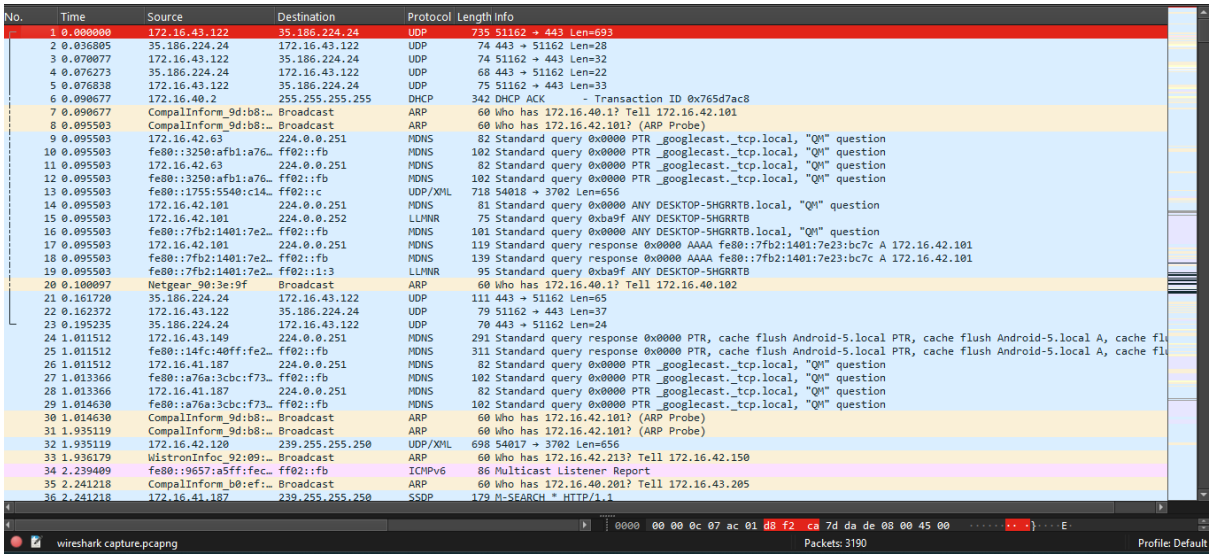
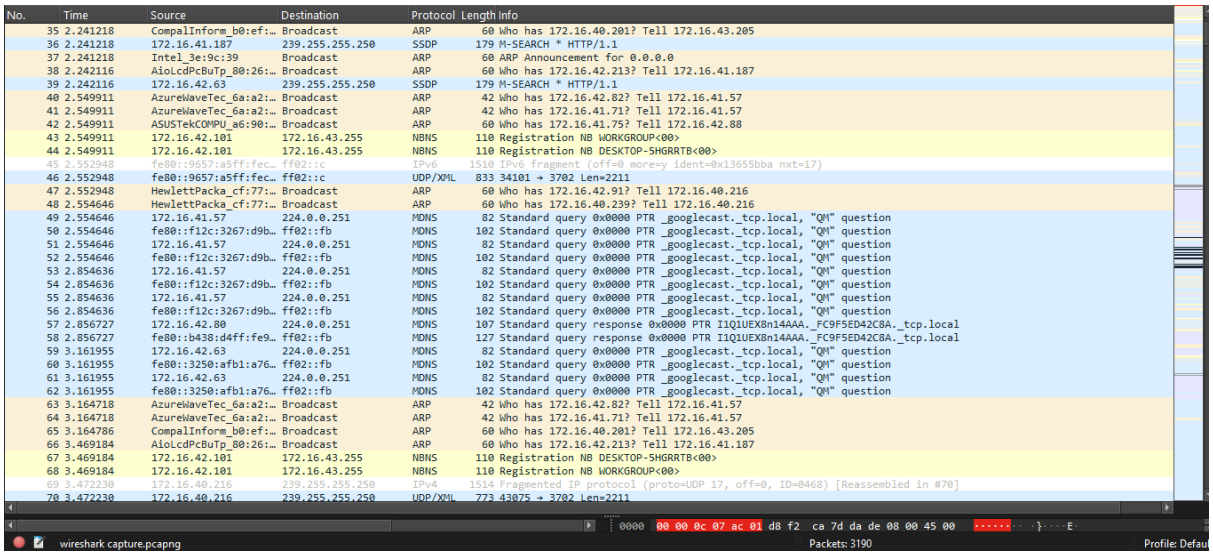
TASK 5

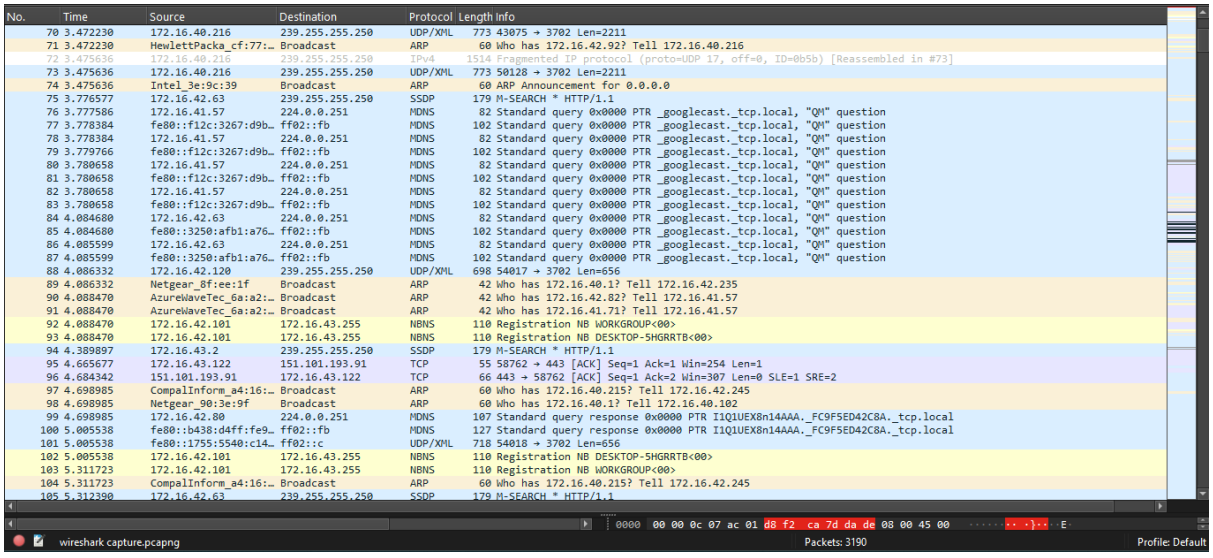
CAPTURES:-



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.43.122	35.186.224.24	UDP	735	51162 → 443 Len=693
2	0.036805	35.186.224.24	172.16.43.122	UDP	74	443 → 51162 Len=28
3	0.070077	172.16.43.122	35.186.224.24	UDP	74	51162 → 443 Len=32
4	0.076273	35.186.224.24	172.16.43.122	UDP	68	443 → 51162 Len=22
5	0.076838	172.16.43.122	35.186.224.24	UDP	75	51162 → 443 Len=33
6	0.090677	172.16.40.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x765d7ac8
7	0.090677	CompalInform_9d:b8:…	Broadcast	ARP	60	Who has 172.16.40.1? Tell 172.16.42.101
8	0.095503	CompalInform_9d:b8:…	Broadcast	ARP	60	Who has 172.16.42.101? (ARP Probe)
9	0.095503	172.16.42.63	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
10	0.095503	fe80::3250:afb1:a76…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
11	0.095503	172.16.42.63	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
12	0.095503	fe80::3250:afb1:a76…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
13	0.095503	fe80::1755:5540:c14…	ff02::c	UDP/XML	718	54018 → 3702 Len=656
14	0.095503	172.16.42.101	224.0.0.251	MDNS	81	Standard query 0x0000 ANY DESKTOP-5HGRRTB.local, "QM" question
15	0.095503	172.16.42.101	224.0.0.252	LLMNR	75	Standard query 0xba9f ANY DESKTOP-5HGRRTB
16	0.095503	fe80::7fb2:1401:7e2…	ff02::fb	MDNS	101	Standard query 0x0000 ANY DESKTOP-5HGRRTB.local, "QM" question
17	0.095503	172.16.42.101	224.0.0.251	MDNS	119	Standard query response 0x0000 AAAA fe80::7fb2:1401:7e23:bc7c A 172.16.42.101
18	0.095503	fe80::7fb2:1401:7e2…	ff02::fb	MDNS	139	Standard query response 0x0000 AAAA fe80::7fb2:1401:7e23:bc7c A 172.16.42.101
19	0.095503	fe80::7fb2:1401:7e2…	ff02::1:3	LLMNR	95	Standard query 0xba9f ANY DESKTOP-5HGRRTB
20	0.100097	Netgear_90:3e:9f	Broadcast	ARP	60	Who has 172.16.40.1? Tell 172.16.40.102
21	0.161720	35.186.224.24	172.16.43.122	UDP	111	443 → 51162 Len=65
22	0.162372	172.16.43.122	35.186.224.24	UDP	79	51162 → 443 Len=37
23	0.195235	35.186.224.24	172.16.43.122	UDP	70	443 → 51162 Len=24
24	1.011512	172.16.43.149	224.0.0.251	MDNS	291	Standard query response 0x0000 PTR, cache flush Android-5.local PTR, cache flush Android-5.local A, cache flu
25	1.011512	fe80::14fc:40ff:fe2…	ff02::fb	MDNS	311	Standard query response 0x0000 PTR, cache flush Android-5.local PTR, cache flush Android-5.local A, cache flu
26	1.011512	172.16.41.187	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
27	1.013366	fe80::a76a:3cbc:f73…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
28	1.013366	172.16.41.187	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
29	1.014630	fe80::a76a:3cbc:f73…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
30	1.014630	CompalInform_9d:b8:…	Broadcast	ARP	60	Who has 172.16.42.101? (ARP Probe)
31	1.935119	CompalInform_9d:b8:…	Broadcast	ARP	60	Who has 172.16.42.101? (ARP Probe)
32	1.935119	172.16.42.120	239.255.255.250	UDP/XML	698	54017 → 3702 Len=656
33	1.936179	WistronInfoc_92:09:…	Broadcast	ARP	60	Who has 172.16.42.213? Tell 172.16.42.150
34	2.239409	fe80::9657:a5ff:fec…	ff02::fb	ICMPv6	86	Multicast Listener Report
35	2.241218	CompalInform_b0:ef:…	Broadcast	ARP	60	Who has 172.16.40.201? Tell 172.16.43.205
36	2.241218	172.16.41.187	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1



No.	Time	Source	Destination	Protocol	Length	Info
35	2.241218	CompalInform_b0:ef:…	Broadcast	ARP	60	Who has 172.16.40.201? Tell 172.16.43.205
36	2.241218	172.16.41.187	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
37	2.241218	Intel_3e:9c:39	Broadcast	ARP	60	ARP Announcement for 0.0.0.0
38	2.242116	AioLcdPcBuTp_80:26:…	Broadcast	ARP	60	Who has 172.16.42.213? Tell 172.16.41.187
39	2.242116	172.16.42.63	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
40	2.549911	AzureWaveTec_6a:a2:…	Broadcast	ARP	42	Who has 172.16.42.82? Tell 172.16.41.57
41	2.549911	AzureWaveTec_6a:a2:…	Broadcast	ARP	42	Who has 172.16.41.71? Tell 172.16.41.57
42	2.549911	ASUSTekCOMPU_a6:90:…	Broadcast	ARP	60	Who has 172.16.41.75? Tell 172.16.42.88
43	2.549911	172.16.42.101	172.16.43.255	NBNS	110	Registration NB WORKGROUP<00>
44	2.549911	172.16.42.101	172.16.43.255	NBNS	110	Registration NB DESKTOP-5HGRRTB<00>
45	2.552948	fe80::9657:a5ff:fec…	ff02::c	IPv6	1510	IPv6 fragment (off=0 more=y ident=0x13655bba nxt=17)
46	2.552948	fe80::9657:a5ff:fec…	ff02::c	UDP/XML	833	34101 → 3702 Len=2211
47	2.552948	HewlettPacka_cf:77:…	Broadcast	ARP	60	Who has 172.16.42.91? Tell 172.16.40.216
48	2.554646	HewlettPacka_cf:77:…	Broadcast	ARP	60	Who has 172.16.40.239? Tell 172.16.40.216
49	2.554646	172.16.41.57	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
50	2.554646	fe80::f12c:3267:d9b…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
51	2.554646	172.16.41.57	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
52	2.554646	fe80::f12c:3267:d9b…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
53	2.854636	172.16.41.57	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
54	2.854636	fe80::f12c:3267:d9b…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
55	2.854636	172.16.41.57	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
56	2.854636	fe80::f12c:3267:d9b…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
57	2.856727	172.16.42.80	224.0.0.251	MDNS	107	Standard query response 0x0000 PTR I1Q1UEX8n14AAA._FC9F5ED42C8A._tcp.local
58	2.856727	fe80::b438:d4ff:fe9…	ff02::fb	MDNS	127	Standard query response 0x0000 PTR I1Q1UEX8n14AAA._FC9F5ED42C8A._tcp.local
59	3.161955	172.16.42.63	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
60	3.161955	fe80::3250:afb1:a76…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
61	3.161955	172.16.42.63	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
62	3.161955	fe80::3250:afb1:a76…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
63	3.164718	AzureWaveTec_6a:a2:…	Broadcast	ARP	42	Who has 172.16.42.82? Tell 172.16.41.57
64	3.164718	AzureWaveTec_6a:a2:…	Broadcast	ARP	42	Who has 172.16.41.71? Tell 172.16.41.57
65	3.164786	CompalInform_b0:ef:…	Broadcast	ARP	60	Who has 172.16.40.201? Tell 172.16.43.205
66	3.469184	AioLcdPcBuTp_80:26:…	Broadcast	ARP	60	Who has 172.16.42.213? Tell 172.16.41.187
67	3.469184	172.16.42.101	172.16.43.255	NBNS	110	Registration NB DESKTOP-5HGRRTB<00>
68	3.469184	172.16.42.101	172.16.43.255	NBNS	110	Registration NB WORKGROUP<00>
69	3.472230	172.16.40.216	239.255.255.250	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=0468) [Reassembled in #70]
70	3.472230	172.16.40.216	239.255.255.250	UDP/XML	773	43075 → 3702 Len=2211



No.	Time	Source	Destination	Protocol	Length	Info
70	3.472230	172.16.40.216	239.255.255.250	UDP/XML	773	43075 → 3702 Len=2211
71	3.472230	HewlettPacka_cf:77:…	Broadcast	ARP	60	Who has 172.16.42.92? Tell 172.16.40.216
72	3.475636	172.16.40.216	239.255.255.250	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=0b5b) [Reassembled in #73]
73	3.475636	172.16.40.216	239.255.255.250	UDP/XML	773	50128 → 3702 Len=2211
74	3.475636	Intel_3e:9c:39	Broadcast	ARP	60	ARP Announcement for 0.0.0.0
75	3.776577	172.16.42.63	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
76	3.777586	172.16.41.57	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
77	3.778384	fe80::f12c:3267:d9b…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
78	3.778384	172.16.41.57	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
79	3.779766	fe80::f12c:3267:d9b…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
80	3.780658	172.16.41.57	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
81	3.780658	fe80::f12c:3267:d9b…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
82	3.780658	172.16.41.57	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
83	3.780658	fe80::f12c:3267:d9b…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
84	4.084680	172.16.42.63	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
85	4.084680	fe80::3250:afb1:a76…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
86	4.085599	172.16.42.63	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
87	4.085599	fe80::3250:afb1:a76…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
88	4.086332	172.16.42.120	239.255.255.250	UDP/XML	698	54017 → 3702 Len=656
89	4.086332	Netgear_8f:ee:1f	Broadcast	ARP	42	Who has 172.16.40.1? Tell 172.16.42.235
90	4.088470	AzureWaveTec_6a:a2:…	Broadcast	ARP	42	Who has 172.16.42.82? Tell 172.16.41.57
91	4.088470	AzureWaveTec_6a:a2:…	Broadcast	ARP	42	Who has 172.16.41.71? Tell 172.16.41.57
92	4.088470	172.16.42.101	172.16.43.255	NBNS	110	Registration NB WORKGROUP<00>
93	4.088470	172.16.42.101	172.16.43.255	NBNS	110	Registration NB DESKTOP-5HGRRTB<00>
94	4.389897	172.16.43.2	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
95	4.665677	172.16.43.122	151.101.193.91	TCP	55	58762 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
96	4.684342	151.101.193.91	172.16.43.122	TCP	66	443 → 58762 [ACK] Seq=1 Ack=2 Win=307 Len=0 SLE=1 SRE=2
97	4.698985	CompalInform_a4:16:…	Broadcast	ARP	60	Who has 172.16.40.215? Tell 172.16.42.245
98	4.698985	Netgear_90:3e:9f	Broadcast	ARP	60	Who has 172.16.40.1? Tell 172.16.40.102
99	4.698985	172.16.42.80	224.0.0.251	MDNS	107	Standard query response 0x0000 PTR I1Q1UEX8n14AAA._FC9F5ED42C8A._tcp.local
100	5.005538	fe80::b438:d4ff:fe9…	ff02::fb	MDNS	127	Standard query response 0x0000 PTR I1Q1UEX8n14AAA._FC9F5ED42C8A._tcp.local
101	5.005538	fe80::1755:5540:c14…	ff02::c	UDP/XML	718	54018 → 3702 Len=656
102	5.005538	172.16.42.101	172.16.43.255	NBNS	110	Registration NB DESKTOP-5HGRRTB<00>
103	5.311723	172.16.42.101	172.16.43.255	NBNS	110	Registration NB WORKGROUP<00>
104	5.311723	CompalInform_a4:16:…	Broadcast	ARP	60	Who has 172.16.40.215? Tell 172.16.42.245
105	5.312390	172.16.42.63	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1

1. Network Overview

- **Protocols observed:**
  - **UDP:** Includes MDNS, SSDP, NBNS, DHCP, and application-specific UDP packets (e.g., Chromecast queries).
  - **ARP:** Frequent ARP requests for IP-to-MAC resolution.
  - **ICMPv6:** Multicast Listener Reports.
  - **TCP:** Handshakes and ACK packets toward port 443 (HTTPS).
  - **IPv4 fragmentation**: Some large UDP packets fragmented and reassembled.
- **Traffic type:** Mostly **local network service discovery** and **device communication**, plus some **outbound HTTPS** traffic to public IPs.

2. Key Observations

- **Device Discovery**:
  - **mDNS** (`_googlecast._tcp.local`): Indicates Google Cast devices (e.g., Chromecast, smart TVs) actively advertising on the LAN.
  - **SSDP**: Simple Service Discovery Protocol broadcasts for UPnP-capable devices.
  - **NBNS**: NetBIOS name service registrations for hostnames like `DESKTOP-5HGRRTB` and `WORKGROUP`.
- **ARP Activity**:
  - Multiple ARP "Who has" requests for various IPs (e.g., `172.16.42.101`, `172.16.42.213`, `172.16.42.82`), showing normal address resolution and possibly network scanning or new devices joining.
- **External Communication**:
  - Packets between **172.16.43.122** and **35.186.224.24** (Google Cloud IP) over UDP/TCP port 443 — likely secure application traffic.
- **IPv6 Activity**:
  - Several multicast queries and UDP/XML exchanges over IPv6 addresses starting with `fe80::`.
- **DHCP**:
  - A DHCP ACK packet confirming an IP lease (`172.16.42.101`)