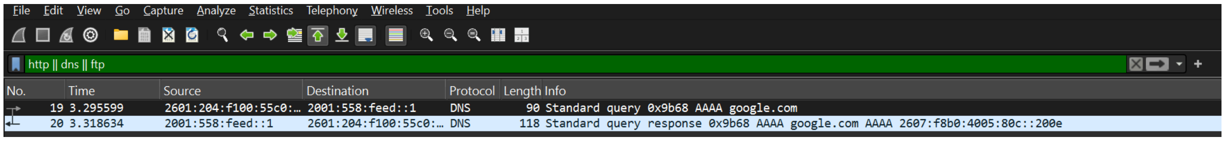
1. Alyssa Vallejo (918606017)
2. Isabel
3. Part 1A source code & PCAP files under folder Part1A: https://github.com/AV-CompSci-Mage/152AProject1.git

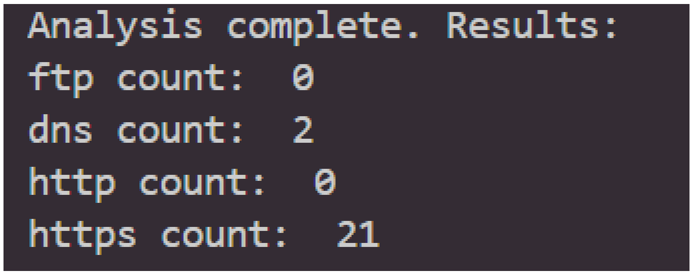
Part 1A Analysis:

1. List the different application layer protocols and their counts for each activity. In your report, specify how you figured out the protocol for each activity.
   For this assignment, I was only aware of a few different application layer protocols, such as HTTP, DNS, FTP, and SMTP (but this is only applicable for emails so we can ignore this protocol for this part). For this part of the analysis, I used the Wireshark filter to sort the traffic on protocols and the example code provided in week 1 discussion (however I did add to it to help with other questions). HTTP requests and responses go through port 80, DNS goes through port 53, and FTP goes through port 20 (for data). First I checked via the filter for HTTP || HTTP2 || HTTP3 || DNS || FTP, and if that did not show up, I checked via the demo code. Here is my analysis results for each activity:
   1. Ping google 20 times: two DNS protocols found via Wireshark and 21 HTTPS counts with my program



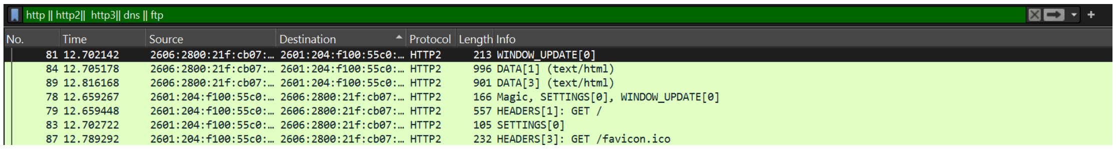
http || dns || ftp

No.	Time	Source	Destination	Protocol	Length	Info
19	3.295599	2601:204:f100:55c0:…	2001:558:feed::1	DNS	90	Standard query 0x9b68 AAAA google.com
20	3.318634	2001:558:feed::1	2601:204:f100:55c0:…	DNS	118	Standard query response 0x9b68 AAAA google.com AAAA 2607:f8b0:4005:80c::200e



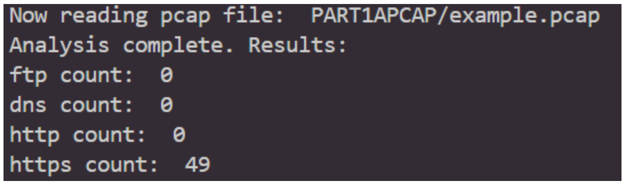
```
Analysis complete. Results:
ftp count:  0
dns count:  2
http count:  0
https count:  21
```

   2. Visiting https://example.com: seven HTTP2 protocols found via Wireshark, although some of might be from other programs running on the background, such as the WINDOW_UPDATE[0] line. I also found 49 HTTPS protocols.



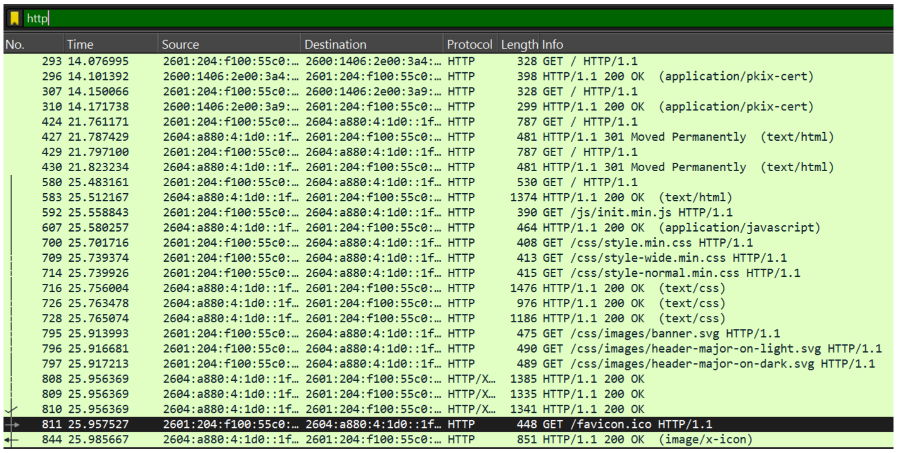
http || http2|| http3|| dns || ftp

No.	Time	Source	Destination	Protocol	Length	Info
81	12.702142	2606:2800:21f:cb07:…	2601:204:f100:55c0:…	HTTP2	213	WINDOW_UPDATE[0]
84	12.705178	2606:2800:21f:cb07:…	2601:204:f100:55c0:…	HTTP2	996	DATA[1] (text/html)
89	12.816168	2606:2800:21f:cb07:…	2601:204:f100:55c0:…	HTTP2	901	DATA[3] (text/html)
78	12.659267	2601:204:f100:55c0:…	2606:2800:21f:cb07:…	HTTP2	166	Magic, SETTINGS[0], WINDOW_UPDATE[0]
79	12.659448	2601:204:f100:55c0:…	2606:2800:21f:cb07:…	HTTP2	557	HEADERS[1]: GET /
83	12.702722	2601:204:f100:55c0:…	2606:2800:21f:cb07:…	HTTP2	105	SETTINGS[0]
87	12.789292	2601:204:f100:55c0:…	2606:2800:21f:cb07:…	HTTP2	232	HEADERS[3]: GET /favicon.ico



```
Now reading pcap file:  PART1APCAP/example.pcap
Analysis complete. Results:
ftp count:  0
dns count:  0
http count:  0
https count:  49
```

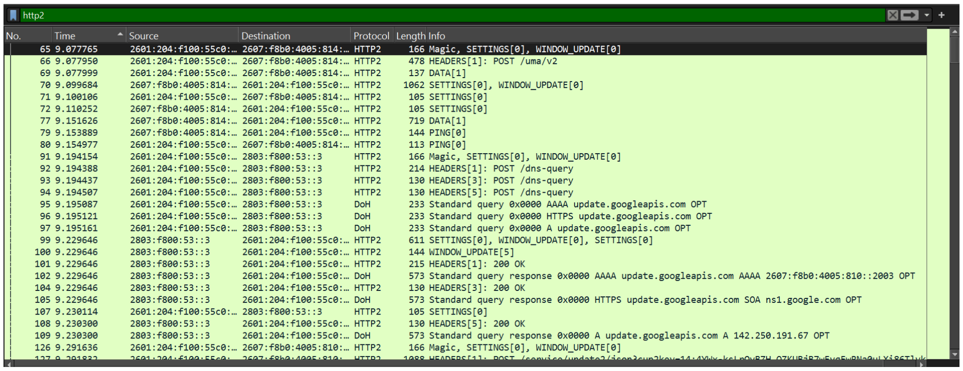
3. Visiting http://httpforever.com: 26 HTTP protocols



http

No.	Time	Source	Destination	Protocol	Length	Info
293	14.076995	2601:204:f100:55c0:…	2600:1406:2e00:3a4:…	HTTP	328	GET / HTTP/1.1
296	14.101392	2600:1406:2e00:3a4:…	2601:204:f100:55c0:…	HTTP	398	HTTP/1.1 200 OK (application/pkix-cert)
307	14.150066	2601:204:f100:55c0:…	2600:1406:2e00:3a9:…	HTTP	328	GET / HTTP/1.1
310	14.171738	2600:1406:2e00:3a9:…	2601:204:f100:55c0:…	HTTP	299	HTTP/1.1 200 OK (application/pkix-cert)
424	21.761171	2601:204:f100:55c0:…	2604:a880:4:1d0::1f…	HTTP	787	GET / HTTP/1.1
427	21.787429	2604:a880:4:1d0::1f…	2601:204:f100:55c0:…	HTTP	481	HTTP/1.1 301 Moved Permanently (text/html)
429	21.797100	2601:204:f100:55c0:…	2604:a880:4:1d0::1f…	HTTP	787	GET / HTTP/1.1
430	21.823234	2604:a880:4:1d0::1f…	2601:204:f100:55c0:…	HTTP	481	HTTP/1.1 301 Moved Permanently (text/html)
580	25.483161	2601:204:f100:55c0:…	2604:a880:4:1d0::1f…	HTTP	530	GET / HTTP/1.1
583	25.512167	2604:a880:4:1d0::1f…	2601:204:f100:55c0:…	HTTP	1374	HTTP/1.1 200 OK (text/html)
592	25.558843	2601:204:f100:55c0:…	2604:a880:4:1d0::1f…	HTTP	390	GET /js/init.min.js HTTP/1.1
607	25.580257	2604:a880:4:1d0::1f…	2601:204:f100:55c0:…	HTTP	464	HTTP/1.1 200 OK (application/javascript)
700	25.701716	2601:204:f100:55c0:…	2604:a880:4:1d0::1f…	HTTP	408	GET /css/style.min.css HTTP/1.1
709	25.739374	2601:204:f100:55c0:…	2604:a880:4:1d0::1f…	HTTP	413	GET /css/style-wide.min.css HTTP/1.1
714	25.739926	2601:204:f100:55c0:…	2604:a880:4:1d0::1f…	HTTP	415	GET /css/style-normal.min.css HTTP/1.1
716	25.756004	2604:a880:4:1d0::1f…	2601:204:f100:55c0:…	HTTP	1476	HTTP/1.1 200 OK (text/css)
726	25.763478	2604:a880:4:1d0::1f…	2601:204:f100:55c0:…	HTTP	976	HTTP/1.1 200 OK (text/css)
728	25.765074	2604:a880:4:1d0::1f…	2601:204:f100:55c0:…	HTTP	1186	HTTP/1.1 200 OK (text/css)
795	25.913993	2601:204:f100:55c0:…	2604:a880:4:1d0::1f…	HTTP	475	GET /css/images/banner.svg HTTP/1.1
796	25.916681	2601:204:f100:55c0:…	2604:a880:4:1d0::1f…	HTTP	490	GET /css/images/header-major-on-light.svg HTTP/1.1
797	25.917213	2601:204:f100:55c0:…	2604:a880:4:1d0::1f…	HTTP	489	GET /css/images/header-major-on-dark.svg HTTP/1.1
808	25.956369	2604:a880:4:1d0::1f…	2601:204:f100:55c0:…	HTTP/X…	1385	HTTP/1.1 200 OK
809	25.956369	2604:a880:4:1d0::1f…	2601:204:f100:55c0:…	HTTP/X…	1335	HTTP/1.1 200 OK
810	25.956369	2604:a880:4:1d0::1f…	2601:204:f100:55c0:…	HTTP/X…	1341	HTTP/1.1 200 OK
811	25.957527	2601:204:f100:55c0:…	2604:a880:4:1d0::1f…	HTTP	448	GET /favicon.ico HTTP/1.1
844	25.985667	2604:a880:4:1d0::1f…	2601:204:f100:55c0:…	HTTP	851	HTTP/1.1 200 OK (image/x-icon)

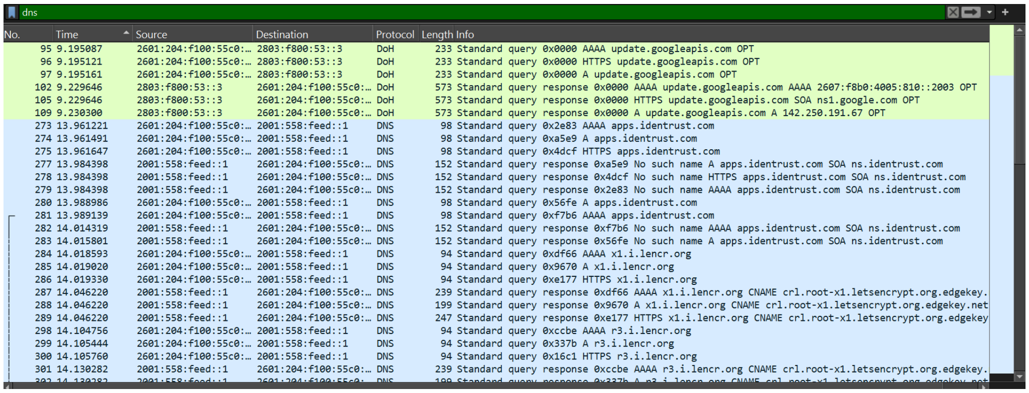
Over 50+ entries for HTTP2



http2

No.	Time	Source	Destination	Protocol	Length	Info
65	9.077765	2601:204:f100:55c0:…	2607:f8b0:4005:814:…	HTTP2	166	Magic, SETTINGS[0], WINDOW_UPDATE[0]
66	9.077950	2601:204:f100:55c0:…	2607:f8b0:4005:814:…	HTTP2	478	HEADERS[1]: POST /uma/v2
69	9.077999	2601:204:f100:55c0:…	2607:f8b0:4005:814:…	HTTP2	137	DATA[1]
70	9.099684	2607:f8b0:4005:814:…	2601:204:f100:55c0:…	HTTP2	1062	SETTINGS[0], WINDOW_UPDATE[0]
71	9.100106	2601:204:f100:55c0:…	2607:f8b0:4005:814:…	HTTP2	105	SETTINGS[0]
72	9.110252	2607:f8b0:4005:814:…	2601:204:f100:55c0:…	HTTP2	105	SETTINGS[0]
77	9.151626	2607:f8b0:4005:814:…	2601:204:f100:55c0:…	HTTP2	719	DATA[1]
79	9.153889	2607:f8b0:4005:814:…	2601:204:f100:55c0:…	HTTP2	144	PING[0]
80	9.154977	2601:204:f100:55c0:…	2607:f8b0:4005:814:…	HTTP2	113	PING[0]
91	9.194154	2601:204:f100:55c0:…	2803:f800:53::3	HTTP2	166	Magic, SETTINGS[0], WINDOW_UPDATE[0]
92	9.194388	2601:204:f100:55c0:…	2803:f800:53::3	HTTP2	214	HEADERS[1]: POST /dns-query
93	9.194437	2601:204:f100:55c0:…	2803:f800:53::3	HTTP2	130	HEADERS[3]: POST /dns-query
94	9.194507	2601:204:f100:55c0:…	2803:f800:53::3	HTTP2	130	HEADERS[5]: POST /dns-query
95	9.195087	2601:204:f100:55c0:…	2803:f800:53::3	DoH	233	Standard query 0x0000 AAAA update.googleapis.com OPT
96	9.195121	2601:204:f100:55c0:…	2803:f800:53::3	DoH	233	Standard query 0x0000 HTTPS update.googleapis.com OPT
97	9.195161	2601:204:f100:55c0:…	2803:f800:53::3	DoH	233	Standard query 0x0000 A update.googleapis.com OPT
99	9.229646	2803:f800:53::3	2601:204:f100:55c0:…	HTTP2	611	SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]
100	9.229646	2803:f800:53::3	2601:204:f100:55c0:…	HTTP2	144	WINDOW_UPDATE[5]
101	9.229646	2803:f800:53::3	2601:204:f100:55c0:…	HTTP2	215	HEADERS[1]: 200 OK
102	9.229646	2803:f800:53::3	2601:204:f100:55c0:…	DoH	573	Standard query response 0x0000 AAAA update.googleapis.com AAAA 2607:f8b0:4005:810::2003 OPT
104	9.229646	2803:f800:53::3	2601:204:f100:55c0:…	HTTP2	130	HEADERS[3]: 200 OK
105	9.229646	2803:f800:53::3	2601:204:f100:55c0:…	DoH	573	Standard query response 0x0000 HTTPS update.googleapis.com SOA ns1.google.com OPT
107	9.230114	2601:204:f100:55c0:…	2803:f800:53::3	HTTP2	105	SETTINGS[0]
108	9.230300	2803:f800:53::3	2601:204:f100:55c0:…	HTTP2	130	HEADERS[5]: 200 OK
109	9.230300	2803:f800:53::3	2601:204:f100:55c0:…	DoH	573	Standard query response 0x0000 A update.googleapis.com A 142.250.191.67 OPT
126	9.291636	2601:204:f100:55c0:…	2607:f8b0:4005:810:…	HTTP2	166	Magic, SETTINGS[0], WINDOW_UPDATE[0]

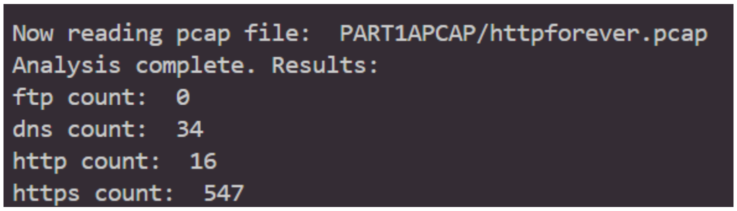
34 DNS protocols



dns

No.	Time	Source	Destination	Protocol	Length	Info
95	9.195087	2601:204:f100:55c0:…	2803:f800:53::3	DoH	233	Standard query 0x0000 AAAA update.googleapis.com OPT
96	9.195121	2601:204:f100:55c0:…	2803:f800:53::3	DoH	233	Standard query 0x0000 HTTPS update.googleapis.com OPT
97	9.195161	2601:204:f100:55c0:…	2803:f800:53::3	DoH	233	Standard query 0x0000 A update.googleapis.com OPT
102	9.229646	2803:f800:53::3	2601:204:f100:55c0:…	DoH	573	Standard query response 0x0000 AAAA update.googleapis.com AAAA 2607:f8b0:4005:810::2003 OPT
105	9.229646	2803:f800:53::3	2601:204:f100:55c0:…	DoH	573	Standard query response 0x0000 HTTPS update.googleapis.com SOA ns1.google.com OPT
109	9.230300	2803:f800:53::3	2601:204:f100:55c0:…	DoH	573	Standard query response 0x0000 A update.googleapis.com A 142.250.191.67 OPT
273	13.961221	2601:204:f100:55c0:…	2001:558:feed::1	DNS	98	Standard query 0x2e83 AAAA apps.identrust.com
274	13.961491	2601:204:f100:55c0:…	2001:558:feed::1	DNS	98	Standard query 0xa5e9 A apps.identrust.com
275	13.961647	2601:204:f100:55c0:…	2001:558:feed::1	DNS	98	Standard query 0x4dcf HTTPS apps.identrust.com
277	13.984398	2001:558:feed::1	2601:204:f100:55c0:…	DNS	152	Standard query response 0xa5e9 No such name A apps.identrust.com SOA ns.identrust.com
278	13.984398	2001:558:feed::1	2601:204:f100:55c0:…	DNS	152	Standard query response 0x4dcf No such name HTTPS apps.identrust.com SOA ns.identrust.com
279	13.984398	2001:558:feed::1	2601:204:f100:55c0:…	DNS	152	Standard query response 0x2e83 No such name AAAA apps.identrust.com SOA ns.identrust.com
280	13.988986	2601:204:f100:55c0:…	2001:558:feed::1	DNS	98	Standard query 0x56fe A apps.identrust.com
281	13.989139	2601:204:f100:55c0:…	2001:558:feed::1	DNS	98	Standard query 0xf7b6 AAAA apps.identrust.com
282	14.014319	2001:558:feed::1	2601:204:f100:55c0:…	DNS	152	Standard query response 0xf7b6 No such name AAAA apps.identrust.com SOA ns.identrust.com
283	14.015801	2001:558:feed::1	2601:204:f100:55c0:…	DNS	152	Standard query response 0x56fe No such name A apps.identrust.com SOA ns.identrust.com
284	14.018593	2601:204:f100:55c0:…	2001:558:feed::1	DNS	94	Standard query 0xdf66 AAAA x1.i.lencr.org
285	14.019020	2601:204:f100:55c0:…	2001:558:feed::1	DNS	94	Standard query 0x9670 A x1.i.lencr.org
286	14.019330	2601:204:f100:55c0:…	2001:558:feed::1	DNS	94	Standard query 0xe177 HTTPS x1.i.lencr.org
287	14.046220	2001:558:feed::1	2601:204:f100:55c0:…	DNS	239	Standard query response 0xdf66 AAAA x1.i.lencr.org CNAME crl.root-x1.letsencrypt.org.edgekey.
288	14.046220	2001:558:feed::1	2601:204:f100:55c0:…	DNS	199	Standard query response 0x9670 A x1.i.lencr.org CNAME crl.root-x1.letsencrypt.org.edgekey.net
289	14.046220	2001:558:feed::1	2601:204:f100:55c0:…	DNS	247	Standard query response 0xe177 HTTPS x1.i.lencr.org CNAME crl.root-x1.letsencrypt.org.edgekey
298	14.104756	2601:204:f100:55c0:…	2001:558:feed::1	DNS	94	Standard query 0xccbe AAAA r3.i.lencr.org
299	14.105444	2601:204:f100:55c0:…	2001:558:feed::1	DNS	94	Standard query 0x337b A r3.i.lencr.org
300	14.105760	2601:204:f100:55c0:…	2001:558:feed::1	DNS	94	Standard query 0x16c1 HTTPS r3.i.lencr.org
301	14.130282	2001:558:feed::1	2601:204:f100:55c0:…	DNS	239	Standard query response 0xccbe AAAA r3.i.lencr.org CNAME crl.root-x1.letsencrypt.org.edgekey.

Also, from my code I found that there were exactly 16 http protocols, 34 DNS protocols, and 547 https protocols!

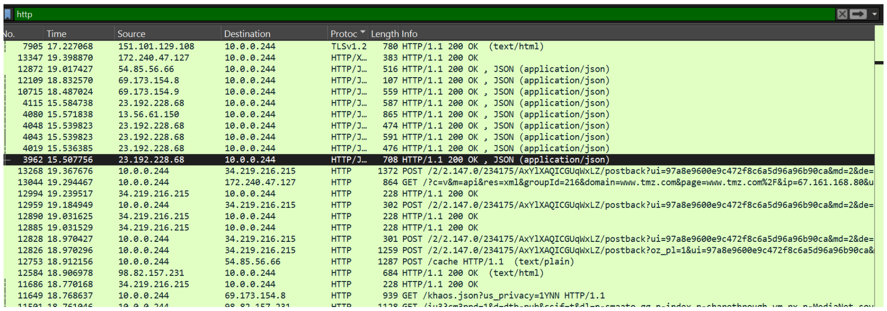


```
Now reading pcap file:  PART1APCAP/httpforever.pcap
Analysis complete. Results:
ftp count:  0
dns count:  34
http count:  16
https count:  547
```

I am not sure why my Wireshark and program differ in http counts, but perhaps Wireshark is counting HTTP protocols even if they are not coming from port 80.

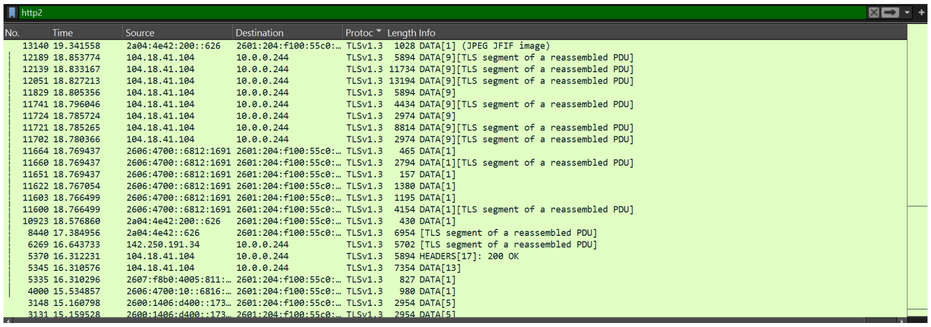
4. Visiting https://www.tmz.com

More than 50+ HTTP protocols



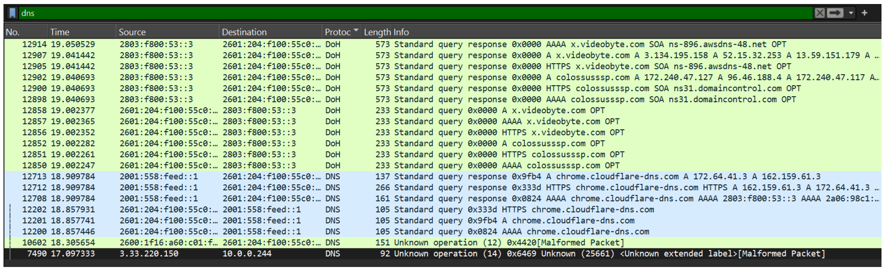
```
http
No.    Time      Source          Destination     Protoc  Length Info
 7905 17.227068  151.101.129.108 10.0.0.244      TLSv1.2   780 HTTP/1.1 200 OK  (text/html)
13347 19.398870  172.240.47.127  10.0.0.244      HTTP/X…   383 HTTP/1.1 200 OK
12872 19.017427  54.85.56.66     10.0.0.244      HTTP/J…   516 HTTP/1.1 200 OK , JSON (application/json)
12109 18.832570  69.173.154.8    10.0.0.244      HTTP/J…   107 HTTP/1.1 200 OK , JSON (application/json)
10715 18.487024  69.173.154.9    10.0.0.244      HTTP/J…   559 HTTP/1.1 200 OK , JSON (application/json)
 4115 15.584738  23.192.228.68   10.0.0.244      HTTP/J…   587 HTTP/1.1 200 OK , JSON (application/json)
 4080 15.571838  13.56.61.150    10.0.0.244      HTTP/J…   865 HTTP/1.1 200 OK , JSON (application/json)
 4048 15.539823  23.192.228.68   10.0.0.244      HTTP/J…   474 HTTP/1.1 200 OK , JSON (application/json)
 4043 15.539823  23.192.228.68   10.0.0.244      HTTP/J…   591 HTTP/1.1 200 OK , JSON (application/json)
 4019 15.536385  23.192.228.68   10.0.0.244      HTTP/J…   476 HTTP/1.1 200 OK , JSON (application/json)
 3962 15.507756  23.192.228.68   10.0.0.244      HTTP/J…   708 HTTP/1.1 200 OK , JSON (application/json)
13268 19.367676  10.0.0.244      34.219.216.215  HTTP     1372 POST /2/2.147.0/234175/AxYlXAQICGUqWxLZ/postback?ui=97a8e9600e9c472f8c6a5d96a96b90ca&md=2&de=
13044 19.294467  10.0.0.244      172.240.47.127  HTTP      864 GET /?c=v&m=api&res=xml&groupId=216&domain=www.tmz.com&page=www.tmz.com%2F&ip=67.161.168.80&u
12994 19.239517  34.219.216.215  10.0.0.244      HTTP      228 HTTP/1.1 200 OK
12959 19.184949  10.0.0.244      34.219.216.215  HTTP      302 POST /2/2.147.0/234175/AxYlXAQICGUqWxLZ/postback?ui=97a8e9600e9c472f8c6a5d96a96b90ca&md=2&de=
12890 19.031625  34.219.216.215  10.0.0.244      HTTP      228 HTTP/1.1 200 OK
12885 19.031529  34.219.216.215  10.0.0.244      HTTP      228 HTTP/1.1 200 OK
12828 18.970427  10.0.0.244      34.219.216.215  HTTP      301 POST /2/2.147.0/234175/AxYlXAQICGUqWxLZ/postback?ui=97a8e9600e9c472f8c6a5d96a96b90ca&md=2&de=
12826 18.970296  10.0.0.244      34.219.216.215  HTTP     1259 POST /2/2.147.0/234175/AxYlXAQICGUqWxLZ/postback?oz_pl=1&ui=97a8e9600e9c472f8c6a5d96a96b90ca&
12753 18.912156  10.0.0.244      54.85.56.66     HTTP     1287 POST /cache HTTP/1.1  (text/plain)
12584 18.906978  98.82.157.231   10.0.0.244      HTTP      684 HTTP/1.1 200 OK  (text/html)
11686 18.770168  34.219.216.215  10.0.0.244      HTTP      228 HTTP/1.1 200 OK
11649 18.768637  10.0.0.244      69.173.154.8    HTTP      939 GET /khaos.json?us_privacy=1YNN HTTP/1.1
```

100+ HTTP2 protocols

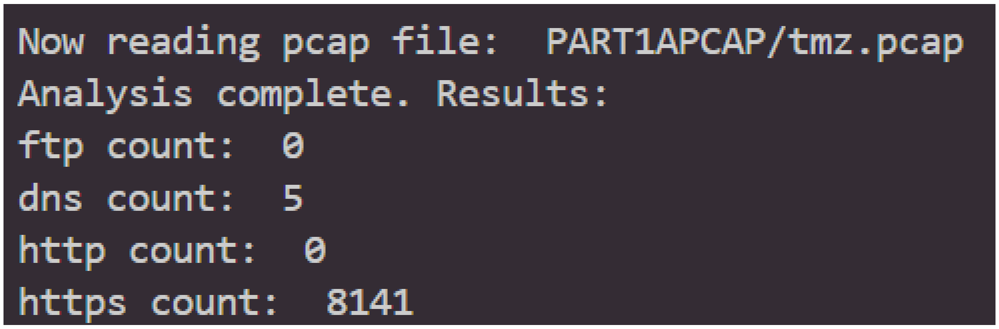


```
http2
No.    Time      Source                Destination           Protoc  Length Info
13140 19.341558  2a04:4e42:200::626    2601:204:f100:55c0:…  TLSv1.3  1028 DATA[1] (JPEG JFIF image)
12189 18.853774  104.18.41.104         10.0.0.244            TLSv1.3  5894 DATA[9][TLS segment of a reassembled PDU]
12139 18.833167  104.18.41.104         10.0.0.244            TLSv1.3 11734 DATA[9][TLS segment of a reassembled PDU]
12051 18.827213  104.18.41.104         10.0.0.244            TLSv1.3 13194 DATA[9][TLS segment of a reassembled PDU]
11829 18.805356  104.18.41.104         10.0.0.244            TLSv1.3  5894 DATA[9]
11741 18.796046  104.18.41.104         10.0.0.244            TLSv1.3  4434 DATA[9][TLS segment of a reassembled PDU]
11724 18.785724  104.18.41.104         10.0.0.244            TLSv1.3  2974 DATA[9]
11721 18.785265  104.18.41.104         10.0.0.244            TLSv1.3  8814 DATA[9][TLS segment of a reassembled PDU]
11702 18.780366  104.18.41.104         10.0.0.244            TLSv1.3  2974 DATA[9][TLS segment of a reassembled PDU]
11664 18.769437  2606:4700::6812:1691  2601:204:f100:55c0:…  TLSv1.3   465 DATA[1]
11660 18.769437  2606:4700::6812:1691  2601:204:f100:55c0:…  TLSv1.3  2794 DATA[1][TLS segment of a reassembled PDU]
11651 18.769437  2606:4700::6812:1691  2601:204:f100:55c0:…  TLSv1.3   157 DATA[1]
11622 18.767054  2606:4700::6812:1691  2601:204:f100:55c0:…  TLSv1.3  1380 DATA[1]
11603 18.766499  2606:4700::6812:1691  2601:204:f100:55c0:…  TLSv1.3  1195 DATA[1]
11600 18.766499  2606:4700::6812:1691  2601:204:f100:55c0:…  TLSv1.3  4154 DATA[1][TLS segment of a reassembled PDU]
10923 18.576860  2a04:4e42:200::626    2601:204:f100:55c0:…  TLSv1.3   430 DATA[1]
 8440 17.384956  2a04:4e42::626        2601:204:f100:55c0:…  TLSv1.3  6954 [TLS segment of a reassembled PDU]
 6269 16.643733  142.250.191.34        10.0.0.244            TLSv1.3  5702 [TLS segment of a reassembled PDU]
 5370 16.312231  104.18.41.104         10.0.0.244            TLSv1.3  5894 HEADERS[17]: 200 OK
 5345 16.310576  104.18.41.104         10.0.0.244            TLSv1.3  7354 DATA[13]
 5335 16.310296  2607:f8b0:4005:811:…  2601:204:f100:55c0:…  TLSv1.3   827 DATA[1]
 4000 15.534857  2606:4700:10::6816:…  2601:204:f100:55c0:…  TLSv1.3   980 DATA[1]
 3148 15.160798  2600:1406:d400::173…  2601:204:f100:55c0:…  TLSv1.3  2954 DATA[5]
 3131 15.159528  2600:1406:d400::173…  2601:204:f100:55c0:…  TLSv1.3  2954 DATA[5]
```

5 DNS protocols



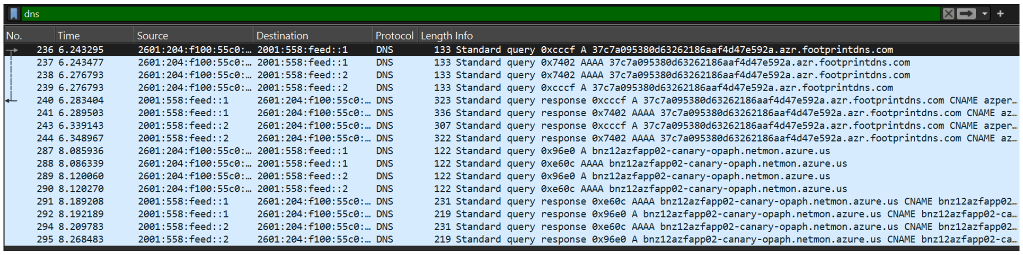
```
dns
No.    Time      Source                Destination           Protoc  Length Info
12914 19.050529  2803:f800:53::3       2601:204:f100:55c0:…  DoH       573 Standard query response 0x0000 AAAA x.videobyte.com SOA ns-896.awsdns-48.net OPT
12907 19.041442  2803:f800:53::3       2601:204:f100:55c0:…  DoH       573 Standard query response 0x0000 A x.videobyte.com A 3.134.195.158 A 52.15.32.253 A 13.59.151.179 A …
12905 19.041442  2803:f800:53::3       2601:204:f100:55c0:…  DoH       573 Standard query response 0x0000 HTTPS x.videobyte.com SOA ns-896.awsdns-48.net OPT
12902 19.040693  2803:f800:53::3       2601:204:f100:55c0:…  DoH       573 Standard query response 0x0000 A colossusssp.com A 172.240.47.127 A 96.46.188.4 A 172.240.47.117 A…
12900 19.040693  2803:f800:53::3       2601:204:f100:55c0:…  DoH       573 Standard query response 0x0000 HTTPS colossusssp.com SOA ns31.domaincontrol.com OPT
12898 19.040693  2803:f800:53::3       2601:204:f100:55c0:…  DoH       573 Standard query response 0x0000 AAAA colossusssp.com SOA ns31.domaincontrol.com OPT
12858 19.002377  2601:204:f100:55c0:…  2803:f800:53::3       DoH       233 Standard query 0x0000 A x.videobyte.com OPT
12857 19.002365  2601:204:f100:55c0:…  2803:f800:53::3       DoH       233 Standard query 0x0000 AAAA x.videobyte.com OPT
12856 19.002352  2601:204:f100:55c0:…  2803:f800:53::3       DoH       233 Standard query 0x0000 HTTPS x.videobyte.com OPT
12852 19.002282  2601:204:f100:55c0:…  2803:f800:53::3       DoH       233 Standard query 0x0000 A colossusssp.com OPT
12851 19.002261  2601:204:f100:55c0:…  2803:f800:53::3       DoH       233 Standard query 0x0000 HTTPS colossusssp.com OPT
12850 19.002247  2601:204:f100:55c0:…  2803:f800:53::3       DoH       233 Standard query 0x0000 AAAA colossusssp.com OPT
12713 18.909784  2001:558:feed::1      2601:204:f100:55c0:…  DNS       137 Standard query response 0x9fb4 A chrome.cloudflare-dns.com A 172.64.41.3 A 162.159.61.3
12712 18.909784  2001:558:feed::1      2601:204:f100:55c0:…  DNS       266 Standard query response 0x333d HTTPS chrome.cloudflare-dns.com HTTPS A 162.159.61.3 A 172.64.41.3 …
12708 18.909784  2001:558:feed::1      2601:204:f100:55c0:…  DNS       161 Standard query response 0x0824 AAAA chrome.cloudflare-dns.com AAAA 2803:f800:53::3 AAAA 2a06:98c1:…
12202 18.857931  2601:204:f100:55c0:…  2001:558:feed::1      DNS       105 Standard query 0x333d HTTPS chrome.cloudflare-dns.com
12201 18.857741  2601:204:f100:55c0:…  2001:558:feed::1      DNS       105 Standard query 0x9fb4 A chrome.cloudflare-dns.com
12200 18.857446  2601:204:f100:55c0:…  2001:558:feed::1      DNS       105 Standard query 0x0824 AAAA chrome.cloudflare-dns.com
10602 18.305654  2600:1f16:a60:c01:f…  2601:204:f100:55c0:…  DNS       151 Unknown operation (12) 0x4420[Malformed Packet]
 7490 17.097333  3.33.220.150          10.0.0.244            DNS        92 Unknown operation (14) 0x6469 Unknown (25661) <Unknown extended label>[Malformed Packet]
```



```
Now reading pcap file:  PART1APCAP/tmz.pcap
Analysis complete. Results:
ftp count:  0
dns count:  5
http count:  0
https count:  8141
```

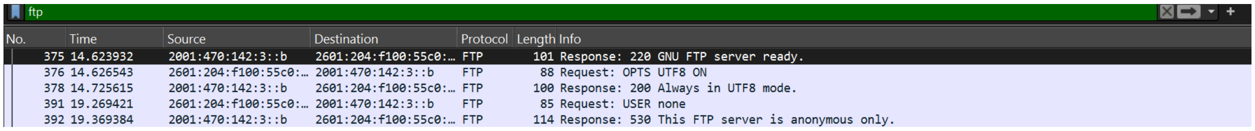
My program is off by one DNS protocol compared to the Wireshark filter, but my DNS count shouldn't be wrong as my DNS counts for both Wireshark and the program are the same in my other activities. Also it's no surprise that https is over 8k, as my HTTP and HTTP2 count on Wireshark are very high.

5. Accessing a ftp server: 16 DNS protocols



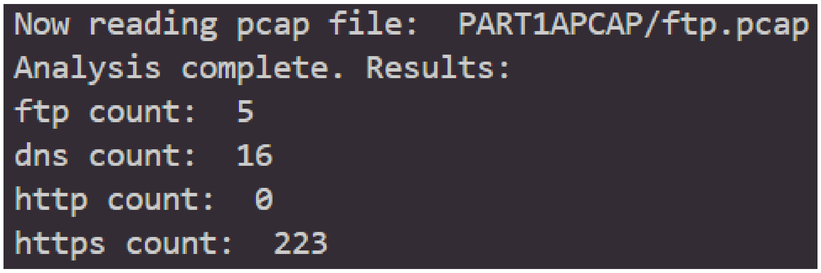
No.	Time	Source	Destination	Protocol	Length	Info
236	6.243295	2601:204:f100:55c0:…	2001:558:feed::1	DNS	133	Standard query 0xcccf A 37c7a095380d63262186aaf4d47e592a.azr.footprintdns.com
237	6.243477	2601:204:f100:55c0:…	2001:558:feed::1	DNS	133	Standard query 0x7402 AAAA 37c7a095380d63262186aaf4d47e592a.azr.footprintdns.com
238	6.276793	2601:204:f100:55c0:…	2001:558:feed::2	DNS	133	Standard query 0x7402 AAAA 37c7a095380d63262186aaf4d47e592a.azr.footprintdns.com
239	6.276793	2601:204:f100:55c0:…	2001:558:feed::2	DNS	133	Standard query 0xcccf A 37c7a095380d63262186aaf4d47e592a.azr.footprintdns.com
240	6.283404	2001:558:feed::1	2601:204:f100:55c0:…	DNS	323	Standard query response 0xcccf A 37c7a095380d63262186aaf4d47e592a.azr.footprintdns.com CNAME azper…
241	6.289503	2001:558:feed::1	2601:204:f100:55c0:…	DNS	336	Standard query response 0x7402 AAAA 37c7a095380d63262186aaf4d47e592a.azr.footprintdns.com CNAME az…
243	6.339143	2001:558:feed::2	2601:204:f100:55c0:…	DNS	307	Standard query response 0xcccf A 37c7a095380d63262186aaf4d47e592a.azr.footprintdns.com CNAME azper…
244	6.348967	2001:558:feed::2	2601:204:f100:55c0:…	DNS	322	Standard query response 0x7402 AAAA 37c7a095380d63262186aaf4d47e592a.azr.footprintdns.com CNAME az…
287	8.085936	2601:204:f100:55c0:…	2001:558:feed::1	DNS	122	Standard query 0x96e0 A bnz12azfapp02-canary-opaph.netmon.azure.us
288	8.086339	2601:204:f100:55c0:…	2001:558:feed::1	DNS	122	Standard query 0xe60c AAAA bnz12azfapp02-canary-opaph.netmon.azure.us
289	8.120060	2601:204:f100:55c0:…	2001:558:feed::2	DNS	122	Standard query 0x96e0 A bnz12azfapp02-canary-opaph.netmon.azure.us
290	8.120270	2601:204:f100:55c0:…	2001:558:feed::2	DNS	122	Standard query 0xe60c AAAA bnz12azfapp02-canary-opaph.netmon.azure.us
291	8.189208	2001:558:feed::1	2601:204:f100:55c0:…	DNS	231	Standard query response 0xe60c AAAA bnz12azfapp02-canary-opaph.netmon.azure.us CNAME bnz12azfapp02…
292	8.192189	2001:558:feed::1	2601:204:f100:55c0:…	DNS	219	Standard query response 0x96e0 A bnz12azfapp02-canary-opaph.netmon.azure.us CNAME bnz12azfapp02-ca…
294	8.209783	2001:558:feed::2	2601:204:f100:55c0:…	DNS	231	Standard query response 0xe60c AAAA bnz12azfapp02-canary-opaph.netmon.azure.us CNAME bnz12azfapp02…
295	8.268483	2001:558:feed::2	2601:204:f100:55c0:…	DNS	219	Standard query response 0x96e0 A bnz12azfapp02-canary-opaph.netmon.azure.us CNAME bnz12azfapp02-ca…

5 FTP protocols, this is higher than it should be as I purposely tried to log in to see what I would get in the capture, if I had not input anything it would have 1 FTP shown



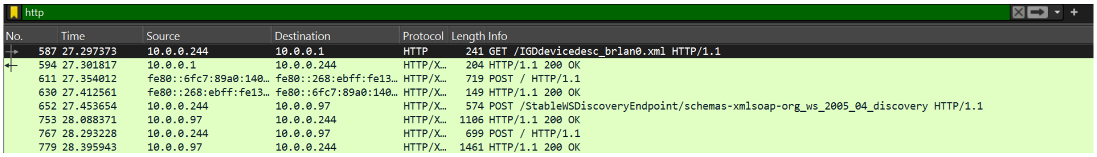
No.	Time	Source	Destination	Protocol	Length	Info
375	14.623932	2001:470:142:3::b	2601:204:f100:55c0:…	FTP	101	Response: 220 GNU FTP server ready.
376	14.626543	2601:204:f100:55c0:…	2001:470:142:3::b	FTP	88	Request: OPTS UTF8 ON
378	14.725615	2001:470:142:3::b	2601:204:f100:55c0:…	FTP	100	Response: 200 Always in UTF8 mode.
391	19.269421	2601:204:f100:55c0:…	2001:470:142:3::b	FTP	85	Request: USER none
392	19.369384	2001:470:142:3::b	2601:204:f100:55c0:…	FTP	114	Response: 530 This FTP server is anonymous only.

My program also gives the same counts, and also counts an additional 223 https protocols!



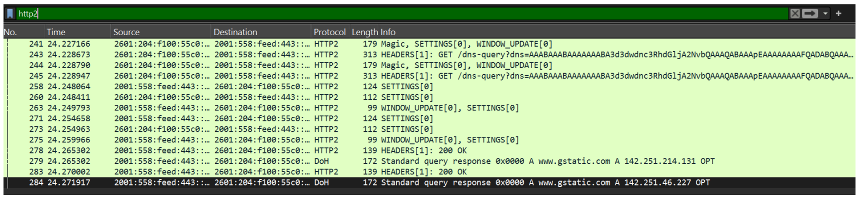
```
Now reading pcap file:  PART1APCAP/ftp.pcap
Analysis complete. Results:
ftp count:  5
dns count:  16
http count:  0
https count:  223
```

6. Logging into ssh: 8 HTTP protocols



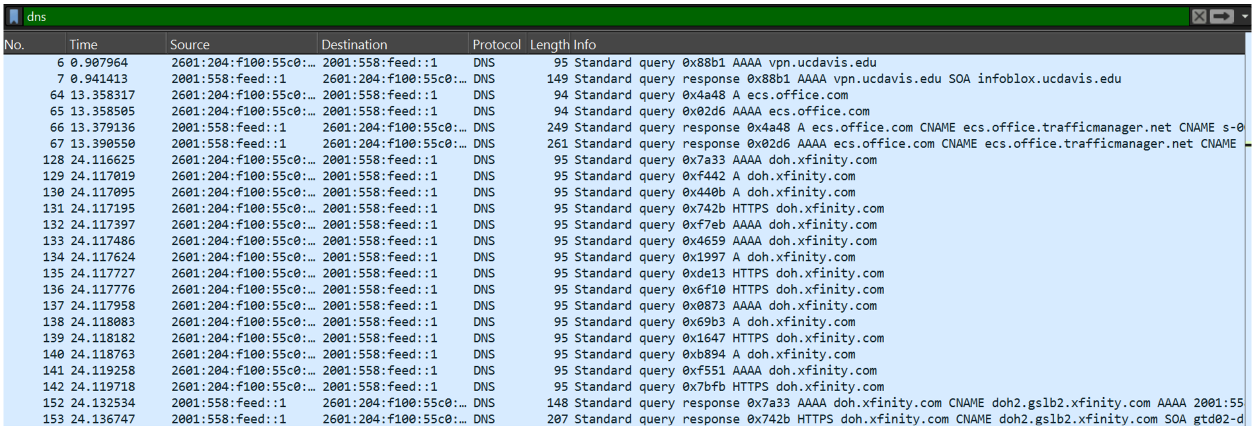
No.	Time	Source	Destination	Protocol	Length	Info
587	27.297373	10.0.0.244	10.0.0.1	HTTP	241	GET /IGDdevicedesc_brlan0.xml HTTP/1.1
594	27.301817	10.0.0.1	10.0.0.244	HTTP/X…	204	HTTP/1.1 200 OK
611	27.354012	fe80::6fc7:89a0:140…	fe80::268:ebff:fe13…	HTTP/X…	719	POST / HTTP/1.1
630	27.412561	fe80::268:ebff:fe13…	fe80::6fc7:89a0:140…	HTTP/X…	149	HTTP/1.1 200 OK
652	27.453654	10.0.0.244	10.0.0.97	HTTP/X…	574	POST /StableWSDiscoveryEndpoint/schemas-xmlsoap-org_ws_2005_04_discovery HTTP/1.1
753	28.088371	10.0.0.97	10.0.0.244	HTTP/X…	1106	HTTP/1.1 200 OK
767	28.293228	10.0.0.244	10.0.0.97	HTTP/X…	699	POST / HTTP/1.1
779	28.395943	10.0.0.97	10.0.0.244	HTTP/X…	1461	HTTP/1.1 200 OK

12 HTTP2 protocols



No.	Time	Source	Destination	Protocol	Length	Info
241	24.227166	2601:204:f100:55c0:…	2001:558:feed:443::…	HTTP2	179	Magic, SETTINGS[0], WINDOW_UPDATE[0]
243	24.228673	2601:204:f100:55c0:…	2001:558:feed:443::…	HTTP2	313	HEADERS[1]: GET /dns-query?dns=AAABAAABAAAAAAABA3d3dwdnc3RhdGljA2NvbQAAAQABAAApEAAAAAAAFQADABQAAA…
244	24.228790	2601:204:f100:55c0:…	2001:558:feed:443::…	HTTP2	179	Magic, SETTINGS[0], WINDOW_UPDATE[0]
245	24.228947	2601:204:f100:55c0:…	2001:558:feed:443::…	HTTP2	313	HEADERS[1]: GET /dns-query?dns=AAABAAABAAAAAAABA3d3dwdnc3RhdGljA2NvbQAAAQABAAApEAAAAAAAFQADABQAAA…
258	24.248064	2001:558:feed:443::…	2601:204:f100:55c0:…	HTTP2	124	SETTINGS[0]
260	24.248411	2601:204:f100:55c0:…	2001:558:feed:443::…	HTTP2	112	SETTINGS[0]
263	24.249793	2001:558:feed:443::…	2601:204:f100:55c0:…	HTTP2	99	WINDOW_UPDATE[0], SETTINGS[0]
271	24.254658	2001:558:feed:443::…	2601:204:f100:55c0:…	HTTP2	124	SETTINGS[0]
273	24.254963	2601:204:f100:55c0:…	2001:558:feed:443::…	HTTP2	112	SETTINGS[0]
275	24.259966	2001:558:feed:443::…	2601:204:f100:55c0:…	HTTP2	99	WINDOW_UPDATE[0], SETTINGS[0]
278	24.265302	2001:558:feed:443::…	2601:204:f100:55c0:…	HTTP2	139	HEADERS[1]: 200 OK
279	24.265302	2001:558:feed:443::…	2601:204:f100:55c0:…	DoH	172	Standard query response 0x0000 A www.gstatic.com A 142.251.214.131 OPT
283	24.270002	2001:558:feed:443::…	2601:204:f100:55c0:…	HTTP2	139	HEADERS[1]: 200 OK
284	24.271917	2001:558:feed:443::…	2601:204:f100:55c0:…	DoH	172	Standard query response 0x0000 A www.gstatic.com A 142.251.46.227 OPT

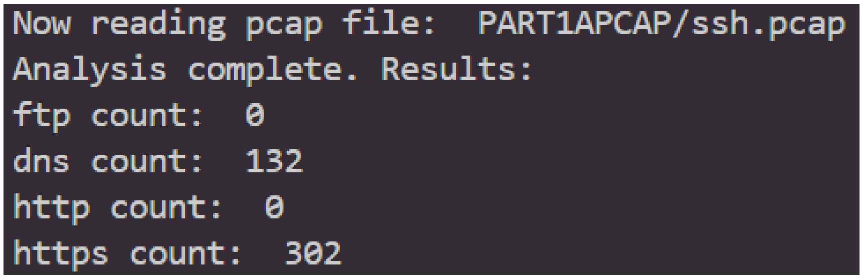
50+ DNS protocols



dns

No.	Time	Source	Destination	Protocol	Length	Info
6	0.907964	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0x88b1 AAAA vpn.ucdavis.edu
7	0.941413	2001:558:feed::1	2601:204:f100:55c0:…	DNS	149	Standard query response 0x88b1 AAAA vpn.ucdavis.edu SOA infoblox.ucdavis.edu
64	13.358317	2601:204:f100:55c0:…	2001:558:feed::1	DNS	94	Standard query 0x4a48 A ecs.office.com
65	13.358505	2601:204:f100:55c0:…	2001:558:feed::1	DNS	94	Standard query 0x02d6 AAAA ecs.office.com
66	13.379136	2001:558:feed::1	2601:204:f100:55c0:…	DNS	249	Standard query response 0x4a48 A ecs.office.com CNAME ecs.office.trafficmanager.net CNAME s-0
67	13.390550	2001:558:feed::1	2601:204:f100:55c0:…	DNS	261	Standard query response 0x02d6 AAAA ecs.office.com CNAME ecs.office.trafficmanager.net CNAME
128	24.116625	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0x7a33 AAAA doh.xfinity.com
129	24.117019	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0xf442 A doh.xfinity.com
130	24.117095	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0x440b A doh.xfinity.com
131	24.117195	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0x742b HTTPS doh.xfinity.com
132	24.117397	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0xf7eb AAAA doh.xfinity.com
133	24.117486	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0x4659 AAAA doh.xfinity.com
134	24.117624	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0x1997 A doh.xfinity.com
135	24.117727	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0xde13 HTTPS doh.xfinity.com
136	24.117776	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0x6f10 HTTPS doh.xfinity.com
137	24.117958	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0x0873 AAAA doh.xfinity.com
138	24.118083	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0x69b3 A doh.xfinity.com
139	24.118182	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0x1647 HTTPS doh.xfinity.com
140	24.118763	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0xb894 A doh.xfinity.com
141	24.119258	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0xf551 AAAA doh.xfinity.com
142	24.119718	2601:204:f100:55c0:…	2001:558:feed::1	DNS	95	Standard query 0x7bfb HTTPS doh.xfinity.com
152	24.132534	2001:558:feed::1	2601:204:f100:55c0:…	DNS	148	Standard query response 0x7a33 AAAA doh.xfinity.com CNAME doh2.gslb2.xfinity.com AAAA 2001:55
153	24.136747	2001:558:feed::1	2601:204:f100:55c0:…	DNS	207	Standard query response 0x742b HTTPS doh.xfinity.com CNAME doh2.gslb2.xfinity.com SOA gtd02-d

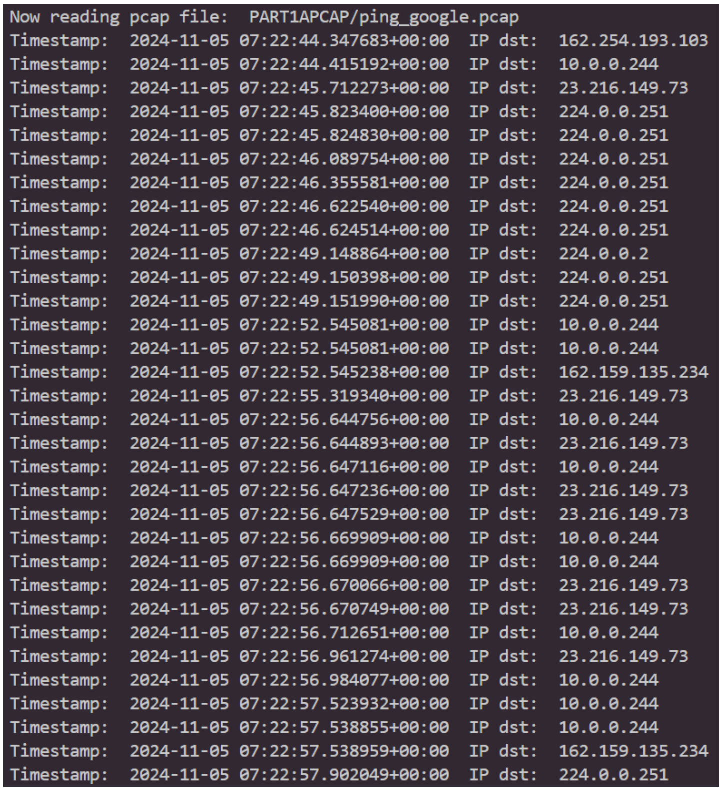
My program reads the exact number of DNS protocols as 132, and 302 HTTPS protocols. I am assuming the 8 HTTP protocols found in Wireshark do not actually go through port 80, so it is not catching it in my program.



```
Now reading pcap file:  PART1APCAP/ssh.pcap
Analysis complete. Results:
ftp count:  0
dns count:  132
http count:  0
https count:  302
```

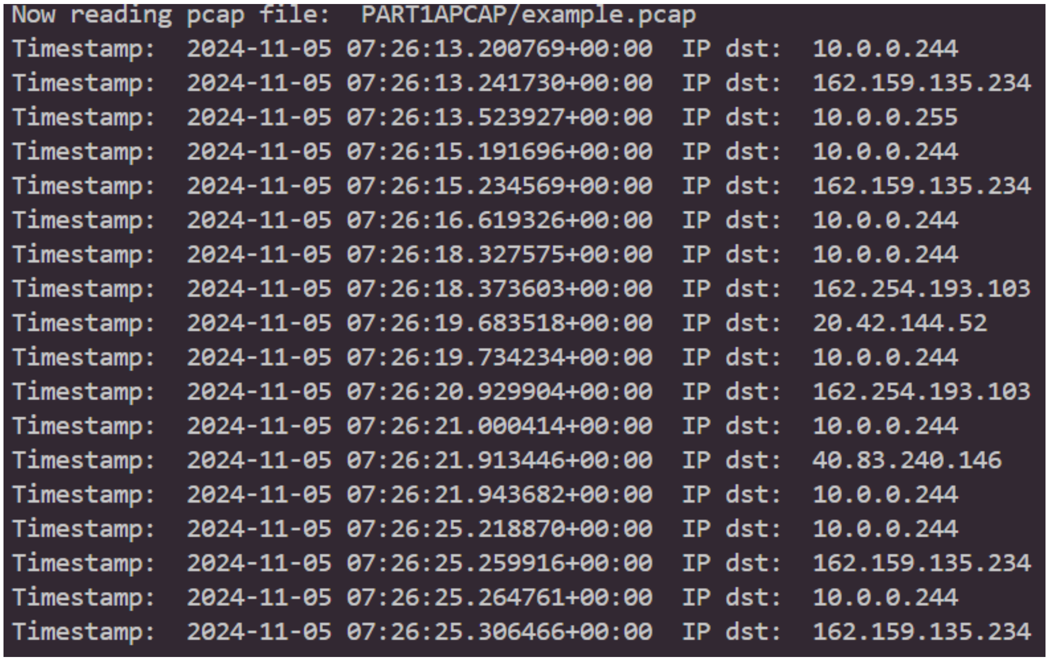
2. How many HTTP and HTTPS packets did you record while performing activities 2 and 3?
   As listed above, activity two resulted in 49 HTTPS packets, and activity three resulted in 16 HTTP packets and 547 HTTPS packets.

3. List the destination IP address used in each activity along with their timestamps. The destination IP address should be in the IPv4 format like x.x.x.x (e.g., “192.168.1.1”, “8.8.8.8”, “10.0.1.150”, etc.).
   I will be posting screenshots of my terminal of the output of my program.
   Ping google.com 20 times:



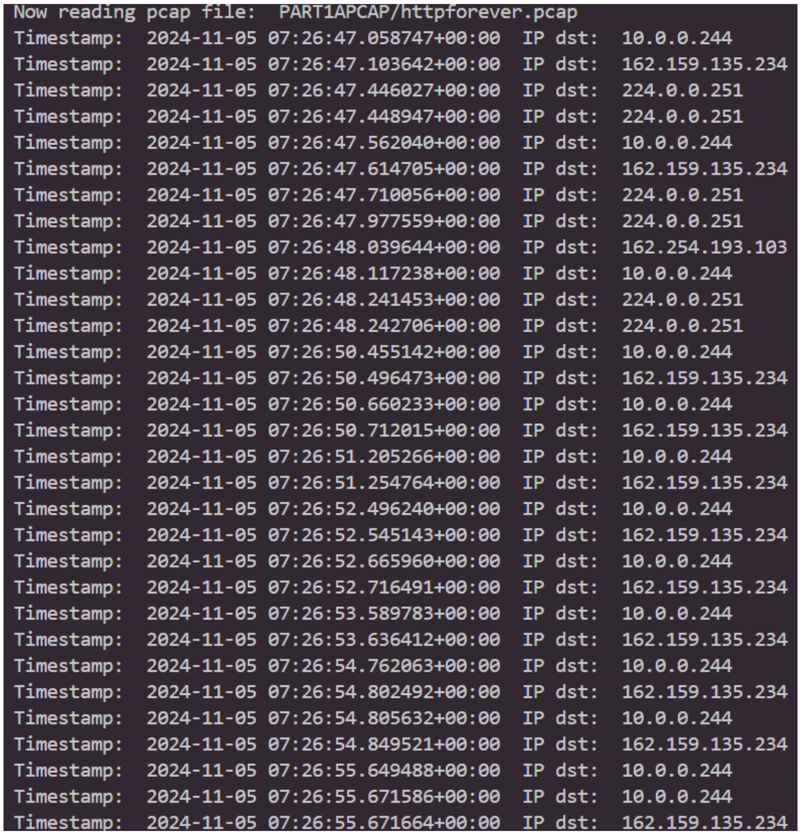
```
Now reading pcap file:  PART1APCAP/ping_google.pcap
Timestamp:  2024-11-05 07:22:44.347683+00:00  IP dst:  162.254.193.103
Timestamp:  2024-11-05 07:22:44.415192+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:22:45.712273+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:22:45.823400+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:22:45.824830+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:22:46.089754+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:22:46.355581+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:22:46.622540+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:22:46.624514+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:22:49.148864+00:00  IP dst:  224.0.0.2
Timestamp:  2024-11-05 07:22:49.150398+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:22:49.151990+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:22:52.545081+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:22:52.545081+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:22:52.545238+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:22:55.319340+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:22:56.644756+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:22:56.644893+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:22:56.647116+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:22:56.647236+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:22:56.647529+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:22:56.669909+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:22:56.669909+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:22:56.670066+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:22:56.670749+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:22:56.712651+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:22:56.961274+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:22:56.984077+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:22:57.523932+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:22:57.538855+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:22:57.538959+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:22:57.902049+00:00  IP dst:  224.0.0.251
```

   Visiting https://example.com:



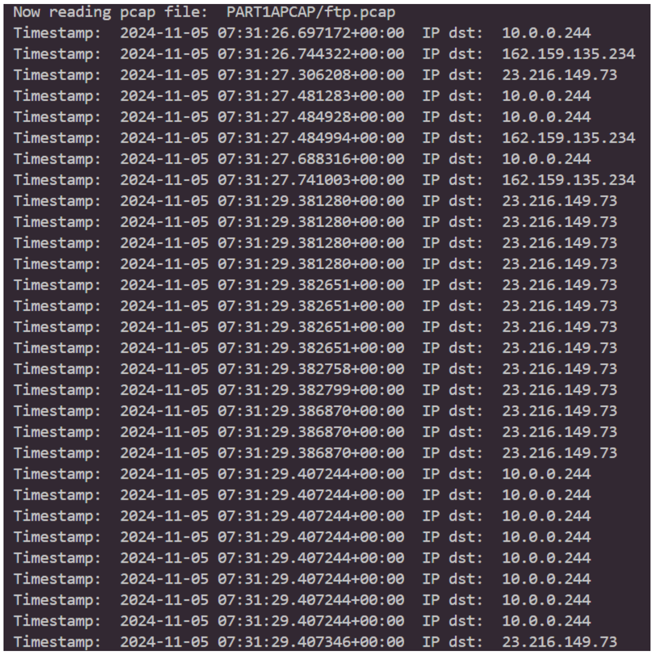
```
Now reading pcap file:  PART1APCAP/example.pcap
Timestamp:  2024-11-05 07:26:13.200769+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:13.241730+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:26:13.523927+00:00  IP dst:  10.0.0.255
Timestamp:  2024-11-05 07:26:15.191696+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:15.234569+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:26:16.619326+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:18.327575+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:18.373603+00:00  IP dst:  162.254.193.103
Timestamp:  2024-11-05 07:26:19.683518+00:00  IP dst:  20.42.144.52
Timestamp:  2024-11-05 07:26:19.734234+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:20.929904+00:00  IP dst:  162.254.193.103
Timestamp:  2024-11-05 07:26:21.000414+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:21.913446+00:00  IP dst:  40.83.240.146
Timestamp:  2024-11-05 07:26:21.943682+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:25.218870+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:25.259916+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:26:25.264761+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:25.306466+00:00  IP dst:  162.159.135.234
```

Visting http://httpforever.com:



```
Now reading pcap file:  PART1APCAP/httpforever.pcap
Timestamp:  2024-11-05 07:26:47.058747+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:47.103642+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:26:47.446027+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:26:47.448947+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:26:47.562040+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:47.614705+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:26:47.710056+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:26:47.977559+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:26:48.039644+00:00  IP dst:  162.254.193.103
Timestamp:  2024-11-05 07:26:48.117238+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:48.241453+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:26:48.242706+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:26:50.455142+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:50.496473+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:26:50.660233+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:50.712015+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:26:51.205266+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:51.254764+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:26:52.496240+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:52.545143+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:26:52.665960+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:52.716491+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:26:53.589783+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:53.636412+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:26:54.762063+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:54.802492+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:26:54.805632+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:54.849521+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:26:55.649488+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:55.671586+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:26:55.671664+00:00  IP dst:  162.159.135.234
```

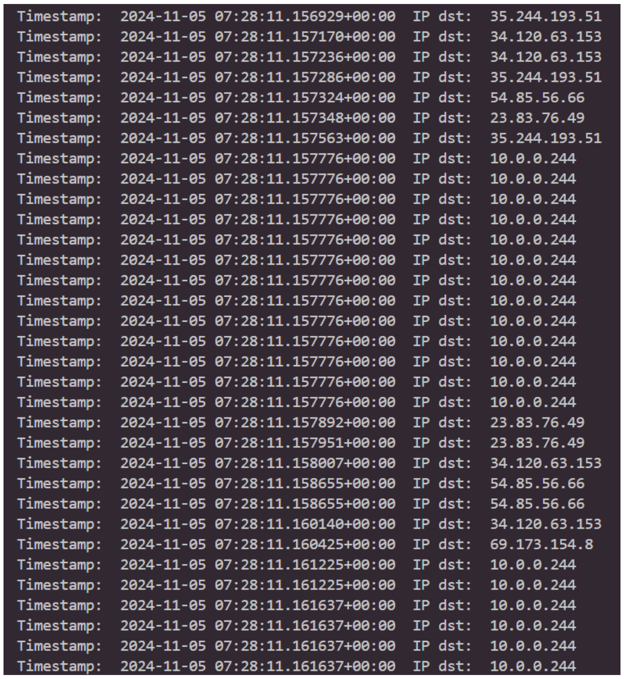
Accessing ftp server:



```
Now reading pcap file:  PART1APCAP/ftp.pcap
Timestamp:  2024-11-05 07:31:26.697172+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:31:26.744322+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:31:27.306208+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:27.481283+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:31:27.484928+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:31:27.484994+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:31:27.688316+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:31:27.741003+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:31:29.381280+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:29.381280+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:29.381280+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:29.381280+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:29.382651+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:29.382651+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:29.382651+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:29.382651+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:29.382758+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:29.382799+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:29.386870+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:29.386870+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:29.386870+00:00  IP dst:  23.216.149.73
Timestamp:  2024-11-05 07:31:29.407244+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:31:29.407244+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:31:29.407244+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:31:29.407244+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:31:29.407244+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:31:29.407244+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:31:29.407244+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:31:29.407244+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:31:29.407346+00:00  IP dst:  23.216.149.73
```

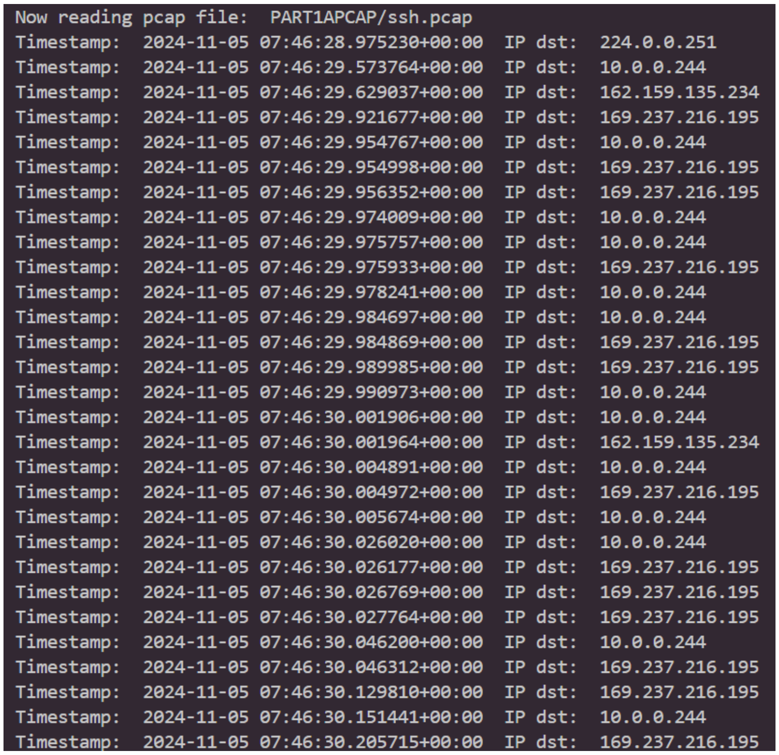
Visiting tmz:

Note: It does not say: “Now reading from file:...” because the output was so long from my terminal that it won’t let me access the beginning of the output.



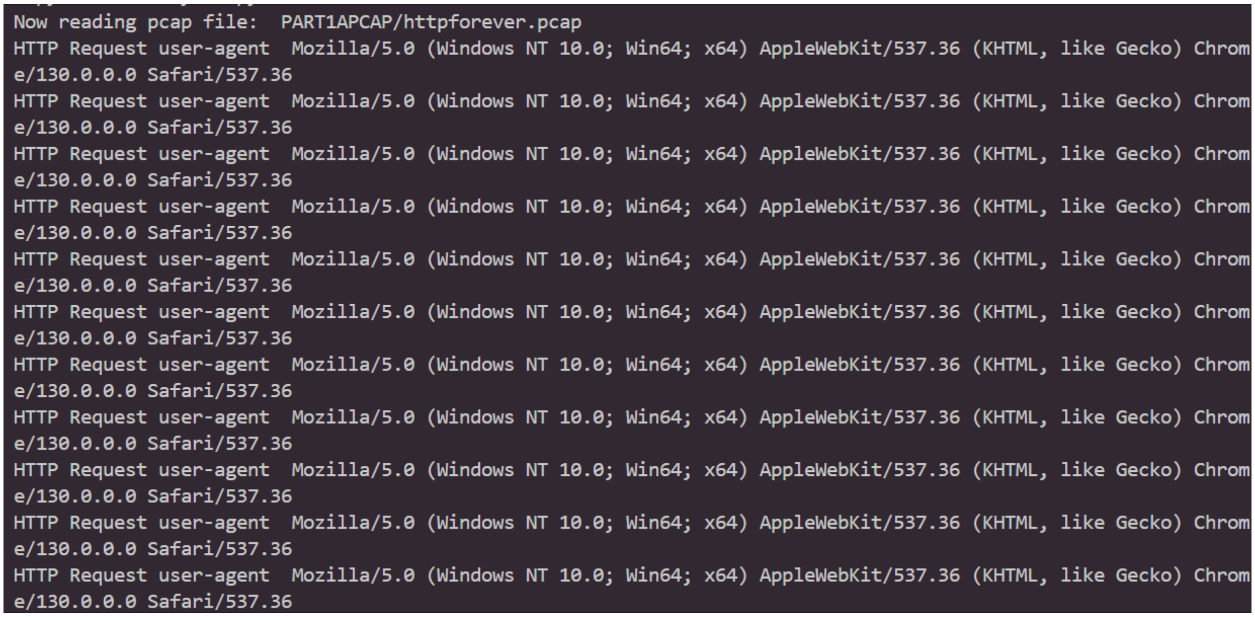
```
Timestamp:  2024-11-05 07:28:11.156929+00:00  IP dst:  35.244.193.51
Timestamp:  2024-11-05 07:28:11.157170+00:00  IP dst:  34.120.63.153
Timestamp:  2024-11-05 07:28:11.157236+00:00  IP dst:  34.120.63.153
Timestamp:  2024-11-05 07:28:11.157286+00:00  IP dst:  35.244.193.51
Timestamp:  2024-11-05 07:28:11.157324+00:00  IP dst:  54.85.56.66
Timestamp:  2024-11-05 07:28:11.157348+00:00  IP dst:  23.83.76.49
Timestamp:  2024-11-05 07:28:11.157563+00:00  IP dst:  35.244.193.51
Timestamp:  2024-11-05 07:28:11.157776+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.157776+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.157776+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.157776+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.157776+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.157776+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.157776+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.157776+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.157776+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.157776+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.157776+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.157776+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.157776+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.157892+00:00  IP dst:  23.83.76.49
Timestamp:  2024-11-05 07:28:11.157951+00:00  IP dst:  23.83.76.49
Timestamp:  2024-11-05 07:28:11.158007+00:00  IP dst:  34.120.63.153
Timestamp:  2024-11-05 07:28:11.158655+00:00  IP dst:  54.85.56.66
Timestamp:  2024-11-05 07:28:11.158655+00:00  IP dst:  54.85.56.66
Timestamp:  2024-11-05 07:28:11.160140+00:00  IP dst:  34.120.63.153
Timestamp:  2024-11-05 07:28:11.160425+00:00  IP dst:  69.173.154.8
Timestamp:  2024-11-05 07:28:11.161225+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.161225+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.161637+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.161637+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.161637+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:28:11.161637+00:00  IP dst:  10.0.0.244
```

Visiting ssh:



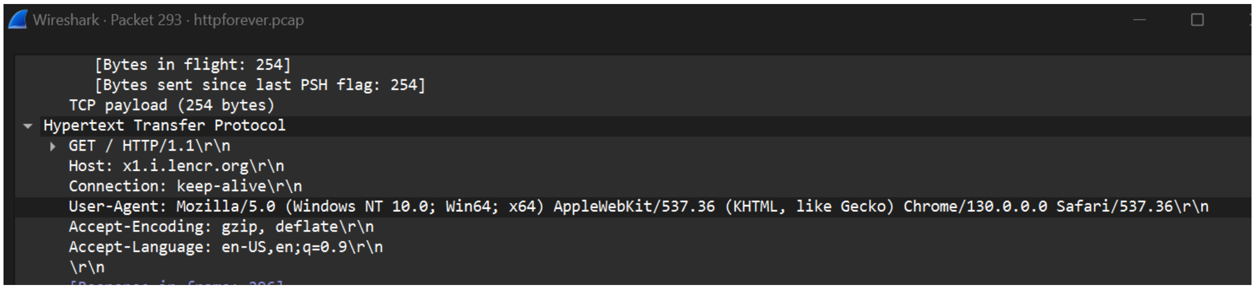
```
Now reading pcap file:  PART1APCAP/ssh.pcap
Timestamp:  2024-11-05 07:46:28.975230+00:00  IP dst:  224.0.0.251
Timestamp:  2024-11-05 07:46:29.573764+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:46:29.629037+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:46:29.921677+00:00  IP dst:  169.237.216.195
Timestamp:  2024-11-05 07:46:29.954767+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:46:29.954998+00:00  IP dst:  169.237.216.195
Timestamp:  2024-11-05 07:46:29.956352+00:00  IP dst:  169.237.216.195
Timestamp:  2024-11-05 07:46:29.974009+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:46:29.975757+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:46:29.975933+00:00  IP dst:  169.237.216.195
Timestamp:  2024-11-05 07:46:29.978241+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:46:29.984697+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:46:29.984869+00:00  IP dst:  169.237.216.195
Timestamp:  2024-11-05 07:46:29.989985+00:00  IP dst:  169.237.216.195
Timestamp:  2024-11-05 07:46:29.990973+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:46:30.001906+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:46:30.001964+00:00  IP dst:  162.159.135.234
Timestamp:  2024-11-05 07:46:30.004891+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:46:30.004972+00:00  IP dst:  169.237.216.195
Timestamp:  2024-11-05 07:46:30.005674+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:46:30.026020+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:46:30.026177+00:00  IP dst:  169.237.216.195
Timestamp:  2024-11-05 07:46:30.026769+00:00  IP dst:  169.237.216.195
Timestamp:  2024-11-05 07:46:30.027764+00:00  IP dst:  169.237.216.195
Timestamp:  2024-11-05 07:46:30.046200+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:46:30.046312+00:00  IP dst:  169.237.216.195
Timestamp:  2024-11-05 07:46:30.129810+00:00  IP dst:  169.237.216.195
Timestamp:  2024-11-05 07:46:30.151441+00:00  IP dst:  10.0.0.244
Timestamp:  2024-11-05 07:46:30.205715+00:00  IP dst:  169.237.216.195
```

4. For activities 2, 3, and 4, can you tell which browser was used for these activities from the captured packets?
   Using the demo code, I was able to see the user-agent of the HTTP packets being sent on activity 3 (httpforever) and they were all labeled as:
   Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36
   Output from the code:



```
Now reading pcap file:  PART1APCAP/httpforever.pcap
HTTP Request user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/130.0.0.0 Safari/537.36
HTTP Request user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/130.0.0.0 Safari/537.36
HTTP Request user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/130.0.0.0 Safari/537.36
HTTP Request user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/130.0.0.0 Safari/537.36
HTTP Request user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/130.0.0.0 Safari/537.36
HTTP Request user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/130.0.0.0 Safari/537.36
HTTP Request user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/130.0.0.0 Safari/537.36
HTTP Request user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/130.0.0.0 Safari/537.36
HTTP Request user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/130.0.0.0 Safari/537.36
HTTP Request user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/130.0.0.0 Safari/537.36
HTTP Request user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/130.0.0.0 Safari/537.36
```

   Through wireshark, I was able to see on activity 3:



```
        [Bytes in flight: 254]
        [Bytes sent since last PSH flag: 254]
     TCP payload (254 bytes)
▾ Hypertext Transfer Protocol
   ▸ GET / HTTP/1.1\r\n
     Host: x1.i.lencr.org\r\n
     Connection: keep-alive\r\n
     User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36\r\n
     Accept-Encoding: gzip, deflate\r\n
     Accept-Language: en-US,en;q=0.9\r\n
     \r\n
```

   However, for the rest of the activities, I wasn't able to see anything else on wireshark or via the code, and this is because the other activities use HTTPS, which encrypts its data, so I would not be able to extra the header data that includes the user-agent information.