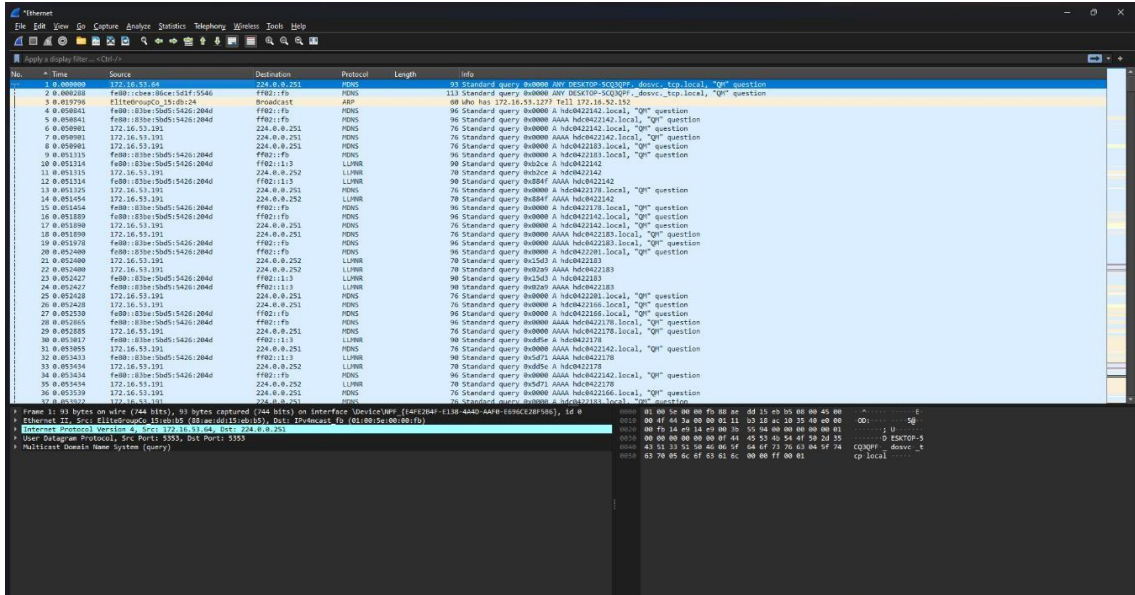


EXPERIMENT – 5

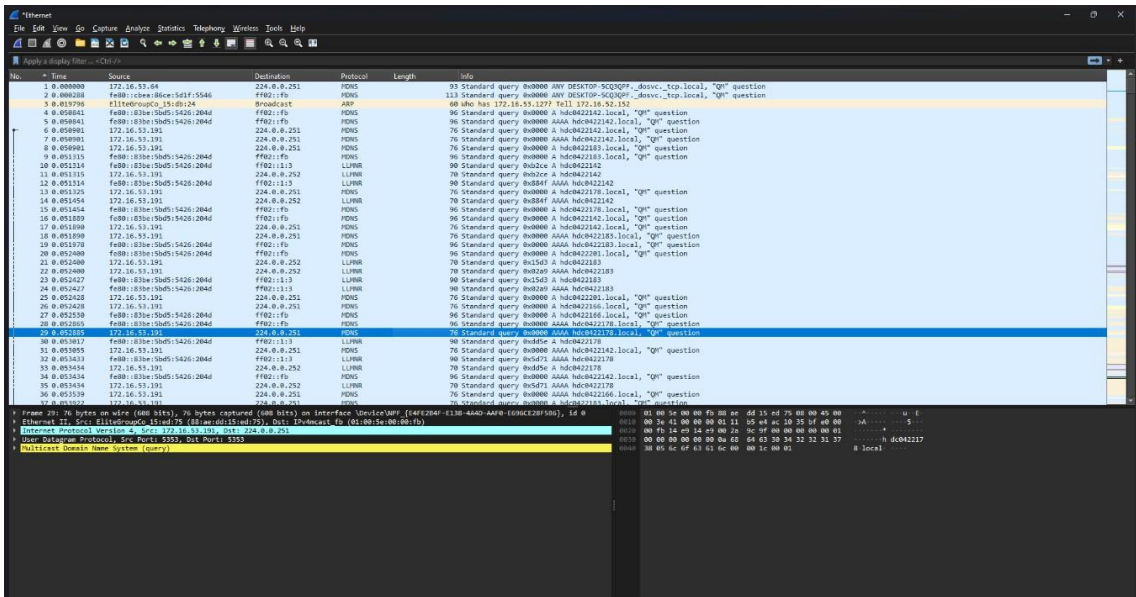
AIM: - Experiments on Packet capture tool: Wireshark

CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL:

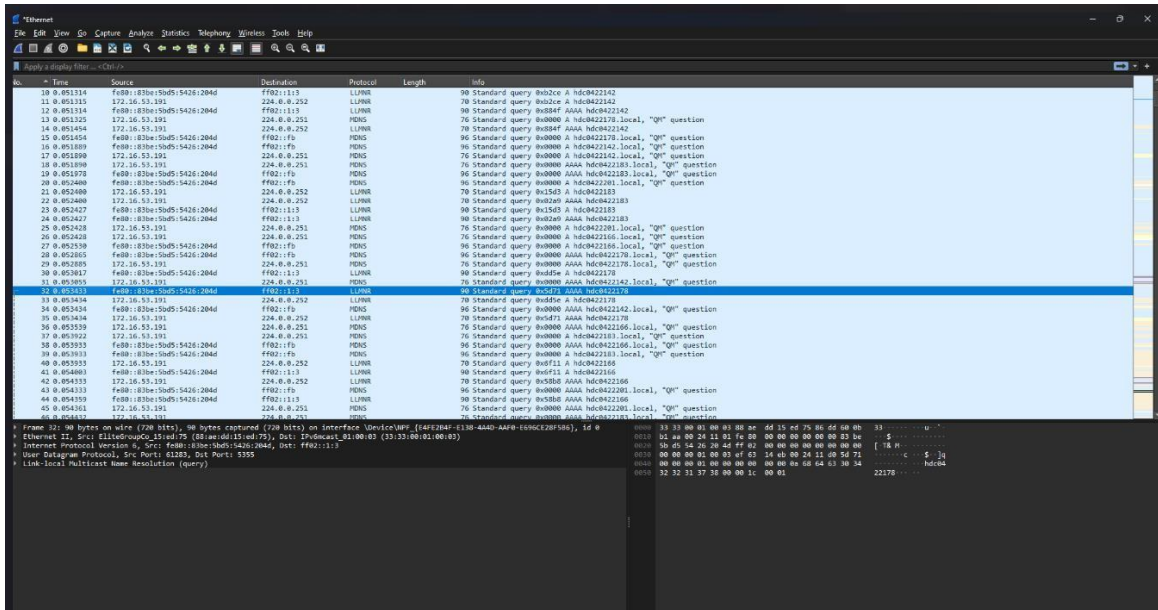
Packet 1:



Packet 2:



Packet 3:

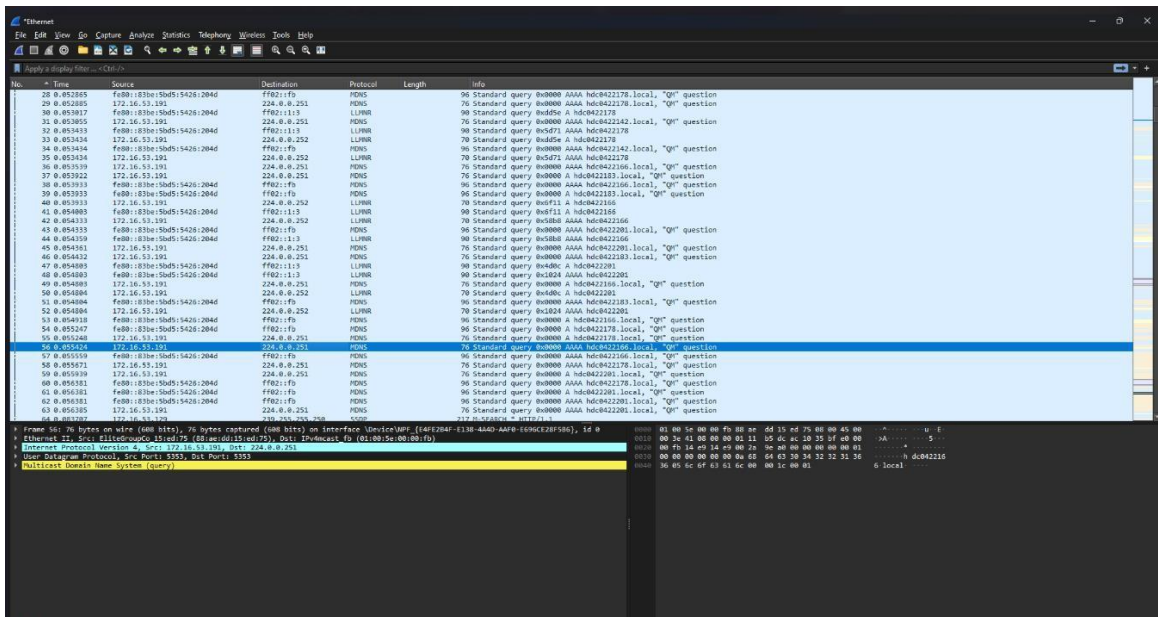


The image shows a Wireshark packet capture of Packet 3. The packet list on the left shows a series of DNS queries from 10.0.0.1 to 10.0.0.255. The selected packet, Packet 3, is a DNS query from 10.0.0.1 to 10.0.0.255. The packet details pane shows the following structure:

- Frame 3: 60 bytes on wire (480 bits), 76 bytes captured (608 bits) on interface vnic-vswan1 (10.0.0.1), 12 B captured (96 bits) on 0
- Ethernet II, Src: vnic-vswan1 (10.0.0.1), Dst: vnic-vswan1 (10.0.0.1)
- Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.1
- User Datagram Protocol, Src Port: 5555, Dst Port: 5555
- Link-Local Multicast Name Resolution (query)

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and UDP header.

Packet 4:



The image shows a Wireshark packet capture of Packet 4. The packet list on the left shows a series of DNS queries from 10.0.0.1 to 10.0.0.255. The selected packet, Packet 4, is a DNS query from 10.0.0.1 to 10.0.0.255. The packet details pane shows the following structure:

- Frame 4: 60 bytes on wire (480 bits), 76 bytes captured (608 bits) on interface vnic-vswan1 (10.0.0.1), 12 B captured (96 bits) on 0
- Ethernet II, Src: vnic-vswan1 (10.0.0.1), Dst: vnic-vswan1 (10.0.0.1)
- Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.1
- User Datagram Protocol, Src Port: 5555, Dst Port: 5555
- Link-Local Multicast Name Resolution (query)

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and UDP header.

Packet 5:

No.	Time	Source	Destination	Protocol	Length	Info
43	0.654133	fe80::83be:5b0f:5426:2046	ff02::1:f	PDNS	96	Standard query 0x0000 AAAA h0c422281.local, "Q"
44	0.654139	fe80::83be:5b0f:5426:2046	ff02::1:1	LWMR	96	Standard query 0x0000 AAAA h0c422281.local, "Q"
45	0.654151	172.16.53.191	224.0.0.251	PDNS	76	Standard query 0x0000 AAAA h0c422281.local, "Q"
46	0.654162	172.16.53.191	224.0.0.251	PDNS	76	Standard query 0x0000 AAAA h0c422281.local, "Q"
47	0.654183	fe80::83be:5b0f:5426:2046	ff02::1:1	LWMR	96	Standard query 0x0000 AAAA h0c422281.local, "Q"
48	0.654188	fe80::83be:5b0f:5426:2046	ff02::1:1	LWMR	96	Standard query 0x0000 AAAA h0c422281.local, "Q"
49	0.654193	172.16.53.191	224.0.0.251	PDNS	76	Standard query 0x0000 AAAA h0c422281.local, "Q"
50	0.654194	172.16.53.191	224.0.0.251	PDNS	76	Standard query 0x0000 AAAA h0c422281.local, "Q"
51	0.654194	fe80::83be:5b0f:5426:2046	ff02::1:f	PDNS	96	Standard query 0x0000 AAAA h0c422281.local, "Q"
52	0.654194	172.16.53.191	224.0.0.251	LWMR	96	Standard query 0x0000 AAAA h0c422281.local, "Q"
53	0.654194	fe80::83be:5b0f:5426:2046	ff02::1:f	PDNS	96	Standard query 0x0000 AAAA h0c422281.local, "Q"
54	0.655147	fe80::83be:5b0f:5426:2046	ff02::1:f	PDNS	96	Standard query 0x0000 AAAA h0c422281.local, "Q"
55	0.655148	172.16.53.191	224.0.0.251	PDNS	76	Standard query 0x0000 AAAA h0c422281.local, "Q"
56	0.655154	172.16.53.191	224.0.0.251	PDNS	76	Standard query 0x0000 AAAA h0c422281.local, "Q"
57	0.655159	fe80::83be:5b0f:5426:2046	ff02::1:f	PDNS	96	Standard query 0x0000 AAAA h0c422281.local, "Q"
58	0.655171	172.16.53.191	224.0.0.251	PDNS	76	Standard query 0x0000 AAAA h0c422281.local, "Q"
59	0.655193	172.16.53.191	224.0.0.251	PDNS	76	Standard query 0x0000 AAAA h0c422281.local, "Q"
60	0.655193	fe80::83be:5b0f:5426:2046	ff02::1:f	PDNS	96	Standard query 0x0000 AAAA h0c422281.local, "Q"
61	0.655193	fe80::83be:5b0f:5426:2046	ff02::1:f	PDNS	96	Standard query 0x0000 AAAA h0c422281.local, "Q"
62	0.655193	fe80::83be:5b0f:5426:2046	ff02::1:f	PDNS	96	Standard query 0x0000 AAAA h0c422281.local, "Q"
63	0.655193	172.16.53.191	224.0.0.251	PDNS	76	Standard query 0x0000 AAAA h0c422281.local, "Q"
64	0.655197	172.16.53.191	224.0.0.251	PDNS	76	Standard query 0x0000 AAAA h0c422281.local, "Q"
65	0.155228	111ed:0000_15:ed:75	Broadcast	ARP	217	60 who has 172.16.53.121? Tell 172.16.53.191
66	0.155228	111ed:0000_15:ed:75	Broadcast	ARP	60	who has 172.16.53.121? Tell 172.16.53.191
67	0.155228	111ed:0000_15:ed:75	Broadcast	ARP	60	who has 172.16.53.121? Tell 172.16.53.191
68	0.155228	111ed:0000_15:ed:75	Broadcast	ARP	60	who has 172.16.53.121? Tell 172.16.53.191
69	0.155228	111ed:0000_15:ed:75	Broadcast	ARP	60	who has 172.16.53.121? Tell 172.16.53.191
70	0.221141	172.16.53.121	224.0.0.251	PDNS	321	Standard query response 0x0000 PING, cache flush 0x0000 h0c422281.local, "Q"
71	0.221141	fe80::83be:5b0f:5426:2046	ff02::1:f	PDNS	341	Standard query response 0x0000 PING, cache flush 0x0000 h0c422281.local, "Q"
72	0.221141	172.16.53.121	224.0.0.251	PDNS	262	Standard query response 0x0000 PING, cache flush 0x0000 h0c422281.local, "Q"
73	0.221141	fe80::83be:5b0f:5426:2046	ff02::1:f	PDNS	282	Standard query response 0x0000 PING, cache flush 0x0000 h0c422281.local, "Q"
74	0.221141	172.16.53.121	224.0.0.251	PDNS	83	Standard query response 0x0000 PING, cache flush 0x0000 h0c422281.local, "Q"
75	0.252193	fe80::83be:5b0f:5426:2046	ff02::1:f	PDNS	113	Standard query response 0x0000 PING, cache flush 0x0000 h0c422281.local, "Q"
76	0.252193	172.16.53.121	224.0.0.251	PDNS	60	who has 172.16.53.121? Tell 172.16.53.191
77	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
78	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
79	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
80	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
81	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
82	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
83	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
84	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
85	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
86	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
87	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
88	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
89	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
90	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
91	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
92	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
93	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
94	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
95	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
96	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
97	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
98	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
99	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO
100	0.252193	172.16.53.121	224.0.0.251	PDNS	1292	Initial, DCID=4714568457122679, PING, 1, CRYPTO

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