

Ex. No 14

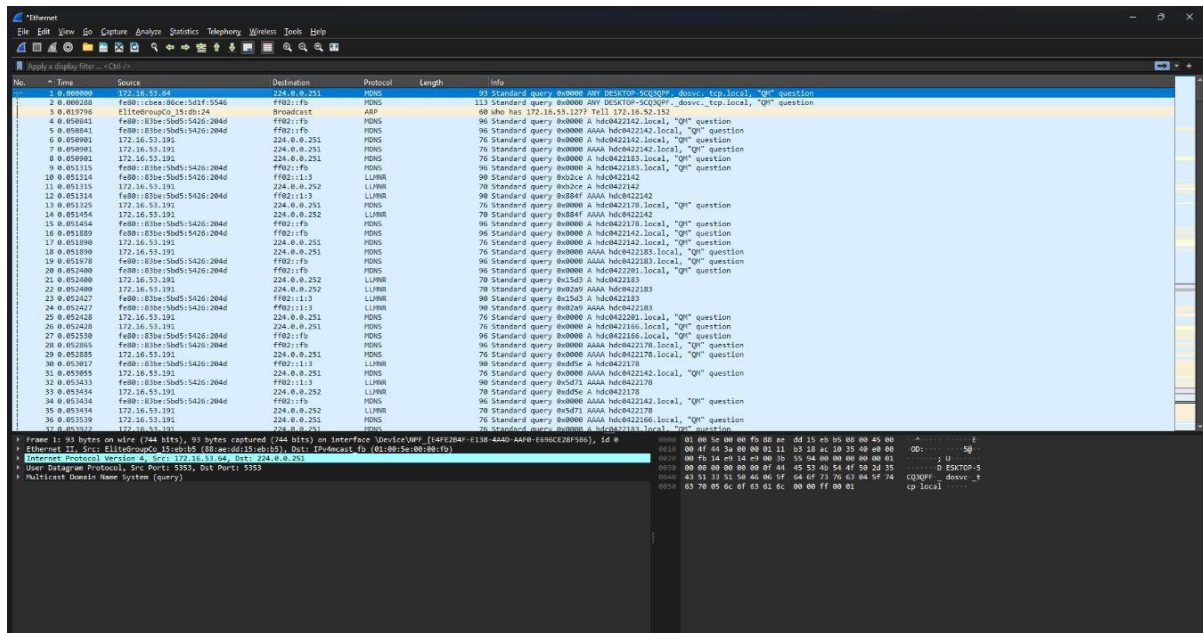
Date: 03.11.2025

Wireshark

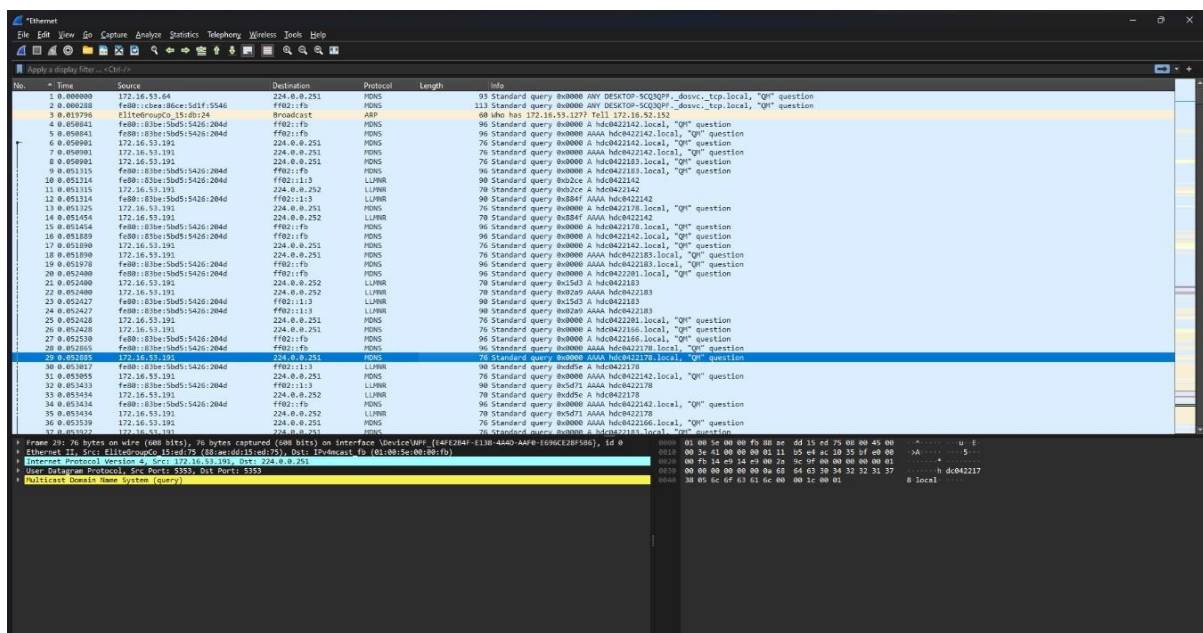
AIM: - Experiments on Packet capture tool: Wireshark

CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL:

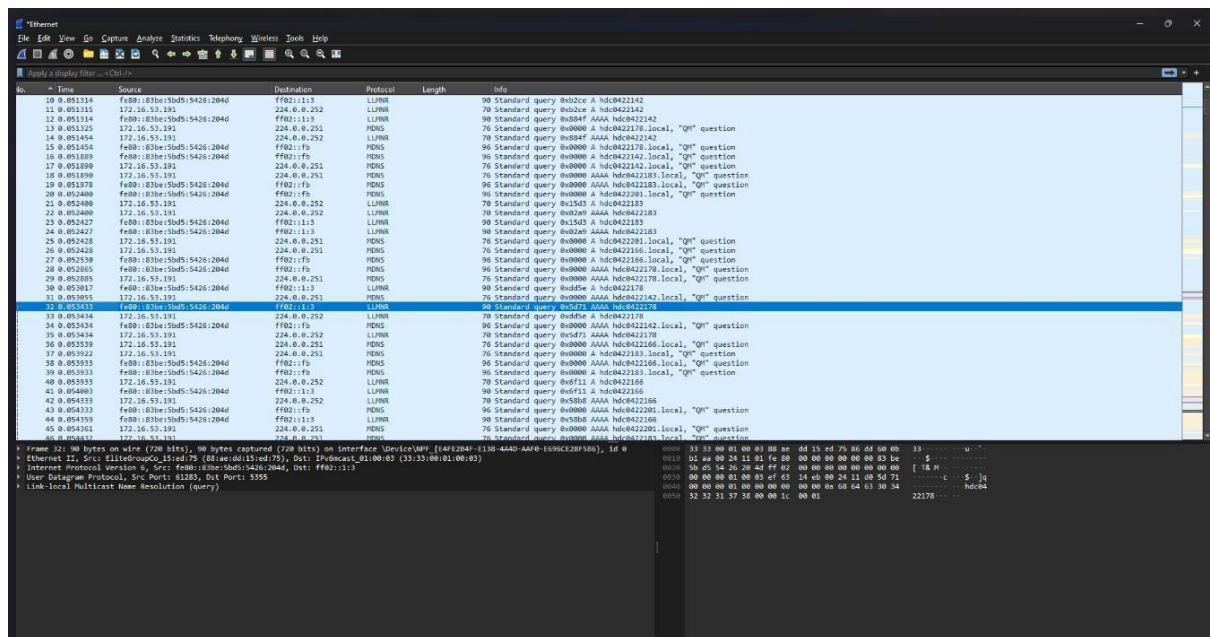
Packet 1:



Packet 2:



Packet 3:



The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for various functions. The main display area shows a list of captured packets. Packet 3 is selected and highlighted in blue. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Link-Local Multicast Name Resolution (query). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
10	0.051114	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x02ce A hc0422142
11	0.051115	172.16.53.191	224.0.0.252	LWMR	70	Standard query 0x02ce A hc0422142
12	0.051114	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x02cf AAAA hc0422142
13	0.051125	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 A hc0422178.local, "QI" question
14	0.051454	172.16.53.191	224.0.0.252	LWMR	70	Standard query 0x02cf AAAA hc0422142
15	0.051454	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 A hc0422178.local, "QI" question
16	0.051889	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 A hc0422142.local, "QI" question
17	0.051889	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 A hc0422143.local, "QI" question
18	0.051890	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422183.local, "QI" question
19	0.051978	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 AAAA hc0422183.local, "QI" question
20	0.052400	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 A hc0422201.local, "QI" question
21	0.052400	172.16.53.191	224.0.0.252	LWMR	70	Standard query 0x15d3 A hc0422183
22	0.052400	172.16.53.191	224.0.0.252	LWMR	70	Standard query 0x0200 AAAA hc0422183
23	0.052427	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x15d3 A hc0422183
24	0.052427	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x0200 AAAA hc0422183
25	0.052428	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 A hc0422201.local, "QI" question
26	0.052428	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 A hc0422166.local, "QI" question
27	0.052539	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 A hc0422166.local, "QI" question
28	0.052885	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 AAAA hc0422178.local, "QI" question
29	0.052885	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422178.local, "QI" question
30	0.053017	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x0200 A hc0422178
31	0.053017	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422142.local, "QI" question
32	0.053017	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x0200 A hc0422178
33	0.053018	172.16.53.191	224.0.0.252	LWMR	70	Standard query 0x0200 A hc0422178
34	0.053018	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 AAAA hc0422142.local, "QI" question
35	0.053018	172.16.53.191	224.0.0.252	LWMR	70	Standard query 0x0200 AAAA hc0422178
36	0.053019	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422166.local, "QI" question
37	0.053022	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 A hc0422183.local, "QI" question
38	0.053033	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 AAAA hc0422166.local, "QI" question
39	0.053033	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 A hc0422183.local, "QI" question
40	0.053033	172.16.53.191	224.0.0.252	LWMR	70	Standard query 0x0200 A hc0422166
41	0.054063	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x0200 A hc0422166
42	0.054033	172.16.53.191	224.0.0.252	LWMR	70	Standard query 0x5008 AAAA hc0422166
43	0.054033	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 AAAA hc0422201.local, "QI" question
44	0.054039	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x0200 AAAA hc0422166
45	0.054051	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422183.local, "QI" question
46	0.054052	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422183.local, "QI" question

Frame 32: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface Vmware (14:00:00:00:00:00), ID 0

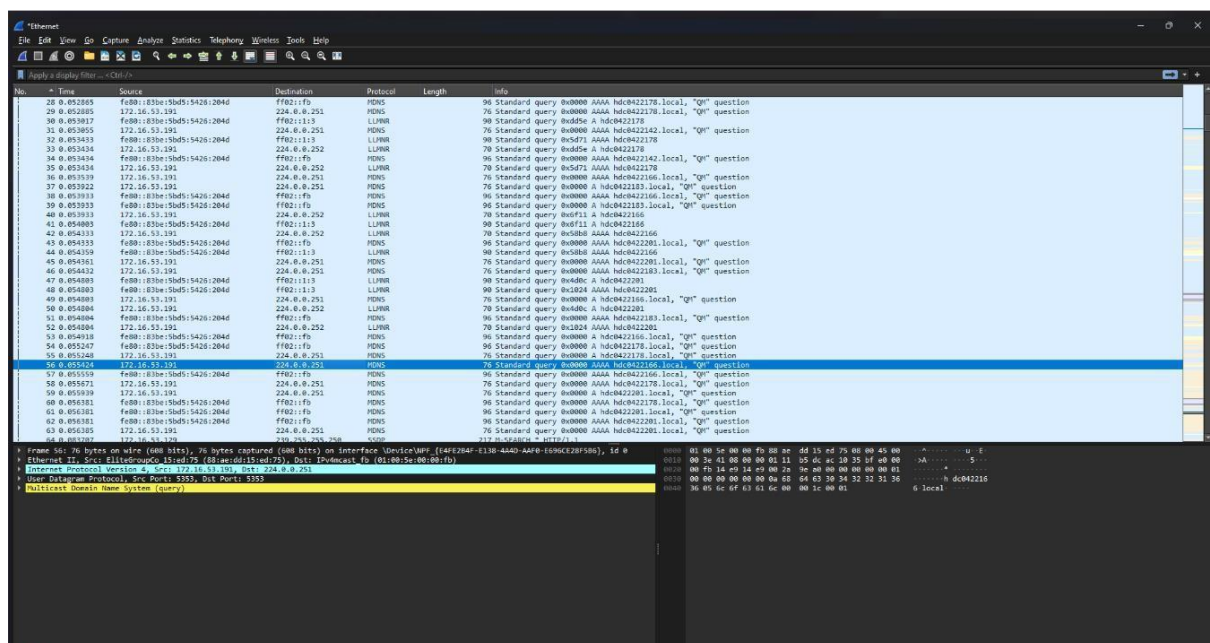
Ethernet II, Src: Intel(R) Ethernet Controller (14:00:00:00:00:00), Dst: IPv6multicast (01:00:5e:00:00:00)

Internet Protocol Version 4, Src: 172.16.53.191, Dst: 224.0.0.251

User Datagram Protocol, Src Port: 5355, Dst Port: 5355

Link-Local Multicast Name Resolution (query)

Packet 4:



The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for various functions. The main display area shows a list of captured packets. Packet 4 is selected and highlighted in blue. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Link-Local Multicast Name Resolution (query). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
28	0.052885	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 AAAA hc0422178.local, "QI" question
29	0.052885	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422178.local, "QI" question
30	0.053017	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x0200 A hc0422178
31	0.053017	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0200 A hc0422142.local, "QI" question
32	0.053033	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x0200 A hc0422178
33	0.053033	172.16.53.191	224.0.0.252	LWMR	90	Standard query 0x0200 A hc0422178
34	0.053034	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 AAAA hc0422142.local, "QI" question
35	0.053034	172.16.53.191	224.0.0.252	LWMR	70	Standard query 0x0200 AAAA hc0422178
36	0.053039	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422166.local, "QI" question
37	0.053022	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 A hc0422183.local, "QI" question
38	0.053033	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 A hc0422183.local, "QI" question
39	0.053033	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 A hc0422183.local, "QI" question
40	0.053033	172.16.53.191	224.0.0.252	LWMR	70	Standard query 0x0200 A hc0422166
41	0.054063	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x0200 A hc0422166
42	0.054033	172.16.53.191	224.0.0.252	LWMR	70	Standard query 0x5008 AAAA hc0422166
43	0.054033	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x0000 AAAA hc0422201.local, "QI" question
44	0.054039	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x0200 AAAA hc0422166
45	0.054051	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422183.local, "QI" question
46	0.054052	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422183.local, "QI" question
47	0.054080	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x0200 A hc0422183.local, "QI" question
48	0.054083	fe80::83be:5bd5:5426:2040	ff02::1:1	LWMR	90	Standard query 0x0200 A hc0422183.local, "QI" question
49	0.054089	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 A hc0422166.local, "QI" question
50	0.054084	172.16.53.191	224.0.0.252	LWMR	70	Standard query 0x0200 A hc0422183.local, "QI" question
51	0.054084	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 AAAA hc0422183.local, "QI" question
52	0.054084	172.16.53.191	224.0.0.252	LWMR	70	Standard query 0x0200 A hc0422183
53	0.054018	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 A hc0422166.local, "QI" question
54	0.054247	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 A hc0422178.local, "QI" question
55	0.055248	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422166.local, "QI" question
56	0.055248	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422166.local, "QI" question
57	0.055349	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 AAAA hc0422166.local, "QI" question
58	0.055671	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422178.local, "QI" question
59	0.055939	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 A hc0422201.local, "QI" question
60	0.056311	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 AAAA hc0422178.local, "QI" question
61	0.056311	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 A hc0422201.local, "QI" question
62	0.056311	fe80::83be:5bd5:5426:2040	ff02::1:f	PENS	90	Standard query 0x0000 AAAA hc0422201.local, "QI" question
63	0.056311	172.16.53.191	224.0.0.251	PENS	70	Standard query 0x0000 AAAA hc0422201.local, "QI" question

Frame 56: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface Vmware (14:00:00:00:00:00), ID 0

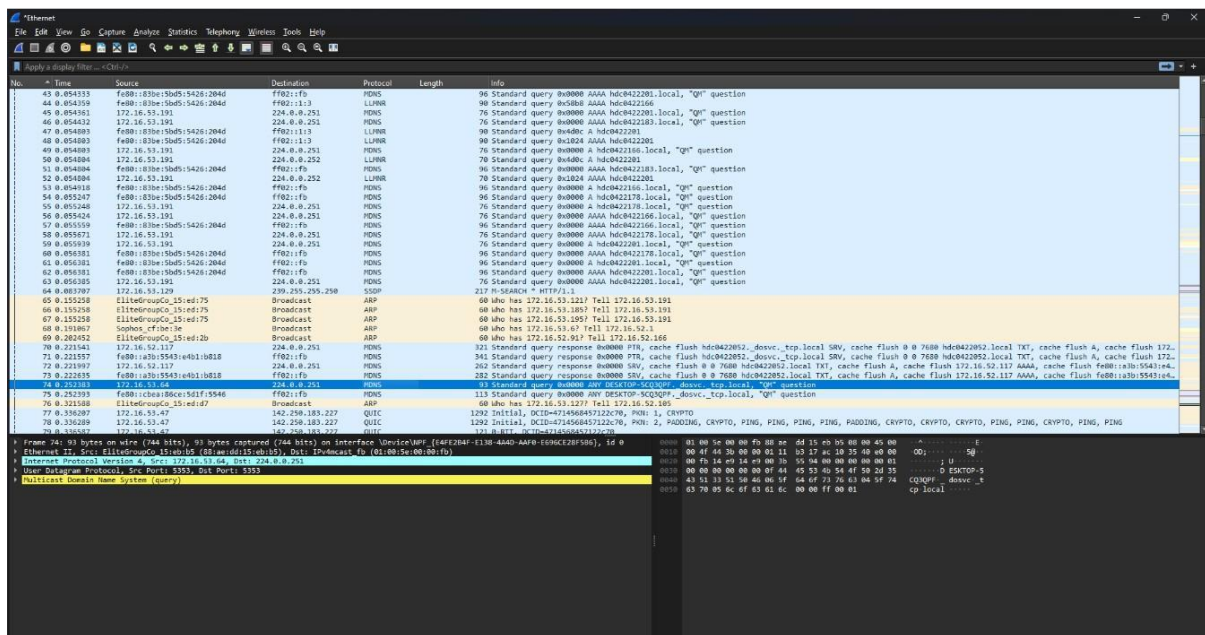
Ethernet II, Src: Intel(R) Ethernet Controller (14:00:00:00:00:00), Dst: IPv6multicast (01:00:5e:00:00:00)

Internet Protocol Version 4, Src: 172.16.53.191, Dst: 224.0.0.251

User Datagram Protocol, Src Port: 5355, Dst Port: 5355

Multicast Domain Name System (query)

Packet 5:



The screenshot shows the Wireshark interface with packet 5 selected. The packet list on the left shows a series of DNS queries and responses between fe80::83be:15db5:5426:204d and 172.16.53.191. Packet 5 is a DNS query from fe80::83be:15db5:5426:204d to 172.16.53.191, asking for the IP address of www.google.com. The packet details pane on the right shows the standard query structure with the question section containing the query name and type.

No.	Time	Source	Destination	Protocol	Length	Info
43	0.054153	fe80::83be:15db5:5426:204d	ff02::1::3	MDNS	96	Standard query 0x0000 AAAA hdc8422201.local, "Q"
44	0.054159	fe80::83be:15db5:5426:204d	ff02::1::3	MDNS	96	Standard query 0x0000 AAAA hdc8422166.local, "Q"
45	0.054161	172.16.53.191	224.0.0.251	MDNS	76	Standard query 0x0000 AAAA hdc8422201.local, "Q"
46	0.054432	172.16.53.191	224.0.0.251	MDNS	76	Standard query 0x0000 AAAA hdc8422183.local, "Q"
47	0.054489	fe80::83be:15db5:5426:204d	ff02::1::3	MDNS	96	Standard query 0x0000 A hdc8422201.local, "Q"
48	0.054809	fe80::83be:15db5:5426:204d	ff02::1::3	MDNS	96	Standard query 0x0000 AAAA hdc8422201.local, "Q"
49	0.054809	172.16.53.191	224.0.0.251	MDNS	76	Standard query 0x0000 A hdc8422166.local, "Q"
50	0.054804	172.16.53.191	224.0.0.252	MDNS	76	Standard query 0x0000 A hdc8422201.local, "Q"
51	0.054804	fe80::83be:15db5:5426:204d	ff02::1::3	MDNS	96	Standard query 0x0000 AAAA hdc8422183.local, "Q"
52	0.054804	172.16.53.191	224.0.0.252	MDNS	76	Standard query 0x0000 A hdc8422201.local, "Q"
53	0.054918	fe80::83be:15db5:5426:204d	ff02::1::3	MDNS	96	Standard query 0x0000 A hdc8422166.local, "Q"
54	0.055337	fe80::83be:15db5:5426:204d	ff02::1::3	MDNS	96	Standard query 0x0000 A hdc8422178.local, "Q"
55	0.055248	172.16.53.191	224.0.0.251	MDNS	76	Standard query 0x0000 A hdc8422178.local, "Q"
56	0.055244	172.16.53.191	224.0.0.251	MDNS	76	Standard query 0x0000 AAAA hdc8422166.local, "Q"
57	0.055559	fe80::83be:15db5:5426:204d	ff02::1::3	MDNS	96	Standard query 0x0000 AAAA hdc8422166.local, "Q"
58	0.055671	172.16.53.191	224.0.0.251	MDNS	76	Standard query 0x0000 AAAA hdc8422178.local, "Q"
59	0.055939	172.16.53.191	224.0.0.251	MDNS	76	Standard query 0x0000 A hdc8422201.local, "Q"
60	0.056161	fe80::83be:15db5:5426:204d	ff02::1::3	MDNS	96	Standard query 0x0000 AAAA hdc8422178.local, "Q"
61	0.056161	fe80::83be:15db5:5426:204d	ff02::1::3	MDNS	96	Standard query 0x0000 A hdc8422201.local, "Q"
62	0.056161	fe80::83be:15db5:5426:204d	ff02::1::3	MDNS	96	Standard query 0x0000 AAAA hdc8422201.local, "Q"
63	0.056305	172.16.53.191	224.0.0.251	MDNS	76	Standard query 0x0000 AAAA hdc8422201.local, "Q"
64	0.063787	172.16.53.129	239.255.255.250	SSDP	217	M-SEARCH = HTTP/1.1
65	0.155258	Ellivdnpocp_15.ed:75	Broadcast	ARP	60	who has 172.16.53.121? Tell 172.16.53.191
66	0.155258	Ellivdnpocp_15.ed:75	Broadcast	ARP	60	who has 172.16.53.185? Tell 172.16.53.191
67	0.155258	Ellivdnpocp_15.ed:75	Broadcast	ARP	60	who has 172.16.53.195? Tell 172.16.53.191
68	0.159687	Sophos-efrnet-16	Broadcast	ARP	60	who has 172.16.53.67? Tell 172.16.52.1
69	0.202452	Ellivdnpocp_15.ed:2b	Broadcast	ARP	60	who has 172.16.52.91? Tell 172.16.52.166
70	0.221941	172.16.52.117	224.0.0.251	MDNS	321	Standard query response 0x0000 PTR, cache flush hdc8422052.dnsvc.tcp.local SRV, cache flush 0 0 7680 hdc8422052.local TXT, cache flush 172.16.52.117 AAAA, cache flush fe80::83be:15db5:5426:204d
71	0.221957	fe80::83be:15db5:5426:204d	ff02::1::3	MDNS	341	Standard query response 0x0000 PTR, cache flush hdc8422052.dnsvc.tcp.local SRV, cache flush 0 0 7680 hdc8422052.local TXT, cache flush 172.16.52.117 AAAA, cache flush fe80::83be:15db5:5426:204d
72	0.221997	172.16.52.117	224.0.0.251	MDNS	262	Standard query response 0x0000 SRV, cache flush 0 0 7680 hdc8422052.local TXT, cache flush 172.16.52.117 AAAA, cache flush fe80::83be:15db5:5426:204d
73	0.221955	fe80::83be:15db5:5426:204d	ff02::1::3	MDNS	252	Standard query response 0x0000 SRV, cache flush 0 0 7680 hdc8422052.local TXT, cache flush 172.16.52.117 AAAA, cache flush fe80::83be:15db5:5426:204d
74	0.221993	172.16.53.66	224.0.0.251	MDNS	83	Standard query 0x0000 SRV DESKTOP-SCQJQPF.dnsvc.tcp.local, "Q"
75	0.221993	fe80::cbea:186c:e15d:f1546	ff02::1::3	MDNS	111	Standard query 0x0000 ANY DESKTOP-SCQJQPF.dnsvc.tcp.local, "Q"
76	0.221998	Ellivdnpocp_15.ed:47	Broadcast	ARP	60	who has 172.16.53.127? Tell 172.16.52.185
77	0.336287	172.16.53.47	142.250.183.227	QUIC	1292	Initial, DCID=4714568457122C79, PRR: 1, CRYPTO
78	0.336289	172.16.53.47	142.250.183.227	QUIC	1292	Initial, DCID=4714568457122C79, PRR: 2, PADDING, CRYPTO, PING, PING, PING, PING, PING, PING, PING, PING
79	0.336504	172.16.53.47	142.250.183.227	QUIC	1292	Initial, DCID=4714568457122C79, PRR: 3, PADDING, CRYPTO, PING, PING, PING, PING, PING, PING, PING, PING

Packet 5 details:

- Frame 5: 1292 bytes on wire (10336 bits), 81 bytes captured (6488 bits) on interface vnic0 (fe80::83be:15db5:5426:204d) (eth0) (fe80::83be:15db5:5426:204d)
- Ethernet II, Src: Ellivdnpocp_15.ed:47 (82:ee:6d:15:ed:47), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 172.16.53.47, Dst: 224.0.0.251
- DNS Query (Standard query type) (query)
- Multicast DNS Name System (query)

RESULT: -

Capturing and analysing the packets have been done successfully using Wireshark.