

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?

No.	Time	Source	Destination	Protocol	Length	Info
20331	160.165954	172.17.42.38	255.255.255.255	DB-LSP...	188	Dropbox LAN sync D
20332	160.166961	172.17.42.38	255.255.255.255	DB-LSP...	188	Dropbox LAN sync D
20333	160.166961	172.17.42.38	172.17.43.255	DB-LSP...	188	Dropbox LAN sync D
20334	160.166961	172.17.42.38	255.255.255.255	DB-LSP...	188	Dropbox LAN sync D
20335	160.166961	172.17.42.38	255.255.255.255	DB-LSP...	188	Dropbox LAN sync D
20336	160.256873	172.17.42.213	224.0.0.251	MDNS	83	Standard query 0x0
20337	160.256873	172.17.42.213	224.0.0.251	MDNS	345	Standard query res
20338	160.278426	172.17.42.2	224.0.0.18	VRRP	60	Announcement (v2)
20339	160.359354	IntelCor_44:dd:24	MegaWELL_c8:39:e7	ARP	56	Who has 169.254.16

Total Duration: 160.359354 s

In hh:mm:ss format :- START

No.	Time	Source	Destination	Protocol	Length	Info
1	06:12:29.212134	fe80::d187:74c8:459...	ff02::1	ICMPv6	86	Neighbor
2	06:12:29.212134	172.17.42.92	239.255.255.250	SSDP	179	M-SEARCH
3	06:12:29.212134	fe80::d187:74c8:459...	ff02::1:2	DHCPv6	157	Solicit
4	06:12:29.212134	172.17.42.182	239.255.255.250	SSDP	216	M-SEARCH
5	06:12:29.212945	Chongqin_28:b2:7d	MegaWELL_c8:39:e7	ARP	56	Who has
6	06:12:29.314697	172.17.43.55	224.0.0.251	MDNS	70	Standard
7	06:12:29.314697	172.17.43.55	224.0.0.251	MDNS	70	Standard
8	06:12:29.314697	fe80::3df9:dce7:671...	ff02::fb	MDNS	90	Standard
9	06:12:29.314697	fe80::3df9:dce7:671...	ff02::fb	MDNS	90	Standard
10	06:12:29.314697	172.17.42.282	239.255.255.250	SSDP	216	M-SEARCH

END:

No.	Time	Source	Destination	Protocol	Length	Info
20331	06:15:09.378088	172.17.42.38	255.255.255.255	DB-LSP...	188	Dropbox LAN sync D
20332	06:15:09.379095	172.17.42.38	255.255.255.255	DB-LSP...	188	Dropbox LAN sync D
20333	06:15:09.379095	172.17.42.38	172.17.43.255	DB-LSP...	188	Dropbox LAN sync D
20334	06:15:09.379095	172.17.42.38	255.255.255.255	DB-LSP...	188	Dropbox LAN sync D
20335	06:15:09.379095	172.17.42.38	255.255.255.255	DB-LSP...	188	Dropbox LAN sync D
20336	06:15:09.469007	172.17.42.213	224.0.0.251	MDNS	83	Standard query 0x0
20337	06:15:09.469007	172.17.42.213	224.0.0.251	MDNS	345	Standard query res
20338	06:15:09.490560	172.17.42.2	224.0.0.18	VRRP	60	Announcement (v2)
20339	06:15:09.571488	IntelCor_44:dd:24	MegaWELL_c8:39:e7	ARP	56	Who has 169.254.16

2) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received for the webpages (at least 3) you visited in your web browser?

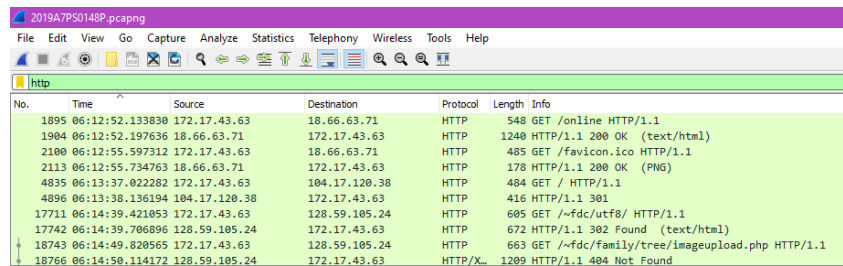
**SITE 1:-0.0636 s**



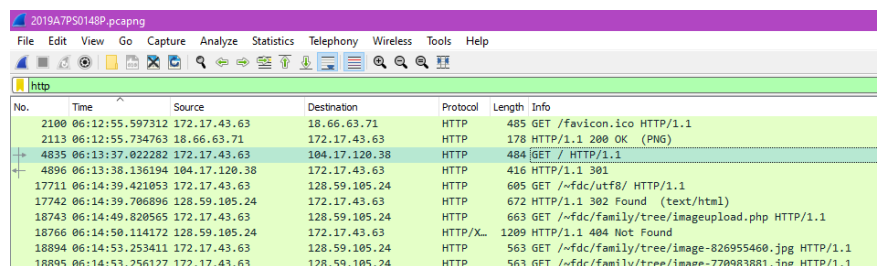
3) What is the Internet (IP) address of the URLs you visited and what is the Internet address of your computer?

IP of the sites:= 18.66.63.71, 104.17.120.58, 65.61.157.117

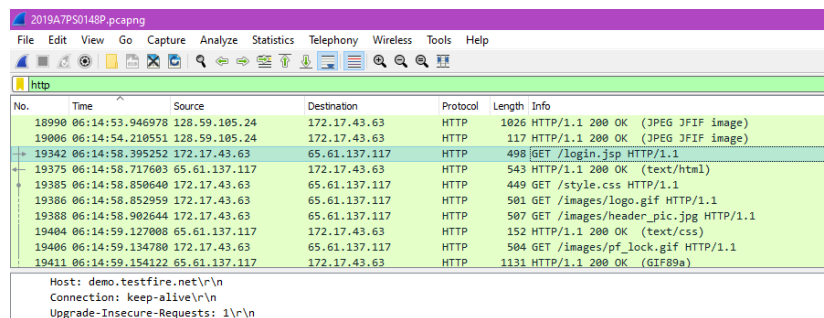
IP of the system:= 172.17.45.63



No.	Time	Source	Destination	Protocol	Length	Info
1895	06:12:52.133830	172.17.43.63	18.66.63.71	HTTP	548	GET /online HTTP/1.1
1904	06:12:52.197636	18.66.63.71	172.17.43.63	HTTP	1240	HTTP/1.1 200 OK (text/html)
2100	06:12:55.597312	172.17.43.63	18.66.63.71	HTTP	485	GET /favicon.ico HTTP/1.1
2113	06:12:55.734763	18.66.63.71	172.17.43.63	HTTP	178	HTTP/1.1 200 OK (PNG)
4835	06:13:37.022282	172.17.43.63	104.17.120.38	HTTP	484	GET / HTTP/1.1
4896	06:13:38.136194	104.17.120.38	172.17.43.63	HTTP	416	HTTP/1.1 301
17711	06:14:39.421053	172.17.43.63	128.59.105.24	HTTP	605	GET /~fdc/utf8/ HTTP/1.1
17742	06:14:39.706896	128.59.105.24	172.17.43.63	HTTP	672	HTTP/1.1 302 Found (text/html)
18743	06:14:49.820565	172.17.43.63	128.59.105.24	HTTP	663	GET /~fdc/family/tree/imageupload.php HTTP/1.1
18766	06:14:50.114172	128.59.105.24	172.17.43.63	HTTP/X	1209	HTTP/1.1 404 Not Found



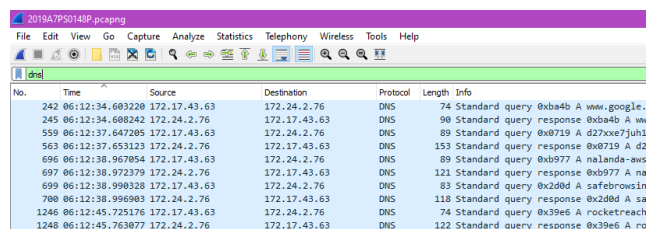
No.	Time	Source	Destination	Protocol	Length	Info
2100	06:12:55.597312	172.17.43.63	18.66.63.71	HTTP	485	GET /favicon.ico HTTP/1.1
2113	06:12:55.734763	18.66.63.71	172.17.43.63	HTTP	178	HTTP/1.1 200 OK (PNG)
4835	06:13:37.022282	172.17.43.63	104.17.120.38	HTTP	484	GET / HTTP/1.1
4896	06:13:38.136194	104.17.120.38	172.17.43.63	HTTP	416	HTTP/1.1 301
17711	06:14:39.421053	172.17.43.63	128.59.105.24	HTTP	605	GET /~fdc/utf8/ HTTP/1.1
17742	06:14:39.706896	128.59.105.24	172.17.43.63	HTTP	672	HTTP/1.1 302 Found (text/html)
18743	06:14:49.820565	172.17.43.63	128.59.105.24	HTTP	663	GET /~fdc/family/tree/imageupload.php HTTP/1.1
18766	06:14:50.114172	128.59.105.24	172.17.43.63	HTTP/X	1209	HTTP/1.1 404 Not Found
18894	06:14:53.253411	172.17.43.63	128.59.105.24	HTTP	563	GET /~fdc/family/tree/image-826955460.jpg HTTP/1.1
18895	06:14:53.256127	172.17.43.63	128.59.105.24	HTTP	563	GET /~fdc/family/tree/image-770983881.jpg HTTP/1.1



No.	Time	Source	Destination	Protocol	Length	Info
18990	06:14:53.946978	128.59.105.24	172.17.43.63	HTTP	1026	HTTP/1.1 200 OK (JPEG JFIF image)
19006	06:14:54.210551	128.59.105.24	172.17.43.63	HTTP	117	HTTP/1.1 200 OK (JPEG JFIF image)
19342	06:14:58.395252	172.17.43.63	65.61.137.117	HTTP	498	GET /login.jsp HTTP/1.1
19375	06:14:58.717603	65.61.137.117	172.17.43.63	HTTP	543	HTTP/1.1 200 OK (text/html)
19385	06:14:58.850640	172.17.43.63	65.61.137.117	HTTP	449	GET /style.css HTTP/1.1
19386	06:14:58.852959	172.17.43.63	65.61.137.117	HTTP	501	GET /images/logo.gif HTTP/1.1
19388	06:14:58.902644	172.17.43.63	65.61.137.117	HTTP	507	GET /images/header_pic.jpg HTTP/1.1
19404	06:14:59.127008	65.61.137.117	172.17.43.63	HTTP	152	HTTP/1.1 200 OK (text/css)
19406	06:14:59.134780	172.17.43.63	65.61.137.117	HTTP	504	GET /images/pf_lock.gif HTTP/1.1
19411	06:14:59.154122	65.61.137.117	172.17.43.63	HTTP	1131	HTTP/1.1 200 OK (GIF89a)

Host: demo.testfire.net\r\n  
Connection: keep-alive\r\n  
Upgrade-Insecure-Requests: 1\r\n

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

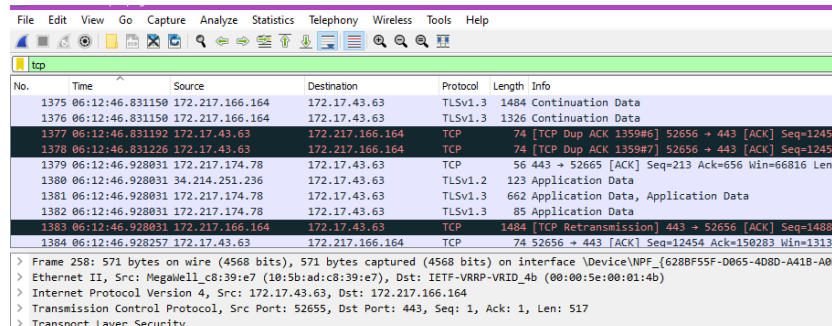


No.	Time	Source	Destination	Protocol	Length	Info
242	06:12:34.603220	172.17.43.63	172.24.2.76	DNS	74	Standard query 0xb4b A www.google.
245	06:12:34.608242	172.24.2.76	172.17.43.63	DNS	90	Standard query response 0xb4b A www.google.
559	06:12:37.647205	172.17.43.63	172.24.2.76	DNS	89	Standard query 0xb719 A d27xxe7juh1
563	06:12:37.653123	172.24.2.76	172.17.43.63	DNS	153	Standard query response 0xb719 A d27xxe7juh1
696	06:12:38.967054	172.17.43.63	172.24.2.76	DNS	89	Standard query 0xb977 A naland-aus
697	06:12:38.972379	172.24.2.76	172.17.43.63	DNS	121	Standard query response 0xb977 A naland-aus
699	06:12:38.990328	172.17.43.63	172.24.2.76	DNS	83	Standard query 0x20bd A safebrowsin
700	06:12:38.996983	172.24.2.76	172.17.43.63	DNS	118	Standard query response 0x20bd A safebrowsin
1246	06:12:45.725176	172.17.43.63	172.24.2.76	DNS	74	Standard query 0x39e6 A rocketreac
1248	06:12:45.763077	172.24.2.76	172.17.43.63	DNS	122	Standard query response 0x39e6 A rocketreac

Ans:- 172.24.2.76

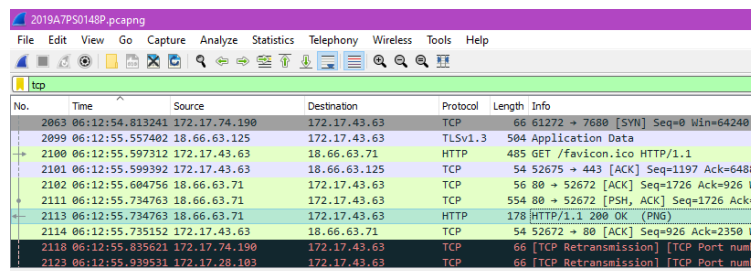
5) List the application layer protocols that you see in protocols field that are using UDP and TCP respectively.

**TCP: TLSv1.2, TLSv1.3, http**



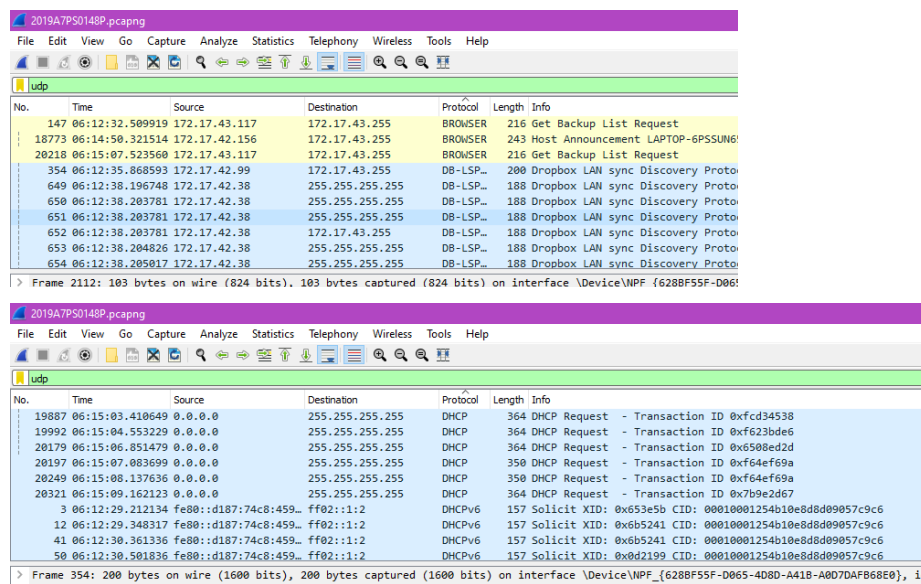
No.	Time	Source	Destination	Protocol	Length	Info
1375	06:12:46.831150	172.217.166.164	172.17.43.63	TLSv1.3	1484	Continuation Data
1376	06:12:46.831150	172.217.166.164	172.17.43.63	TLSv1.3	1326	Continuation Data
1377	06:12:46.831192	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 1359#6] 52656 → 443 [ACK] Seq=1245
1378	06:12:46.831226	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 1359#7] 52656 → 443 [ACK] Seq=1245
1379	06:12:46.928031	172.217.174.78	172.17.43.63	TCP	56	443 → 52665 [ACK] Seq=213 Ack=656 Win=66816 Len=
1380	06:12:46.928031	34.214.251.236	172.17.43.63	TLSv1.2	123	Application Data
1381	06:12:46.928031	172.217.174.78	172.17.43.63	TLSv1.3	662	Application Data, Application Data
1382	06:12:46.928031	172.217.174.78	172.17.43.63	TLSv1.3	85	Application Data
1383	06:12:46.928031	172.217.166.164	172.17.43.63	TCP	1484	[TCP Retransmission] 443 → 52656 [ACK] Seq=1488
1384	06:12:46.928257	172.17.43.63	172.217.166.164	TCP	74	52656 → 443 [ACK] Seq=12454 Ack=150283 Win=1313

> Frame 258: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF\_{628BF55F-D065-4D8D-A41B-A007DAF68E00} (00:00:00:00:00:00) on interface 0  
> Ethernet II, Src: MegaWell\_c8:39:e7 (10:5b:ad:c8:39:e7), Dst: IETF-VRRP-VRID\_4b (00:00:5e:00:01:4b)  
> Internet Protocol Version 4, Src: 172.17.43.63, Dst: 172.217.166.164  
> Transmission Control Protocol, Src Port: 52655, Dst Port: 443, Seq: 1, Ack: 1, Len: 517  
> Transport Layer Security



No.	Time	Source	Destination	Protocol	Length	Info
2063	06:12:54.813241	172.17.74.190	172.17.43.63	TCP	66	61272 → 7680 [SYN] Seq=0 Win=64240
2099	06:12:55.557402	18.66.63.125	172.17.43.63	TLSv1.3	504	Application Data
2100	06:12:55.597312	172.17.43.63	18.66.63.71	HTTP	485	GET /favicon.ico HTTP/1.1
2101	06:12:55.599392	172.17.43.63	18.66.63.125	TCP	54	52675 → 443 [ACK] Seq=1197 Ack=6488
2102	06:12:55.604756	18.66.63.71	172.17.43.63	TCP	56	80 → 52672 [ACK] Seq=1726 Ack=926 W
2111	06:12:55.734763	18.66.63.71	172.17.43.63	TCP	554	80 → 52672 [PSH, ACK] Seq=1726 Ack=
2113	06:12:55.734763	18.66.63.71	172.17.43.63	HTTP	178	HTTP/1.1 200 OK (PNG)
2114	06:12:55.735152	172.17.43.63	18.66.63.71	TCP	54	52672 → 80 [ACK] Seq=926 Ack=2350 W
2118	06:12:55.835621	172.17.74.190	172.17.43.63	TCP	66	[TCP Retransmission] [TCP Port numb
2123	06:12:55.939531	172.17.28.103	172.17.43.63	TCP	66	[TCP Retransmission] [TCP Port numb

**Udp: BROWSER, Dropbox LAN sync Discovery Protocol, DHCP, DHCPv6, DNS, IPv6, LLMNR, MDNS, NBNS, RIPv1, SSDP, UDP**



No.	Time	Source	Destination	Protocol	Length	Info
147	06:12:32.509919	172.17.43.117	172.17.43.255	BROWSER	216	Get Backup List Request
18773	06:14:50.321514	172.17.42.156	172.17.43.255	BROWSER	243	Host Announcement LAPTOP-6PSSUN6
20218	06:15:07.523560	172.17.43.117	172.17.43.255	BROWSER	216	Get Backup List Request
354	06:12:35.868593	172.17.42.99	172.17.43.255	DB-LSP...	200	Dropbox LAN sync Discovery Proto
649	06:12:38.196748	172.17.42.38	255.255.255.255	DB-LSP...	188	Dropbox LAN sync Discovery Proto
650	06:12:38.203781	172.17.42.38	255.255.255.255	DB-LSP...	188	Dropbox LAN sync Discovery Proto
651	06:12:38.203781	172.17.42.38	255.255.255.255	DB-LSP...	188	Dropbox LAN sync Discovery Proto
652	06:12:38.203781	172.17.42.38	172.17.43.255	DB-LSP...	188	Dropbox LAN sync Discovery Proto
653	06:12:38.204826	172.17.42.38	255.255.255.255	DB-LSP...	188	Dropbox LAN sync Discovery Proto
654	06:12:38.205017	172.17.42.38	255.255.255.255	DB-LSP...	188	Dropbox LAN sync Discovery Proto

> Frame 2112: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF\_{628BF55F-D065-4D8D-A41B-A007DAF68E00} (00:00:00:00:00:00) on interface 0

No.	Time	Source	Destination	Protocol	Length	Info
19887	06:15:03.410649	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xfcd34538
19992	06:15:04.553229	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xf623bde6
20179	06:15:06.851479	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x6590ed2d
20197	06:15:07.003699	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0xf64ef69a
20249	06:15:08.137636	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0xf64ef69a
20321	06:15:09.162123	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x7b9e2d67
3	06:12:29.212134	fe80::d187:74c8:459...	ff02::1:2	DHCPv6	157	Solicit XID: 0x653e5b CID: 00010001254b10e8d8d09057c9c6
12	06:12:29.348317	fe80::d187:74c8:459...	ff02::1:2	DHCPv6	157	Solicit XID: 0x6b5241 CID: 00010001254b10e8d8d09057c9c6
41	06:12:30.361336	fe80::d187:74c8:459...	ff02::1:2	DHCPv6	157	Solicit XID: 0x6b5241 CID: 00010001254b10e8d8d09057c9c6
50	06:12:30.501836	fe80::d187:74c8:459...	ff02::1:2	DHCPv6	157	Solicit XID: 0x0d2199 CID: 00010001254b10e8d8d09057c9c6

> Frame 354: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF\_{628BF55F-D065-4D8D-A41B-A007DAF68E00} (00:00:00:00:00:00) on interface 0

2019A7P50148P.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
20248	06:15:06.041311	fe80::d187:74c8:459...	ff02::1:2	DHCPv6	157	Solicit XID: 0xdc37fb CI
20318	06:15:09.059486	fe80::d187:74c8:459...	ff02::1:2	DHCPv6	157	Solicit XID: 0xdc37fb CI
20323	06:15:09.172528	fe80::d187:74c8:459...	ff02::1:2	DHCPv6	157	Solicit XID: 0xf45c69 CI
242	06:12:34.603220	172.17.43.63	172.24.2.76	DNS	74	Standard query 0xba4b A
245	06:12:34.608242	172.24.2.76	172.17.43.63	DNS	90	Standard query response
559	06:12:37.647205	172.17.43.63	172.24.2.76	DNS	89	Standard query 0xb719 A
563	06:12:37.653123	172.24.2.76	172.17.43.63	DNS	153	Standard query response
696	06:12:38.967054	172.17.43.63	172.24.2.76	DNS	89	Standard query 0xb977 A
697	06:12:38.972379	172.24.2.76	172.17.43.63	DNS	121	Standard query response
699	06:12:38.990328	172.17.43.63	172.24.2.76	DNS	83	Standard query 0x2d0d A

2019A7P50148P.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
19474	06:14:59.479478	172.24.2.76	172.17.43.63	DNS	86	Standard query response 0xidac A g
19595	06:15:00.490595	172.17.43.63	172.24.2.76	DNS	81	Standard query 0x739e A plugin.roc
19602	06:15:00.529398	172.24.2.76	172.17.43.63	DNS	113	Standard query response 0x739e A p
19737	06:15:01.141064	2001:0:2051:fc00:3c...	ff02::1	IPv6	82	IPv6 no next header
70	06:12:30.985609	fe80::59c6:aa81:9d5...	ff02::1:3	LLMNR	92	Standard query 0x990b A MACBOOKAIR
71	06:12:30.985609	172.17.43.103	224.0.0.252	LLMNR	75	Standard query 0x990b A MACBOOKAIR
89	06:12:31.465701	fe80::59c6:aa81:9d5...	ff02::1:3	LLMNR	95	Standard query 0x990b A MACBOOKAIR
90	06:12:31.465701	172.17.43.103	224.0.0.252	LLMNR	75	Standard query 0x990b A MACBOOKAIR
303	06:12:35.461225	fe80::faf3:6eff:409...	ff02::1:3	LLMNR	84	Standard query 0x3823 A wpad
304	06:12:35.461225	172.17.43.105	224.0.0.252	LLMNR	64	Standard query 0x3823 A wpad

> Frame 354: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF\_{628BF55F-D065-4D80-A418-A0D7DAF68E0}

2019A7P50148P.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
20044	06:15:04.860933	172.17.43.105	224.0.0.252	LLMNR	64	Standard query 0xbd5d AAAA wpad
20276	06:15:08.484429	fe80::fda3:4c14:104...	ff02::1:3	LLMNR	95	Standard query 0x8b91 ANY LAPTOP-3T3A\WD24
20277	06:15:08.484429	172.17.43.203	224.0.0.252	LLMNR	75	Standard query 0x8b91 ANY LAPTOP-3T3A\WD24
20291	06:15:08.500392	fe80::fda3:4c14:104...	ff02::1:3	LLMNR	95	Standard query 0x41c2 ANY LAPTOP-3T3A\WD24
20292	06:15:08.500392	172.17.43.203	224.0.0.252	LLMNR	75	Standard query 0x41c2 ANY LAPTOP-3T3A\WD24
6	06:12:29.314697	172.17.43.55	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
7	06:12:29.314697	172.17.43.55	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
8	06:12:29.314697	fe80::3df9:dce7:671...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
9	06:12:29.314697	fe80::3df9:dce7:671...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
22	06:12:29.783661	172.17.42.102	224.0.0.251	MDNS	79	Standard query 0xd4ee PTR arduino.tcp.local, "QM"

> Frame 354: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF\_{628BF55F-D065-4D80-A418-A0D7DAF68E0}, id 0

20118	06:15:05.931748	172.17.43.105	172.17.43.255	NBNS	92	Name query NB WPAD<00>
20119	06:15:05.947376	172.17.43.105	172.17.43.255	NBNS	92	Name query NB WPAD<00>
20120	06:15:05.949496	172.17.43.105	172.17.43.255	NBNS	92	Name query NB WPAD<00>
20217	06:15:07.523560	172.17.43.117	172.17.43.255	NBNS	92	Name query NB WORKGROUP<1d>
12683	06:14:00.767102	172.17.43.81	172.17.43.255	RIPv1	66	Request
13248	06:14:04.430635	172.17.43.81	172.17.43.255	RIPv1	66	Request
13495	06:14:05.694626	172.17.43.81	172.17.43.255	RIPv1	66	Request
2	06:12:29.212134	172.17.42.92	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
4	06:12:29.212134	172.17.42.102	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

> Frame 354: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF\_{628BF55F-D065-4D80-A418-A0D7DAF68E0}, id 0

2019A7P50148P.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
20271	06:15:08.467414	172.17.43.119	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
20296	06:15:08.649828	172.17.42.249	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
20299	06:15:08.649828	172.17.43.167	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
20305	06:15:08.791057	172.17.43.167	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
20317	06:15:09.059486	172.17.42.54	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
33	06:12:30.031802	172.17.42.162	172.17.43.255	UDP	305	54915 → 54915 Len=263
74	06:12:31.008472	172.17.42.162	172.17.43.255	UDP	305	54915 → 54915 Len=263
126	06:12:32.007124	172.17.42.162	172.17.43.255	UDP	305	54915 → 54915 Len=263
162	06:12:32.003910	172.17.43.97	172.17.43.255	UDP	86	57621 → 57621 Len=44
171	06:12:33.049036	172.17.42.162	172.17.43.255	UDP	305	54915 → 54915 Len=263

> Frame 354: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF\_{628BF55F-D065-4D80-A418-A0D7DAF68E0}, id 0

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.

Multiple Instances of handshakes occur. The SEQ and ACK however is constant for all. We have shown the Screenshots for some.

Syn: seq = 0

Syn, ack : seq = 0, ack = 1

Ack: seq = 1, ack = 1

236	5.257475	128.59.105.24	172.17.43.63	TCP	54 80 → 52635 [ACK] Seq=1 Ack=2 Win=11447 Len=0
237	5.258812	128.59.105.24	172.17.43.63	TCP	54 80 → 52638 [ACK] Seq=1 Ack=2 Win=11098 Len=0
246	5.398911	172.17.43.63	172.217.166.164	TCP	54 52652 → 443 [FIN, ACK] Seq=2 Ack=1 Win=513 Len=0
247	5.400793	172.17.43.63	172.217.166.164	TCP	66 52655 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
248	5.529257	172.217.166.164	172.17.43.63	TCP	66 443 → 52655 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
255	5.529525	172.17.43.63	172.217.166.164	TCP	54 52655 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0

435	7.120345	172.17.43.63	128.59.105.24	TCP	54 52638 → 80 [ACK] Seq=3 Ack=2 Win=64240 Len=0
443	7.214366	172.17.43.63	172.217.166.164	TCP	66 52656 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
447	7.251986	172.217.166.164	172.17.43.63	TCP	66 443 → 52656 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
448	7.252204	172.17.43.63	172.217.166.164	TCP	54 52656 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
449	7.253681	172.17.43.63	172.217.166.164	TLSv1.3	772 Client Hello
452	7.274888	172.217.166.164	172.17.43.63	TFO	56 443 → 52656 [ACK] Seq=1 Ack=2 Win=65536 Len=0

564	8.442392	172.17.43.63	18.66.85.53	TCP	66 52657 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
568	8.461307	18.66.85.53	172.17.43.63	TCP	66 443 → 52657 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM=1 WS=512
569	8.461468	172.17.43.63	18.66.85.53	TCP	54 52657 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
570	8.462176	172.17.43.63	18.66.85.53	TLSv1.3	571 Client Hello
571	8.466888	18.66.85.53	172.17.43.63	TCP	56 443 → 52657 [ACK] Seq=1 Ack=518 Win=65536 Len=0
578	8.488341	18.66.85.53	172.17.43.63	TLSv1.3	1494 Server Hello, Change Cipher Spec, Application Data

954	11.974627	172.17.43.63	13.232.160.203	TCP	66 52661 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
955	12.015047	172.17.43.63	172.217.166.164	TLSv1.3	243 Application Data
956	12.018379	13.232.160.203	172.17.43.63	TCP	66 443 → 52661 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM=1 WS=256
957	12.018379	18.66.85.53	172.17.43.63	TCP	1494 [TCP Spurious Retransmission] 443 → 52657 [PSH, ACK] Seq=1 Ack=518 Win=65536 Len=1440
958	12.018640	172.17.43.63	18.66.85.53	TCP	66 [TCP Dup ACK 595#2] 52657 → 443 [ACK] Seq=1113 Ack=6415 Win=131840 Len=0 SLE=1 SRE=1441
959	12.018844	172.17.43.63	13.232.160.203	TCP	54 52661 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
960	12.019779	172.17.43.63	13.232.160.203	TLSv1.2	571 Client Hello
962	12.024941	13.232.160.203	172.17.43.63	TCP	56 443 → 52661 [ACK] Seq=1 Ack=518 Win=65536 Len=0
968	12.052022	172.217.166.164	172.17.43.63	TCP	56 443 → 52656 [ACK] Seq=14677 Ack=7681 Win=110080 Len=0

1095	13.778550	172.17.43.63	172.217.166.164	TCP	54 52656 → 443 [ACK] Seq=9193 Ack=34192 Win=131328 Len=0
1099	13.875282	172.17.43.63	142.251.12.100	TCP	66 52662 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1101	13.967669	142.251.12.100	172.17.43.63	TCP	66 443 → 52662 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
1102	13.967789	172.17.43.63	142.251.12.100	TCP	54 52662 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
1103	13.968390	172.17.43.63	142.251.12.100	TLSv1.3	649 Client Hello
1104	13.972720	142.251.12.100	172.17.43.63	TCP	56 443 → 52662 [ACK] Seq=1 Ack=596 Win=65536 Len=0
1106	14.067911	142.251.12.100	172.17.43.63	TLSv1.3	266 Server Hello, Change Cipher Spec, Application Data
1107	14.069866	172.17.43.63	142.251.12.100	TLSv1.3	118 Change Cipher Spec, Application Data
1108	14.070577	172.17.43.63	142.251.12.100	TLSv1.3	146 Application Data
1109	14.071245	172.17.43.63	142.251.12.100	TLSv1.3	563 Application Data
1113	14.163604	142.251.12.100	172.17.43.63	TLSv1.3	663 Application Data, Application Data

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

1904	06:12:52.197636	18.66.63.71	172.17.43.63	HTTP	1240 HTTP/1.1 200 OK (text/html)
2113	06:12:55.734763	18.66.63.71	172.17.43.63	HTTP	178 HTTP/1.1 200 OK (PNG)
4896	06:13:38.136194	104.17.120.38	172.17.43.63	HTTP	416 HTTP/1.1 301
17742	06:14:39.706896	128.59.105.24	172.17.43.63	HTTP	672 HTTP/1.1 302 Found (text/html)
18766	06:14:50.114172	128.59.105.24	172.17.43.63	HTTP/X.	1209 HTTP/1.1 404 Not Found
18913	06:14:53.597415	128.59.105.24	172.17.43.63	HTTP	898 HTTP/1.1 200 OK (JPEG JFIF image)
18926	06:14:53.599105	128.59.105.24	172.17.43.63	HTTP	308 HTTP/1.1 200 OK (JPEG JFIF image)
18958	06:14:53.888012	128.59.105.24	172.17.43.63	HTTP	631 HTTP/1.1 200 OK (JPEG JFIF image)
18966	06:14:53.894159	128.59.105.24	172.17.43.63	HTTP	1215 HTTP/1.1 200 OK (JPEG JFIF image)
18972	06:14:53.898083	128.59.105.24	172.17.43.63	HTTP	1033 HTTP/1.1 200 OK (JPEG JFIF image)
18976	06:14:53.899818	128.59.105.24	172.17.43.63	HTTP	1291 HTTP/1.1 200 OK (JPEG JFIF image)
18981	06:14:53.916500	128.59.105.24	172.17.43.63	HTTP	1243 HTTP/1.1 200 OK (JPEG JFIF image)
18990	06:14:53.946978	128.59.105.24	172.17.43.63	HTTP	1026 HTTP/1.1 200 OK (JPEG JFIF image)
19006	06:14:54.210551	128.59.105.24	172.17.43.63	HTTP	117 HTTP/1.1 200 OK (JPEG JFIF image)
19375	06:14:58.717603	65.61.137.117	172.17.43.63	HTTP	543 HTTP/1.1 200 OK (text/html)
19404	06:14:59.127008	65.61.137.117	172.17.43.63	HTTP	152 HTTP/1.1 200 OK (text/css)
19411	06:14:59.154122	65.61.137.117	172.17.43.63	HTTP	1131 HTTP/1.1 200 OK (GIF89a)
19439	06:14:59.433562	65.61.137.117	172.17.43.63	HTTP	354 HTTP/1.1 200 OK (GIF89a)
19479	06:14:59.501489	65.61.137.117	172.17.43.63	HTTP	594 HTTP/1.1 200 OK (JPEG JFIF image)
19500	06:14:59.563320	65.61.137.117	172.17.43.63	HTTP	1175 HTTP/1.1 200 OK (JPEG JFIF image)
19693	06:15:00.785718	65.61.137.117	172.17.43.63	HTTP	232 HTTP/1.1 404 Not Found (text/html)
20019	06:15:04.760855	65.61.137.117	172.17.43.63	HTTP	1150 HTTP/1.1 200 OK (text/html)
20062	06:15:05.168286	65.61.137.117	172.17.43.63	HTTP	117 HTTP/1.1 200 OK (JPEG JFIF image)
1895	06:12:52.133830	172.17.43.63	18.66.63.71	HTTP	548 GET /online HTTP/1.1

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

All the red marked lines in the wireshark are an example of the Reset connection. Connection is reset if multiple ACK packets of the same sequence number is sent/received.



2019A7P50148P.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
6953	06:13:45.047081	172.17.43.63	23.213.56.92	TCP	82	52715 → 443 [ACK] Seq=4257 Ack=840795 Win=1059840 Len=0 SLE=887515 SRE=913795 SLE=852475 SRE=884595 SLE=8...
6987	06:13:45.079990	172.17.43.63	23.213.56.92	TCP	82	52715 → 443 [ACK] Seq=4257 Ack=846635 Win=1059840 Len=0 SLE=919635 SRE=937155 SLE=887515 SRE=916715 SLE=8...
6992	06:13:45.080123	172.17.43.63	23.213.56.92	TCP	82	52715 → 443 [ACK] Seq=4257 Ack=849555 Win=1059840 Len=0 SLE=919635 SRE=945915 SLE=887515 SRE=916715 SLE=8...
6994	06:13:45.080212	172.17.43.63	23.213.56.92	TCP	74	52715 → 443 [ACK] Seq=4257 Ack=884595 Win=1059840 Len=0 SLE=919635 SRE=948835 SLE=887515 SRE=916715
7000	06:13:45.080475	172.17.43.63	23.213.56.92	TCP	74	52715 → 443 [ACK] Seq=4257 Ack=916715 Win=1059840 Len=0 SLE=966355 SRE=986795 SLE=919635 SRE=963435
7027	06:13:45.089970	172.17.43.63	23.213.56.92	TCP	90	52715 → 443 [ACK] Seq=4257 Ack=963435 Win=1059840 Len=0 SLE=1029241 SRE=1035081 SLE=1016101 SRE=1027781 S...
5606	06:13:44.351430	172.17.43.63	23.213.56.92	TCP	54	52715 → 443 [ACK] Seq=518 Ack=3923 Win=131328 Len=0
7475	06:13:46.100739	172.17.43.63	23.213.56.92	TCP	54	52715 → 443 [FIN, ACK] Seq=4257 Ack=1185494 Win=2122752 Len=0
7543	06:13:46.139078	172.17.43.63	23.213.56.92	TCP	54	52715 → 443 [RST, ACK] Seq=4256 Ack=1185518 Win=0 Len=0
3504	06:13:44.256064	172.17.43.63	23.213.56.92	TCP	66	52715 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5531	06:13:44.290682	172.17.43.63	23.213.56.92	TCP	54	52716 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
5625	06:13:44.356047	172.17.43.63	23.213.56.92	TCP	54	52716 → 443 [ACK] Seq=518 Ack=3923 Win=131328 Len=0
5638	06:13:44.369557	172.17.43.63	23.213.56.92	TCP	54	52716 → 443 [FIN, ACK] Seq=598 Ack=3923 Win=131328 Len=0
5722	06:13:44.474794	172.17.43.63	23.213.56.92	TCP	54	52716 → 443 [RST, ACK] Seq=599 Ack=4497 Win=0 Len=0
5505	06:13:44.257464	172.17.43.63	23.213.56.92	TCP	66	52716 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5541	06:13:44.301241	172.17.43.63	23.213.56.92	TCP	54	52717 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
5621	06:13:44.355563	172.17.43.63	23.213.56.92	TCP	54	52717 → 443 [ACK] Seq=518 Ack=3923 Win=131328 Len=0
5637	06:13:44.368476	172.17.43.63	23.213.56.92	TCP	54	52717 → 443 [FIN, ACK] Seq=598 Ack=3923 Win=131328 Len=0
5729	06:13:44.475405	172.17.43.63	23.213.56.92	TCP	54	52717 → 443 [RST, ACK] Seq=599 Ack=4497 Win=0 Len=0
5586	06:13:44.257819	172.17.43.63	23.213.56.92	TCP	66	52717 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5532	06:13:44.299725	172.17.43.63	23.213.56.92	TCP	54	52718 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
5640	06:13:44.368063	172.17.43.63	23.213.56.92	TCP	54	52718 → 443 [FIN, ACK] Seq=518 Ack=1 Win=131328 Len=0
7578	06:13:46.233466	172.17.43.63	23.213.56.92	TCP	54	52718 → 443 [RST, ACK] Seq=519 Ack=1461 Win=0 Len=0
5597	06:13:44.258165	172.17.43.63	23.213.56.92	TCP	66	52718 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6263	06:13:44.702842	172.17.43.63	18.66.70.162	TCP	54	52719 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
6490	06:13:44.784390	172.17.43.63	18.66.70.162	TCP	54	52719 → 443 [ACK] Seq=1048 Ack=17578 Win=132352 Len=0

> Frame 7516: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{628BF55F-D065-4080-A418-A0D7DAFB8E0}, id 0

> Ethernet II, Src: MegaWell\_c8:39:e7 (10:5b:ad:c8:39:e7), Dst: IETF-VRRP-VRID\_4b (00:00:5e:00:01:4b)

> Internet Protocol Version 4, Src: 172.17.43.63, Dst: 3.110.244.204

> Transmission Control Protocol, Src Port: 52725, Dst Port: 443, Seq: 1627, Ack: 7927, Len: 0

0000 00 00 5e 00 01 4b 10 5b ad c8 39 e7 00 00 45 00 ...K: [ ...9...E

0010 00 28 db 79 40 00 00 06 4f cb ac 11 2b 3f 03 6e ...@... O...+?n

0020 f4 cc cd f5 01 bb 2f cb 39 4d 58 89 af b3 50 14 ...X...P

0030 00 00 9f 3f 00 00 ...?

Frame (Frame), 54 bytes

Packets: 20339 · Displayed: 12329 (60.6%) · Dropped: 0 (0.0%) Profile: Default

12:16 06-03-2022

2019A7P50148P.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
10901	06:13:56.100781	172.17.43.63	3.108.50.194	TCP	54	52730 → 443 [FIN, ACK] Seq=4621 Ack=4898 Win=129792 Len=0
7421	06:13:45.897199	172.17.43.63	3.108.50.194	TCP	66	52730 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
7569	06:13:46.222394	172.17.43.63	34.208.124.133	TCP	54	52731 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
7626	06:13:46.505598	172.17.43.63	34.208.124.133	TCP	54	52731 → 443 [ACK] Seq=518 Ack=1561 Win=131328 Len=0
7630	06:13:46.506742	172.17.43.63	34.208.124.133	TCP	54	52731 → 443 [ACK] Seq=518 Ack=3354 Win=131328 Len=0
7700	06:13:46.784538	172.17.43.63	34.208.124.133	TCP	54	52731 → 443 [ACK] Seq=644 Ack=3524 Win=131072 Len=0
10891	06:13:56.098082	172.17.43.63	34.208.124.133	TCP	54	52731 → 443 [FIN, ACK] Seq=644 Ack=3524 Win=131072 Len=0
11277	06:13:56.375083	172.17.43.63	34.208.124.133	TCP	54	52731 → 443 [RST, ACK] Seq=645 Ack=3555 Win=0 Len=0
7436	06:13:46.944093	172.17.43.63	34.208.124.133	TCP	66	52731 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
7645	06:13:46.679433	172.17.43.63	104.16.148.64	TCP	54	52732 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
7673	06:13:46.728772	172.17.43.63	104.16.148.64	TCP	54	52732 → 443 [ACK] Seq=1119 Ack=2639 Win=130816 Len=0
7710	06:13:46.823483	172.17.43.63	104.16.148.64	TCP	54	52732 → 443 [ACK] Seq=1150 Ack=4597 Win=131584 Len=0
8298	06:13:47.629152	172.17.43.63	104.16.148.64	TCP	54	52732 → 443 [ACK] Seq=1267 Ack=18645 Win=131584 Len=0
8302	06:13:47.629452	172.17.43.63	104.16.148.64	TCP	54	52732 → 443 [ACK] Seq=1267 Ack=19694 Win=130304 Len=0
8292	06:13:47.628600	172.17.43.63	104.16.148.64	TCP	54	52732 → 443 [ACK] Seq=1267 Ack=7379 Win=131584 Len=0
8623	06:13:47.910109	172.17.43.63	104.16.148.64	TCP	54	52732 → 443 [ACK] Seq=1354 Ack=24185 Win=131584 Len=0
8648	06:13:47.952581	172.17.43.63	104.16.148.64	TCP	54	52732 → 443 [ACK] Seq=1354 Ack=24216 Win=131328 Len=0
10948	06:13:56.119244	172.17.43.63	104.16.148.64	TCP	54	52732 → 443 [ACK] Seq=1355 Ack=24217 Win=131328 Len=0
7656	06:13:46.708281	172.17.43.63	104.16.148.64	TCP	54	52732 → 443 [ACK] Seq=518 Ack=2096 Win=131584 Len=0
10899	06:13:56.100402	172.17.43.63	104.16.148.64	TCP	54	52732 → 443 [FIN, ACK] Seq=1354 Ack=24216 Win=131328 Len=0
7639	06:13:46.659577	172.17.43.63	104.16.148.64	TCP	66	52732 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
7650	06:13:46.702775	172.17.43.63	35.154.60.116	TCP	54	52733 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
7706	06:13:46.822481	172.17.43.63	35.154.60.116	TCP	54	52733 → 443 [ACK] Seq=1533 Ack=1015 Win=130304 Len=0
10893	06:13:56.099161	172.17.43.63	35.154.60.116	TCP	54	52733 → 443 [FIN, ACK] Seq=1533 Ack=1015 Win=130304 Len=0
10997	06:13:56.132736	172.17.43.63	35.154.60.116	TCP	54	52733 → 443 [RST, ACK] Seq=1534 Ack=1046 Win=0 Len=0
7641	06:13:46.667874	172.17.43.63	35.154.60.116	TCP	66	52733 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 7516: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{628BF55F-D065-4080-A418-A0D7DAFB8E0}, id 0

> Ethernet II, Src: MegaWell\_c8:39:e7 (10:5b:ad:c8:39:e7), Dst: IETF-VRRP-VRID\_4b (00:00:5e:00:01:4b)

> Internet Protocol Version 4, Src: 172.17.43.63, Dst: 3.110.244.204

> Transmission Control Protocol, Src Port: 52725, Dst Port: 443, Seq: 1627, Ack: 7927, Len: 0

0000 00 00 5e 00 01 4b 10 5b ad c8 39 e7 00 00 45 00 ...K: [ ...9...E

0010 00 28 db 79 40 00 00 06 4f cb ac 11 2b 3f 03 6e ...@... O...+?n

0020 f4 cc cd f5 01 bb 2f cb 39 4d 58 89 af b3 50 14 ...X...P

0030 00 00 9f 3f 00 00 ...?

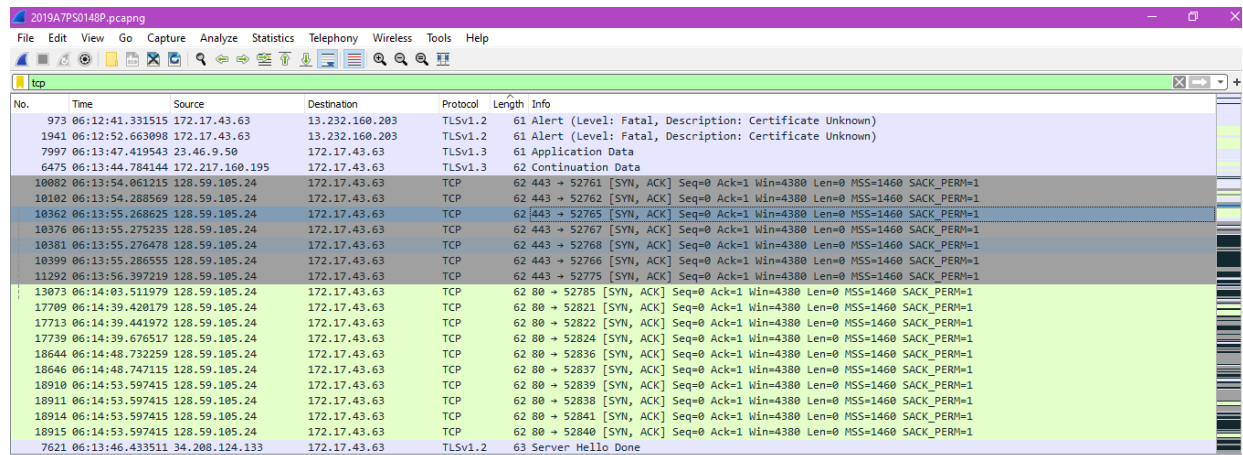
Frame (Frame), 54 bytes

Packets: 20339 · Displayed: 12329 (60.6%) · Dropped: 0 (0.0%) Profile: Default

12:16 06-03-2022

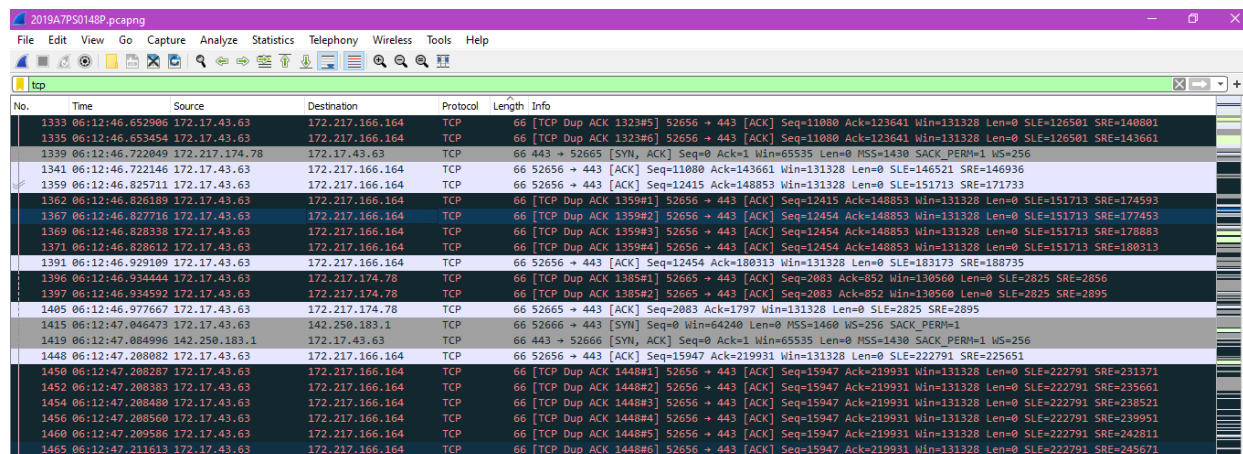
9) List all TCP segments which are send and received by your machine having header length more than 20 bytes. Give the appropriate reason for header length larger than the default size.

All SYN ACK packets (additional 8 bytes) and DUP ACK, PSH ACK packets (additional 12 bytes) have a header length greater than 20 bytes. This includes optional fields like Window size extension, parameter negotiations, padding and time stamps.



The screenshot shows a Wireshark packet capture of a TCP connection. The packet list pane displays several packets, with the selected packet (No. 61) expanded to show its details. The packet is a SYN ACK from 172.17.43.63 to 13.232.160.203. The details pane shows the TCP header and options, including a window size extension of 4380. The packet length is 61 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
973	06:12:41.331515	172.17.43.63	13.232.160.203	TLsv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)
1941	06:12:52.663098	172.17.43.63	13.232.160.203	TLsv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)
7997	06:13:47.419543	23.46.9.50	172.17.43.63	TLsv1.3	61	Application Data
6475	06:13:44.784144	172.217.160.195	172.17.43.63	TLsv1.3	62	Continuation Data
10082	06:13:54.061215	128.59.105.24	172.17.43.63	TCP	62	443 → 52761 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
10102	06:13:54.288569	128.59.105.24	172.17.43.63	TCP	62	443 → 52762 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
10362	06:13:55.268625	128.59.105.24	172.17.43.63	TCP	62	443 → 52765 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
10376	06:13:55.275235	128.59.105.24	172.17.43.63	TCP	62	443 → 52767 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
10381	06:13:55.276478	128.59.105.24	172.17.43.63	TCP	62	443 → 52768 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
10399	06:13:55.286555	128.59.105.24	172.17.43.63	TCP	62	443 → 52766 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
11292	06:13:56.397219	128.59.105.24	172.17.43.63	TCP	62	443 → 52775 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
13073	06:14:03.511979	128.59.105.24	172.17.43.63	TCP	62	80 → 52785 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
17799	06:14:39.420179	128.59.105.24	172.17.43.63	TCP	62	80 → 52821 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
17713	06:14:39.441972	128.59.105.24	172.17.43.63	TCP	62	80 → 52822 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
17739	06:14:39.676517	128.59.105.24	172.17.43.63	TCP	62	80 → 52824 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
18644	06:14:48.732259	128.59.105.24	172.17.43.63	TCP	62	80 → 52836 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
18646	06:14:48.747115	128.59.105.24	172.17.43.63	TCP	62	80 → 52837 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
18910	06:14:53.597415	128.59.105.24	172.17.43.63	TCP	62	80 → 52839 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
18911	06:14:53.597415	128.59.105.24	172.17.43.63	TCP	62	80 → 52838 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
18914	06:14:53.597415	128.59.105.24	172.17.43.63	TCP	62	80 → 52841 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
18915	06:14:53.597415	128.59.105.24	172.17.43.63	TCP	62	80 → 52840 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
7621	06:13:46.433511	34.208.124.133	172.17.43.63	TLsv1.2	63	Server Hello Done



The screenshot shows a Wireshark packet capture of a TCP connection. The packet list pane displays several packets, with the selected packet (No. 66) expanded to show its details. The packet is a duplicate ACK from 172.217.166.164 to 172.17.43.63. The details pane shows the TCP header and options, including a window size extension of 4380. The packet length is 66 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
1333	06:12:46.652906	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 132345] 52656 → 443 [ACK] Seq=1080 Ack=123641 Win=131328 Len=0 SLE=126501 SRE=140801
1335	06:12:46.653454	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 132346] 52656 → 443 [ACK] Seq=1080 Ack=123641 Win=131328 Len=0 SLE=126501 SRE=143661
1339	06:12:46.722049	172.217.174.78	172.17.43.63	TCP	66	443 → 52665 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
1341	06:12:46.722146	172.17.43.63	172.217.166.164	TCP	66	52656 → 443 [ACK] Seq=1080 Ack=143661 Win=131328 Len=0 SLE=146521 SRE=146936
1359	06:12:46.825711	172.17.43.63	172.217.166.164	TCP	66	52656 → 443 [ACK] Seq=12415 Ack=148853 Win=131328 Len=0 SLE=151713 SRE=171733
1362	06:12:46.826189	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 135901] 52656 → 443 [ACK] Seq=12415 Ack=148853 Win=131328 Len=0 SLE=151713 SRE=174593
1367	06:12:46.827716	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 135902] 52656 → 443 [ACK] Seq=12454 Ack=148853 Win=131328 Len=0 SLE=151713 SRE=177453
1369	06:12:46.828338	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 135903] 52656 → 443 [ACK] Seq=12454 Ack=148853 Win=131328 Len=0 SLE=151713 SRE=178883
1371	06:12:46.828612	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 135904] 52656 → 443 [ACK] Seq=12454 Ack=148853 Win=131328 Len=0 SLE=151713 SRE=180313
1391	06:12:46.929109	172.17.43.63	172.217.166.164	TCP	66	52656 → 443 [ACK] Seq=12454 Ack=180313 Win=131328 Len=0 SLE=183173 SRE=188735
1396	06:12:46.934444	172.17.43.63	172.217.174.78	TCP	66	[TCP Dup ACK 138501] 52665 → 443 [ACK] Seq=2083 Ack=852 Win=130560 Len=0 SLE=2825 SRE=2856
1397	06:12:46.934592	172.17.43.63	172.217.174.78	TCP	66	[TCP Dup ACK 138502] 52665 → 443 [ACK] Seq=2083 Ack=852 Win=130560 Len=0 SLE=2825 SRE=2895
1405	06:12:46.977667	172.17.43.63	172.217.174.78	TCP	66	52665 → 443 [ACK] Seq=2083 Ack=1797 Win=131328 Len=0 SLE=2825 SRE=2895
1415	06:12:47.046473	172.17.43.63	142.250.183.1	TCP	66	52666 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1419	06:12:47.084996	142.250.183.1	172.17.43.63	TCP	66	443 → 52666 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
1448	06:12:47.208082	172.17.43.63	172.217.166.164	TCP	66	52656 → 443 [ACK] Seq=15947 Ack=219931 Win=131328 Len=0 SLE=222791 SRE=225651
1450	06:12:47.208287	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 144801] 52656 → 443 [ACK] Seq=15947 Ack=219931 Win=131328 Len=0 SLE=222791 SRE=231371
1452	06:12:47.208383	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 144802] 52656 → 443 [ACK] Seq=15947 Ack=219931 Win=131328 Len=0 SLE=222791 SRE=235661
1454	06:12:47.208480	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 144803] 52656 → 443 [ACK] Seq=15947 Ack=219931 Win=131328 Len=0 SLE=222791 SRE=238521
1456	06:12:47.208586	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 144804] 52656 → 443 [ACK] Seq=15947 Ack=219931 Win=131328 Len=0 SLE=222791 SRE=239951
1460	06:12:47.209586	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 144805] 52656 → 443 [ACK] Seq=15947 Ack=219931 Win=131328 Len=0 SLE=222791 SRE=242811
1465	06:12:47.211613	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 144806] 52656 → 443 [ACK] Seq=15947 Ack=219931 Win=131328 Len=0 SLE=222791 SRE=245671

10) List all the duplicate ACK TCP segments.

Multiple DUP ACKs exist. Some are shown:



2019A7P50148P.pcapng						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
tcp						
No.	Time	Source	Destination	Protocol	Length	Info
1211	06:12:44.373873	13.234.71.216	172.17.43.63	TCP	56	[TCP ACKed unseen segment] 443 + 52660 [RST, ACK] Seq=1 Ack=305 Win=0 Len=0
10035	06:13:53.806530	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 10013810] 52692 + 443 [ACK] Seq=15044 Ack=51312 Win=131328 Len=0 SLE=55305 SRE=56735
10017	06:13:53.785791	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 10013811] 52692 + 443 [ACK] Seq=15044 Ack=51312 Win=131328 Len=0 SLE=55305 SRE=56735
10019	06:13:53.786954	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 10013812] 52692 + 443 [ACK] Seq=15044 Ack=51312 Win=131328 Len=0 SLE=55305 SRE=56735
10021	06:13:53.788959	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 10013813] 52692 + 443 [ACK] Seq=15044 Ack=51312 Win=131328 Len=0 SLE=55305 SRE=56735
10023	06:13:53.794080	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 10013814] 52692 + 443 [ACK] Seq=15044 Ack=51312 Win=131328 Len=0 SLE=55305 SRE=56735
10025	06:13:53.795004	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 10013815] 52692 + 443 [ACK] Seq=15044 Ack=51312 Win=131328 Len=0 SLE=55305 SRE=56735
10027	06:13:53.797757	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 10013816] 52692 + 443 [ACK] Seq=15044 Ack=51312 Win=131328 Len=0 SLE=55305 SRE=56735
10029	06:13:53.799206	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 10013817] 52692 + 443 [ACK] Seq=15044 Ack=51312 Win=131328 Len=0 SLE=55305 SRE=56735
10031	06:13:53.801477	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 10013818] 52692 + 443 [ACK] Seq=15044 Ack=51312 Win=131328 Len=0 SLE=55305 SRE=56735
10033	06:13:53.804122	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 10013819] 52692 + 443 [ACK] Seq=15044 Ack=51312 Win=131328 Len=0 SLE=55305 SRE=56735
10070	06:13:53.866681	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1006881] 52692 + 443 [ACK] Seq=15044 Ack=100653 Win=131328 Len=0 SLE=103713 SRE=106732
10096	06:13:54.179658	128.59.105.24	172.17.43.63	TCP	56	[TCP Dup ACK 1009081] 443 + 52761 [ACK] Seq=1 Ack=518 Win=4380 Len=0
10121	06:13:54.466279	128.59.105.24	172.17.43.63	TCP	56	[TCP Dup ACK 1010661] 443 + 52762 [ACK] Seq=1 Ack=518 Win=4380 Len=0
10143	06:13:54.697687	34.214.251.236	172.17.43.63	TCP	56	[TCP Dup ACK 1013181] 443 + 52763 [ACK] Seq=1 Ack=518 Win=65536 Len=0
10155	06:13:54.909733	34.214.251.236	172.17.43.63	TCP	56	[TCP Dup ACK 1014881] 443 + 52764 [ACK] Seq=1 Ack=518 Win=65536 Len=0
10240	06:13:55.111188	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1023781] 52692 + 443 [ACK] Seq=18549 Ack=107278 Win=130816 Len=0 SLE=108708 SRE=114428
10242	06:13:55.114159	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 1023782] 52692 + 443 [ACK] Seq=18549 Ack=107278 Win=130816 Len=0 SLE=117288 SRE=120148 SLE=1...
10245	06:13:55.115520	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 1023783] 52692 + 443 [ACK] Seq=18549 Ack=107278 Win=130816 Len=0 SLE=117288 SRE=121578 SLE=1...
10248	06:13:55.117445	172.17.43.63	172.217.166.164	TCP	82	[TCP Dup ACK 1023784] 52692 + 443 [ACK] Seq=18549 Ack=107278 Win=130816 Len=0 SLE=123008 SRE=124438 SLE=1...
10249	06:13:55.117506	172.17.43.63	172.217.166.164	TCP	82	[TCP Dup ACK 1023785] 52692 + 443 [ACK] Seq=18549 Ack=107278 Win=130816 Len=0 SLE=123008 SRE=125499 SLE=1...
10392	06:13:55.282222	172.17.43.63	172.217.166.164	TCP	82	[TCP Dup ACK 10355810] 52692 + 443 [ACK] Seq=20015 Ack=127173 Win=131328 Len=0 SLE=160063 SRE=162923 SLE=...

2019A7P50148P.pcapng						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
tcp						
No.	Time	Source	Destination	Protocol	Length	Info
10739	06:13:55.838021	172.17.43.63	172.217.166.164	TCP	82	[TCP Dup ACK 1068287] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=263420 SRE=332060 SLE=...
10741	06:13:55.839423	172.17.43.63	172.217.166.164	TCP	82	[TCP Dup ACK 1068288] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=263420 SRE=334920 SLE=...
10743	06:13:55.839562	172.17.43.63	172.217.166.164	TCP	82	[TCP Dup ACK 1068289] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=263420 SRE=339210 SLE=...
10685	06:13:55.817691	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1068282] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=228988 SRE=236250
10745	06:13:55.839965	172.17.43.63	172.217.166.164	TCP	82	[TCP Dup ACK 1068283] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=263420 SRE=340640 SLE=...
10747	06:13:55.841779	172.17.43.63	172.217.166.164	TCP	82	[TCP Dup ACK 1068283] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=263420 SRE=344930 SLE=...
10750	06:13:55.843630	172.17.43.63	172.217.166.164	TCP	90	[TCP Dup ACK 1068283] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=346360 SRE=347790 SLE=...
10752	06:13:55.843199	172.17.43.63	172.217.166.164	TCP	90	[TCP Dup ACK 1068283] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=349220 SRE=353510 SLE=...
10799	06:13:55.855933	172.17.43.63	172.217.166.164	TCP	90	[TCP Dup ACK 1068283] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=349220 SRE=356370 SLE=...
10804	06:13:55.856048	172.17.43.63	172.217.166.164	TCP	90	[TCP Dup ACK 1068283] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=349220 SRE=357800 SLE=...
10687	06:13:55.818046	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1068283] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=228988 SRE=237680
10689	06:13:55.819164	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1068283] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=228988 SRE=239110
10691	06:13:55.820134	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 1068283] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=241978 SRE=246260 SLE=2...
10693	06:13:55.820495	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 1068283] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=241978 SRE=250550 SLE=2...
10695	06:13:55.822193	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 1068283] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=241978 SRE=256270 SLE=2...
10698	06:13:55.822448	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 1068283] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=241978 SRE=259130 SLE=2...
10702	06:13:55.823980	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 1068283] 52692 + 443 [ACK] Seq=23611 Ack=228957 Win=131328 Len=0 SLE=241978 SRE=261990 SLE=2...
10754	06:13:55.846290	128.59.105.24	172.17.43.63	TCP	56	[TCP Dup ACK 1075381] 443 + 52765 [ACK] Seq=152 Ack=569 Win=4948 Len=0
10806	06:13:55.856144	172.17.43.63	172.217.166.164	TCP	90	[TCP Dup ACK 1080581] 52692 + 443 [ACK] Seq=23611 Ack=239110 Win=131328 Len=0 SLE=349220 SRE=359230 SLE=3...
10807	06:13:55.856192	172.17.43.63	172.217.166.164	TCP	90	[TCP Dup ACK 1080582] 52692 + 443 [ACK] Seq=23611 Ack=239110 Win=131328 Len=0 SLE=349220 SRE=360285 SLE=3...
10810	06:13:55.860966	128.59.105.24	172.17.43.63	TCP	56	[TCP Dup ACK 1080981] 443 + 52768 [ACK] Seq=152 Ack=569 Win=4948 Len=0
10829	06:13:55.894166	172.17.43.63	172.217.166.164	TCP	82	[TCP Dup ACK 1082181] 52692 + 443 [ACK] Seq=23611 Ack=261990 Win=131328 Len=0 SLE=349220 SRE=366005 SLE=3...

2019A7P50148P.pcapng						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
tcp						
No.	Time	Source	Destination	Protocol	Length	Info
13049	06:14:03.292082	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 13018812] 52692 + 443 [ACK] Seq=31243 Ack=404304 Win=131328 Len=0 SLE=407164 SRE=442289
13052	06:14:03.293329	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 13018813] 52692 + 443 [ACK] Seq=31243 Ack=404304 Win=131328 Len=0 SLE=407164 SRE=445149
13053	06:14:03.293433	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 13018814] 52692 + 443 [ACK] Seq=31243 Ack=404304 Win=131328 Len=0 SLE=407164 SRE=445939
13055	06:14:03.293504	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 13018815] 52692 + 443 [ACK] Seq=31243 Ack=404304 Win=131328 Len=0 SLE=407164 SRE=445978
13020	06:14:03.269598	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1301881] 52692 + 443 [ACK] Seq=30841 Ack=404304 Win=131328 Len=0 SLE=407164 SRE=412884
13022	06:14:03.269710	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1301882] 52692 + 443 [ACK] Seq=30841 Ack=404304 Win=131328 Len=0 SLE=407164 SRE=415744
13024	06:14:03.270052	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1301883] 52692 + 443 [ACK] Seq=30841 Ack=404304 Win=131328 Len=0 SLE=407164 SRE=418604
13026	06:14:03.270658	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1301884] 52692 + 443 [ACK] Seq=30841 Ack=404304 Win=131328 Len=0 SLE=407164 SRE=418772
13028	06:14:03.276531	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1301885] 52692 + 443 [ACK] Seq=30841 Ack=404304 Win=131328 Len=0 SLE=407164 SRE=423062
13030	06:14:03.276848	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1301886] 52692 + 443 [ACK] Seq=30841 Ack=404304 Win=131328 Len=0 SLE=407164 SRE=425922
13032	06:14:03.277071	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1301887] 52692 + 443 [ACK] Seq=30841 Ack=404304 Win=131328 Len=0 SLE=407164 SRE=428782
13035	06:14:03.277760	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1301888] 52692 + 443 [ACK] Seq=30841 Ack=404304 Win=131328 Len=0 SLE=407164 SRE=431642
13036	06:14:03.277830	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1301889] 52692 + 443 [ACK] Seq=30841 Ack=404304 Win=131328 Len=0 SLE=407164 SRE=432279
13188	06:14:04.298482	34.214.251.236	172.17.43.63	TCP	56	[TCP Dup ACK 1311381] 443 + 52786 [ACK] Seq=1 Ack=518 Win=65536 Len=0
13168	06:14:04.265473	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 13148810] 52692 + 443 [ACK] Seq=34252 Ack=449104 Win=131328 Len=0 SLE=474844 SRE=492004 SLE=...
13170	06:14:04.265655	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 13148811] 52692 + 443 [ACK] Seq=34252 Ack=449104 Win=131328 Len=0 SLE=474844 SRE=494864 SLE=...
13172	06:14:04.265740	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 13148812] 52692 + 443 [ACK] Seq=34252 Ack=449104 Win=131328 Len=0 SLE=474844 SRE=497724 SLE=...
13174	06:14:04.266807	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 13148813] 52692 + 443 [ACK] Seq=34252 Ack=449104 Win=131328 Len=0 SLE=474844 SRE=500584 SLE=...
13176	06:14:04.266399	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 13148814] 52692 + 443 [ACK] Seq=34252 Ack=449104 Win=131328 Len=0 SLE=474844 SRE=503444 SLE=...
13178	06:14:04.266634	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 13148815] 52692 + 443 [ACK] Seq=34252 Ack=449104 Win=131328 Len=0 SLE=474844 SRE=506304 SLE=...
13180	06:14:04.267287	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 13148816] 52692 + 443 [ACK] Seq=34252 Ack=449104 Win=131328 Len=0 SLE=474844 SRE=509164 SLE=...
13150	06:14:04.261114	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1314881] 52692 + 443 [ACK] Seq=34252 Ack=449104 Win=131328 Len=0 SLE=450534 SRE=457684

No.	Time	Source	Destination	Protocol	Length	Info
1367	06:12:46.827716	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1359#2] 52656 → 443 [ACK] Seq=12454 Ack=148853 Win=131328 Len=0 SLE=151713 SRE=177453
1369	06:12:46.828338	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1359#3] 52656 → 443 [ACK] Seq=12454 Ack=148853 Win=131328 Len=0 SLE=151713 SRE=178883
1371	06:12:46.828612	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 1359#4] 52656 → 443 [ACK] Seq=12454 Ack=148853 Win=131328 Len=0 SLE=151713 SRE=180313
1374	06:12:46.831051	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 1359#5] 52656 → 443 [ACK] Seq=12454 Ack=148853 Win=131328 Len=0 SLE=183173 SRE=186033 SLE=15...
1377	06:12:46.831192	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 1359#6] 52656 → 443 [ACK] Seq=12454 Ack=148853 Win=131328 Len=0 SLE=183173 SRE=187463 SLE=15...
1378	06:12:46.831226	172.17.43.63	172.217.166.164	TCP	74	[TCP Dup ACK 1359#7] 52656 → 443 [ACK] Seq=12454 Ack=148853 Win=131328 Len=0 SLE=183173 SRE=188735 SLE=15...
13780	06:14:08.839267	172.17.43.63	172.217.166.164	TCP	54	[TCP Dup ACK 1369#1] 52788 → 443 [ACK] Seq=2727 Ack=1228 Win=130304 Len=0
13782	06:14:08.839652	172.17.43.63	172.217.166.164	TCP	54	[TCP Dup ACK 1369#2] 52788 → 443 [ACK] Seq=2727 Ack=1228 Win=130304 Len=0
13761	06:14:08.936875	172.17.43.63	142.250.67.174	TCP	66	[TCP Dup ACK 13759#1] 52789 → 443 [ACK] Seq=2187 Ack=9110 Win=131328 Len=0 SLE=11970 SRE=12210
13764	06:14:08.971142	172.17.43.63	142.250.67.174	TCP	66	[TCP Dup ACK 13759#2] 52789 → 443 [ACK] Seq=2187 Ack=9110 Win=131328 Len=0 SLE=11970 SRE=15070
13765	06:14:08.971370	172.17.43.63	142.250.67.174	TCP	66	[TCP Dup ACK 13759#3] 52789 → 443 [ACK] Seq=2187 Ack=9110 Win=131328 Len=0 SLE=11970 SRE=16191
13767	06:14:08.972676	172.17.43.63	142.250.67.174	TCP	66	[TCP Dup ACK 13759#4] 52789 → 443 [ACK] Seq=2187 Ack=9110 Win=131328 Len=0 SLE=11970 SRE=16468
13889	06:14:08.830125	172.217.174.78	172.17.43.63	TCP	56	[TCP Dup ACK 13794#1] 443 → 52792 [ACK] Seq=1 Ack=592 Win=65536 Len=0
13826	06:14:08.868261	172.17.43.63	172.217.174.78	TCP	54	[TCP Dup ACK 13821#1] 52792 → 443 [ACK] Seq=2089 Ack=852 Win=130560 Len=0
13827	06:14:08.868324	172.17.43.63	172.217.174.78	TCP	54	[TCP Dup ACK 13821#2] 52792 → 443 [ACK] Seq=2089 Ack=852 Win=130560 Len=0
13841	06:14:08.937464	172.17.43.63	172.217.174.78	TCP	66	[TCP Dup ACK 13821#3] 52792 → 443 [ACK] Seq=2089 Ack=852 Win=130560 Len=0 SLE=2842 SRE=2873
13842	06:14:08.937615	172.17.43.63	172.217.174.78	TCP	66	[TCP Dup ACK 13821#4] 52792 → 443 [ACK] Seq=2089 Ack=852 Win=130560 Len=0 SLE=2842 SRE=2912
13861	06:14:08.816355	172.17.43.63	172.217.166.164	TCP	66	[TCP Dup ACK 13847#1] 52788 → 443 [ACK] Seq=3471 Ack=1904 Win=131072 Len=0 SLE=2626 SRE=3229
1396	06:12:46.934444	172.17.43.63	172.217.174.78	TCP	66	[TCP Dup ACK 1385#1] 52665 → 443 [ACK] Seq=2083 Ack=852 Win=130560 Len=0 SLE=2825 SRE=2856
1397	06:12:46.934592	172.17.43.63	172.217.174.78	TCP	66	[TCP Dup ACK 1385#2] 52665 → 443 [ACK] Seq=2083 Ack=852 Win=130560 Len=0 SLE=2825 SRE=2895
13952	06:14:09.329417	172.17.43.63	216.58.203.46	TCP	66	[TCP Dup ACK 13908#10] 52794 → 443 [ACK] Seq=2296 Ack=213 Win=131328 Len=0 SLE=821 SRE=9164
13954	06:14:09.331957	172.17.43.63	216.58.203.46	TCP	66	[TCP Dup ACK 13908#11] 52794 → 443 [ACK] Seq=2296 Ack=213 Win=131328 Len=0 SLE=821 SRE=12024

11) Provide the sequence number of any one out-of-order TCP segment captured in your trace file.

Seq numbers of some of them: - 213, 852, etc

No.	Time	Source	Destination	Protocol	Length	Info
13114	06:14:04.087262	172.17.43.63	74.125.200.188	TCP	55	[TCP Keep-Alive] 52174 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1
18696	06:14:49.179977	172.17.43.63	74.125.200.188	TCP	55	[TCP Keep-Alive] 52174 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1
11966	06:13:57.906367	172.17.43.63	52.209.91.195	TCP	55	[TCP Keep-Alive] 52179 → 8382 [ACK] Seq=1 Ack=1 Win=511 Len=1
18256	06:14:46.833792	172.17.43.63	52.209.91.195	TCP	55	[TCP Keep-Alive] 52179 → 8382 [ACK] Seq=455 Ack=1 Win=511 Len=1
1519	06:12:47.339159	172.217.166.164	172.17.43.63	TCP	2914	[TCP Out-Of-Order] 443 → 52656 [PSH, ACK] Seq=251391 Ack=15947 Win=146432 Len=2860
1522	06:12:47.339159	172.217.166.164	172.17.43.63	TCP	2914	[TCP Out-Of-Order] 443 → 52656 [PSH, ACK] Seq=265691 Ack=15947 Win=146432 Len=2860
1541	06:12:47.374919	172.217.166.164	172.17.43.63	TCP	2914	[TCP Out-Of-Order] 443 → 52656 [PSH, ACK] Seq=298581 Ack=15947 Win=146432 Len=2860
1543	06:12:47.375429	172.217.166.164	172.17.43.63	TCP	2914	[TCP Out-Of-Order] 443 → 52656 [PSH, ACK] Seq=321461 Ack=15947 Win=146432 Len=2860
1545	06:12:47.375945	172.217.166.164	172.17.43.63	TCP	2914	[TCP Out-Of-Order] 443 → 52656 [PSH, ACK] Seq=324321 Ack=15947 Win=146432 Len=2860
1484	06:12:46.977600	172.217.174.78	172.17.43.63	TCP	1082	[TCP Out-Of-Order] 443 → 52665 [PSH, ACK] Seq=1797 Ack=2083 Win=69632 Len=1028
1483	06:12:46.977600	172.217.174.78	172.17.43.63	TCP	999	[TCP Out-Of-Order] 443 → 52665 [PSH, ACK] Seq=852 Ack=2083 Win=69632 Len=945
1650	06:12:48.102300	172.217.166.162	172.17.43.63	TCP	662	[TCP Out-Of-Order] 443 → 52668 [PSH, ACK] Seq=213 Ack=2025 Win=69632 Len=608
2464	06:13:00.253686	172.217.166.164	172.17.43.63	TCP	1484	[TCP Out-Of-Order] 443 → 52677 [ACK] Seq=18874 Ack=4997 Win=81408 Len=1430
2479	06:13:00.545668	172.217.166.164	172.17.43.63	TCP	1484	[TCP Out-Of-Order] 443 → 52677 [ACK] Seq=20304 Ack=5687 Win=87048 Len=1430
2273	06:12:58.600442	142.251.12.100	172.17.43.63	TCP	662	[TCP Out-Of-Order] 443 → 52678 [PSH, ACK] Seq=213 Ack=1261 Win=68096 Len=608
10462	06:13:55.332400	172.217.166.164	172.17.43.63	TCP	1484	[TCP Out-Of-Order] 443 → 52692 [ACK] Seq=147193 Ack=20015 Win=171264 Len=1430
10835	06:13:55.902420	172.217.166.164	172.17.43.63	TCP	1484	[TCP Out-Of-Order] 443 → 52692 [ACK] Seq=344930 Ack=23611 Win=188416 Len=1430
10836	06:13:55.902420	172.217.166.164	172.17.43.63	TCP	1484	[TCP Out-Of-Order] 443 → 52692 [ACK] Seq=347790 Ack=23611 Win=188416 Len=1430
13222	06:14:04.364177	172.217.166.164	172.17.43.63	TCP	2914	[TCP Out-Of-Order] 443 → 52692 [ACK] Seq=514884 Ack=34252 Win=245760 Len=2860
13224	06:14:04.365256	172.217.166.164	172.17.43.63	TCP	1484	[TCP Out-Of-Order] 443 → 52692 [ACK] Seq=517744 Ack=34252 Win=245760 Len=1430
13249	06:14:04.434079	172.217.166.164	172.17.43.63	TCP	1484	[TCP Out-Of-Order] 443 → 52692 [ACK] Seq=519174 Ack=34252 Win=245760 Len=1430
13230	06:14:04.395112	172.217.166.164	172.17.43.63	TCP	1484	[TCP Out-Of-Order] 443 → 52692 [ACK] Seq=520604 Ack=34252 Win=245760 Len=1430

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

**GET: 23**

**Post: 0**

No.	Time	Source	Destination	Protocol	Length	Info
4835	06:13:37.822282	172.17.43.63	104.17.120.38	HTTP	484	GET / HTTP/1.1
2100	06:12:55.597312	172.17.43.63	18.66.63.71	HTTP	485	GET /favicon.ico HTTP/1.1
19594	06:15:00.490048	172.17.43.63	65.61.137.117	HTTP	497	GET /favicon.ico HTTP/1.1
20046	06:15:04.863437	172.17.43.63	65.61.137.117	HTTP	535	GET /images/b_deposit.jpg HTTP/1.1
19425	06:14:59.263651	172.17.43.63	65.61.137.117	HTTP	505	GET /images/gradient.jpg HTTP/1.1
19388	06:14:58.902644	172.17.43.63	65.61.137.117	HTTP	507	GET /images/header_pic.jpg HTTP/1.1
19386	06:14:58.852959	172.17.43.63	65.61.137.117	HTTP	501	GET /images/Logo.gif HTTP/1.1
19406	06:14:59.134780	172.17.43.63	65.61.137.117	HTTP	504	GET /images/pf_lock.gif HTTP/1.1
19943	06:15:04.372015	172.17.43.63	65.61.137.117	HTTP	625	GET /index.jsp?content=business_deposit.htm HTTP/1.1
19342	06:14:58.395252	172.17.43.63	65.61.137.117	HTTP	498	GET /login.jsp HTTP/1.1
18095	06:12:52.133830	172.17.43.63	18.66.63.71	HTTP	548	GET /online HTTP/1.1
19385	06:14:58.850640	172.17.43.63	65.61.137.117	HTTP	449	GET /style.css HTTP/1.1
18930	06:14:53.599540	172.17.43.63	128.59.105.24	HTTP	563	GET /-fdcfamily/tree/image-107868501.jpg HTTP/1.1
18939	06:14:53.646661	172.17.43.63	128.59.105.24	HTTP	563	GET /-fdcfamily/tree/image-122569384.jpg HTTP/1.1
18924	06:14:53.599074	172.17.43.63	128.59.105.24	HTTP	563	GET /-fdcfamily/tree/image-358197608.jpg HTTP/1.1
18933	06:14:53.608300	172.17.43.63	128.59.105.24	HTTP	563	GET /-fdcfamily/tree/image-393262874.jpg HTTP/1.1
18932	06:14:53.600278	172.17.43.63	128.59.105.24	HTTP	563	GET /-fdcfamily/tree/image-665284549.jpg HTTP/1.1
18895	06:14:53.256127	172.17.43.63	128.59.105.24	HTTP	563	GET /-fdcfamily/tree/image-770983881.jpg HTTP/1.1
18894	06:14:53.253411	172.17.43.63	128.59.105.24	HTTP	563	GET /-fdcfamily/tree/image-826955460.jpg HTTP/1.1
18931	06:14:53.599668	172.17.43.63	128.59.105.24	HTTP	563	GET /-fdcfamily/tree/image-884426350.jpg HTTP/1.1
18977	06:14:53.912973	172.17.43.63	128.59.105.24	HTTP	563	GET /-fdcfamily/tree/image-938931815.jpg HTTP/1.1
18743	06:14:49.820565	172.17.43.63	128.59.105.24	HTTP	663	GET /-fdcfamily/tree/imageupload.php HTTP/1.1
17711	06:14:39.421053	172.17.43.63	128.59.105.24	HTTP	605	GET /-fdcfamily/tree/imageupload.php HTTP/1.1
19411	06:14:59.154122	65.61.137.117	172.17.43.63	HTTP	1131	HTTP/1.1 200 OK (GIF89a)
19430	06:14:59.433562	65.61.137.117	172.17.43.63	HTTP	354	HTTP/1.1 200 OK (GIF89a)

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

No.	Time	Source	Destination	Protocol	Length	Info
1888	22.853220	172.17.43.63	18.66.63.71	TCP	66	52671 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1889	22.855378	172.17.43.63	18.66.63.71	TCP	66	52672 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1890	22.917298	172.17.43.63	18.66.63.71	TCP	66	52673 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1891	22.920358	18.66.63.71	172.17.43.63	TCP	66	80 → 52671 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM=1 WS=512
1892	22.920358	18.66.63.71	172.17.43.63	TCP	66	80 → 52672 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM=1 WS=512
1893	22.920634	172.17.43.63	18.66.63.71	TCP	54	52671 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
1894	22.920079	172.17.43.63	18.66.63.71	TCP	54	52672 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
1895	22.921696	172.17.43.63	18.66.63.71	HTTP	548	GET /online HTTP/1.1
1896	22.927898	18.66.63.71	172.17.43.63	TCP	56	80 → 52672 [ACK] Seq=1 Ack=495 Win=65024 Len=0
1901	22.971909	18.66.63.71	172.17.43.63	TCP	66	80 → 52673 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM=1 WS=512
1902	22.972176	172.17.43.63	18.66.63.71	TCP	54	52673 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
1903	22.985502	18.66.63.71	172.17.43.63	TCP	593	80 → 52672 [PSH, ACK] Seq=1 Ack=495 Win=67072 Len=539 [TCP segment of a reassembled PDU]
1904	22.985502	18.66.63.71	172.17.43.63	HTTP	1240	HTTP/1.1 200 OK (text/html)
1905	22.985553	172.17.43.63	18.66.63.71	TCP	54	52672 → 80 [ACK] Seq=495 Ack=1726 Win=132352 Len=0
2100	26.385178	172.17.43.63	18.66.63.71	HTTP	485	GET /favicon.ico HTTP/1.1
2102	26.392622	18.66.63.71	172.17.43.63	TCP	56	80 → 52672 [ACK] Seq=1726 Ack=926 Win=67072 Len=0
2111	26.522629	18.66.63.71	172.17.43.63	TCP	554	80 → 52672 [PSH, ACK] Seq=1726 Ack=926 Win=68096 Len=500 [TCP segment of a reassembled PDU]
2113	26.522629	18.66.63.71	172.17.43.63	HTTP	178	HTTP/1.1 200 OK (PNG)
2114	26.523018	172.17.43.63	18.66.63.71	TCP	54	52672 → 80 [ACK] Seq=926 Ack=2350 Win=131840 Len=0
2551	31.824137	172.17.43.63	18.66.63.71	TCP	54	52671 → 80 [FIN, ACK] Seq=1 Ack=1 Win=132352 Len=0
2552	31.824387	172.17.43.63	18.66.63.71	TCP	54	52673 → 80 [FIN, ACK] Seq=1 Ack=1 Win=132352 Len=0
2553	31.824510	172.17.43.63	18.66.63.71	TCP	54	52672 → 80 [FIN, ACK] Seq=926 Ack=2350 Win=131840 Len=0
2573	31.950392	18.66.63.71	172.17.43.63	TCP	54	80 → 52673 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0
2574	31.950392	18.66.63.71	172.17.43.63	TCP	56	80 → 52672 [FIN, ACK] Seq=2350 Ack=927 Win=68096 Len=0
2580	31.950609	172.17.43.63	18.66.63.71	TCP	54	52673 → 80 [ACK] Seq=2 Ack=2 Win=132352 Len=0
2581	31.950631	172.17.43.63	18.66.63.71	TCP	54	52672 → 80 [ACK] Seq=927 Ack=2351 Win=131840 Len=0
2595	32.127086	172.17.43.63	18.66.63.71	TCP	54	[TCP Retransmission] 52671 → 80 [FIN, ACK] Seq=1 Ack=1 Win=132352 Len=0
2605	32.256193	18.66.63.71	172.17.43.63	TCP	54	80 → 52671 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0
2606	32.256193	18.66.63.71	172.17.43.63	TCP	66	[TCP Dup ACK 2605#1] 80 → 52671 [ACK] Seq=2 Ack=2 Win=65536 Len=0 SLE=1 SRE=2
2607	32.256324	172.17.43.63	18.66.63.71	TCP	54	52671 → 80 [ACK] Seq=2 Ack=2 Win=132352 Len=0

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

Packets into consideration:

1903 :- Seq =1

2581 :- ACK = 2351

Diff = 2350 bytes

time= 31.950631 - 22.985502 = 8.965129

Throughput =  $2350 \times 8 / 8.965129 = 2097.0138$  bits/sec