

## EXPERIMENT-25

### NETWORK LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK – ARP AND HTTP

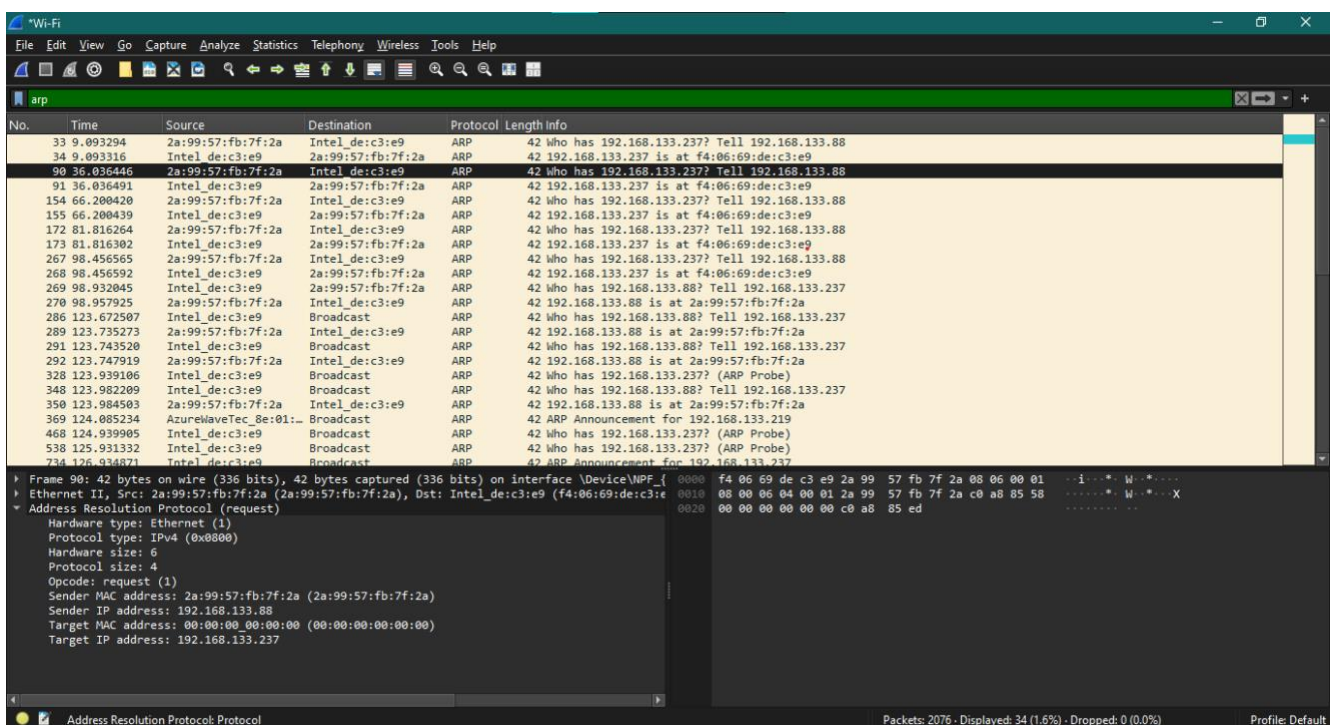
**AIM:** To analyze capturing of Transport layer protocol header analysis using Wire shark- ARP and HTTP.

#### SOFTWARE USED:

Wire shark network analyzer

#### PROCEDURE:

1. Open wire shark.
2. Click on list the available capture interface.
3. Choose the LAN interface.
4. Click on start button.
5. Active packets will be displayed.
6. Capture the packets & select any IP address from the source.
7. Click on the expression and select IPV4 ☐ IP addr source address in the field name.
8. Select the double equals (==) from the selection and enter the selected IP source address.
9. Click on apply button.
10. All the packets will be filtered using source address.



No.	Time	Source	Destination	Protocol	Length	Info
13	0.353035	192.168.133.237	210.148.85.30	HTTP	204	GET /api/check/online?t=1726303882 HTTP/1.1
16	0.529424	210.148.85.30	192.168.133.237	HTTP	356	HTTP/1.1 200 OK (image/jpeg)
74	30.528538	192.168.133.237	210.148.85.30	HTTP	204	GET /api/check/online?t=1726303912 HTTP/1.1
84	30.739020	192.168.133.237	210.148.85.30	HTTP	204	GET /api/check/online?t=1726303912 HTTP/1.1
86	31.011661	210.148.85.30	192.168.133.237	HTTP	352	HTTP/1.1 200 OK (image/jpeg)
99	37.042760	2409:40f4:3f:615a:3...	2606:2800:247:57cb:...	HTTP	328	GET /DigiCertGlobalRootG2.crl HTTP/1.1
101	37.075503	2606:2800:247:57cb:...	2409:40f4:3f:615a:3...	HTTP	358	HTTP/1.1 304 Not Modified
110	37.154193	2409:40f4:3f:615a:3...	2405:200:1630:181:...	HTTP	301	GET / HTTP/1.1
112	37.201587	2405:200:1630:181:...	2409:40f4:3f:615a:3...	HTTP	337	HTTP/1.1 304 Not Modified
121	37.320425	2409:40f4:3f:615a:3...	2404:6800:4007:81f:...	HTTP	276	GET /r/gsr1.crl HTTP/1.1
122	37.354487	2404:6800:4007:81f:...	2409:40f4:3f:615a:3...	HTTP	296	HTTP/1.1 304 Not Modified
123	37.367690	2409:40f4:3f:615a:3...	2404:6800:4007:81f:...	HTTP	274	GET /r/r4.crl HTTP/1.1
126	37.416038	2404:6800:4007:81f:...	2409:40f4:3f:615a:3...	HTTP	296	HTTP/1.1 304 Not Modified
149	61.185148	192.168.133.237	210.148.85.30	HTTP	204	GET /api/check/online?t=1726303943 HTTP/1.1
151	61.345293	210.148.85.30	192.168.133.237	HTTP	356	HTTP/1.1 200 OK (image/jpeg)
220	91.341552	192.168.133.237	210.148.85.30	HTTP	204	GET /api/check/online?t=1726303973 HTTP/1.1
230	91.937053	192.168.133.237	210.148.85.30	HTTP	204	GET /api/check/online?t=1726303973 HTTP/1.1
234	92.117726	210.148.85.30	192.168.133.237	HTTP	364	HTTP/1.1 200 OK (image/jpeg)
352	124.004583	192.168.133.237	91.108.56.200	HTTP	290	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
372	124.086193	192.168.133.237	91.108.23.100	HTTP	190	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
392	124.282705	192.168.133.237	91.108.23.100	HTTP	94	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
397	124.303011	192.168.133.237	91.108.23.100	HTTP	346	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
416	124.491923	2409:40f4:3f:615a:3...	64:ff9b::312c:74e7	HTTP	185	GET /connecttest.txt HTTP/1.1

Frame 86: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits) on interface \Device...	0000	f4 06 69 de c3 e9 2a 99 57 fb 7f 2a 08 00 45 00	...
Ethernet II, Src: 2a:99:57:fb:7f:2a (2a:99:57:fb:7f:2a), Dst: Intel_de:c3:e9 (f4:06:69:de:c3...	0010	01 52 00 00 40 00 26 06 e5 5d d2 94 55 1e c0 a8	...
Internet Protocol Version 4, Src: 210.148.85.30, Dst: 192.168.133.237	0020	85 ed 00 50 f5 0b f3 9e ce 99 17 f5 ef d6 50 18	...
Transmission Control Protocol, Src Port: 80, Dst Port: 62731, Seq: 1, Ack: 151, Len: 298	0030	03 b4 a4 05 00 00 48 54 54 50 2f 31 2e 31 20 32	...
Hypertext Transfer Protocol	0040	30 30 20 4f 4b 0d 0a 43 6f 6e 65 63 74 69 6f	...
HTTP/1.1 200 OK\r\n	0050	6e 3a 20 6b 65 65 70 2d 61 6e 69 76 65 0d 0a 43	...
Connection: keep-alive\r\n	0060	6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 69 6d 61	...
Content-Type: image/jpeg\r\n	0070	67 65 2f 6a 70 65 67 0d 0a 4a 61 74 65 3a 20 53	...
Date: Sat, 14 Sep 2024 08:51:53 GMT\r\n	0080	61 74 2c 20 31 3a 20 53 65 70 20 32 30 32 34 20	...
Flow-Level: 3\r\n	0090	30 38 3a 35 31 3a 35 33 20 47 4d 54 0d 0a 46 6c	...
Http-X-Isis-Logid: 212245776715368825\r\n	00a0	6f 77 2d 4c 65 76 65 6c 3a 20 33 0d 0a 48 74 74	...
Logid: 212245776715368825\r\n	00b0	70 2d 58 2d 49 73 69 73 2d 4c 6f 67 69 64 3a 20	...
Server: nginx\r\n	00c0	32 31 32 32 34 35 37 37 36 37 31 35 33 36 38 38	...
Yld: 212245776715368825\r\n	00d0	32 35 0d 0a 4c 6f 67 69 64 3a 20 32 31 32 32 34	...
Yme: ZIGW+S3QEstDtcDUmr/tG1HvuU25xz3owpNwyGAjq2I\r\n	00e0	35 37 37 36 37 31 35 33 36 38 38 32 35 0d 0a 53	...
	00f0	65 72 76 65 72 3a 20 6e 67 69 6e 78 0d 0a 59 6c	...

**Result:** Hence, the capturing of packets using wire shark network analyzer was analyzed for ARP and HTTP.