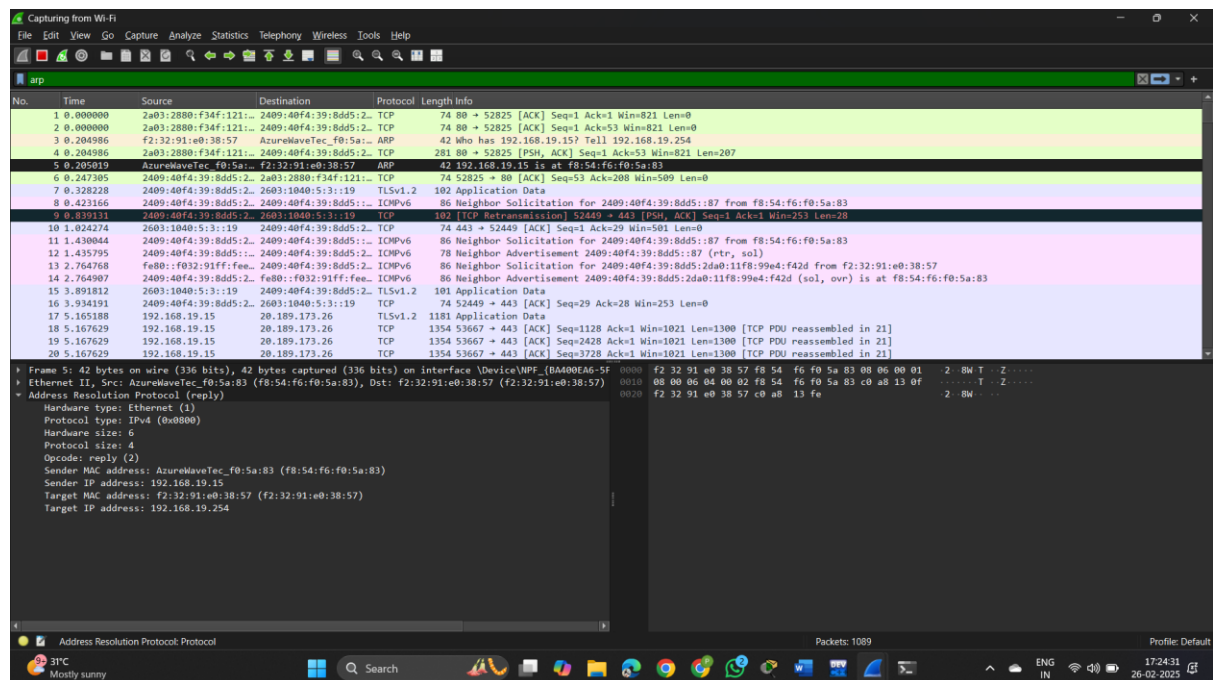


## 25. Network layer protocol header analysis using Wire shark – ARP and HTTP.

### ARP



The image shows a Wireshark capture of ARP traffic. The packet list on the left shows several packets, with packet 5 selected. The packet details pane on the right shows the structure of the ARP request (Opcode: request (2)). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates the capture is on the 'arp' interface.

No.	Time	Source	Destination	Protocol	Length	Info
0	0.000000	2a03:2880:f34f:121::	2409:40f4:39:8d45::2	TCP	74	80 → 52825 [ACK] Seq=1 Ack=1 Win=821 Len=0
0	0.000000	2a03:2880:f34f:121::	2409:40f4:39:8d45::2	TCP	74	80 → 52825 [ACK] Seq=1 Ack=53 Win=821 Len=0
0	0.204986	f2:32:91:e0:38:57	AzureWaveTec_f0:5a:83	ARP	42	Who has 192.168.19.15? Tell 192.168.19.254
4	0.204986	2a03:2880:f34f:121::	2409:40f4:39:8d45::2	TCP	281	80 → 52825 [PSH, ACK] Seq=1 Ack=53 Win=821 Len=207
5	0.205019	AzureWaveTec_f0:5a:83	f2:32:91:e0:38:57	ARP	42	192.168.19.15 is at f8:54:f6:f0:5a:83
6	0.247305	2409:40f4:39:8d45::2	2a03:2880:f34f:121::	TCP	74	52825 → 80 [ACK] Seq=53 Ack=208 Win=509 Len=0
7	0.328228	2409:40f4:39:8d45::2	2603:1040:5:3:19	TLSv1.2	102	Application Data
8	0.423166	2409:40f4:39:8d45::2	2409:40f4:39:8d45::2	ICMPv6	86	Neighbor Solicitation for 2409:40f4:39:8d45::87 from f8:54:f6:f0:5a:83
9	0.839131	2409:40f4:39:8d45::2	2603:1040:5:3:19	TCP	102	[TCP Retransmission] 52449 → 443 [PSH, ACK] Seq=1 Ack=1 Win=253 Len=20
10	1.024274	2603:1040:5:3:19	2409:40f4:39:8d45::2	TCP	74	443 → 52449 [ACK] Seq=1 Ack=29 Win=501 Len=0
11	1.430044	2409:40f4:39:8d45::2	2409:40f4:39:8d45::2	ICMPv6	86	Neighbor Solicitation for 2409:40f4:39:8d45::87 from f8:54:f6:f0:5a:83
12	1.435795	2409:40f4:39:8d45::2	2409:40f4:39:8d45::2	ICMPv6	78	Neighbor Advertisement 2409:40f4:39:8d45::87 (rtr, sol)
13	2.764768	fe80::f032:91ff:fee::	2409:40f4:39:8d45::2	ICMPv6	86	Neighbor Solicitation for 2409:40f4:39:8d45::2da0:11f8:99e4:f42d from f2:32:91:e0:38:57
14	2.764907	2409:40f4:39:8d45::2	fe80::f032:91ff:fee::	ICMPv6	86	Neighbor Advertisement 2409:40f4:39:8d45::2da0:11f8:99e4:f42d (sol, ovr) is at f8:54:f6:f0:5a:83
15	3.891812	2603:1040:5:3:19	2409:40f4:39:8d45::2	TLSv1.2	101	Application Data
16	3.934191	192.168.19.15	20.189.173.26	TCP	74	52449 → 443 [ACK] Seq=29 Ack=28 Win=253 Len=0
17	5.165188	192.168.19.15	20.189.173.26	TLSv1.2	1181	Application Data
18	5.167629	192.168.19.15	20.189.173.26	TCP	1354	53667 → 443 [ACK] Seq=1128 Ack=1 Win=1021 Len=1300 [TCP PDU reassembled in 21]
19	5.167629	192.168.19.15	20.189.173.26	TCP	1354	53667 → 443 [ACK] Seq=2428 Ack=1 Win=1021 Len=1300 [TCP PDU reassembled in 21]
20	5.167629	192.168.19.15	20.189.173.26	TCP	1354	53667 → 443 [ACK] Seq=3728 Ack=1 Win=1021 Len=1300 [TCP PDU reassembled in 21]

Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF\_{BA400EAG-5F-0000-0000-0000-0000-0000-0000-0000-0000-0000-0000-0000-0000-0000-0000-0000} (f8:54:f6:f0:5a:83), Dst: f2:32:91:e0:38:57 (f2:32:91:e0:38:57)

Ethernet II, Src: AzureWaveTec\_f0:5a:83 (f8:54:f6:f0:5a:83), Dst: f2:32:91:e0:38:57 (f2:32:91:e0:38:57)

Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

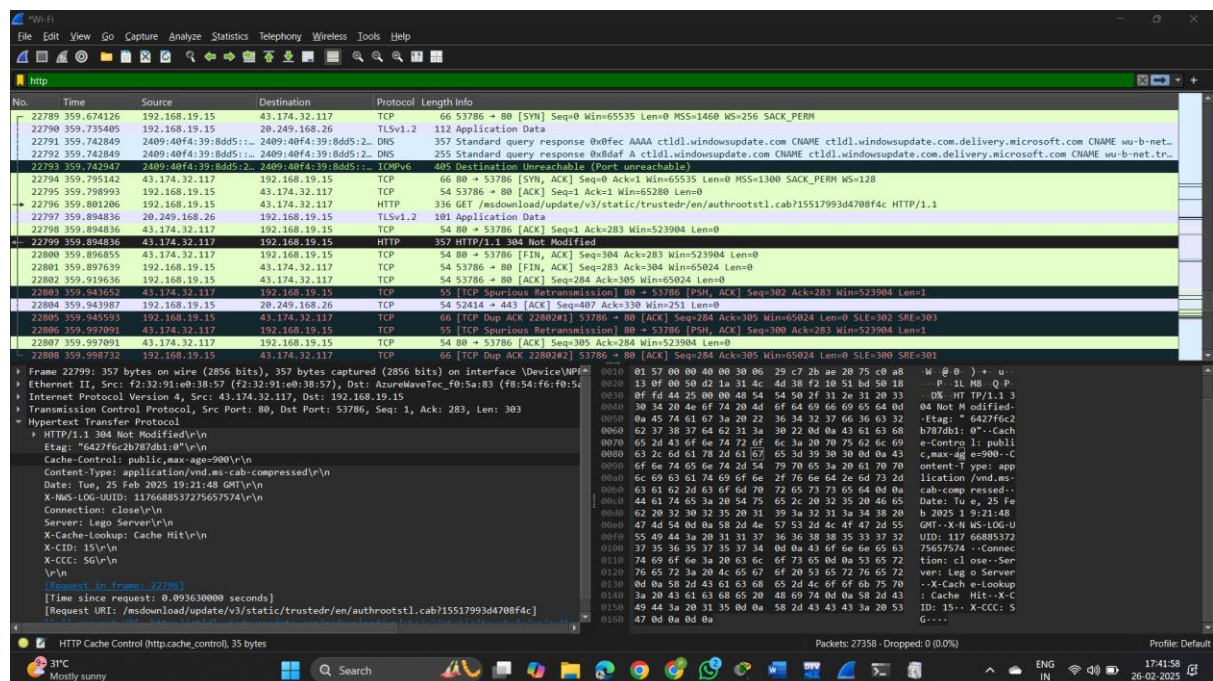
Sender MAC address: AzureWaveTec\_f0:5a:83 (f8:54:f6:f0:5a:83)

Sender IP address: 192.168.19.15

Target MAC address: f2:32:91:e0:38:57 (f2:32:91:e0:38:57)

Target IP address: 192.168.19.254

### HTTP



The image shows a Wireshark capture of HTTP traffic. The packet list on the left shows several packets, with packet 22799 selected. The packet details pane on the right shows the structure of the HTTP GET request. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates the capture is on the 'http' interface.

No.	Time	Source	Destination	Protocol	Length	Info
22789	359.674126	192.168.19.15	43.174.32.117	TCP	66	53786 → 80 [SYN] Seq=0 Min=65535 Len=0 MSS=1460 WS=256 SACK_PERM
22790	359.735405	192.168.19.15	20.249.168.26	TLSv1.2	112	Application Data
22791	359.742849	2409:40f4:39:8d45::2	2409:40f4:39:8d45::2	DNS	357	Standard query response 0x0fec AAAA ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com.delivery.microsoft.com CNAME wu-b-net-
22792	359.742849	2409:40f4:39:8d45::2	2409:40f4:39:8d45::2	DNS	355	Standard query response 0x8daf A ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com.delivery.microsoft.com CNAME wu-b-net-tr-
22793	359.742947	2409:40f4:39:8d45::2	2409:40f4:39:8d45::2	ICMPv6	405	Destination Unreachable (Port unreachable)
22794	359.795142	43.174.32.117	192.168.19.15	TCP	66	80 → 53786 [SYN, ACK] Seq=0 Ack=1 Min=65535 Len=0 MSS=1300 SACK_PERM WS=128
22795	359.798993	192.168.19.15	43.174.32.117	TCP	54	53786 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
22796	359.801206	192.168.19.15	43.174.32.117	HTTP	336	GET /msdownload/update/v3/static/trusted/en/autorootstl cab?15517993d4708f4c HTTP/1.1
22797	359.894836	20.249.168.26	192.168.19.15	TLSv1.2	101	Application Data
22798	359.894836	43.174.32.117	192.168.19.15	TCP	54	80 → 53786 [ACK] Seq=1 Ack=283 Win=523904 Len=0
22799	359.894836	43.174.32.117	192.168.19.15	HTTP	357	HTTP/1.1 304 Not Modified
22800	359.896955	43.174.32.117	192.168.19.15	TCP	54	80 → 53786 [FIN, ACK] Seq=304 Ack=283 Win=523904 Len=0
22801	359.897639	192.168.19.15	43.174.32.117	TCP	54	53786 → 80 [FIN, ACK] Seq=283 Ack=304 Win=55024 Len=0
22802	359.919636	192.168.19.15	43.174.32.117	TCP	54	53786 → 80 [ACK] Seq=284 Ack=305 Win=55024 Len=0
22803	359.943652	43.174.32.117	192.168.19.15	TCP	55	[TCP Spurious Retransmission] 80 → 53786 [PSH, ACK] Seq=302 Ack=283 Win=523904 Len=1
22804	359.943987	192.168.19.15	20.249.168.26	TCP	54	52414 → 443 [ACK] Seq=407 Ack=330 Win=251 Len=0
22805	359.945559	192.168.19.15	43.174.32.117	TCP	68	[TCP Dup ACK 22802] 53786 → 80 [ACK] Seq=284 Ack=305 Win=55024 Len=0 SLE=302 SRE=303
22806	359.997091	43.174.32.117	192.168.19.15	TCP	55	[TCP Spurious Retransmission] 80 → 53786 [PSH, ACK] Seq=300 Ack=283 Win=523904 Len=1
22807	359.997091	43.174.32.117	192.168.19.15	TCP	54	80 → 53786 [ACK] Seq=305 Ack=284 Win=523904 Len=0
22808	359.998732	192.168.19.15	43.174.32.117	TCP	66	[TCP Dup ACK 22802] 53786 → 80 [ACK] Seq=284 Ack=305 Win=55024 Len=0 SLE=300 SRE=301

Frame 22799: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface \Device\NPF\_{BA400EAG-5F-0000-0000-0000-0000-0000-0000-0000-0000-0000-0000-0000-0000-0000-0000-0000} (f8:54:f6:f0:5a:83)

Ethernet II, Src: f2:32:91:e0:38:57 (f2:32:91:e0:38:57), Dst: AzureWaveTec\_f0:5a:83 (f8:54:f6:f0:5a:83)

Internet Protocol Version 4, Src: 43.174.32.117, Dst: 192.168.19.15

Transmission Control Protocol, Src Port: 80, Dst Port: 53786, Seq: 1, Ack: 283, Len: 303

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

Etag: "6427f6c2b7801d04v3"\r\n

Cache-Control: public,max-age=900\r\n

Content-Type: application/vnd.ms-cab-compressed\r\n

Date: Tue, 25 Feb 2025 19:21:48 GMT\r\n

X-MS-LOG-UUID: 1176688537275657574\r\n

Connection: close\r\n

Server: Lego Server\r\n

X-Cache-Lookup: Cache Hit\r\n

X-CID: 15\r\n

X-CCC: 56\r\n

\r\n

[Request in frame: 22796]

[Time since request: 0.093630000 seconds]

[Request URI: /msdownload/update/v3/static/trusted/en/autorootstl cab?15517993d4708f4c]