

Assignment -2

1. To capture and analyze ICMP packets (Ping request and reply)

The screenshot shows a Wireshark packet capture on the interface 'Device'. The packet list on the left shows several ICMP Echo (ping) requests and replies. The selected packet is packet 14, an ICMP Echo (ping) reply from 172.16.84.212 to 103.3.33.16. The packet details pane shows the ICMP Echo (ping) reply structure, including the type (0), code (0), and checksum (0x0000). The packet bytes pane shows the raw data of the ICMP Echo (ping) reply, including the type (0), code (0), checksum (0x0000), and the 32-bit identifier (0x00000000).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::12fa:ed5e:b74a::ff02::fb	ff02::fb	IPv6	1510	IPv6 Fragment (off=12720 more=0 more=0x000024c nst=17)
2	0.000509	fe80::12fa:ed5e:b74a::ff02::fb	ff02::fb	IPv6	1510	IPv6 Fragment (off=18824 more=0 more=0x000024c nst=17)
3	0.000589	fe80::12fa:ed5e:b74a::ff02::fb	ff02::fb	IPv6	241	IPv6 Fragment (off=20272 more=0 more=0x000024c nst=17)
4	0.000661	172.16.82.163	224.0.0.251	MDNS	110	Standard query 0x0000 TXT Kashyap's MacBook Air_companion-link_tcp.local, "QU" question
5	0.000661	fe80::1c7d:2740:391::ff02::fb	ff02::fb	MDNS	130	Standard query 0x0000 TXT Kashyap's MacBook Air_companion-link_tcp.local, "QU" question
6	0.002903	172.16.77.216	224.0.0.251	MDNS	112	Standard query 0x0000 TXT Samar's MacBook Air (2)_companion-link_tcp.local, "QU" question
7	0.002903	fe80::10a:595d:1fa::ff02::fb	ff02::fb	MDNS	132	Standard query 0x0000 TXT Samar's MacBook Air (2)_companion-link_tcp.local, "QU" question
8	0.002903	172.16.74.117	224.0.0.251	MDNS	112	Standard query 0x0000 TXT Agampreet's MacBook Air_companion-link_tcp.local, "QU" question
9	0.002903	fe80::1cfc:9225:7cfa::ff02::fb	ff02::fb	MDNS	132	Standard query 0x0000 TXT Agampreet's MacBook Air_companion-link_tcp.local, "QU" question
10	0.002903	172.16.94.214	224.0.0.251	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=33d5)
11	0.002903	172.16.94.39	224.0.0.251	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8f21)
12	0.006830	fe80::68f2:829f:69e::ff02::fb	ff02::fb	IPv6	1510	IPv6 Fragment (off=0 more=0 more=0x0003f9f8 nst=17)
13	0.006830	fe80::68f2:829f:69e::ff02::fb	ff02::fb	IPv6	1510	IPv6 Fragment (off=1448 more=0 more=0x0003f9f8 nst=17)
14	0.006830	fe80::b3be:31a9:aba::ff02::16	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
15	0.006830	fe80::b3be:31a9:aba::ff02::16	ff02::16	IPv6	1510	IPv6 Fragment (off=2896 more=0 more=0x0003f9f8 nst=17)
16	0.006830	fe80::b3be:31a9:aba::ff02::16	ff02::16	IPv6	1510	IPv6 Fragment (off=1244 more=0 more=0x0003f9f8 nst=17)
17	0.006830	fe80::b3be:31a9:aba::ff02::16	ff02::16	IPv6	1510	IPv6 Fragment (off=5792 more=0 more=0x0003f9f8 nst=17)

> Frame 14: Packet, 1510 bytes on wire (12080 bits), 1510 bytes captured (12080 bits) on interface 'Device'
> Ethernet II, Src: EliteGroupCo, 28:41:a3 (88:ae:dd:28:41:a3), Dst: IPv6multicast_fb (33:33:00:00:00:fb)
> Internet Protocol Version 6, Src: fe80::12fa:ed5e:b74a::ff02::fb, Dst: ff02::fb
> Data (1448 bytes)

2. To analyze TCP packets and observe the TCP three-way handshake

The screenshot shows a Wireshark packet capture on the interface 'Device'. The packet list on the left shows several TCP packets. The selected packet is packet 2603, a TCP Reset (RST) from 172.16.84.212 to 103.3.33.16. The packet details pane shows the TCP Reset (RST) structure, including the type (6), code (0), and checksum (0x0000). The packet bytes pane shows the raw data of the TCP Reset (RST), including the type (6), code (0), checksum (0x0000), and the 32-bit identifier (0x00000000).

No.	Time	Source	Destination	Protocol	Length	Info
2603	2.531677	172.16.84.212	103.3.33.16	TCP	66	56859 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2625	2.531943	103.3.33.16	172.16.84.212	TCP	66	443 → 56859 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460 SACK_PERM WS=256
2626	2.534122	172.16.84.212	103.3.33.16	TCP	54	56859 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2627	2.545466	172.16.84.212	103.3.33.16	TLSv1.3	837	Client Hello (SNI=assets.msn.com)
2628	2.549512	103.3.33.16	172.16.84.212	TCP	60	443 → 56859 [ACK] Seq=1 Ack=784 Win=16384 Len=0
2765	2.586160	103.3.33.16	172.16.84.212	TLSv1.3	318	Server Hello, Change Cipher Spec, Application Data
2766	2.590713	172.16.84.212	103.3.33.16	TCP	54	56859 → 443 [ACK] Seq=784 Ack=265 Win=261632 Len=0
2767	2.625679	172.16.84.212	103.3.33.16	TLSv1.3	134	Change Cipher Spec, Application Data
2768	2.626729	172.16.84.212	103.3.33.16	TLSv1.3	134	Application Data
2769	2.630593	103.3.33.16	172.16.84.212	TCP	60	443 → 56859 [ACK] Seq=265 Ack=944 Win=16384 Len=0
2770	2.644248	172.16.84.212	103.3.33.16	TLSv1.3	1496	Application Data
2771	2.650828	103.3.33.16	172.16.84.212	TLSv1.3	365	Application Data
2772	2.650828	103.3.33.16	172.16.84.212	TLSv1.3	115	Application Data
2773	2.651058	172.16.84.212	103.3.33.16	TCP	54	56859 → 443 [ACK] Seq=2386 Ack=637 Win=261376 Len=0
2774	2.651158	103.3.33.16	172.16.84.212	TLSv1.3	85	Application Data
2775	2.651218	172.16.84.212	103.3.33.16	TCP	54	56859 → 443 [ACK] Seq=2386 Ack=668 Win=261376 Len=0
2776	2.653356	172.16.84.212	103.3.33.16	TLSv1.3	85	Application Data

> Frame 2603: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 'Device'
> Ethernet II, Src: AzureWaveTec, ef:54:71 (80:d2:1d:ef:54:71), Dst: Broadcast, 90:00:00:00:00:00 (74:0e:fb:90:00:00)
> Internet Protocol Version 4, Src: 172.16.84.212, Dst: 103.3.33.16
> Transmission Control Protocol, Src Port: 56859, Dst Port: 443, Seq: 0, Len: 0

3. To capture and analyze UDP packets

The screenshot shows a Wireshark capture of UDP traffic. The packet list on the left shows several DNS queries and responses. The selected packet (No. 123) is a standard query from PTR Aryaman's MacBook Air to PTR Rohit's MacBook Air. The packet details pane shows the Ethernet II, Internet Protocol Version 6, User Datagram Protocol, and Multicast Domain Name System (query) layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
229713	225.494555	fe80::5d77:4bf2:627... ff02::fb	ff02::fb	MDNS	123	Standard query 0xcfe PTR Aryaman's MacBook Air._airplay._tcp.local, "QM" question
229714	225.494555	fe80::5d77:4bf2:627... ff02::fb	ff02::fb	MDNS	123	Standard query 0x304d PTR Aryaman's MacBook Air._airplay._tcp.local, "QM" question
229715	225.494555	fe80::5d77:4bf2:627... ff02::fb	ff02::fb	MDNS	121	Standard query 0x8907 PTR Rohit's MacBook Air._airplay._tcp.local, "QM" question
229716	225.494555	172.16.89.0	224.0.0.251	MDNS	100	Standard query 0x0000 TXT Rhea's MacBook Air._airplay._tcp.local, "QM" question
229717	225.494555	fe80::1cd8:20ac:15e... ff02::fb	ff02::fb	MDNS	120	Standard query 0x0000 TXT Rhea's MacBook Air._airplay._tcp.local, "QM" question
229718	225.494555	172.16.82.161	224.0.0.251	MDNS	109	Standard query 0x0000 TXT Ishani's MacBook Air._companion-link._tcp.local, "QM" question
229719	225.494555	fe80::1044:51d8:383... ff02::fb	ff02::fb	MDNS	120	Standard query 0x0000 TXT Ishani's MacBook Air._companion-link._tcp.local, "QM" question
229720	225.494555	172.16.74.73	224.0.0.251	MDNS	111	Standard query response 0x0000 NSEC, cache flush iPad (12)._companion-link._tcp.local
229721	225.494555	172.16.70.56	224.0.0.251	MDNS	137	Standard query 0x0000 TXT anshh's MacBook Air._companion-link._tcp.local, "QM" question TXT Ishani's MacBook Air._companion-link
229722	225.494555	fe80::5:51de:1322:8... ff02::fb	ff02::fb	MDNS	157	Standard query 0x0000 TXT anshh's MacBook Air._companion-link._tcp.local, "QM" question TXT Ishani's MacBook Air._companion-link
229723	225.494555	fe80::6:f18c:a248:1... ff02::fb	ff02::fb	MDNS	131	Standard query response 0x0000 NSEC, cache flush iPad (12)._companion-link._tcp.local
229726	225.494555	172.16.76.48	224.0.0.251	MDNS	109	Standard query 0x0000 TXT Ishani's MacBook Air._companion-link._tcp.local, "QM" question
229728	225.494555	fe80::f7:351b:ebc5... ff02::fb	ff02::fb	MDNS	129	Standard query 0x0000 TXT Ishani's MacBook Air._companion-link._tcp.local, "QM" question
229731	225.494555	172.16.81.88	224.0.0.251	MDNS	109	Standard query 0x0000 TXT Ishani's MacBook Air._companion-link._tcp.local, "QM" question
229732	225.494555	fe80::68:b080:fa44... ff02::fb	ff02::fb	MDNS	129	Standard query 0x0000 TXT Ishani's MacBook Air._companion-link._tcp.local, "QM" question
229733	225.494555	fe80::2f1b:23eb:a4c... ff02::fb	ff02::fb	MDNS	133	Standard query 0x00a5 PTR 4d04e6967ef38boushka's MacBook Pro._raop._tcp.local, "QM" question
229735	225.494555	172.16.73.67	224.0.0.251	MDNS	1472	Standard query 0x0000 PTR airplay._tcp.local, "QM" question PTR Pearl's MacBook Air (2)._airplay._tcp.local PTR Aaditya's MacBo

Frame 230854: Packet, 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface \Device\NPF... Ethernet II, Src: 7e:b1:2b:17:a2:93 (7e:b1:2b:17:a2:93), Dst: IPv6multicast_fb (33:33:00:00:00:00:00:00)

Internet Protocol Version 6, Src: fe80::142e:feb7:8c64:a8a7, Dst: ff02::fb

User Datagram Protocol, Src Port: 5353, Dst Port: 5353

Multicast Domain Name System (query)

4. To capture and analyze DNS query and response packets

The screenshot shows a Wireshark capture of DNS traffic. The packet list on the left shows several DNS queries and responses. The selected packet (No. 4270) is a standard query from 172.16.84.212 to 172.31.1.6. The packet details pane shows the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query) layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
4270	3.840157	172.16.84.212	172.31.1.6	DNS	75	Standard query 0x1672 A windows.msn.com
4289	3.861831	172.31.1.6	172.16.84.212	DNS	245	Standard query response 0x1672 A windows.msn.com CNAME win-msn-com-world-atm-default.trafficmanager.net CNAME windows.msn-com-io
5135	4.577150	172.16.84.212	172.31.1.6	DNS	79	Standard query 0x2240 HTTPS deff.nelreports.net
5160	4.587580	172.31.1.6	172.31.1.6	DNS	79	Standard query 0x2ee1 A deff.nelreports.net
5161	4.599973	172.31.1.6	172.16.84.212	DNS	219	Standard query response 0x2240 HTTPS deff.nelreports.net CNAME deff.nelreports.net.akamaized.net CNAME a1858.dscd.akamai.net SGA
5162	4.599973	172.31.1.6	172.16.84.212	DNS	187	Standard query response 0x2ee1 A deff.nelreports.net CNAME deff.nelreports.net.akamaized.net CNAME a1858.dscd.akamai.net A 103.3
5563	5.021398	172.16.84.212	172.31.1.6	DNS	71	Standard query 0x8140 HTTPS www.msn.com
5578	5.030249	172.16.84.212	172.31.1.6	DNS	71	Standard query 0xcdb9 A www.msn.com
5672	5.076969	172.31.1.6	172.16.84.212	DNS	215	Standard query response 0xcdb9 A www.msn.com CNAME www-msn-com-world-atm-default.trafficmanager.net CNAME www.msn.com.edgekey.net
5673	5.076969	172.31.1.6	172.16.84.212	DNS	257	Standard query response 0x8140 HTTPS www.msn.com CNAME www-msn-com-world-atm-default.trafficmanager.net CNAME www.msn.com.edgekey
8834	7.691663	172.16.84.212	172.31.1.6	DNS	71	Standard query 0xb205 HTTPS th.bing.com
8867	7.701099	172.16.84.212	172.31.1.6	DNS	71	Standard query 0xae1b A th.bing.com
8935	7.740296	172.31.1.6	172.16.84.212	DNS	249	Standard query response 0xb205 HTTPS th.bing.com CNAME p-th.bing.com.trafficmanager.net CNAME th.bing.com.edgekey.net CNAME e863d
8936	7.740296	172.31.1.6	172.16.84.212	DNS	332	Standard query response 0xae1b A th.bing.com CNAME p-th.bing.com.trafficmanager.net CNAME th.bing.com.edgekey.net CNAME e863d
9211	8.007786	172.16.84.212	172.31.1.6	DNS	74	Standard query 0x978e HTTPS assets.msn.com
9244	8.015423	172.16.84.212	172.31.1.6	DNS	74	Standard query 0x574d A assets.msn.com
9293	8.064049	172.31.1.6	172.16.84.212	DNS	246	Standard query response 0x574d A assets.msn.com CNAME assets-msn-com-world-atm-default.trafficmanager.net CNAME assets.msn-com-i

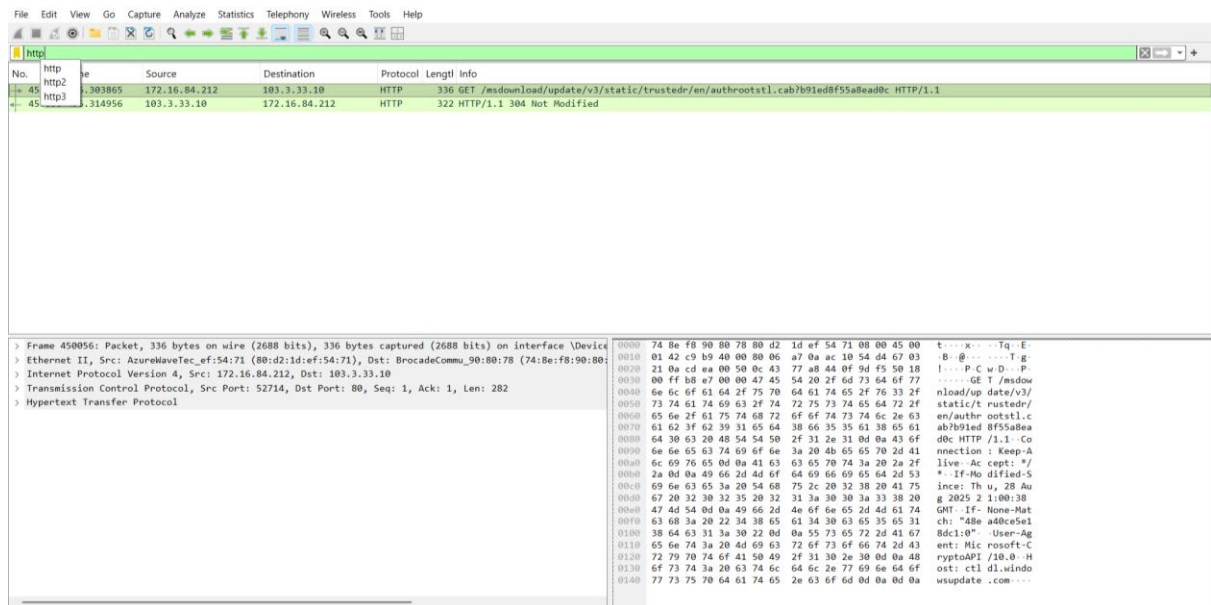
Frame 4270: Packet, 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF... Ethernet II, Src: AzureWaveTec_ef:54:71 (80:d2:1def:54:71), Dst: BrocadeCommu_90:80:78 (74:8e:f8:90:80:78)

Internet Protocol Version 4, Src: 172.16.84.212, Dst: 172.31.1.6

User Datagram Protocol, Src Port: 49521, Dst Port: 53

Domain Name System (query)

5. To capture and analyze HTTP packets



The image shows a Wireshark capture of HTTP packets. The packet list on the left shows three packets: a GET request (No. 45), a 200 OK response (No. 46), and a 304 Not Modified response (No. 47). The selected packet (No. 45) is expanded, showing the details of the HTTP GET request. The packet structure is as follows:

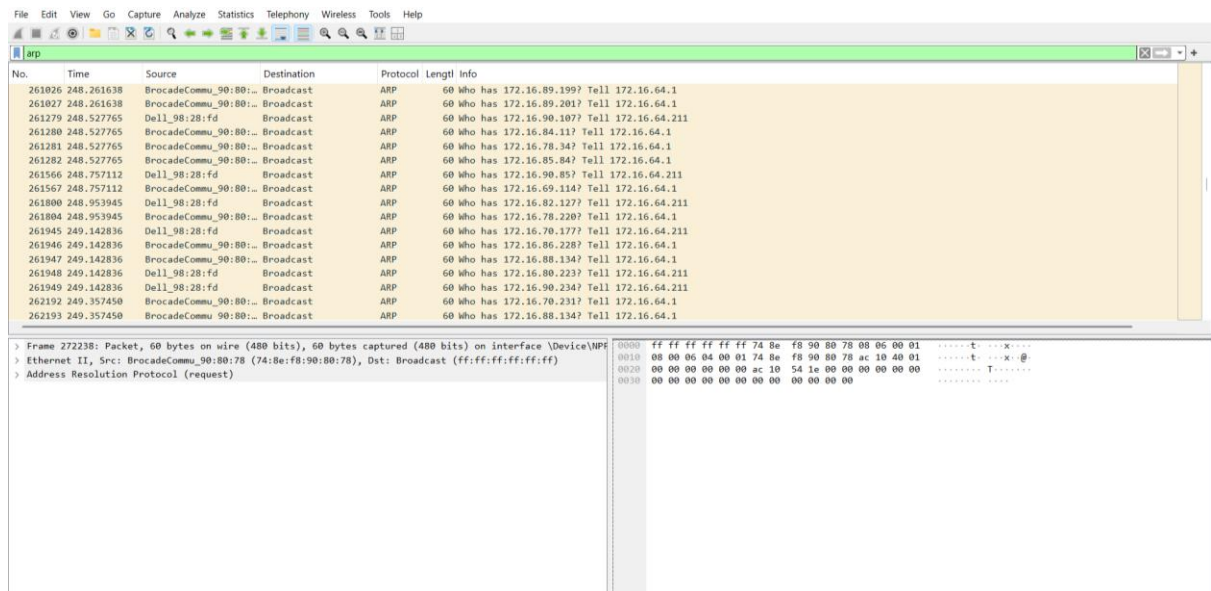
No.	Time	Source	Destination	Protocol	Length	Info
45	0.30865	172.16.84.212	103.3.33.10	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/authrootst1.cab?b01ed8f55a8ead0c HTTP/1.1
46	0.314956	103.3.33.10	172.16.84.212	HTTP	322	HTTP/1.1 200 Not Modified

The packet details for the selected packet (No. 45) are:

- Frame 450056: Packet, 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits) on interface \Device\NPF...
- Ethernet II, Src: AzureWaveTec_ef:54:71 (80:d2:1def:54:71), Dst: BrocadeCommu_90:80:78 (74:8e:f8:90:80:78)
- Internet Protocol Version 4, Src: 172.16.84.212, Dst: 103.3.33.10
- Transmission Control Protocol, Src Port: 52714, Dst Port: 80, Seq: 1, Ack: 1, Len: 282
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the HTTP GET request, including the status bar, method, URI, and headers.

6. To analyze ARP request and reply packets



The image shows a Wireshark capture of ARP packets. The packet list on the left shows a series of ARP requests and replies. The selected packet (No. 261026) is expanded, showing the details of the ARP request. The packet structure is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
261026	248.261638	BrocadeCommu_90:80:78	Broadcast	ARP	60	Who has 172.16.89.199? Tell 172.16.64.1
261027	248.261638	BrocadeCommu_90:80:78	Broadcast	ARP	60	Who has 172.16.89.201? Tell 172.16.64.1
261279	248.527765	Dell_98:28:fd	Broadcast	ARP	60	Who has 172.16.90.107? Tell 172.16.64.211
261280	248.527765	BrocadeCommu_90:80:78	Broadcast	ARP	60	Who has 172.16.84.11? Tell 172.16.64.1
261281	248.527765	BrocadeCommu_90:80:78	Broadcast	ARP	60	Who has 172.16.78.34? Tell 172.16.64.1
261282	248.527765	BrocadeCommu_90:80:78	Broadcast	ARP	60	Who has 172.16.85.84? Tell 172.16.64.1
261566	248.757112	Dell_98:28:fd	Broadcast	ARP	60	Who has 172.16.90.85? Tell 172.16.64.211
261567	248.757112	BrocadeCommu_90:80:78	Broadcast	ARP	60	Who has 172.16.69.114? Tell 172.16.64.1
261800	248.953945	Dell_98:28:fd	Broadcast	ARP	60	Who has 172.16.82.127? Tell 172.16.64.211
261804	248.953945	BrocadeCommu_90:80:78	Broadcast	ARP	60	Who has 172.16.78.220? Tell 172.16.64.1
261945	249.142836	Dell_98:28:fd	Broadcast	ARP	60	Who has 172.16.70.177? Tell 172.16.64.211
261946	249.142836	BrocadeCommu_90:80:78	Broadcast	ARP	60	Who has 172.16.86.228? Tell 172.16.64.1
261947	249.142836	BrocadeCommu_90:80:78	Broadcast	ARP	60	Who has 172.16.88.134? Tell 172.16.64.1
261948	249.142836	Dell_98:28:fd	Broadcast	ARP	60	Who has 172.16.80.223? Tell 172.16.64.211
261949	249.142836	Dell_98:28:fd	Broadcast	ARP	60	Who has 172.16.90.234? Tell 172.16.64.211
262192	249.357450	BrocadeCommu_90:80:78	Broadcast	ARP	60	Who has 172.16.70.231? Tell 172.16.64.1
262193	249.357450	BrocadeCommu_90:80:78	Broadcast	ARP	60	Who has 172.16.88.134? Tell 172.16.64.1

The packet details for the selected packet (No. 261026) are:

- Frame 272238: Packet, 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF...
- Ethernet II, Src: BrocadeCommu_90:80:78 (74:8e:f8:90:80:78), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (request)

The packet bytes pane shows the raw data of the ARP request, including the Ethernet II header and the ARP payload.

7. To identify source and destination MAC and IP addresses in captured packets

The image displays the Wireshark network traffic analysis interface. The top pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows the detailed view of a selected packet (No. 272238), including the Ethernet II header, Internet Protocol Version 4 header, and the payload data.

No.	Time	Source	Destination	Protocol	Length	Info
272230	257.246240	fe80::b77:758a:4347::fb	ff02::fb	MDNS	300	Standard query response 0x0000 TXT, cache flush PTR Devansh (2)...companion-link_tcp.local TXT HSEC, cache flush Devansh (2)...com
272231	257.246240	BrocadeCommu_90:80::	Broadcast	ARP	60	Who has 172.16.88.204? Tell 172.16.64.1
272232	257.246240	BrocadeCommu_90:80::	Broadcast	ARP	60	Who has 172.16.71.226? Tell 172.16.64.1
272233	257.246240	BrocadeCommu_90:80::	Broadcast	ARP	60	Who has 172.16.93.236? Tell 172.16.64.1
272234	257.246240	BrocadeCommu_90:80::	Broadcast	ARP	60	Who has 172.16.86.228? Tell 172.16.64.1
272235	257.246240	Dell_90:28:fd	Broadcast	ARP	60	Who has 172.16.80.244? Tell 172.16.64.211
272236	257.250089	BrocadeCommu_90:80::	Broadcast	ARP	60	Who has 172.16.76.164? Tell 172.16.64.1
272237	257.250089	BrocadeCommu_90:80::	Broadcast	ARP	60	Who has 172.16.81.142? Tell 172.16.64.1
272238	257.250089	BrocadeCommu_90:80::	Broadcast	ARP	60	Who has 172.16.84.30? Tell 172.16.64.1
272239	257.250089	fe80::b28:724d:3868::fb	ff02::fb	MDNS	115	Standard query 0xb280 PTR Devansh (2)...device-info_tcp.local, "QM" question
272240	257.250089	fe80::5d:5f54:98a:2::	ff02::fb	MDNS	115	Standard query 0x4306 PTR Devansh (2)...device-info_tcp.local, "QM" question
272241	257.250089	fe80::fb47:87df:7dd::fb	ff02::fb	MDNS	115	Standard query 0x5e04 PTR Devansh (2)...device-info_tcp.local, "QM" question
272242	257.250089	172.16.87.35	224.0.0.251	MDNS	103	Standard query 0x0000 TXT Aryaman's MacBook Air...airplay_tcp.local, "QM" question
272243	257.250089	fe80::1c9a:f39d:c91::	ff02::fb	MDNS	123	Standard query 0x0000 TXT Aryaman's MacBook Air...airplay_tcp.local, "QM" question
272244	257.250089	172.16.76.177	224.0.0.251	MDNS	112	Standard query 0x0000 TXT samar's MacBook Air (3)...companion-link_tcp.local, "QM" question
272245	257.250089	fe80::c7:21a:c39f:a::	ff02::fb	MDNS	132	Standard query 0x0000 TXT samar's MacBook Air (3)...companion-link_tcp.local, "QM" question
272246	257.250089	fe80::14b9:6da9:35f::	ff02::fb	MDNS	140	Standard query 0x0000 TXT iPad (146)...companion-link_tcp.local, "QM" question

Frame 272238: Packet, 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF... Ethernet II, Src: BrocadeCommu_90:80:78 (74:8e:f8:90:80:78), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: BrocadeCommu_90:80:78 (74:8e:f8:90:80:78)
Sender IP address: 172.16.64.1
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 172.16.84.30

0000 ff ff ff ff ff ff 74 8e f8 90 80 78 00 00 00 01t...x...p
0010 00 00 00 04 00 01 74 8e f8 90 80 78 ac 10 40 01T.....
0020 00 00 00 00 00 00 ac 10 54 1d 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00