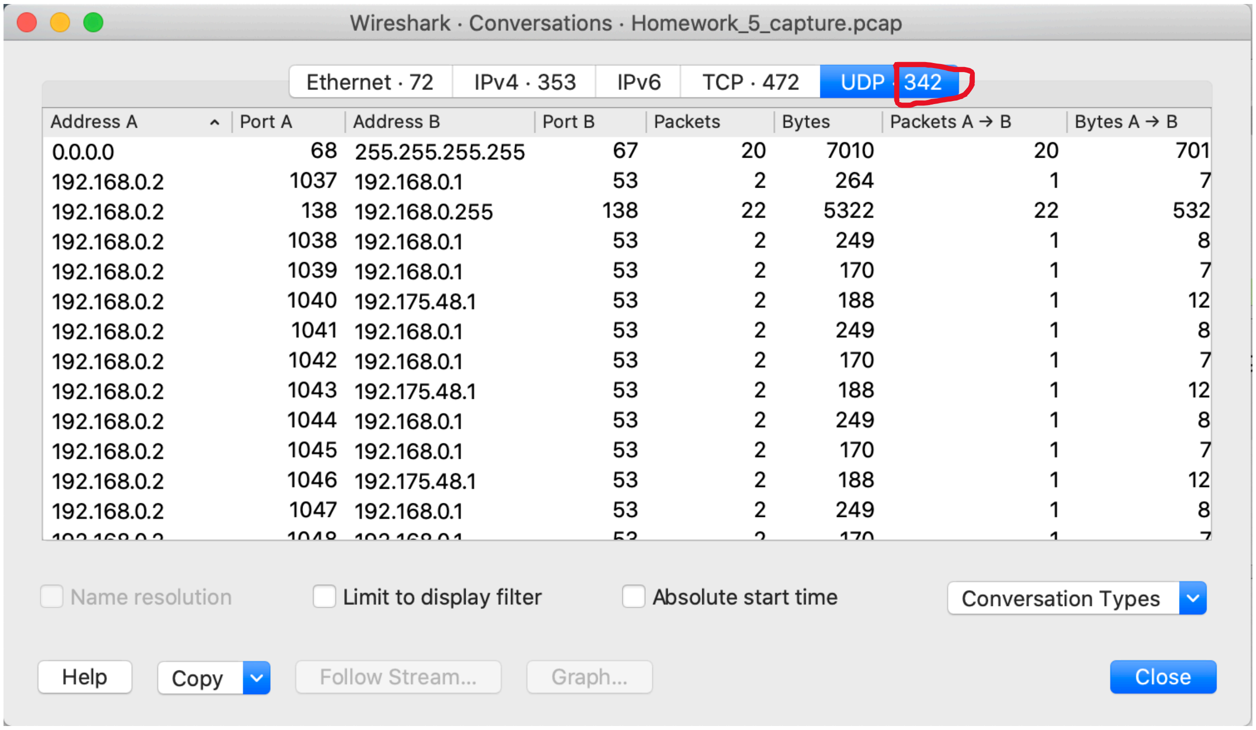
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	Ci
209.133.121.124	47	20 k	22	18 k	25	2096	—	—
209.133.121.190	17	1510	8	705	9	805	—	—
209.191.122.70	40	2960	20	1480	20	1480	—	—
209.225.0.103	96	23 k	46	14 k	50	8338	—	—
209.244.156.19	9	3669	4	2927	5	742	—	—
212.58.226.33	37	20 k	18	19 k	19	1785	—	—
212.58.226.139	40	31 k	24	29 k	16	1712	—	—
212.58.226.141	34	30 k	22	29 k	12	1547	—	—
212.58.226.143	37	31 k	23	29 k	14	1592	—	—
216.8.177.25	127	41 k	58	33 k	69	7942	—	—
216.34.181.45	59	33 k	28	30 k	31	2759	—	—
216.34.181.46	416	240 k	227	200 k	189	40 k	—	—
216.34.181.48	11	1658	5	892	6	766	—	—
216.73.86.52	32	7465	13	3783	19	3682	—	—

☐ Name resolution ☐ Limit to display filter

4) The "ip.addr == 192.168.0.0/24" filter will show the IP traffic that originated and was destined for the 192.168.0.0/24 network.

Hunter Donald
Hzd0011
COMP 5370
Homework 5

5) There are 342 UDP conversations. This is found by going to Statistics, Conversations, then the UDP tab.

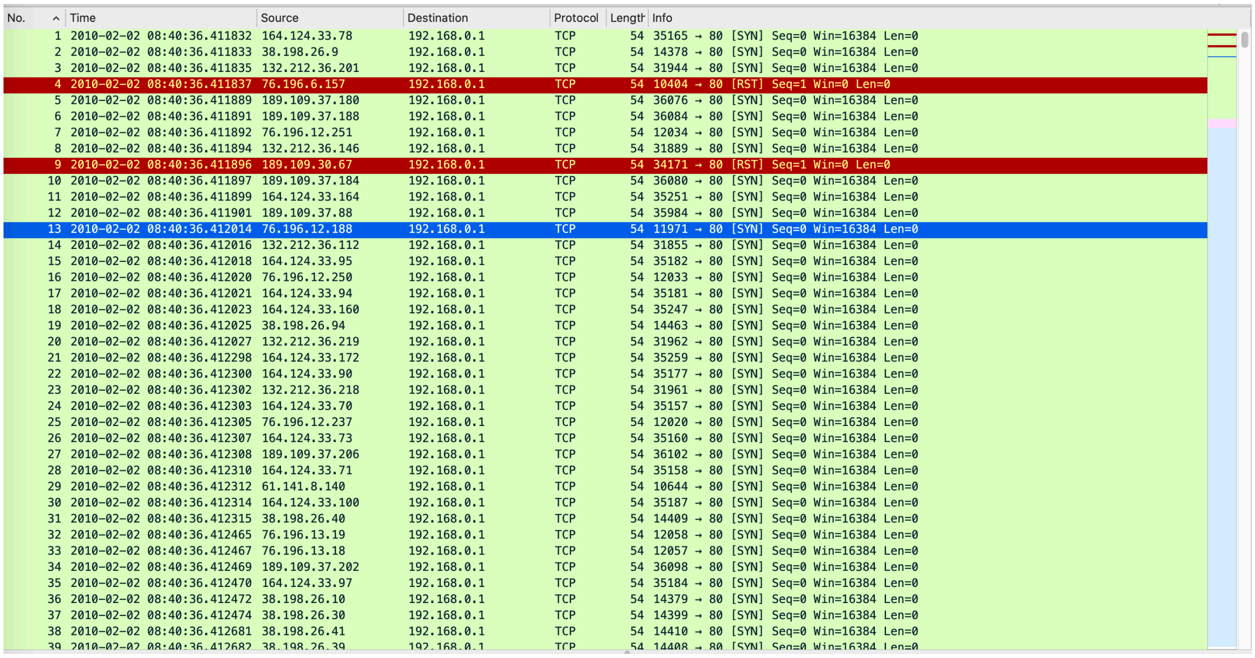


Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B
0.0.0.0	68	255.255.255.255	67	20	7010	20	701
192.168.0.2	1037	192.168.0.1	53	2	264	1	7
192.168.0.2	138	192.168.0.255	138	22	5322	22	532
192.168.0.2	1038	192.168.0.1	53	2	249	1	8
192.168.0.2	1039	192.168.0.1	53	2	170	1	7
192.168.0.2	1040	192.175.48.1	53	2	188	1	12
192.168.0.2	1041	192.168.0.1	53	2	249	1	8
192.168.0.2	1042	192.168.0.1	53	2	170	1	7
192.168.0.2	1043	192.175.48.1	53	2	188	1	12
192.168.0.2	1044	192.168.0.1	53	2	249	1	8
192.168.0.2	1045	192.168.0.1	53	2	170	1	7
192.168.0.2	1046	192.175.48.1	53	2	188	1	12
192.168.0.2	1047	192.168.0.1	53	2	249	1	8
192.168.0.2	1048	192.168.0.1	53	2	170	1	7

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Hunter Donald
Hzd0011
COMP 5370
Homework 5

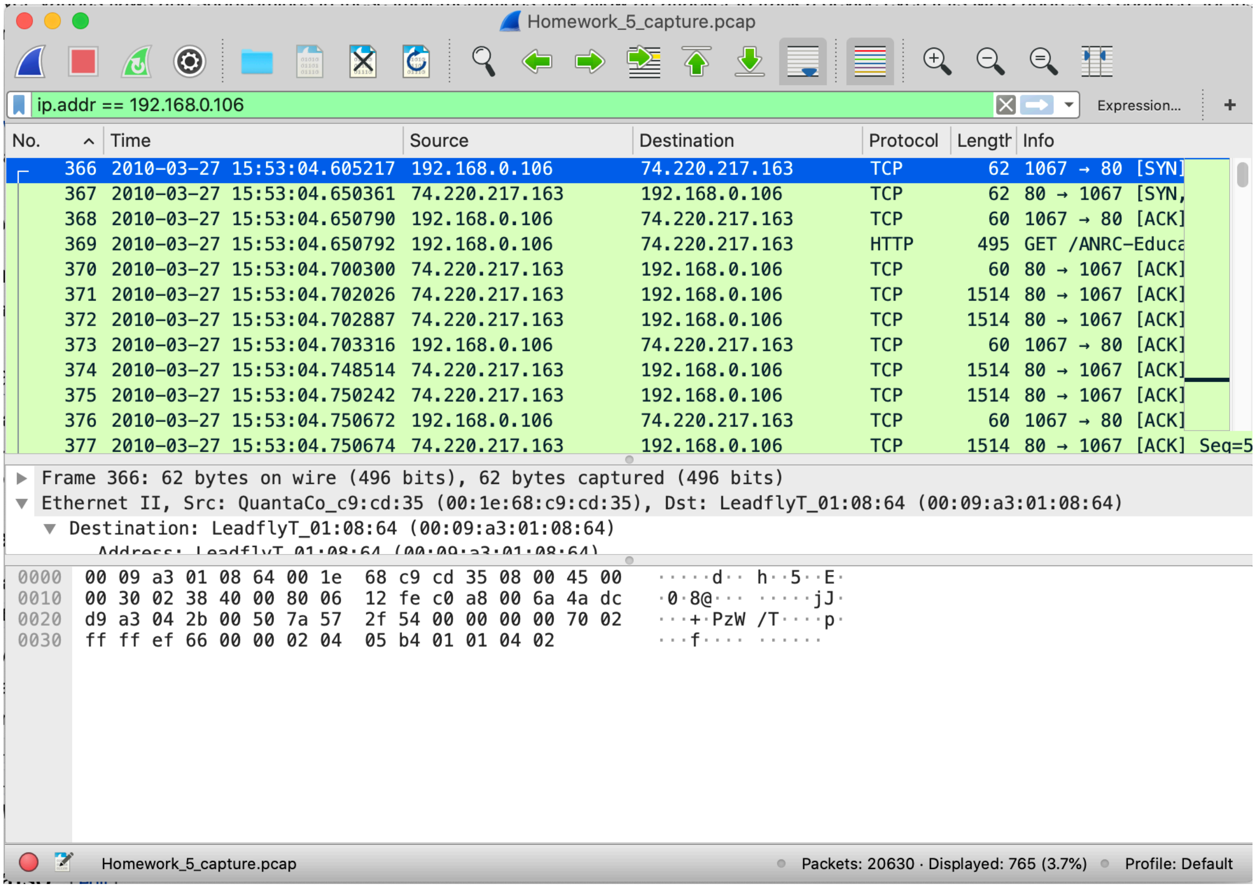
6) On the date 2010-02-02, there were 40 packets sent to host 192.168.0.1 all from different source IP addresses. Also, all of the packets were identical and sent at nearly the exact same time. Almost all of the packets were SYN packets which indicates that there was an attempted SYN Flood DoS attack on the host 192.168.0.1 on 2010-02-02 at around 08:40:36.



No.	Time	Source	Destination	Protocol	Length	Info
1	2010-02-02 08:40:36.411832	164.124.33.78	192.168.0.1	TCP	54	35165 → 80 [SYN] Seq=0 Win=16384 Len=0
2	2010-02-02 08:40:36.411833	38.198.26.9	192.168.0.1	TCP	54	14378 → 80 [SYN] Seq=0 Win=16384 Len=0
3	2010-02-02 08:40:36.411835	132.212.36.201	192.168.0.1	TCP	54	31944 → 80 [SYN] Seq=0 Win=16384 Len=0
4	2010-02-02 08:40:36.411837	76.196.6.157	192.168.0.1	TCP	54	10404 → 80 [RST] Seq=1 Win=0 Len=0
5	2010-02-02 08:40:36.411889	189.109.37.180	192.168.0.1	TCP	54	36076 → 80 [SYN] Seq=0 Win=16384 Len=0
6	2010-02-02 08:40:36.411891	189.109.37.188	192.168.0.1	TCP	54	36084 → 80 [SYN] Seq=0 Win=16384 Len=0
7	2010-02-02 08:40:36.411892	76.196.12.251	192.168.0.1	TCP	54	12034 → 80 [SYN] Seq=0 Win=16384 Len=0
8	2010-02-02 08:40:36.411894	132.212.36.146	192.168.0.1	TCP	54	31889 → 80 [SYN] Seq=0 Win=16384 Len=0
9	2010-02-02 08:40:36.411896	189.109.30.67	192.168.0.1	TCP	54	34171 → 80 [RST] Seq=1 Win=0 Len=0
10	2010-02-02 08:40:36.411897	189.109.37.184	192.168.0.1	TCP	54	36080 → 80 [SYN] Seq=0 Win=16384 Len=0
11	2010-02-02 08:40:36.411899	164.124.33.164	192.168.0.1	TCP	54	35251 → 80 [SYN] Seq=0 Win=16384 Len=0
12	2010-02-02 08:40:36.411901	189.109.37.88	192.168.0.1	TCP	54	35984 → 80 [SYN] Seq=0 Win=16384 Len=0
13	2010-02-02 08:40:36.412014	76.196.12.188	192.168.0.1	TCP	54	11971 → 80 [SYN] Seq=0 Win=16384 Len=0
14	2010-02-02 08:40:36.412016	132.212.36.112	192.168.0.1	TCP	54	31855 → 80 [SYN] Seq=0 Win=16384 Len=0
15	2010-02-02 08:40:36.412018	164.124.33.95	192.168.0.1	TCP	54	35182 → 80 [SYN] Seq=0 Win=16384 Len=0
16	2010-02-02 08:40:36.412020	76.196.12.250	192.168.0.1	TCP	54	12033 → 80 [SYN] Seq=0 Win=16384 Len=0
17	2010-02-02 08:40:36.412021	164.124.33.94	192.168.0.1	TCP	54	35181 → 80 [SYN] Seq=0 Win=16384 Len=0
18	2010-02-02 08:40:36.412023	164.124.33.160	192.168.0.1	TCP	54	35247 → 80 [SYN] Seq=0 Win=16384 Len=0
19	2010-02-02 08:40:36.412025	38.198.26.94	192.168.0.1	TCP	54	14463 → 80 [SYN] Seq=0 Win=16384 Len=0
20	2010-02-02 08:40:36.412027	132.212.36.219	192.168.0.1	TCP	54	31962 → 80 [SYN] Seq=0 Win=16384 Len=0
21	2010-02-02 08:40:36.412298	164.124.33.172	192.168.0.1	TCP	54	35259 → 80 [SYN] Seq=0 Win=16384 Len=0
22	2010-02-02 08:40:36.412300	164.124.33.90	192.168.0.1	TCP	54	35177 → 80 [SYN] Seq=0 Win=16384 Len=0
23	2010-02-02 08:40:36.412302	132.212.36.218	192.168.0.1	TCP	54	31961 → 80 [SYN] Seq=0 Win=16384 Len=0
24	2010-02-02 08:40:36.412303	164.124.33.70	192.168.0.1	TCP	54	35157 → 80 [SYN] Seq=0 Win=16384 Len=0
25	2010-02-02 08:40:36.412305	76.196.12.237	192.168.0.1	TCP	54	12020 → 80 [SYN] Seq=0 Win=16384 Len=0
26	2010-02-02 08:40:36.412307	164.124.33.73	192.168.0.1	TCP	54	35160 → 80 [SYN] Seq=0 Win=16384 Len=0
27	2010-02-02 08:40:36.412308	189.109.37.206	192.168.0.1	TCP	54	36102 → 80 [SYN] Seq=0 Win=16384 Len=0
28	2010-02-02 08:40:36.412310	164.124.33.71	192.168.0.1	TCP	54	35158 → 80 [SYN] Seq=0 Win=16384 Len=0
29	2010-02-02 08:40:36.412312	61.141.8.140	192.168.0.1	TCP	54	10644 → 80 [SYN] Seq=0 Win=16384 Len=0
30	2010-02-02 08:40:36.412314	164.124.33.100	192.168.0.1	TCP	54	35187 → 80 [SYN] Seq=0 Win=16384 Len=0
31	2010-02-02 08:40:36.412315	38.198.26.40	192.168.0.1	TCP	54	14409 → 80 [SYN] Seq=0 Win=16384 Len=0
32	2010-02-02 08:40:36.412465	76.196.13.19	192.168.0.1	TCP	54	12058 → 80 [SYN] Seq=0 Win=16384 Len=0
33	2010-02-02 08:40:36.412467	76.196.13.18	192.168.0.1	TCP	54	12057 → 80 [SYN] Seq=0 Win=16384 Len=0
34	2010-02-02 08:40:36.412469	189.109.37.202	192.168.0.1	TCP	54	36098 → 80 [SYN] Seq=0 Win=16384 Len=0
35	2010-02-02 08:40:36.412470	164.124.33.97	192.168.0.1	TCP	54	35184 → 80 [SYN] Seq=0 Win=16384 Len=0
36	2010-02-02 08:40:36.412472	38.198.26.10	192.168.0.1	TCP	54	14379 → 80 [SYN] Seq=0 Win=16384 Len=0
37	2010-02-02 08:40:36.412474	38.198.26.30	192.168.0.1	TCP	54	14399 → 80 [SYN] Seq=0 Win=16384 Len=0
38	2010-02-02 08:40:36.412681	38.198.26.41	192.168.0.1	TCP	54	14410 → 80 [SYN] Seq=0 Win=16384 Len=0
39	2010-02-02 08:40:36.412682	38.198.26.39	192.168.0.1	TCP	54	14408 → 80 [SYN] Seq=0 Win=16384 Len=0

Hunter Donald
Hzd0011
COMP 5370
Homework 5

7) By using the filter “ip.addr == 192.168.0.106” to find the IP address in question, then clicking on a packet with that IP address, then expanding Ethernet II and looking at source since 192.168.0.1 is the source for this packet, the MAC address is shown as 00:1e:68:c9:cd:35.



ip.addr == 192.168.0.106

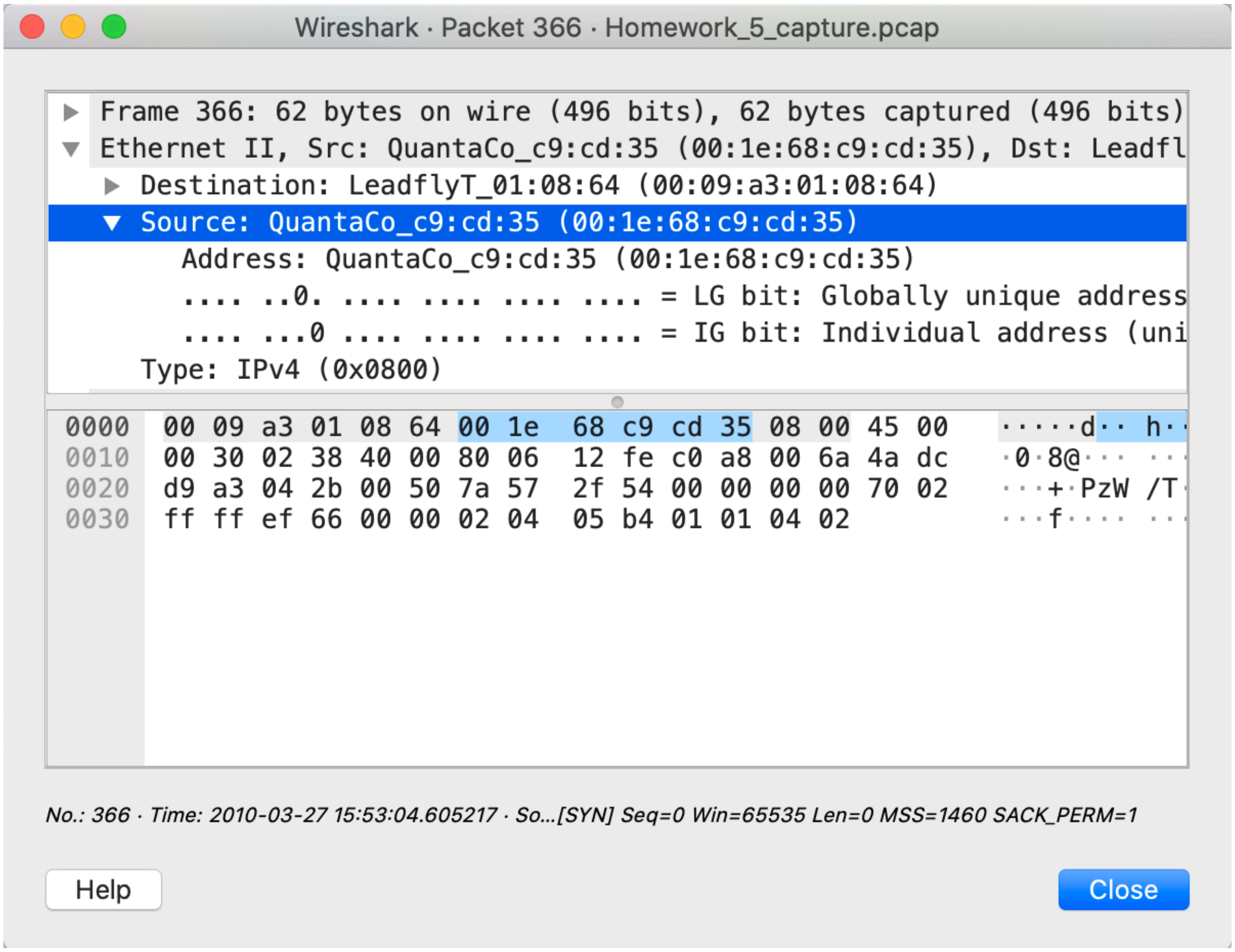
No.	Time	Source	Destination	Protocol	Length	Info
366	2010-03-27 15:53:04.605217	192.168.0.106	74.220.217.163	TCP	62	1067 → 80 [SYN]
367	2010-03-27 15:53:04.650361	74.220.217.163	192.168.0.106	TCP	62	80 → 1067 [SYN,
368	2010-03-27 15:53:04.650790	192.168.0.106	74.220.217.163	TCP	60	1067 → 80 [ACK]
369	2010-03-27 15:53:04.650792	192.168.0.106	74.220.217.163	HTTP	495	GET /ANRC-Educa
370	2010-03-27 15:53:04.700300	74.220.217.163	192.168.0.106	TCP	60	80 → 1067 [ACK]
371	2010-03-27 15:53:04.702026	74.220.217.163	192.168.0.106	TCP	1514	80 → 1067 [ACK]
372	2010-03-27 15:53:04.702887	74.220.217.163	192.168.0.106	TCP	1514	80 → 1067 [ACK]
373	2010-03-27 15:53:04.703316	192.168.0.106	74.220.217.163	TCP	60	1067 → 80 [ACK]
374	2010-03-27 15:53:04.748514	74.220.217.163	192.168.0.106	TCP	1514	80 → 1067 [ACK]
375	2010-03-27 15:53:04.750242	74.220.217.163	192.168.0.106	TCP	1514	80 → 1067 [ACK]
376	2010-03-27 15:53:04.750672	192.168.0.106	74.220.217.163	TCP	60	1067 → 80 [ACK]
377	2010-03-27 15:53:04.750674	74.220.217.163	192.168.0.106	TCP	1514	80 → 1067 [ACK] Seq=5

```
▶ Frame 366: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▼ Ethernet II, Src: QuantaCo_c9:cd:35 (00:1e:68:c9:cd:35), Dst: LeadflyT_01:08:64 (00:09:a3:01:08:64)
  ▼ Destination: LeadflyT_01:08:64 (00:09:a3:01:08:64)
      Address: LeadflyT_01:08:64 (00:09:a3:01:08:64)
```

```
0000  00 09 a3 01 08 64 00 1e  68 c9 cd 35 08 00 45 00   ·····d·· h··5··E·
0010  00 30 02 38 40 00 80 06  12 fe c0 a8 00 6a 4a dc   ·0·8@··· ·····jJ·
0020  d9 a3 04 2b 00 50 7a 57  2f 54 00 00 00 00 70 02   ···+·PzW /T····p·
0030  ff ff ef 66 00 00 02 04  05 b4 01 01 04 02         ···f···· ······
```

Homework_5_capture.pcap   Packets: 20630 · Displayed: 765 (3.7%)   Profile: Default

Hunter Donald
Hzd0011
COMP 5370
Homework 5



```
▶ Frame 366: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▼ Ethernet II, Src: QuantaCo_c9:cd:35 (00:1e:68:c9:cd:35), Dst: Leadfl
  ▶ Destination: LeadflyT_01:08:64 (00:09:a3:01:08:64)
  ▼ Source: QuantaCo_c9:cd:35 (00:1e:68:c9:cd:35)
      Address: QuantaCo_c9:cd:35 (00:1e:68:c9:cd:35)
      .... ..0. .... .... .... .... = LG bit: Globally unique address
      .... ...0 .... .... .... .... = IG bit: Individual address (uni
    Type: IPv4 (0x0800)

0000  00 09 a3 01 08 64 00 1e  68 c9 cd 35 08 00 45 00   ·····d·· h··
0010  00 30 02 38 40 00 80 06  12 fe c0 a8 00 6a 4a dc   ·0·8@··· ···
0020  d9 a3 04 2b 00 50 7a 57  2f 54 00 00 00 00 70 02   ···+·PzW /T·
0030  ff ff ef 66 00 00 02 04  05 b4 01 01 04 02         ···f···· ···
```

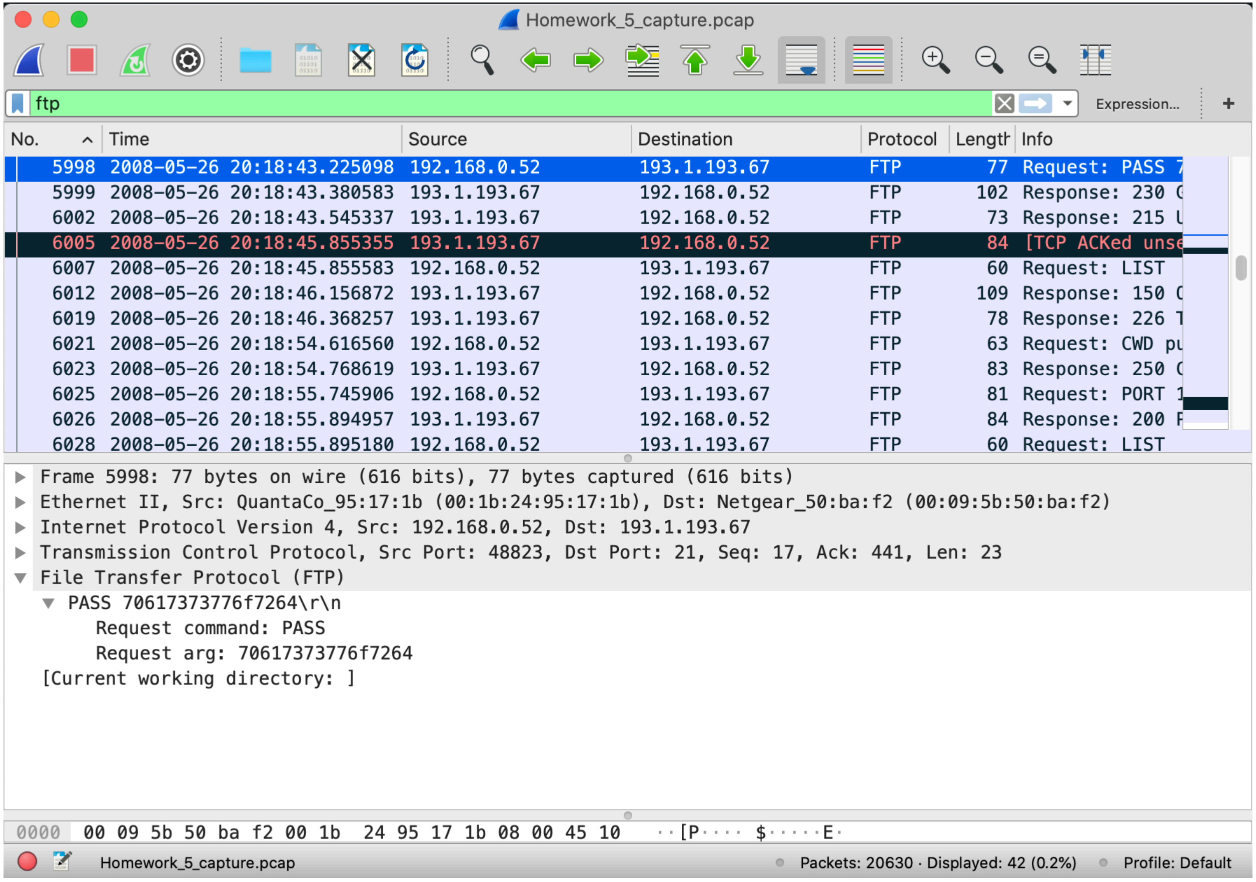
No.: 366 · Time: 2010-03-27 15:53:04.605217 · So...[SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1

8) There were two FTP sessions established. This was found by using the filter “ftp” and looking through the contents of the packets to see how many separate times the user actually connected to the FTP server. The user connected once, but quit before they logged in. Then they connected again, logged in, and performed some FTP commands before they quit again. Since the user quit twice, this means that there were two FTP sessions for the user to quit.

Hunter Donald
Hzd0011
COMP 5370
Homework 5

9)

The password used to login was 70617373776f7264 which is a hexadecimal value which translates to “password” in plain text. So, their password is “password”.



```
No.   ^ Time                        Source          Destination     Protocol Length Info
 5998 2008-05-26 20:18:43.225098 192.168.0.52   193.1.193.67   FTP          77 Request: PASS 7
 5999 2008-05-26 20:18:43.380583 193.1.193.67   192.168.0.52   FTP         102 Response: 230 (
 6002 2008-05-26 20:18:43.545337 193.1.193.67   192.168.0.52   FTP          73 Response: 215 U
 6005 2008-05-26 20:18:45.855355 193.1.193.67   192.168.0.52   FTP          84 [TCP ACKed unse
 6007 2008-05-26 20:18:45.855583 192.168.0.52   193.1.193.67   FTP          60 Request: LIST
 6012 2008-05-26 20:18:46.156872 193.1.193.67   192.168.0.52   FTP         109 Response: 150 (
 6019 2008-05-26 20:18:46.368257 193.1.193.67   192.168.0.52   FTP          78 Response: 226 T
 6021 2008-05-26 20:18:54.616560 192.168.0.52   193.1.193.67   FTP          63 Request: CWD pu
 6023 2008-05-26 20:18:54.768619 193.1.193.67   192.168.0.52   FTP          83 Response: 250 (
 6025 2008-05-26 20:18:55.745906 192.168.0.52   193.1.193.67   FTP          81 Request: PORT 1
 6026 2008-05-26 20:18:55.894957 193.1.193.67   192.168.0.52   FTP          84 Response: 200 F
 6028 2008-05-26 20:18:55.895180 192.168.0.52   193.1.193.67   FTP          60 Request: LIST
```

```
▶ Frame 5998: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
▶ Ethernet II, Src: QuantaCo_95:17:1b (00:1b:24:95:17:1b), Dst: Netgear_50:ba:f2 (00:09:5b:50:ba:f2)
▶ Internet Protocol Version 4, Src: 192.168.0.52, Dst: 193.1.193.67
▶ Transmission Control Protocol, Src Port: 48823, Dst Port: 21, Seq: 17, Ack: 441, Len: 23
▼ File Transfer Protocol (FTP)
  ▼ PASS 70617373776f7264\r\n
      Request command: PASS
      Request arg: 70617373776f7264
  [Current working directory: ]
```

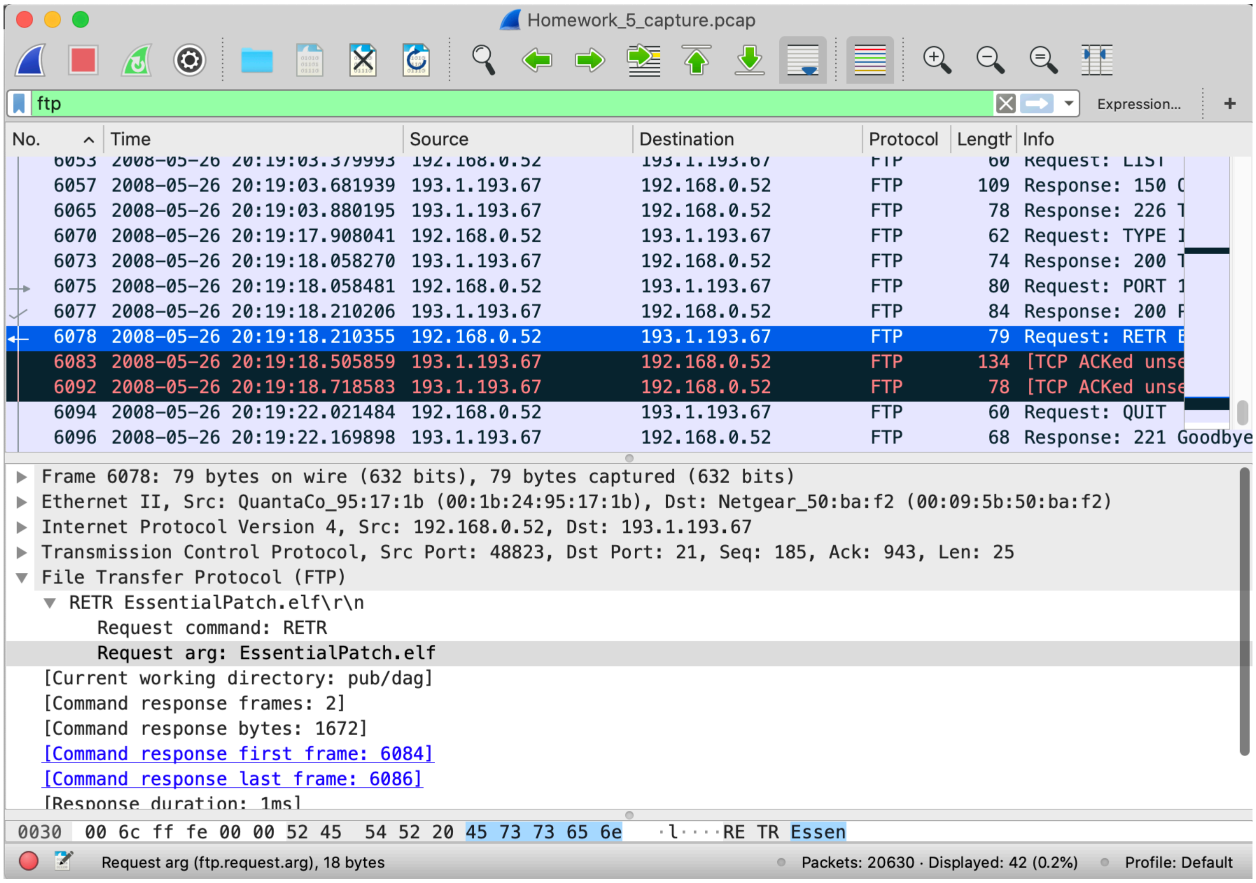
```
0000  00 09 5b 50 ba f2 00 1b  24 95 17 1b 08 00 45 10   ··[P····$·····E·
```

Homework_5_capture.pcap   Packets: 20630 · Displayed: 42 (0.2%)   Profile: Default

Hunter Donald
Hzd0011
COMP 5370
Homework 5

10)

The name of the file that was downloaded is “EssentialPatch.elf”.



Homework_5_capture.pcap

ftp

```
No.   Time                        Source          Destination     Protocol Length Info
6053  2008-05-26 20:19:03.379993  192.168.0.52    193.1.193.67    FTP       60 Request: LIST
6057  2008-05-26 20:19:03.681939  193.1.193.67    192.168.0.52    FTP      109 Response: 150 (
6065  2008-05-26 20:19:03.880195  193.1.193.67    192.168.0.52    FTP       78 Response: 226 T
6070  2008-05-26 20:19:17.908041  192.168.0.52    193.1.193.67    FTP       62 Request: TYPE I
6073  2008-05-26 20:19:18.058270  193.1.193.67    192.168.0.52    FTP       74 Response: 200 T
6075  2008-05-26 20:19:18.058481  192.168.0.52    193.1.193.67    FTP       80 Request: PORT 1
6077  2008-05-26 20:19:18.210206  193.1.193.67    192.168.0.52    FTP       84 Response: 200 P
6078  2008-05-26 20:19:18.210355  192.168.0.52    193.1.193.67    FTP       79 Request: RETR E
6083  2008-05-26 20:19:18.505859  193.1.193.67    192.168.0.52    FTP      134 [TCP ACKed unse
6092  2008-05-26 20:19:18.718583  193.1.193.67    192.168.0.52    FTP       78 [TCP ACKed unse
6094  2008-05-26 20:19:22.021484  192.168.0.52    193.1.193.67    FTP       60 Request: QUIT
6096  2008-05-26 20:19:22.169898  193.1.193.67    192.168.0.52    FTP       68 Response: 221 Goodbye
```

```
▶ Frame 6078: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
▶ Ethernet II, Src: QuantaCo_95:17:1b (00:1b:24:95:17:1b), Dst: Netgear_50:ba:f2 (00:09:5b:50:ba:f2)
▶ Internet Protocol Version 4, Src: 192.168.0.52, Dst: 193.1.193.67
▶ Transmission Control Protocol, Src Port: 48823, Dst Port: 21, Seq: 185, Ack: 943, Len: 25
▼ File Transfer Protocol (FTP)
  ▼ RETR EssentialPatch.elf\r\n
      Request command: RETR
      Request arg: EssentialPatch.elf
  [Current working directory: pub/dag]
  [Command response frames: 2]
  [Command response bytes: 1672]
  [Command response first frame: 6084]
  [Command response last frame: 6086]
  [Response duration: 1ms]
```

```
0030  00 6c ff fe 00 00 52 45  54 52 20 45 73 73 65 6e   ·l····RE TR Essen
```

Request arg (ftp.request.arg), 18 bytes   Packets: 20630 · Displayed: 42 (0.2%)   Profile: Default