

Task 5: Capture and Analyze Network Traffic Using Wireshark

Objective: Capture live network packets and identify basic protocols and traffic types.

Tool Used: Wireshark

1. Installation of Wireshark

Wireshark was downloaded and installed from the official website <https://www.wireshark.org/>. It is a free and open-source packet analyzer used for network troubleshooting, analysis, and protocol development.

2. Starting Packet Capture

After launching Wireshark:

- The active network interface (e.g., Ethernet or Wi-Fi) was selected.
 - Packet capture was started by clicking the "Start Capturing Packets" button.
-

3. Generating Network Traffic

To generate traffic:

- A website (e.g., www.google.com) was opened in a browser.
 - This triggered web (HTTP), DNS, and TCP traffic.
-

4. Stopping Packet Capture

After around 1 minute of activity:

- The capture was stopped using the red "Stop" button in Wireshark.
-

5. Filtering Packets by Protocol

Wireshark provides a filter bar to view specific protocols. The following filters were applied:

- http to view HTTP traffic
- tcp to view TCP-level communication

- dns to view DNS queries and responses
- arp to observe ARP requests and replies within the local network

6. Protocols Identified

From the capture, the following protocols were identified:

a. HTTP (Hypertext Transfer Protocol)

- Used for web browsing.
- Example: GET request to www.google.com.
- Contains headers like Host, User-Agent, Accept, etc.

No.	Time	Source	Destination	Protocol	Length	Info
1509	16.827467	192.168.0.102	47.252.97.14	HTTP/POST(UNKNOWN)	696	POST /logstore/logstore-ens_ip/shards/1b HTTP/1.1 (PROTOBUF)
1550	17.862331	47.252.97.14	192.168.0.102	HTTP	296	HTTP/1.1 200 OK
1761	25.778714	192.168.0.102	44.228.249.3	HTTP	531	GET /index.php HTTP/1.1
1770	26.005616	44.228.249.3	192.168.0.102	HTTP	1153	HTTP/1.1 200 OK (text/html)
1772	26.004626	192.168.0.102	44.228.249.3	HTTP	431	GET /style.css HTTP/1.1
1773	26.006283	192.168.0.102	44.228.249.3	HTTP	483	GET /images/logo.gif HTTP/1.1
1795	26.382934	44.228.249.3	192.168.0.102	HTTP	874	HTTP/1.1 200 OK (GIF89a)
1800	26.385230	44.228.249.3	192.168.0.102	HTTP	1156	HTTP/1.1 200 OK (text/css)
1829	27.909120	192.168.0.102	44.228.249.3	HTTP	578	GET /login.php HTTP/1.1
1834	28.272418	44.228.249.3	192.168.0.102	HTTP	1342	HTTP/1.1 200 OK (text/html)
1953	45.110183	192.168.0.102	44.228.249.3	HTTP	748	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
1956	45.404197	44.228.249.3	192.168.0.102	HTTP	330	HTTP/1.1 302 Found (text/html)
1957	45.408764	192.168.0.102	44.228.249.3	HTTP	604	GET /login.php HTTP/1.1
1960	45.703043	44.228.249.3	192.168.0.102	HTTP	1342	HTTP/1.1 200 OK (text/html)

Frame 1509: 696 bytes on wire (5568 bits), 696 bytes captured (5568 bits)	0000	b0 a7 b9 79 b6 bb f4 c8	8a 71 16 4b 08 00 45 00	...	q K E
Ethernet II, Src: Intel_71:16:4b (f4:c8:8a:71:16:4b), Dst: TPLink_79:b6:bb (b0:a7:b9:79:b6:bb)	0010	02 aa 1f 0e 40 00 80 06	00 00 c0 a8 00 66 2f fc
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 47.252.97.14	0020	61 0e 2d 3f 00 50 e4 6b	d0 fa ab 49 95 06 50 18	...	a-? P k @ P
Transmission Control Protocol, Src Port: 11583, Dst Port: 80, Seq: 1, Ack: 642	0030	00 ff 54 b5 00 00 50 4f	53 54 20 2f 6c 6f 67 73	...	T PD S! /logs
Hypertext Transfer Protocol	0040	74 6f 72 65 73 2f 6c 6f	67 73 74 6f 72 65 5f 65	...	tores/lo gstore_e
Protocol Buffers	0050	6e 73 5f 69 70 2f 73 68	61 72 64 73 2f 6c 62 20	...	ns_ip/sh ards/1b
	0060	4b 54 54 50 2f 31 2e 31	0d 0a 48 6f 73 74 2a 65	...	HTTP/1.1 Hoste
	0070	61 73 65 75 73 69 6e 66	6f 2e 75 73 2d 65 61 73	...	aseusinf ou-s-eas
	0080	74 2d 31 2e 6c 6f 67 2e	61 6c 69 79 75 6e 63 73	...	t-1.log. aliyncs
	0090	2e 63 6f 6d 0a 55 73	65 72 2d 41 67 65 6e 74com Us er-Agent
	00a0	3a 20 6c 6f 67 2d 63 2d	6c 69 74 65 5f 30 2e 31	...	: log-s- lttle.0.1
	00b0	2e 30 0d 0a 41 63 63 65	70 74 3a 20 2a 2f 2a 0d0 Acce pt: */*
	00c0	0a 43 6f 6e 74 65 6e 74	2d 54 79 70 65 3a 61 70	...	Content -type:ap
	00d0	70 6c 69 63 61 74 69 6f	6e 2f 78 2d 70 72 6f 74	...	plicatio n/x-prot
	00e0	6f 62 75 66 0d 0a 78 2d	6c 6f 67 2d 61 70 69 76	...	obuf x- log-apiv
	00f0	65 72 73 69 6f 6e 3a 30	2e 36 2e 30 0d 0a 78 2d	...	ersion:0 .6.0 x-
	0100	6c 6f 67 2d 63 6f 6d 70	72 65 73 73 74 79 70 65	...	log-comp resstype
	0110	3a 6c 7a 3a 0d 0a 78 2d	6c 6f 67 2d 73 69 67 6e	...	:124 x- log-sign
	0120	61 74 75 72 65 6d 65 74	68 6f 64 3a 68 6d 61 63	...	aturemet hodi:hm
	0130	2d 73 68 61 31 0d 0a 44	61 74 65 3a 4d 6f 6e 2c	...	-sha1 D ate:Mon,
	0140	20 33 30 20 44 75 6e 20	32 30 32 35 20 31 33 3a	...	30 Jun 2025 13:
	0150	32 39 3a 30 39 20 47 4d	54 0d 0a 43 6f 6e 74 65	...	29:09 GM T Conte
	0160	6e 74 2d 4d 44 35 3a 44	44 37 34 32 34 38 41 44	...	nt-MD5:D 74248AD
	0170	30 43 45 34 30 41 30 30	30 44 43 45 33 42 31 33	...	0CE40A00 0DCE3013

b. TCP (Transmission Control Protocol)

- Underlying transport protocol for HTTP.
- Responsible for connection setup (SYN), data transfer, and teardown (FIN).
- TCP handshakes and data segments were captured.

Captured_Packets.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
6	1.119131	192.168.0.102	192.168.0.107	TCP	164	11311 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=250 Len=110 [TCP PDU reassembled in 1882]
7	1.147967	192.168.0.107	192.168.0.102	TCP	164	8009 → 11311 [PSH, ACK] Seq=1 Ack=111 Win=1207 Len=110 [TCP PDU reassembled in 1883]
8	1.198352	192.168.0.102	192.168.0.107	TCP	54	11311 → 8009 [ACK] Seq=111 Ack=111 Win=255 Len=0
9	1.943181	192.168.0.102	192.168.0.107	TCP	54	11311 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=255 Len=0
34	4.446292	13.107.253.68	192.168.0.102	TLSv1.2	93	Application Data
35	4.446390	13.107.253.68	192.168.0.102	TLSv1.2	78	Application Data
36	4.446390	13.107.253.68	192.168.0.102	TCP	54	443 → 11557 [FIN, ACK] Seq=64 Ack=1 Win=83 Len=0
37	4.446460	192.168.0.102	13.107.253.68	TCP	54	11557 → 443 [ACK] Seq=1 Ack=65 Win=255 Len=0
38	4.446700	192.168.0.102	13.107.253.68	TCP	54	11557 → 443 [FIN, ACK] Seq=1 Ack=65 Win=255 Len=0
39	4.491500	13.107.253.68	192.168.0.102	TCP	54	443 → 11557 [ACK] Seq=65 Ack=2 Win=83 Len=0
42	4.804506	91.108.56.136	192.168.0.102	SSL	159	Continuation Data
43	4.858367	192.168.0.102	91.108.56.136	TCP	54	11557 → 443 [ACK] Seq=1 Ack=106 Win=252 Len=0
44	4.954004	192.168.0.102	104.18.31.173	TCP	55	11559 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
45	4.999943	104.18.31.173	192.168.0.102	TCP	66	443 → 11559 [ACK] Seq=1 Ack=2 Win=16 Len=0 SLE=1 SRE=2
47	5.815495	192.168.0.102	140.82.112.21	TCP	55	11556 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
51	6.111311	140.82.112.21	192.168.0.102	TCP	66	443 → 11556 [ACK] Seq=1 Ack=2 Win=84 Len=0 SLE=1 SRE=2
52	6.150732	192.168.0.102	192.168.0.107	TCP	164	11311 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=255 Len=110 [TCP PDU reassembled in 1882]
53	6.188433	192.168.0.107	192.168.0.102	TCP	164	8009 → 11311 [PSH, ACK] Seq=111 Ack=221 Win=1207 Len=110 [TCP PDU reassembled in 1883]
54	6.230519	192.168.0.102	192.168.0.107	TCP	54	11311 → 8009 [ACK] Seq=221 Ack=221 Win=255 Len=0
55	6.788465	91.108.56.136	192.168.0.102	SSL	159	Continuation Data

Frame 6: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface 0
 Ethernet II, Src: Intel 71:16:4b (f4:c8:8a:71:16:4b), Dst: OnePilotlect_4f:85:0f (a0:91:a2:4f:85:0f)
 Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.107
 Transmission Control Protocol, Src Port: 11311, Dst Port: 8009, Seq: 1, Ack: 1, Len: 110

0000 a0 91 a2 4f 85 0f f4 c8 8a 71 16 4b 08 00 45 00 ... 0... q K E
 0010 00 9c 71 f5 40 00 80 06 00 00 c0 a8 00 66 c0 a8 ... q 0 ... f
 0020 00 0b 2c 2f 1f 49 10 d4 6d 2a f5 e2 90 ae 50 18 ... k / I m * P
 0030 00 fa 82 aa 00 00 17 03 03 00 69 92 8b eb ce d9 1...
 0040 5f a4 5a 75 d0 93 8c fd 8c 8a ad a8 21 69 50 1P
 0050 3e 70 c0 0f 63 a7 eb d4 3d ce 6c f0 73 4b 5f a1 1M
 0060 9c 5a 3c db e1 6e eb 17 be d5 3d 79 fd 40 d4 b8 1M
 0070 69 15 b9 e5 34 ef 21 bd e5 d4 5c a0 46 a3 84 8d 1M
 0080 c9 35 86 5b bd df c5 77 79 a8 0b 3e 8e 15 24 8b 1M
 0090 8c 80 0d 16 88 e7 c9 8f 2a 66 86 e4 93 7f 33 19 1M
 00a0 22 aa 9e f7

Transmission Control Protocol Protocol Packets: 3489 - Displayed: 1324 (37.9%) - Dropped: 0 (0.0%) Profile: Default

c. DNS (Domain Name System)

- Resolves domain names to IP addresses.
- Example: DNS query and response for www.google.com.

Captured_Packets.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
143	10.307882	192.168.0.102	192.168.0.1	DNS	72	Standard query 0x4d44 A www.bing.com
144	10.308027	192.168.0.102	192.168.0.1	DNS	72	Standard query 0x988e HTTPS www.bing.com
146	10.308319	192.168.0.1	192.168.0.102	DNS	212	Standard query response 0x02e7 HTTPS r.msftstatic.com CNAME r.msftstatic.com.a-0016.a-msedge.net CNAME a-0016.a-msedge.net SOA ns1
150	10.309925	192.168.0.1	192.168.0.102	DNS	263	Standard query response 0x4d44 A www.bing.com CNAME www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e830
155	10.310525	192.168.0.1	192.168.0.102	DNS	277	Standard query response 0x988e HTTPS www.bing.com CNAME www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e
298	10.628687	192.168.0.102	192.168.0.1	DNS	70	Standard query 0x9319 A c.bing.com
299	10.628801	192.168.0.102	192.168.0.1	DNS	70	Standard query 0x27a3 HTTPS c.bing.com
300	10.638879	192.168.0.1	192.168.0.102	DNS	203	Standard query response 0x27a3 HTTPS c.bing.com CNAME c-bing-com.ax-0001.ax-msedge.net CNAME ax-0001.ax-msedge.net SOA ns1.ax-msed
301	10.631171	192.168.0.1	192.168.0.102	DNS	162	Standard query response 0x9319 A c.bing.com CNAME c-bing-com.ax-0001.ax-msedge.net CNAME ax-0001.ax-msedge.net A 150.171.27.10 A 1
402	11.311517	192.168.0.102	192.168.0.1	DNS	74	Standard query 0xd8e3 A www.google.com
403	11.313092	192.168.0.1	192.168.0.102	DNS	80	Standard query response 0xd8e3 A www.google.com A 142.250.70.36
404	11.316548	192.168.0.102	192.168.0.1	DNS	74	Standard query 0x10f4 A www.google.com
405	11.316765	192.168.0.102	192.168.0.1	DNS	74	Standard query 0x47f3 HTTPS www.google.com
406	11.316918	192.168.0.102	192.168.0.1	DNS	77	Standard query 0x2912 A fonts.gstatic.com
407	11.317011	192.168.0.102	192.168.0.1	DNS	77	Standard query 0xcae2 HTTPS fonts.gstatic.com
408	11.317211	192.168.0.102	192.168.0.1	DNS	75	Standard query 0x937e A www.gstatic.com
409	11.317344	192.168.0.102	192.168.0.1	DNS	75	Standard query 0x533a HTTPS www.gstatic.com
412	11.318889	192.168.0.1	192.168.0.102	DNS	90	Standard query response 0x10f4 A www.google.com A 142.250.70.36
413	11.319541	192.168.0.1	192.168.0.102	DNS	91	Standard query response 0x937e A www.gstatic.com A 142.250.77.131
414	11.319541	192.168.0.1	192.168.0.102	DNS	93	Standard query response 0x2912 A fonts.gstatic.com A 216.58.203.35
415	11.319541	192.168.0.1	192.168.0.102	DNS	93	Standard query response 0x47f3 HTTPS www.gstatic.com A 142.250.70.36

Frame 40: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
 Ethernet II, Src: Intel 71:16:4b (f4:c8:8a:71:16:4b), Dst: TPlink 79:b6:bb (b0:a7:b9:79:b6:bb)
 Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1
 User Datagram Protocol, Src Port: 59155, Dst Port: 53
 Domain Name System (query)

0000 b0 a7 b9 79 b6 bb f4 c8 8a 71 16 4b 08 00 45 00 ... y ... q K E
 0010 00 50 20 c0 00 00 80 11 00 00 c0 a8 00 66 c0 a8 ... P f
 0020 00 01 e7 13 00 35 00 3c 82 05 33 5b 01 00 00 01 5 < 3
 0030 00 00 00 00 00 00 00 70 32 70 20 62 ef 60 12 09 2p 2p 2p 2p
 0040 66 69 72 61 6f 7a 65 72 29 40 23 74 65 61 6d 73 Discover p 2p 2p
 0050 65 72 76 65 72 03 6e 65 74 80 00 01 00 01 reverse t

Domain Name System: Protocol Packets: 3489 - Displayed: 153 (4.4%) - Dropped: 0 (0.0%) Profile: Default

d. ARP (Address Resolution Protocol)

- Resolves IP addresses to MAC addresses in the local network.

- Captured ARP requests like “Who has 192.168.0.103? Tell 192.168.0.1”.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
2	0.000058	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
3	1.023993	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
4	1.024142	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
5	1.024457	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
10	2.047830	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
11	2.048013	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
30	2.969572	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
31	2.969635	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
32	2.969981	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
33	3.993705	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
46	5.017648	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
48	6.045922	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
49	6.045922	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
50	6.045946	Intel_71:16:4b	TPLink_79:b6:bb	ARP	42	192.168.0.102 is at f4:c8:8a:71:16:4b
57	6.963171	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
58	6.963201	Intel_71:16:4b	TPLink_79:b6:bb	ARP	42	192.168.0.102 is at f4:c8:8a:71:16:4b
59	6.963247	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
60	7.987208	TPLink_79:b6:bb	Broadcast	ARP	42	Who has 192.168.0.103? Tell 192.168.0.1
61	7.987234	Intel_71:16:4b	TPLink_79:b6:bb	ARP	42	192.168.0.102 is at f4:c8:8a:71:16:4b

Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)	0000	ff ff ff ff ff ff b0 a7 b9 79 b6 bb 08 06 00 01y.....
Ethernet II, Src: TPLink_79:b6:bb (b0:a7:b9:79:b6:bb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	0010	08 00 06 04 00 01 b0 a7 b9 79 b6 bb c0 a8 00 01y.....
Address Resolution Protocol (request)	0020	00 00 00 00 00 00 c0 a8 00 07g.....

7. Exporting the Capture

The capture file was saved as a .pcap file using:

- File > Save As
- File name: Captured_Packets.pcap

8. Summary of Findings

Protocol	Function	Example Packet Details
HTTP	Web traffic	GET request to www.google.com
TCP	Data transport	SYN, ACK, FIN packets
DNS	Name resolution	Query for www.google.com
ARP	MAC resolution	Request: Who has 192.168.1.1?

Conclusion

The task demonstrated successful capture and analysis of network traffic using Wireshark. Four protocols (HTTP, TCP, DNS, and ARP) were filtered and analyzed. The exported .pcap file contains detailed records of captured packets and supports further inspection.