

COMPUTER NETWORKS (CS F303)

Assignment #1

Wireshark and Network Programming

Aniket Jain

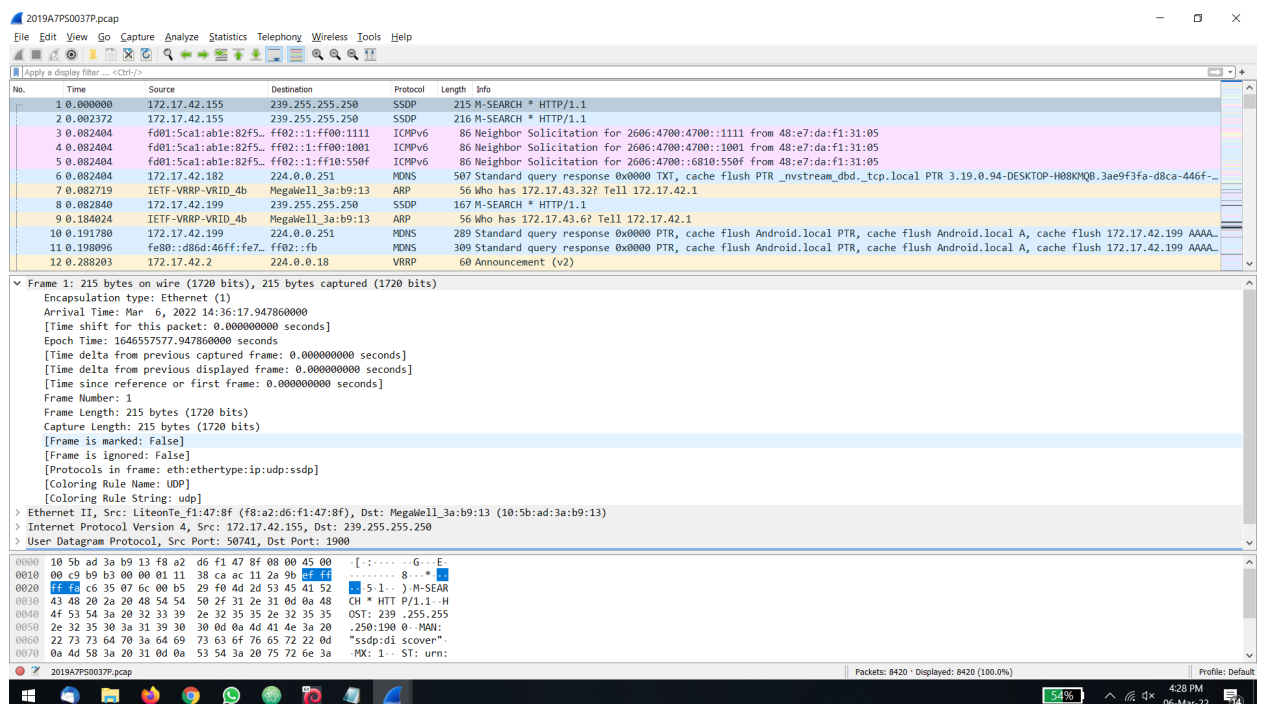
2019A7PS0037P

f20190037@pilani.bits-pilani.ac.in

Q.2 Traffic capturing and analysis using Wireshark.

1) What is the duration of your packet capture in seconds? What about the start and end time of the capture expressed in hh:mm:ss?

A. Duration of packet capture - 105.4550



B. Start and end time -

Arrival Time: 14:36:38.025

End Time - 14.36.38.209

Difference - 0.184 seconds

2019A7P50037P.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1663	15.853780	172.17.43.137	34.104.35.123	HTTP	348	HEAD /edged1/release2/chrome_component/aizfau43cwtbv7por6blaz3fnu_2022.3.4.1/kiabhabjdbkjdjbpigfodbdjmbg1coo_2022.03.04.01_a1_...
1861	20.077529	172.17.43.137	188.184.21.108	HTTP	544	GET /hypertext/WM/TheProject.html HTTP/1.1
1872	20.261757	188.184.21.108	172.17.43.137	HTTP	1044	HTTP/1.1 200 OK (text/html)
1957	22.125167	172.17.43.137	188.184.21.108	HTTP	574	GET /hypertext/DataSources/Top.html HTTP/1.1
1970	22.304041	188.184.21.108	172.17.43.137	HTTP	950	HTTP/1.1 200 OK (text/html)
2065	24.594205	172.17.43.137	188.184.21.108	HTTP	590	GET /hypertext/DataSources/bySubject/Overview.html HTTP/1.1
2098	25.378643	188.184.21.108	172.17.43.137	HTTP	427	HTTP/1.1 200 OK (text/html)
2183	27.331683	172.17.43.137	152.19.134.40	HTTP	550	GET /home/fullton/hypertext/nasa.html HTTP/1.1
2198	27.740844	152.19.134.40	172.17.43.137	HTTP	501	HTTP/1.1 302 Found (text/html)
2264	29.507465	172.17.43.137	152.19.134.40	HTTP	550	GET /home/fullton/hypertext/nasa.html HTTP/1.1
2285	29.909556	152.19.134.40	172.17.43.137	HTTP	460	HTTP/1.1 403 Forbidden (text/html)
2287	29.968013	172.17.43.137	152.19.134.40	HTTP	463	GET /favicon.ico HTTP/1.1
2314	30.298506	152.19.134.40	172.17.43.137	HTTP	1034	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
2418	31.762253	172.17.43.137	34.104.35.123	HTTP	451	HEAD /edged1/delta-update/gcmjkgd1gnkkccmoeminaijmjmjni/1.2e57d294ae2ce37ac58485ec6052861ef075fea318f9fce8facedb6dd86ef57/_...
4013	62.959139	172.17.43.137	34.104.35.123	HTTP	374	HEAD /edged1/release2/chrome_component/actk47kv3afhenygr3vulhmdua_20220222.431134436/obedbbhpmojnkancicoggnmlmoomoc_202202...
4042	63.605771	172.17.43.137	174.129.226.102	HTTP	552	GET /usr2/wwwtext/lii.table.html HTTP/1.1

Frame 1861: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface 0

Encapsulation type: Ethernet (1)

Arrival Time: Mar 6, 2022 14:36:38.025389000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1646557598.025389000 seconds

[Time delta from previous captured frame: 0.026936000 seconds]

[Time delta from previous displayed frame: 4.223749000 seconds]

[Time since reference or first frame: 20.077529000 seconds]

Frame Number: 1861

Frame Length: 544 bytes (4352 bits)

Capture Length: 544 bytes (4352 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http]

[Coloring Rule Name: HTTP]

0000 00 00 5e 00 01 4b 10 5b ad 3a b9 13 08 00 45 00 ...K [: : : : :E

0010 02 12 6d d9 40 00 80 06 e1 4d ac 11 2b 89 bc b8 ...m @ : : : : :M : + : : :

0020 15 6c cf db 00 50 16 28 8d 8a 8a 80 bd 78 50 18 ...l : : P (: : : : :xP

0030 02 01 ec 42 00 00 47 45 54 20 2f 68 79 65 72 ...B : G E T /hyper

0040 74 65 78 74 2f 57 57 57 2f 54 68 65 50 72 6f 6a text/WM/TheProj

0050 65 63 74 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e ect.html HTTP/1.

0060 31 0d 0a 48 6f 73 74 3a 20 69 6e 66 6f 2e 63 65 1-Host: info.ce

0070 72 6e 2e 63 68 0d 0a 43 6f 6e 6e 63 74 69 6f rn.ch : : C connectio

Absolute time when this frame was captured (Frame.time)

Packets: 8420 · Displayed: 26 (0.3%)

Profile: Default

2019A7P50037P.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1663	15.853780	172.17.43.137	34.104.35.123	HTTP	348	HEAD /edged1/release2/chrome_component/aizfau43cwtbv7por6blaz3fnu_2022.3.4.1/kiabhabjdbkjdjbpigfodbdjmbg1coo_2022.03.04.01_a1_...
1861	20.077529	172.17.43.137	188.184.21.108	HTTP	544	GET /hypertext/WM/TheProject.html HTTP/1.1
1872	20.261757	188.184.21.108	172.17.43.137	HTTP	1044	HTTP/1.1 200 OK (text/html)
1957	22.125167	172.17.43.137	188.184.21.108	HTTP	574	GET /hypertext/DataSources/Top.html HTTP/1.1
1970	22.304041	188.184.21.108	172.17.43.137	HTTP	950	HTTP/1.1 200 OK (text/html)
2065	24.594205	172.17.43.137	188.184.21.108	HTTP	590	GET /hypertext/DataSources/bySubject/Overview.html HTTP/1.1
2098	25.378643	188.184.21.108	172.17.43.137	HTTP	427	HTTP/1.1 200 OK (text/html)
2183	27.331683	172.17.43.137	152.19.134.40	HTTP	550	GET /home/fullton/hypertext/nasa.html HTTP/1.1
2198	27.740844	152.19.134.40	172.17.43.137	HTTP	501	HTTP/1.1 302 Found (text/html)
2264	29.507465	172.17.43.137	152.19.134.40	HTTP	550	GET /home/fullton/hypertext/nasa.html HTTP/1.1
2285	29.909556	152.19.134.40	172.17.43.137	HTTP	460	HTTP/1.1 403 Forbidden (text/html)
2287	29.968013	172.17.43.137	152.19.134.40	HTTP	463	GET /favicon.ico HTTP/1.1
2314	30.298506	152.19.134.40	172.17.43.137	HTTP	1034	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
2418	31.762253	172.17.43.137	34.104.35.123	HTTP	451	HEAD /edged1/delta-update/gcmjkgd1gnkkccmoeminaijmjmjni/1.2e57d294ae2ce37ac58485ec6052861ef075fea318f9fce8facedb6dd86ef57/_...
4013	62.959139	172.17.43.137	34.104.35.123	HTTP	374	HEAD /edged1/release2/chrome_component/actk47kv3afhenygr3vulhmdua_20220222.431134436/obedbbhpmojnkancicoggnmlmoomoc_202202...
4042	63.605771	172.17.43.137	174.129.226.102	HTTP	552	GET /usr2/wwwtext/lii.table.html HTTP/1.1

Frame 1872: 1044 bytes on wire (8352 bits), 1044 bytes captured (8352 bits) on interface 0

Encapsulation type: Ethernet (1)

Arrival Time: Mar 6, 2022 14:36:38.209617000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1646557598.209617000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.184228000 seconds]

[Time since reference or first frame: 20.261757000 seconds]

Frame Number: 1872

Frame Length: 1044 bytes (8352 bits)

Capture Length: 1044 bytes (8352 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]

[Coloring Rule Name: HTTP]

0000 10 5b ad 3a b9 13 f9 3e 90 b8 6f ac 08 00 45 00 ...[: : : : :> : : : : :E

0010 04 06 72 04 40 00 20 06 33 2f bc b8 15 6c ac 11 ...r @ (: : / : : : : :l

0020 2b 89 00 50 cf db 8a 80 c3 2c 16 28 8f 74 50 18 ...+ : P : : : : : , (: : P

0030 00 ed ba ab 00 00 41 0a 4e 41 4d 45 3d 33 35 20A : NAME=35

0040 48 52 45 46 3d 22 53 74 61 74 75 73 2e 68 74 6d HREF="St atus.htm

0050 6c 23 33 35 22 3e 56 69 6f 6c 61 3c 2f 41 3e 20 1835">vi olac

0060 2c 20 20 3c 41 0a 4e 41 4d 45 3d 32 36 20 48 52 , <A-NA ME=26 HR

Frame (1044 bytes) Reassembled TCP (2450 bytes)

Absolute time when this frame was captured (Frame.time)

Packets: 8420 · Displayed: 26 (0.3%)

Profile: Default

- 2) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received for the web pages (at least 3) you visited in your web browser?
 - a) 0.184 second b) 0.178 sec c) 0.209 sec
- 3) What is the Internet (IP) address of the URLs you visited and what is the Internet address of your computer?

IP address of websites visited =
(Info.cern.ch) - 188.184.21.108

4) What is the IP address of the DNS server you are connecting to?
172.24.2.76

2019A7P5037P.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	dns	Source	Destination	Protocol	Length	Info
176	dns	172.24.2.76	172.17.43.137	DNS	91	Standard query response 0x6f50 A www.gstatic.com A 172.217.166.195
1067	8.309300	172.17.43.137	172.24.2.76	DNS	75	Standard query 0x7eeb A ssl.gstatic.com
1068	8.311306	172.24.2.76	172.17.43.137	DNS	91	Standard query response 0x7eeb A ssl.gstatic.com A 142.250.194.67
1092	8.538978	172.17.43.137	172.24.2.76	DNS	75	Standard query 0xf9e4 A play.google.com
1096	8.582726	172.24.2.76	172.17.43.137	DNS	91	Standard query response 0xf9e4 A play.google.com A 142.250.193.78
1160	8.994842	172.17.43.137	172.24.2.76	DNS	72	Standard query 0xffff6 A www.iana.org
1161	9.061100	172.17.43.137	172.24.2.76	DNS	72	Standard query 0xffff6 A www.iana.org
1228	10.065156	172.17.43.137	172.24.2.76	DNS	72	Standard query 0xffff6 A www.iana.org
1266	10.527642	172.24.2.76	172.17.43.137	DNS	120	Standard query response 0xffff6 A www.iana.org CNAME ianawww.vip.icann.org A 192.0.33.8
1757	17.505401	172.17.43.137	172.24.2.76	DNS	77	Standard query 0x1544 A line-mode.cern.ch
1758	17.505401	172.17.43.137	172.24.2.76	DNS	76	Standard query 0xec3e A home.web.cern.ch
1760	17.572427	172.17.43.137	172.24.2.76	DNS	77	Standard query 0x1544 A line-mode.cern.ch
1761	17.572427	172.17.43.137	172.24.2.76	DNS	76	Standard query 0xec3e A home.web.cern.ch
1783	17.913465	172.24.2.76	172.17.43.137	DNS	157	Standard query response 0x1544 A line-mode.cern.ch CNAME paas-apps-shard-1.cern.ch A 188.184.28.132 A 188.184.103.181 A 188.18...
1802	18.576710	172.17.43.137	172.24.2.76	DNS	76	Standard query 0xec3e A home.web.cern.ch
1806	18.719803	172.24.2.76	172.17.43.137	DNS	158	Standard query response 0xec3e A home.web.cern.ch CNAME drupal-apps-shard-1.cern.ch A 188.185.87.101 A 188.185.88.30 A 137.138...

Frame 1806: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface 0

Encapsulation type: Ethernet (1)

Arrival Time: Mar 6, 2022 14:36:36.667663000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1646557596.667663000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.143093000 seconds]

[Time since reference or first frame: 18.719803000 seconds]

Frame Number: 1806

Frame Length: 158 bytes (1264 bits)

Capture Length: 158 bytes (1264 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:udp:dns]

[Coloring Rule Name: UDP]

0000 10 5b ad 3a b9 13 7c e2 ca b6 d7 f0 08 00 45 00 --[...].E-

0010 00 00 4a a7 00 00 3f 11 aa b7 ac 18 02 4c ac 11 --J...?L..

0020 2b 89 00 35 e0 25 00 7c c1 25 ec 3e 81 80 00 01 +-5.%| .%>....

0030 00 04 00 00 00 04 68 6f 6d 65 03 77 65 62 04h ome.web-

0040 63 65 72 6e 02 63 68 00 01 00 01 c0 0c 00 05 cern.ch.

0050 00 01 00 00 0c 00 16 13 64 72 75 70 61 6c 2d- drupal-

0060 61 70 70 73 2d 73 68 61 72 64 2d 31 c0 15 c0 2e apps-sha rd-1....

0070 00 01 00 01 00 00 3c 00 04 bc b9 57 65 c0 2e<We..

Domain Name System: Protocol

Packets: 8420 · Displayed: 162 (1.9%)

Profile: Default

4:48 PM 06-Mar-22

5) List the application layer protocols that you see in protocols field that are using UDP and TCP respectively.

6) Locate TCP handshake segments and find the sequence number of SYN, SYN+ACK and ACK messages of all the TCP connections made by your computer.

7) Find out all incoming (received by your machine) http traffic.

2019A7P50037P.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http && ip.dst == 172.17.43.137

No.	Time	Source	Destination	Protocol	Length	Info
1872	20.261757	188.184.21.108	172.17.43.137	HTTP	1044	HTTP/1.1 200 OK (text/html)
1970	22.304041	188.184.21.108	172.17.43.137	HTTP	950	HTTP/1.1 200 OK (text/html)
2008	25.378643	188.184.21.108	172.17.43.137	HTTP	427	HTTP/1.1 200 OK (text/html)
2198	27.740844	152.19.134.40	172.17.43.137	HTTP	501	HTTP/1.1 302 Found (text/html)
2285	29.909556	152.19.134.40	172.17.43.137	HTTP	460	HTTP/1.1 403 Forbidden (text/html)
2314	30.298506	152.19.134.40	172.17.43.137	HTTP	1034	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
4056	63.881308	174.129.226.102	172.17.43.137	HTTP	567	HTTP/1.1 301 Moved Permanently (text/html)
6257	71.996995	188.184.21.108	172.17.43.137	HTTP	1279	HTTP/1.1 200 OK (text/html)
6716	82.210565	134.158.69.34	172.17.43.137	HTTP	856	HTTP/1.1 200 OK (text/html)
7024	87.125681	134.79.138.26	172.17.43.137	HTTP	172	HTTP/1.0 302 Found

Frame 1872: 1044 bytes on wire (8352 bits), 1044 bytes captured (8352 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 6, 2022 14:36:30.209617000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1646557598.209617000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 20.261757000 seconds]

Frame Number: 1872

Frame Length: 1044 bytes (8352 bits)

Capture Length: 1044 bytes (8352 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]

[Coloring Rule Name: HTTP]

0000 10 5b ad 3a b9 13 f0 3e 90 b8 6f ac 08 00 45 00 ...[:...> ..o...E:
 0010 04 06 72 04 40 00 28 06 33 2f bc b8 15 6c ac 11 ...r.@.(. 3/-...l..
 0020 2b 89 00 50 cf db 8a 80 c3 2c 16 28 8f 74 50 18 ...P.....,(.tP..
 0030 00 ed ba ab 00 00 41 0a 4e 41 dd 45 3d 33 35 20A. NAME=35
 0040 48 52 45 46 3d 22 53 74 61 74 75 73 2e 68 74 6d HREF="st atos.htm
 0050 6c 23 33 35 22 3e 56 69 6f 6c 61 3c 2f 41 3e 20 1835">Vi ola
 0060 2c 20 20 3c 41 0a 4e 41 dd 45 3d 32 36 20 48 52 , <A-NA ME=26 HR

Frame (1044 bytes) Reassembled TCP (2450 bytes)

Epoch time when this frame was captured (frame.time_epoch)

Packets: 8420 · Displayed: 10 (0.1%)

Profile: Default

8) Find out the list of all TCP connections which have been reset. Provide appropriate reason for connection reset.

9) List all TCP segments which are sent and received by your machine having header length more than 20 bytes. Give the appropriate reason for header length larger than the default size.

10) List all the duplicate ACK TCP segments.

2019A7P50037P.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.analysis.duplicate_ack

No.	Time	Source	Destination	Protocol	Length	Info
1022	8.060737	172.17.43.137	142.250.193.14	TCP	66	[TCP Dup ACK 1021#1] 53204 → 443 [ACK] Seq=518 Ack=6073 Win=130560 Len=0 SLE=1 SRE=1431
1033	8.117796	172.17.43.137	142.250.193.14	TCP	66	[TCP Dup ACK 1021#2] 53204 → 443 [ACK] Seq=518 Ack=6073 Win=130560 Len=0 SLE=1 SRE=1431
1106	9.685143	172.217.166.195	172.17.43.137	TCP	56	[TCP Dup ACK 1090#1] 443 → 53209 [ACK] Seq=1 Ack=518 Win=65536 Len=0
1120	9.715153	172.17.43.137	172.217.166.195	TCP	66	[TCP Dup ACK 1114#1] 53205 → 443 [ACK] Seq=582 Ack=4340 Win=131328 Len=0 SLE=4291 SRE=4340
1132	9.812461	142.250.193.78	172.17.43.137	TCP	56	[TCP Dup ACK 1117#1] 443 → 53206 [ACK] Seq=1 Ack=518 Win=65536 Len=0
1222	9.923111	172.17.43.137	142.250.192.196	TCP	66	[TCP Dup ACK 911#1] 53203 → 443 [ACK] Seq=592 Ack=4408 Win=131328 Len=0 SLE=1 SRE=1431
1320	11.757900	172.17.43.137	172.217.194.188	TCP	66	[TCP Dup ACK 721#1] 53201 → 5228 [ACK] Seq=758 Ack=7313 Win=130816 Len=0 SLE=1 SRE=1431
1326	11.859242	172.17.43.137	142.250.206.99	TCP	66	[TCP Dup ACK 830#1] 53202 → 443 [ACK] Seq=5594 Ack=7023 Win=131328 Len=0 SLE=1 SRE=1431
1339	12.269245	172.17.43.137	142.250.193.14	TCP	66	[TCP Dup ACK 1061#1] 53204 → 443 [ACK] Seq=2204 Ack=23327 Win=131328 Len=0 SLE=1 SRE=1431
1465	13.805248	172.17.43.137	172.217.166.195	TCP	66	[TCP Dup ACK 1143#1] 53205 → 443 [ACK] Seq=582 Ack=4948 Win=130816 Len=0 SLE=1 SRE=1431
1483	13.941094	172.17.43.137	142.250.192.196	TCP	54	[TCP Dup ACK 1481#1] 53199 → 443 [ACK] Seq=5780 Ack=58258 Win=130560 Len=0
1486	13.941081	172.17.43.137	142.250.192.196	TCP	54	[TCP Dup ACK 1481#2] 53199 → 443 [ACK] Seq=5780 Ack=58258 Win=130560 Len=0
1528	14.428469	142.250.194.238	172.17.43.137	TCP	56	[TCP Dup ACK 1524#1] 443 → 53209 [ACK] Seq=1 Ack=518 Win=65536 Len=0
1561	14.623737	172.17.43.137	142.250.192.196	TCP	66	[TCP Dup ACK 1560#1] 53199 → 443 [ACK] Seq=7135 Ack=60800 Win=130384 Len=0 SLE=62230 SRE=62505
1592	14.931814	172.17.43.137	142.250.193.78	TCP	66	[TCP Dup ACK 1170#1] 53206 → 443 [ACK] Seq=1124 Ack=7828 Win=130384 Len=0 SLE=1 SRE=1431
1793	18.122924	172.17.43.137	142.250.194.238	TCP	66	[TCP Dup ACK 1614#1] 53209 → 443 [ACK] Seq=1341 Ack=8620 Win=131328 Len=0 SLE=1 SRE=1431
3695	57.019037	172.17.43.137	188.184.21.108	TCP	66	[TCP Dup ACK 2093#1] 53214 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 SLE=0 SRE=1
3939	62.044386	142.250.182.163	172.17.43.137	TCP	56	[TCP Dup ACK 3931#1] 443 → 53230 [ACK] Seq=1 Ack=518 Win=65536 Len=0
4111	64.402481	174.129.226.102	172.17.43.137	TCP	56	[TCP Dup ACK 4105#1] 443 → 53235 [ACK] Seq=1 Ack=518 Win=65664 Len=0
4138	64.083012	174.129.226.102	172.17.43.137	TCP	56	[TCP Dup ACK 4117#1] 443 → 53236 [ACK] Seq=1 Ack=518 Win=65664 Len=0
4235	65.109335	172.17.43.137	174.129.226.102	TCP	66	[TCP Dup ACK 4173#1] 53235 → 443 [ACK] Seq=2742 Ack=17500 Win=131328 Len=0 SLE=6684 SRE=6958
4244	65.140242	172.17.43.137	188.184.21.108	TCP	66	[TCP Dup ACK 2532#1] 53223 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 SLE=0 SRE=1
4310	65.314562	172.17.43.137	35.227.219.160	TCP	66	[TCP Dup ACK 4204#1] 53237 → 443 [ACK] Seq=3934 Ack=4702 Win=131328 Len=0 SLE=4291 SRE=4702
4322	65.335389	172.17.43.137	174.129.226.102	TCP	66	[TCP Dup ACK 4284#1] 53235 → 443 [ACK] Seq=2742 Ack=43279 Win=131328 Len=0 SLE=6684 SRE=6958
4323	65.346049	172.217.166.194	172.17.43.137	TCP	56	[TCP Dup ACK 4305#1] 443 → 53239 [ACK] Seq=1 Ack=518 Win=65536 Len=0

Frame 4138: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 6, 2022 14:37:22.551672000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1646557642.551672000 seconds

[Time delta from previous captured frame: 0.005079000 seconds]

0000 10 5b ad 3a b9 13 7c e2 ca b6 d7 f0 08 00 45 00 ...[:...>l..
 0010 00 28 42 0d 00 00 3f 06 d1 0a ae 81 e2 66 ac 11 ... (B...? .@...f..
 0020 2b 89 01 bb cf f4 23 3f ee dd 6f c2 87 11 50 10#? ..o...P..
 0030 02 01 6a b9 00 00 00 00 ...[:...> ..o...P..
 0040 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0050 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0060 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0070 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0080 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0090 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0100 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0110 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0120 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0130 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0140 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0150 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0160 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0170 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0180 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0190 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0200 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0210 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0220 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0230 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0240 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0250 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0260 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0270 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0280 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0290 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0300 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0310 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0320 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0330 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0340 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0350 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0360 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0370 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0380 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0390 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0400 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0410 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0420 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0430 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0440 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0450 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0460 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0470 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0480 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0490 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0500 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0510 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0520 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0530 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0540 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0550 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0560 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0570 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0580 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0590 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0600 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0610 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0620 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0630 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0640 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0650 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0660 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0670 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0680 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0690 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0700 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0710 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0720 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0730 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0740 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0750 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0760 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0770 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0780 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0790 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0800 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0810 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0820 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0830 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0840 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0850 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0860 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0870 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0880 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0890 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0900 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0910 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0920 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0930 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0940 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0950 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0960 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0970 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0980 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 0990 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1000 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1010 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1020 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1030 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1040 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1050 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1060 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1070 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1080 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1090 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1100 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1110 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1120 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1130 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1140 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1150 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1160 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1170 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1180 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1190 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1200 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1210 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1220 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1230 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1240 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1250 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1260 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1270 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1280 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1290 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1300 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1310 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1320 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1330 00 00 00 00 00 00 00 00 ...[:...> ..o...P..
 1340 00 00 00 00 00 00 00 00 ...[:...> ..o...P..

228

2019A7P50037P.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.analysis_out_order

No.	Time	Source	Destination	Protocol	Length	Info
228	2.163673	142.250.206.131	172.17.43.137	TCP	662	[TCP Out-Of-Order] 443 → 53194 [PSH, ACK] Seq=4680 Ack=994 Win=67840 Len=608
446	2.951544	142.250.192.196	172.17.43.137	TCP	1484	[TCP Out-Of-Order] 443 → 53200 [ACK] Seq=1 Ack=519 Win=66816 Len=1430
478	3.051986	142.250.192.196	172.17.43.137	TCP	93	[TCP Out-Of-Order] 443 → 53199 [PSH, ACK] Seq=6038 Ack=1617 Win=68352 Len=39
479	3.051986	142.250.192.196	172.17.43.137	TCP	149	[TCP Out-Of-Order] 443 → 53199 [PSH, ACK] Seq=6318 Ack=1617 Win=68352 Len=95
4370	65.450989	35.227.219.168	172.17.43.137	TCP	85	[TCP Out-Of-Order] 443 → 53237 [PSH, ACK] Seq=5282 Ack=3965 Win=76288 Len=31
4383	65.510779	172.217.166.194	172.17.43.137	TCP	992	[TCP Out-Of-Order] 443 → 53238 [PSH, ACK] Seq=4693 Ack=1120 Win=67840 Len=938
4642	66.031373	172.217.166.194	172.17.43.137	TCP	1484	[TCP Out-Of-Order] 443 → 53239 [ACK] Seq=5194 Ack=1100 Win=67840 Len=1430
5936	67.362774	216.58.221.46	172.17.43.137	TCP	662	[TCP Out-Of-Order] 443 → 53246 [PSH, ACK] Seq=4551 Ack=674 Win=66816 Len=608
5940	67.363152	216.58.221.46	172.17.43.137	TCP	85	[TCP Out-Of-Order] 443 → 53246 [PSH, ACK] Seq=5159 Ack=674 Win=66816 Len=31
5088	67.465107	216.58.221.46	172.17.43.137	TCP	1484	[TCP Out-Of-Order] 443 → 53246 [ACK] Seq=7021 Ack=1051 Win=67840 Len=1430
5089	67.465107	216.58.221.46	172.17.43.137	TCP	1484	[TCP Out-Of-Order] 443 → 53246 [ACK] Seq=8451 Ack=1051 Win=67840 Len=1430
5271	67.874581	142.250.194.162	172.17.43.137	TCP	662	[TCP Out-Of-Order] 443 → 53247 [PSH, ACK] Seq=4326 Ack=1169 Win=67840 Len=608
5411	68.181876	216.58.200.162	172.17.43.137	TCP	1484	[TCP Out-Of-Order] 443 → 53243 [ACK] Seq=36598 Ack=2364 Win=70912 Len=1430
5763	68.795548	142.250.194.162	172.17.43.137	TCP	1484	[TCP Out-Of-Order] 443 → 53255 [ACK] Seq=30559 Ack=1232 Win=67840 Len=1430
5764	68.795548	142.250.194.162	172.17.43.137	TCP	1484	[TCP Out-Of-Order] 443 → 53255 [ACK] Seq=31989 Ack=1232 Win=67840 Len=1430
5765	68.795548	142.250.194.162	172.17.43.137	TCP	1484	[TCP Out-Of-Order] 443 → 53255 [ACK] Seq=76319 Ack=1232 Win=67840 Len=1430
5766	68.795548	142.250.194.162	172.17.43.137	TCP	1484	[TCP Out-Of-Order] 443 → 53255 [PSH, ACK] Seq=77749 Ack=1232 Win=67840 Len=1430
5927	69.000342	172.217.167.34	172.17.43.137	TCP	1484	[TCP Out-Of-Order] 443 → 53245 [ACK] Seq=57593 Ack=1237 Win=67840 Len=1430
6013	69.139669	172.217.166.225	172.17.43.137	TCP	1484	[TCP Out-Of-Order] 443 → 53257 [ACK] Seq=29339 Ack=1582 Win=68864 Len=1430
7764	93.408170	142.250.194.10	172.17.43.137	TCP	1055	[TCP Out-Of-Order] 443 → 53286 [PSH, ACK] Seq=5846 Ack=1197 Win=67840 Len=1001
7841	93.986118	172.217.27.163	172.17.43.137	TCP	66	[TCP Out-Of-Order] 443 → 53289 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=256

Frame 479: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 6, 2022 14:36:20.999846000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1646557580.999846000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

0000 10 5b ad 3a b9 13 f0 3e 80 b8 6f ac 08 00 45 00 ...:....:o....

0010 00 28 72 05 40 00 20 06 37 0c bc b8 15 6e ac 31 ...:o-8(-7-...1-

0020 2b 89 00 5b cf db 8a 80 c7 0a 16 28 8f 74 50 11 ...:P....:..(-TP

0030 80 ed 3d 34 00 00 00 00 ...:....

Packets: 8420 · Displayed: 21 (0.2%)

Profile: Default

12) How many number of HTTP request (i.e., GET and POST) messages did your browser send?

Number of http - 11

13) Find out all the traffic between your machine and a particular (of your choice) web site (IP address).

2019A7P50037P.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 188.184.21.108 || ip.dst == 188.184.21.108

No.	Time	Source	Destination	Protocol	Length	Info
1748	17.396710	172.17.43.137	188.184.21.108	TCP	66	53211 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1749	17.397040	172.17.43.137	188.184.21.108	TCP	66	53212 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1763	17.594769	188.184.21.108	172.17.43.137	TCP	66	80 → 53212 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
1764	17.594769	188.184.21.108	172.17.43.137	TCP	66	80 → 53211 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
1766	17.594902	172.17.43.137	188.184.21.108	TCP	54	53212 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
1767	17.594908	172.17.43.137	188.184.21.108	TCP	54	53211 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
1861	20.077529	172.17.43.137	188.184.21.108	HTTP	544	GET /hypertext/WWW/TheProject.html HTTP/1.1
1862	20.081163	188.184.21.108	172.17.43.137	TCP	56	80 → 53211 [ACK] Seq=1 Ack=491 Win=29184 Len=0
1871	20.261757	188.184.21.108	172.17.43.137	TCP	1514	80 → 53211 [ACK] Seq=1 Ack=491 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
1872	20.261757	188.184.21.108	172.17.43.137	HTTP	1044	HTTP/1.1 200 OK (text/html)
1873	20.261757	188.184.21.108	172.17.43.137	TCP	56	80 → 53211 [FIN, ACK] Seq=2451 Ack=491 Win=30336 Len=0
1874	20.261861	172.17.43.137	188.184.21.108	TCP	54	53211 → 80 [ACK] Seq=491 Ack=2452 Win=131328 Len=0
1877	20.262611	172.17.43.137	188.184.21.108	TCP	54	53211 → 80 [FIN, ACK] Seq=491 Ack=2452 Win=131328 Len=0
1893	20.461227	188.184.21.108	172.17.43.137	TCP	56	80 → 53211 [ACK] Seq=2452 Ack=492 Win=30336 Len=0
1956	22.124155	172.17.43.137	188.184.21.108	TCP	66	53213 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1957	22.125167	172.17.43.137	188.184.21.108	HTTP	574	GET /hypertext/DataSources/Top.html HTTP/1.1
1958	22.128049	188.184.21.108	172.17.43.137	TCP	56	80 → 53212 [ACK] Seq=1 Ack=521 Win=29184 Len=0
1970	22.304041	188.184.21.108	172.17.43.137	HTTP	950	HTTP/1.1 200 OK (text/html)
1971	22.304041	188.184.21.108	172.17.43.137	TCP	56	80 → 53212 [FIN, ACK] Seq=897 Ack=521 Win=30336 Len=0
1972	22.304248	172.17.43.137	188.184.21.108	TCP	54	53212 → 80 [ACK] Seq=521 Ack=898 Win=130304 Len=0
1973	22.305273	172.17.43.137	188.184.21.108	TCP	54	53212 → 80 [FIN, ACK] Seq=521 Ack=898 Win=130304 Len=0
1979	22.407312	188.184.21.108	172.17.43.137	TCP	66	80 → 53213 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
1980	22.407389	172.17.43.137	188.184.21.108	TCP	54	53213 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
1991	22.509927	188.184.21.108	172.17.43.137	TCP	56	80 → 53212 [ACK] Seq=898 Ack=522 Win=30336 Len=0
2064	24.593523	172.17.43.137	188.184.21.108	TCP	66	53214 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

Frame 1873: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 6, 2022 14:36:38.209617000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1646557598.209617000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

0000 10 5b ad 3a b9 13 f0 3e 80 b8 6f ac 08 00 45 00 ...:....:o....

0010 00 28 72 05 40 00 20 06 37 0c bc b8 15 6e ac 31 ...:o-8(-7-...1-

0020 2b 89 00 5b cf db 8a 80 c7 0a 16 28 8f 74 50 11 ...:P....:..(-TP

0030 80 ed 3d 34 00 00 00 00 ...:....

Frame (frame), 56 bytes

Packets: 8420 · Displayed: 84 (1.0%)

Profile: Default

14) Calculate the throughput of all the TCP connection involved in question 13.

