

Wireshark Live Packet Capture Report

Task 5

From: Gautam Oza

Objective

The objective of this activity is to capture live network packets and identify basic protocols and traffic types using Wireshark. This includes analyzing various traffic types such as TCP, UDP, TLS, QUIC, and DNS, and interpreting their role in the network communication.

Tool Used

Wireshark (Free and open-source packet analyzer).

Observations and Findings

1. **TCP Traffic**: Multiple TCP streams were captured, including acknowledgment (ACK) packets and keep-alive signals, indicating ongoing connections.
2. **TLS/SSL Traffic**: Presence of TLS 1.3 encrypted packets shows secure communication, possibly HTTPS traffic.
3. **QUIC Protocol**: Observed QUIC packets, often used by HTTP/3, indicating modern web traffic.
4. **DNS Queries**: Queries to domains such as 'teams.events.data.microsoft.com' indicate communication with Microsoft services.
5. **UDP Multicast Streams**: Detected mDNS and SSDP multicast traffic, typically used for local network service discovery.
6. **RST Packets**: Presence of TCP RST (Reset) packets suggests some connections were forcefully closed.

Captured Evidence

Below are the screenshots from Wireshark showing the captured packets and analysis windows.

Wireshark Live Packet Capture Report

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
146	5.529430	103.157.178.210	192.168.0.105	QUIC	66	Protected Payload (KP0)
147	5.530046	192.168.0.105	103.157.178.210	QUIC	73	Protected Payload (KP0), DCID=07dc7aa73c00b32a
148	5.940388	57.144.125.33	192.168.0.105	TCP	281	5222 → 50349 [PSH, ACK] Seq=1 Ack=1 Win=286 Len=227
149	5.956415	192.168.0.105	57.144.125.33	XMP/XL	125	
150	5.957771	192.168.0.105	57.144.125.33	TCP	125	50349 → 5222 [PSH, ACK] Seq=72 Ack=228 Win=255 Len=71 [TCP PDU reassembled in 152]
151	5.959366	57.144.125.33	192.168.0.105	TCP	54	5222 → 50349 [ACK] Seq=228 Ack=72 Win=286 Len=0
152	5.960051	192.168.0.105	57.144.125.33	TCP	125	50349 → 5222 [PSH, ACK] Seq=143 Ack=228 Win=255 Len=71 [TCP PDU reassembled in 152]
153	5.960138	57.144.125.33	192.168.0.105	TCP	54	5222 → 50349 [ACK] Seq=228 Ack=143 Win=286 Len=0
154	5.962051	57.144.125.33	192.168.0.105	TCP	54	5222 → 50349 [ACK] Seq=228 Ack=214 Win=286 Len=0
155	6.048905	192.168.0.105	20.42.65.88	TLSv1.3	315	Application Data
156	6.049026	192.168.0.105	20.42.65.88	TLSv1.3	9539	Application Data
157	6.353547	20.42.65.88	192.168.0.105	TCP	54	443 → 50394 [ACK] Seq=7263 Ack=16370 Win=4194560 Len=0
158	6.353547	20.42.65.88	192.168.0.105	TCP	54	443 → 50394 [ACK] Seq=7263 Ack=17810 Win=4194560 Len=0
159	6.353547	20.42.65.88	192.168.0.105	TCP	54	443 → 50394 [ACK] Seq=7263 Ack=22130 Win=4194560 Len=0
160	6.353547	20.42.65.88	192.168.0.105	TCP	54	443 → 50394 [ACK] Seq=7263 Ack=22975 Win=4193792 Len=0
161	6.353547	20.42.65.88	192.168.0.105	TLSv1.3	363	Application Data
162	6.399303	192.168.0.105	20.42.65.88	TCP	54	50394 → 443 [ACK] Seq=22975 Ack=7572 Win=64256 Len=0
163	7.812790	192.168.0.105	192.168.0.1	DNS	91	Standard query 0xcac A teams.events.data.microsoft.com

Frame 1: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on interface \Device\NPF...
Ethernet II, Src: Intel_7d:6c:02 (dc:21:5c:7d:6c:02), Dst: TPLink_80:d1:76 (e8:48:b8:0d:17:6)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 20.42.65.88
Transmission Control Protocol, Src Port: 50390, Dst Port: 443, Seq: 1, Ack: 1, Len: 261
Transport Layer Security

0000 e8 48 b8 0d 17 6d c2 15 c7 d6 c0 02 08 00 45 00 ...H...v...!...E...
0010 01 2d 29 c6 40 00 80 06 00 00 c0 a8 00 69 14 2a ...-)@...i...*...
0020 41 58 c4 d6 01 bb bc 35 a0 28 90 c3 a7 03 50 18 AX...5...P...
0030 00 fc 17 b3 00 00 17 03 03 01 00 ea dc 6d ef b6 ...Q...W...Z...M...I...
0040 af f5 51 8f 57 aa f3 cb 5a c9 bd 57 9a af 04 49 ...n...X...Q...n...
0050 cb 9c b3 6e a5 d0 85 2c de d9 58 86 51 a7 6e 0a ...6...D...4...a...
0060 09 03 91 05 36 cb d9 9c 2d fb 44 2c b4 34 5e 61 ...P...5...K...u...
0070 3e 30 18 f2 50 a5 c5 20 cd 35 2a 9c 60 04 b5 75 ...>...y...
0080 af 0d b9 0d 16 3e da 79 18 86 10 d3 0c 1f a7 7f ...:...L...Q...
0090 e9 ef de 87 ae cb 6c f4 13 b8 10 c7 b6 51 c8 5f ...fd...4G+...
00a0 82 66 64 b4 9a a3 dc 16 87 dd 01 99 e6 34 47 2b ...m*...C...Q...
00b0 5e 6d 8b 2a fa ce 0e 8e 8b b6 b8 43 c4 51 be 05 ...fH...cqmgx...R...
00c0 9f cc cc 1e 66 48 e4 85 63 71 6d 67 78 c4 52 bf ...U...L...
00d0 9a 2a 00 1f 08 9a 7e 56 a2 3c 81 ea e5 d6 70 75 ...1+...H...R...
00e0 ee 31 fa 2b 05 bc a7 f5 9d 1a e3 af 48 d5 7e 52 ...U...L...
00f0 1e 8d d2 83 55 2c 9c c9 fe b2 f5 4c 3b 20 b9 b2 ...f...J...P...
0100 92 00 c1 66 f5 ec e8 4a cc 14 50 d8 a8 89 f9 c9 ...Z...e...1...4a...
0110 ee 8d b9 5d 5a ed a8 65 1c 7f 31 00 12 34 61 fe ...hTfN...k...F...
0120 e2 bf b9 a3 68 54 66 4e c9 2e 6b c6 46 de 2e fe

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.ack

No.	Time	Source	Destination	Protocol	Length	Info
248	42.741711	192.168.0.105	52.2.223.15	TCP	55	50500 → 443 [ACK] Seq=...
249	44.159030	192.168.0.105	148.113.8.203	TCP	55	[TCP Keep-Alive] 5033...
250	44.169700	148.113.8.203	192.168.0.105	TCP	66	[TCP Keep-Alive ACK]...
251	45.020005	192.168.0.105	142.250.70.42	TCP	55	[TCP Keep-Alive] 5053...
252	45.022940	142.250.70.42	192.168.0.105	TCP	66	[TCP Keep-Alive ACK]...
273	51.409173	20.190.146.39	192.168.0.105	TCP	54	443 → 50483 [RST, ACK]...
274	53.579051	192.168.0.105	57.144.125.32	TLSv1.2	123	Application Data
275	53.581294	57.144.125.32	192.168.0.105	TCP	54	443 → 50517 [ACK] Seq=...
276	53.732087	57.144.125.32	192.168.0.105	TLSv1.2	125	Application Data
277	53.783246	192.168.0.105	57.144.125.32	TCP	54	50517 → 443 [ACK] Seq=...
278	54.177626	192.168.0.105	148.113.8.203	TCP	55	[TCP Keep-Alive] 5033...
279	54.185961	148.113.8.203	192.168.0.105	TCP	66	[TCP Keep-Alive ACK]...

Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF...
Ethernet II, Src: Intel_7d:6c:02 (dc:21:5c:7d:6c:02), Dst: TPLink_80:d1:76 (e8:48:b8:0d:17:6)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 52.2.223.15
Transmission Control Protocol, Src Port: 50514, Dst Port: 443, Seq: 1, Ack: 1, Len: 261

0000 e8 48 b8 0d 17 6d c2 15 c7 d6 c0 02 08 00 45 00 ...H...v...!...E...
0010 00 29 59 73 40 00 80 06 00 00 c0 a8 00 69 8e ...-)@...i...*...
0020 46 2a c5 52 01 bb c0 da 35 e8 9e 86 55 32 50 AX...5...P...
0030 00 fa 96 51 00 00 00 ...Q...W...Z...M...I...
0040 af f5 51 8f 57 aa f3 cb 5a c9 bd 57 9a af 04 49 ...n...X...Q...n...
0050 cb 9c b3 6e a5 d0 85 2c de d9 58 86 51 a7 6e 0a ...6...D...4...a...
0060 09 03 91 05 36 cb d9 9c 2d fb 44 2c b4 34 5e 61 ...P...5...K...u...
0070 3e 30 18 f2 50 a5 c5 20 cd 35 2a 9c 60 04 b5 75 ...>...y...
0080 af 0d b9 0d 16 3e da 79 18 86 10 d3 0c 1f a7 7f ...:...L...Q...
0090 e9 ef de 87 ae cb 6c f4 13 b8 10 c7 b6 51 c8 5f ...fd...4G+...
00a0 82 66 64 b4 9a a3 dc 16 87 dd 01 99 e6 34 47 2b ...m*...C...Q...
00b0 5e 6d 8b 2a fa ce 0e 8e 8b b6 b8 43 c4 51 be 05 ...fH...cqmgx...R...
00c0 9f cc cc 1e 66 48 e4 85 63 71 6d 67 78 c4 52 bf ...U...L...
00d0 9a 2a 00 1f 08 9a 7e 56 a2 3c 81 ea e5 d6 70 75 ...1+...H...R...
00e0 ee 31 fa 2b 05 bc a7 f5 9d 1a e3 af 48 d5 7e 52 ...U...L...
00f0 1e 8d d2 83 55 2c 9c c9 fe b2 f5 4c 3b 20 b9 b2 ...f...J...P...
0100 92 00 c1 66 f5 ec e8 4a cc 14 50 d8 a8 89 f9 c9 ...Z...e...1...4a...
0110 ee 8d b9 5d 5a ed a8 65 1c 7f 31 00 12 34 61 fe ...hTfN...k...F...
0120 e2 bf b9 a3 68 54 66 4e c9 2e 6b c6 46 de 2e fe

Wireshark Live Packet Capture Report

Wireshark · Packet 279 · Wi-Fi

- ▶ Frame 279: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface
- ▶ Ethernet II, Src: TPLink_80:d1:76 (e8:48:b8:80:d1:76), Dst: Intel_7d:6c:02 (dc:14:6c:02)
- ▶ Internet Protocol Version 4, Src: 148.113.8.203, Dst: 192.168.0.105
- ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 50336, Seq: 1, Ack: 2,

0000 dc 21 5c 7d 6c 02 e8 48 b8 80 d1 76 08 00 45 10 ·!\\}1·H·v·E·
0010 00 34 a8 46 40 00 36 06 3e 20 94 71 08 cb c0 a8 ·4·F@·6·>·q·
0020 00 69 01 bb c4 a0 88 28 7a a3 c0 35 80 81 80 10 ·i·(·z·5·
0030 01 f5 8e 2e 00 00 01 01 05 0a c0 35 80 80 c0 35 ······5··5
0040 80 81 ···

Bytes 26-29: Source Address (ip.src)

☒ Show packet bytes Layout: Vertical (Stacked)

Close Help

Wireshark · UDP Multicast Streams · Wi-Fi

Source Address	Source Port	Destination Address	Destination Port	Packets	Packets/s	Avg BW (bps)	Max BW (bps)
192.168.0.107	5353	224.0.0.251	5353	9	0.12	108	19 k
192.168.0.103	5353	224.0.0.251	5353	4	0.07	89	0
169.254.239.234	49678	239.255.255.250	1900	4	1.24	2154	0

2 streams, avg bw: 216bps, max bw: 19 kbps, max burst: 2 / 100ms, max buffer: 1688

Burst measurement interval (ms): 100 Burst alarm threshold (packets): 50 Buffer alarm threshold (B): 10000

Stream empty speed (Kb/s): 5000 Total empty speed (Kb/s): 100000

Display filter: Enter a display filter ... Apply

Copy Save as... Close