

1.1P Real-time Network Packet Capturing and Analysis

1. Starting network traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	216.58.199.34	TLSv1.2	93	Application Data
2	0.001096808	216.58.199.34	10.0.2.15	TCP	60	443 → 42772 [ACK] Seq=1 Ack=40 Win=65535 Len=0
3	0.020799783	216.58.199.34	10.0.2.15	TLSv1.2	93	Application Data
4	0.065375209	10.0.2.15	216.58.199.34	TCP	54	42772 → 443 [ACK] Seq=40 Ack=40 Win=63900 Len=0
5	1.952560628	220.244.223.77	10.0.2.15	TCP	60	443 → 38312 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
6	1.952687742	10.0.2.15	220.244.223.77	TLSv1.2	78	Application Data
7	1.952712531	10.0.2.15	220.244.223.77	TCP	54	38312 → 443 [FIN, ACK] Seq=25 Ack=2 Win=63900 Len=0
8	1.953025260	220.244.223.77	10.0.2.15	TCP	60	443 → 38312 [ACK] Seq=2 Ack=25 Win=65535 Len=0
9	1.953031933	220.244.223.77	10.0.2.15	TCP	60	443 → 38312 [ACK] Seq=2 Ack=26 Win=65535 Len=0
10	2.318342820	10.0.2.15	220.244.223.77	TCP	54	38318 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
11	2.318366989	10.0.2.15	220.244.223.77	TCP	54	38310 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
12	2.318373687	10.0.2.15	172.217.25.131	TCP	54	38504 → 80 [ACK] Seq=1 Ack=1 Win=63882 Len=0
13	2.318654736	220.244.223.77	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 443 → 38318 [ACK] Seq=1 Ack=2 Win=65535...
14	2.318661617	220.244.223.77	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 443 → 38310 [ACK] Seq=1 Ack=2 Win=65535...
15	2.318662752	172.217.25.131	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 80 → 38504 [ACK] Seq=1 Ack=2 Win=65535...
16	3.696976366	10.0.2.15	220.244.223.77	TLSv1.2	1337	[TCP Previous segment not captured], Application Data
17	3.697389895	220.244.223.77	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 443 → 38318 [ACK] Seq=1 Ack=1285 Win=65...
18	3.709287027	220.244.223.77	10.0.2.15	TLSv1.2	2934	Application Data
19	3.709369701	10.0.2.15	220.244.223.77	TCP	54	38318 → 443 [ACK] Seq=1285 Ack=2881 Win=65535 Len=0
20	3.710364014	220.244.223.77	10.0.2.15	TCP	4374	443 → 38318 [PSH, ACK] Seq=2881 Ack=1285 Win=65535 Len=4320 [TCP s...
21	3.710425175	10.0.2.15	220.244.223.77	TCP	54	38318 → 443 [ACK] Seq=1285 Ack=7201 Win=65535 Len=0
22	3.710965909	220.244.223.77	10.0.2.15	TCP	2934	443 → 38318 [PSH, ACK] Seq=7201 Ack=1285 Win=65535 Len=2880 [TCP s...
23	3.711039402	10.0.2.15	220.244.223.77	TCP	54	38318 → 443 [ACK] Seq=1285 Ack=10081 Win=65535 Len=0

Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
Ethernet II, Src: PcsCompu_7d:62:aa (08:00:27:7d:62:aa), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.58.199.34
Transmission Control Protocol, Src Port: 42772, Dst Port: 443, Seq: 1, Ack: 1, Len: 39
Transport Layer Security

0000 52 54 00 12 35 02 08 00 27 7d 62 aa 08 00 45 00 RT..5...'}b...E.
0010 00 4f 68 3b 40 00 00 06 27 02 0a 00 02 0f d8 3a .Oh;@.:'......:
0020 c7 22 a7 14 01 bb 92 00 3c a5 0f 30 be 7b 50 18 .".....<..0.{P..
0030 f9 9c ab ad 00 00 17 03 03 00 22 c6 69 13 7d f5~".i..}.
0040 d0 5a 42 2a c8 b4 df 84 a4 9c 51 c7 e8 1b 24 e5 .ZB*.....Q...\$.
0050 58 d6 43 ab 72 09 cc 18 cf 24 14 16 89 X.C.r...~\$...

enp0s3: <live capture in progress> Packets: 3875 · Displayed: 3855 (99.5%) Profile: Default

2. Stopping capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
4236	92.110502125	216.58.196.132	10.0.2.15	TLSv1.2	93	Application Data
4237	92.110516413	10.0.2.15	216.58.196.132	TCP	54	53372 → 443 [ACK] Seq=79 Ack=79 Win=63900 Len=0
4238	92.111049899	216.58.199.70	10.0.2.15	TLSv1.2	93	Application Data
4239	92.111068853	10.0.2.15	216.58.199.70	TCP	54	41866 → 443 [ACK] Seq=79 Ack=79 Win=63900 Len=0
4240	92.427558663	10.0.2.15	220.244.223.77	TCP	54	[TCP Keep-Alive] 38318 → 443 [ACK] Seq=7477 Ack=7531014 Win=65...
4241	92.427953187	220.244.223.77	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 443 → 38318 [ACK] Seq=7531014 Ack=7478 Wi...
4242	97.058513185	91.189.92.38	10.0.2.15	TLSv1.2	295	Application Data
4243	97.058546342	10.0.2.15	91.189.92.38	TCP	54	32938 → 443 [ACK] Seq=316 Ack=3349 Win=63900 Len=0
4244	97.058802579	91.189.92.38	10.0.2.15	TLSv1.2	85	Encrypted Alert
4245	97.058811414	10.0.2.15	91.189.92.38	TCP	54	32938 → 443 [ACK] Seq=316 Ack=3380 Win=63900 Len=0
4246	97.059100581	91.189.92.38	10.0.2.15	TCP	60	443 → 32938 [FIN, ACK] Seq=3380 Ack=316 Win=65535 Len=0
4247	97.067314609	10.0.2.15	91.189.92.38	TLSv1.2	85	Encrypted Alert
4248	97.067498409	10.0.2.15	91.189.92.38	TCP	54	32938 → 443 [RST, ACK] Seq=347 Ack=3381 Win=63900 Len=0
4249	97.067999392	91.189.92.38	10.0.2.15	TCP	60	443 → 32938 [ACK] Seq=3381 Ack=347 Win=65535 Len=0
4250	97.068019538	10.0.2.15	91.189.92.38	TCP	54	32938 → 443 [RST] Seq=347 Win=0 Len=0
4251	97.068496555	91.189.92.38	10.0.2.15	TCP	60	443 → 32938 [RST, ACK] Seq=4026871295 Ack=347 Win=0 Len=0
4252	101.889986968	10.0.2.15	216.58.200.110	TLSv1.2	627	Application Data
4253	101.890293721	10.0.2.15	216.58.200.110	TLSv1.2	85	Application Data
4254	101.890400650	216.58.200.110	10.0.2.15	TCP	60	443 → 48136 [ACK] Seq=1036 Ack=7369 Win=65535 Len=0
4255	101.890592231	216.58.200.110	10.0.2.15	TCP	60	443 → 48136 [ACK] Seq=1036 Ack=7400 Win=65535 Len=0
4256	102.060293329	216.58.200.110	10.0.2.15	TLSv1.2	196	Application Data, Application Data, Application Data
4257	102.060741437	10.0.2.15	216.58.200.110	TLSv1.2	93	Application Data
4258	102.061158418	216.58.200.110	10.0.2.15	TCP	60	443 → 48136 [ACK] Seq=1178 Ack=7439 Win=65535 Len=0

Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_7d:62:aa (08:00:27:7d:62:aa)
Internet Protocol Version 4, Src: 220.244.223.77, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 443, Dst Port: 38312, Seq: 1, Ack: 1, Len: 0

0000 08 00 27 7d 62 aa 52 54 00 12 35 02 08 00 45 00 ...'}b.RT..5...E.
0010 00 28 3f 02 00 00 40 06 73 7d dc f4 df 4d 0a 00 .(?..@.s)...M..
0020 02 0f 01 bb 95 a8 0f 6e 3f c9 c3 15 b4 ba 50 11 .02..n?...P..
0030 ff ff 89 17 00 00 00 00 00 00 00 00

wireshark_enp0s3_20200321194428_bgtPzC.pcapng Packets: 4260 · Displayed: 4217 (99.0%) Profile: Default

1.1P Real-time Network Packet Capturing and Analysis

3. Filters [ip.src == 10.0.2.15, not arp, ip.src_host]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src_host

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.0.2.15	216.58.199.34	TLSv1.2	93	Application Data
2	0.001096808	216.58.199.34	10.0.2.15	TCP	60	443 → 42772 [ACK] Seq=1 Ack=40 Win=65535 Len=0
3	0.002079783	216.58.199.34	10.0.2.15	TLSv1.2	93	Application Data
4	0.005375209	10.0.2.15	216.58.199.34	TCP	54	42772 → 443 [ACK] Seq=40 Ack=40 Win=63900 Len=0
5	1.952560628	220.244.223.77	10.0.2.15	TCP	60	443 → 38312 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
6	1.952687742	10.0.2.15	220.244.223.77	TLSv1.2	78	Application Data
7	1.952712531	10.0.2.15	220.244.223.77	TCP	54	38312 → 443 [FIN, ACK] Seq=25 Ack=2 Win=63900 Len=0
8	1.953025260	220.244.223.77	10.0.2.15	TCP	60	443 → 38312 [ACK] Seq=2 Ack=25 Win=65535 Len=0
9	1.953031933	220.244.223.77	10.0.2.15	TCP	60	443 → 38312 [ACK] Seq=2 Ack=26 Win=65535 Len=0
10	2.318342820	10.0.2.15	220.244.223.77	TCP	54	38318 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
11	2.318366989	10.0.2.15	220.244.223.77	TCP	54	38310 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
12	2.318373687	10.0.2.15	172.217.25.131	TCP	54	38504 → 80 [ACK] Seq=1 Ack=1 Win=63882 Len=0
13	2.318654736	220.244.223.77	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 443 → 38318 [ACK] Seq=1 Ack=2 Win=6...
14	2.318661617	220.244.223.77	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 443 → 38310 [ACK] Seq=1 Ack=2 Win=6...
15	2.318662752	172.217.25.131	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 80 → 38504 [ACK] Seq=1 Ack=2 Win=65...
16	3.696976366	10.0.2.15	220.244.223.77	TLSv1.2	1337	[TCP Previous segment not captured], Application Data
17	3.697389895	220.244.223.77	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 443 → 38318 [ACK] Seq=1 Ack=1285 Wi...
18	3.709287027	220.244.223.77	10.0.2.15	TLSv1.2	2934	Application Data
19	3.709399701	10.0.2.15	220.244.223.77	TCP	54	38318 → 443 [ACK] Seq=1285 Ack=2881 Win=65535 Len=0
20	3.710364014	220.244.223.77	10.0.2.15	TCP	4374	443 → 38318 [PSH, ACK] Seq=2881 Ack=1285 Win=65535 Ack=4320 [T...
21	3.710425175	10.0.2.15	220.244.223.77	TCP	54	38318 → 443 [ACK] Seq=1285 Ack=7201 Win=65535 Len=0
22	3.710985909	220.244.223.77	10.0.2.15	TCP	2934	443 → 38318 [PSH, ACK] Seq=7201 Ack=1285 Win=65535 Len=2880 [T...
23	3.711039402	10.0.2.15	220.244.223.77	TCP	54	38318 → 443 [ACK] Seq=1285 Ack=10081 Win=65535 Len=0

Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: RealtekU12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_7d:62:aa (08:00:27:7d:62:aa)
Internet Protocol Version 4, Src: 220.244.223.77, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 443, Dst Port: 38312, Seq: 1, Ack: 1, Len: 0

savecap.pcapng

Packets: 4260 · Displayed: 4248 (99.7%) · Dropped: 0 (0.0%) · Profile: Default

4. Filter to check ACK

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.ack==0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000	164.124.33.78	192.168.0.1	TCP	54	35165 → 80 [SYN] Seq=0 Win=16384 Len=0
2	0.0000001	38.198.26.9	192.168.0.1	TCP	54	14378 → 80 [SYN] Seq=0 Win=16384 Len=0
3	0.0000003	132.212.36.201	192.168.0.1	TCP	54	31944 → 80 [SYN] Seq=0 Win=16384 Len=0
4	0.0000005	76.196.0.157	192.168.0.1	TCP	54	10404 → 80 [RST] Seq=1 Win=0 Len=0
5	0.0000057	189.109.37.180	192.168.0.1	TCP	54	36076 → 80 [SYN] Seq=0 Win=16384 Len=0
6	0.0000059	189.109.37.188	192.168.0.1	TCP	54	36084 → 80 [SYN] Seq=0 Win=16384 Len=0
7	0.0000060	76.196.12.251	192.168.0.1	TCP	54	12034 → 80 [SYN] Seq=0 Win=16384 Len=0
8	0.0000062	132.212.36.146	192.168.0.1	TCP	54	31889 → 80 [SYN] Seq=0 Win=16384 Len=0
9	0.0000064	189.109.30.67	192.168.0.1	TCP	54	34171 → 80 [RST] Seq=1 Win=0 Len=0
10	0.0000065	189.109.37.184	192.168.0.1	TCP	54	36080 → 80 [SYN] Seq=0 Win=16384 Len=0
11	0.0000067	164.124.33.164	192.168.0.1	TCP	54	35251 → 80 [SYN] Seq=0 Win=16384 Len=0
12	0.0000069	189.109.37.88	192.168.0.1	TCP	54	35984 → 80 [SYN] Seq=0 Win=16384 Len=0
13	0.0000182	76.196.12.188	192.168.0.1	TCP	54	11971 → 80 [SYN] Seq=0 Win=16384 Len=0
14	0.0000184	132.212.36.112	192.168.0.1	TCP	54	31855 → 80 [SYN] Seq=0 Win=16384 Len=0
15	0.0000186	164.124.33.94	192.168.0.1	TCP	54	35182 → 80 [SYN] Seq=0 Win=16384 Len=0
16	0.0000188	76.196.12.250	192.168.0.1	TCP	54	12033 → 80 [SYN] Seq=0 Win=16384 Len=0
17	0.0000189	164.124.33.94	192.168.0.1	TCP	54	35181 → 80 [SYN] Seq=0 Win=16384 Len=0
18	0.0000191	164.124.33.160	192.168.0.1	TCP	54	35247 → 80 [SYN] Seq=0 Win=16384 Len=0
19	0.0000193	38.198.26.94	192.168.0.1	TCP	54	14463 → 80 [SYN] Seq=0 Win=16384 Len=0
20	0.0000195	132.212.36.219	192.168.0.1	TCP	54	31962 → 80 [SYN] Seq=0 Win=16384 Len=0
21	0.0000466	164.124.33.172	192.168.0.1	TCP	54	35259 → 80 [SYN] Seq=0 Win=16384 Len=0
22	0.0000468	164.124.33.90	192.168.0.1	TCP	54	35177 → 80 [SYN] Seq=0 Win=16384 Len=0
23	0.0000470	132.212.36.218	192.168.0.1	TCP	54	31961 → 80 [SYN] Seq=0 Win=16384 Len=0

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Cisco_c0:ff:ee (00:19:30:c0:ff:ee), Dst: Intel_c0:ff:ee (00:0e:0c:c0:ff:ee)
Internet Protocol Version 4, Src: 164.124.33.78, Dst: 192.168.0.1
Transmission Control Protocol, Src Port: 35165, Dst Port: 80, Seq: 0, Len: 0

SynFlood Sample.pcap

Packets: 40 · Displayed: 40 (100.0%) · Profile: Default