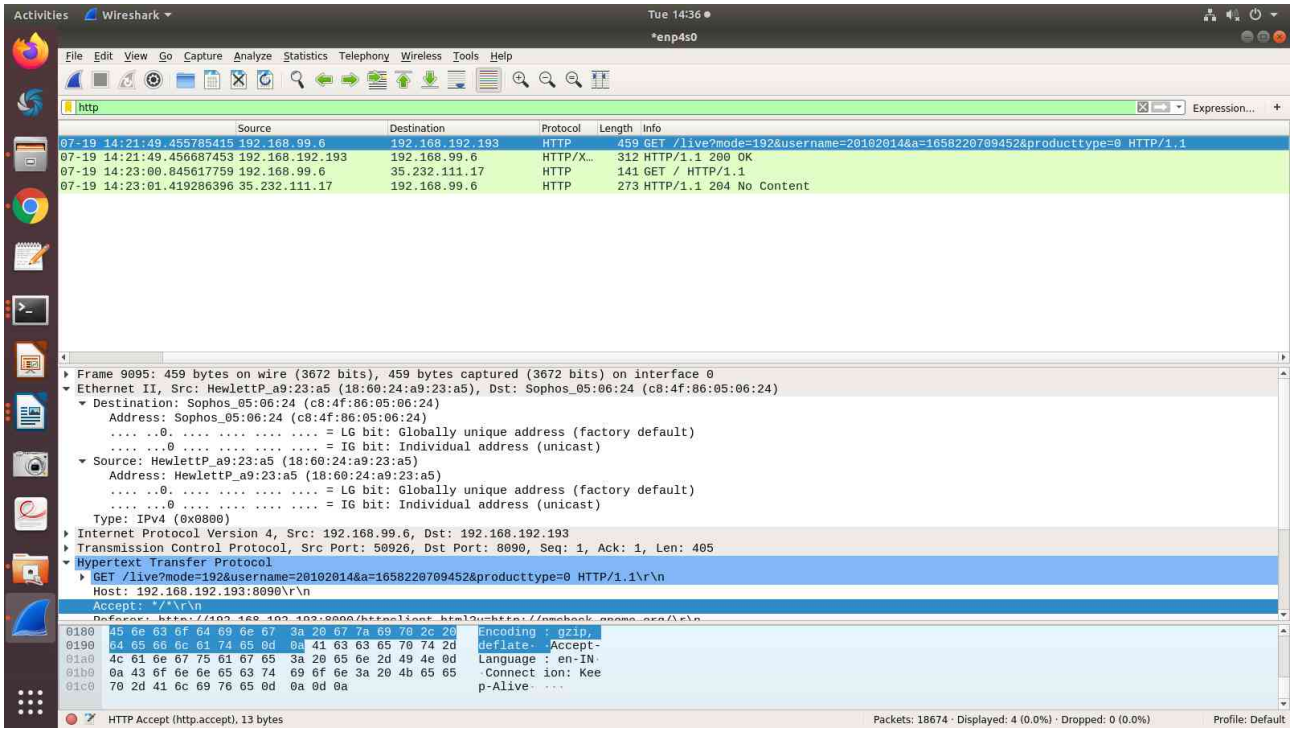
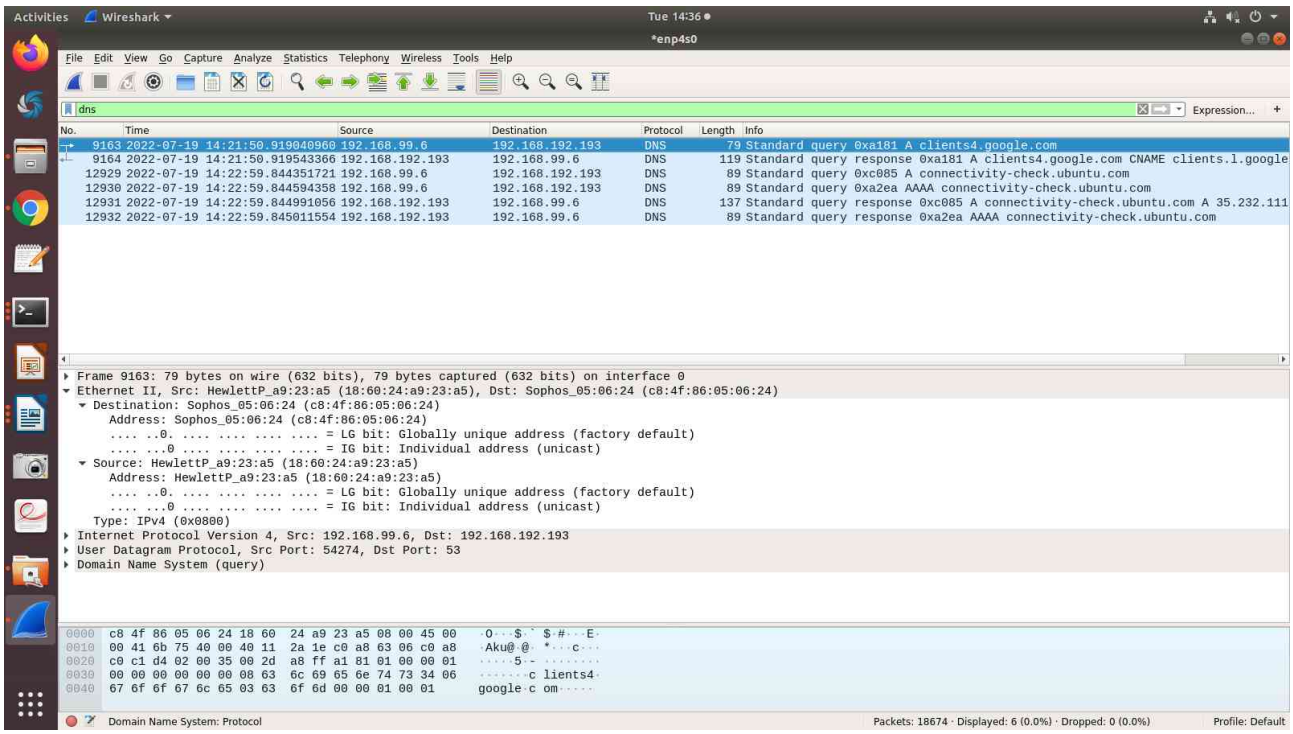
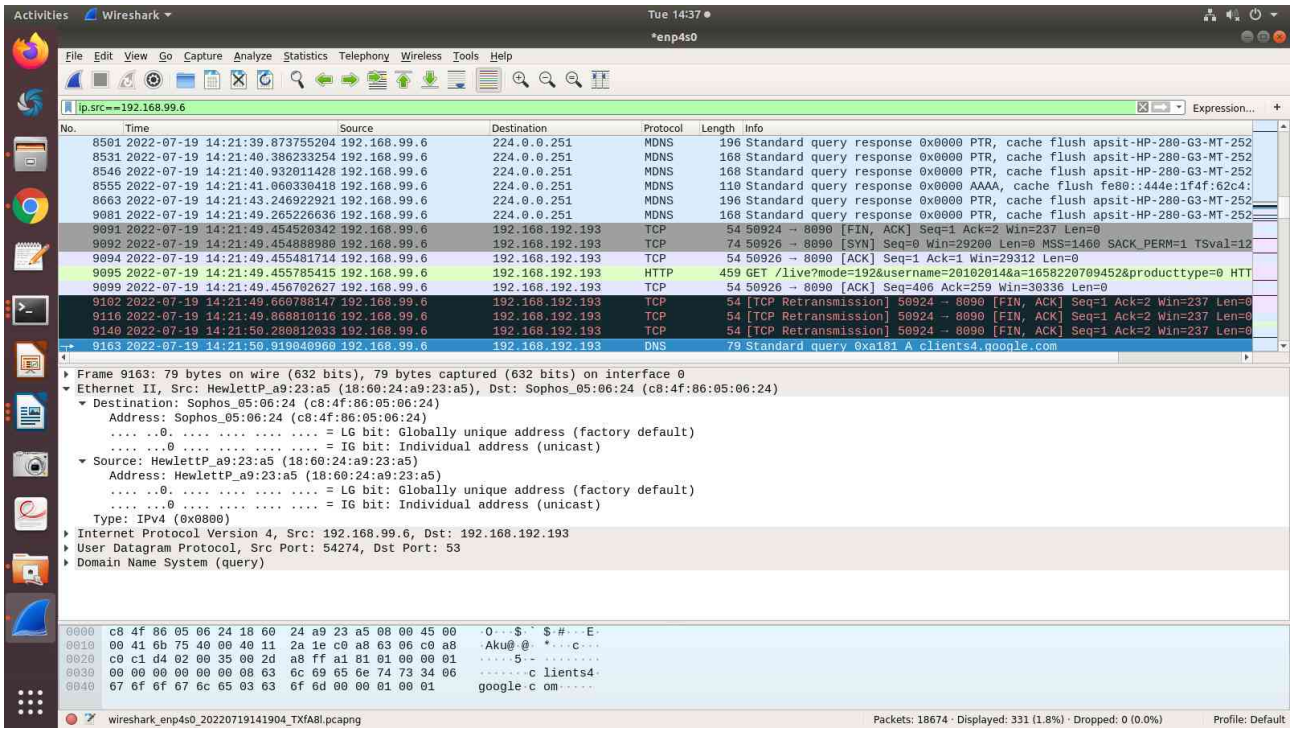
Name: Mokshada Sawant
Moodle Id: 20102041
Rollno: 23

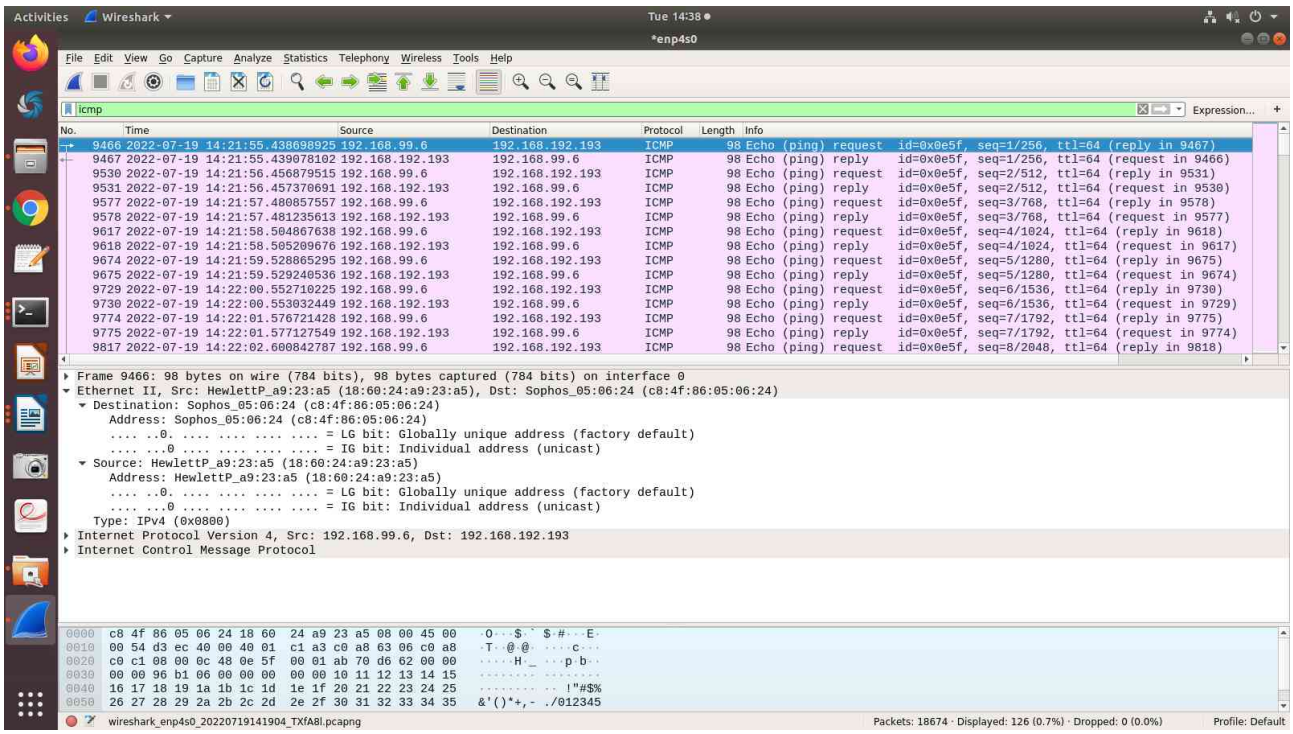
Experiment no. 2

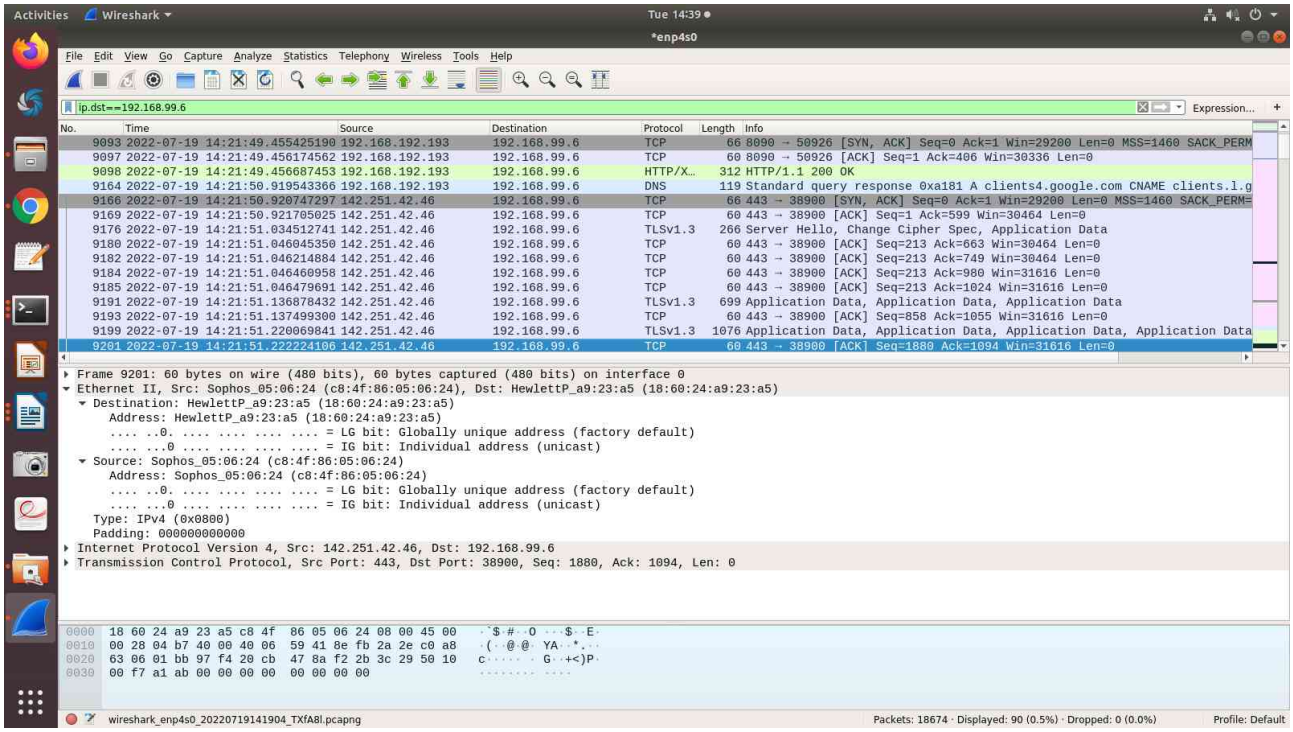
Aim: to study Wireshark packet analyser

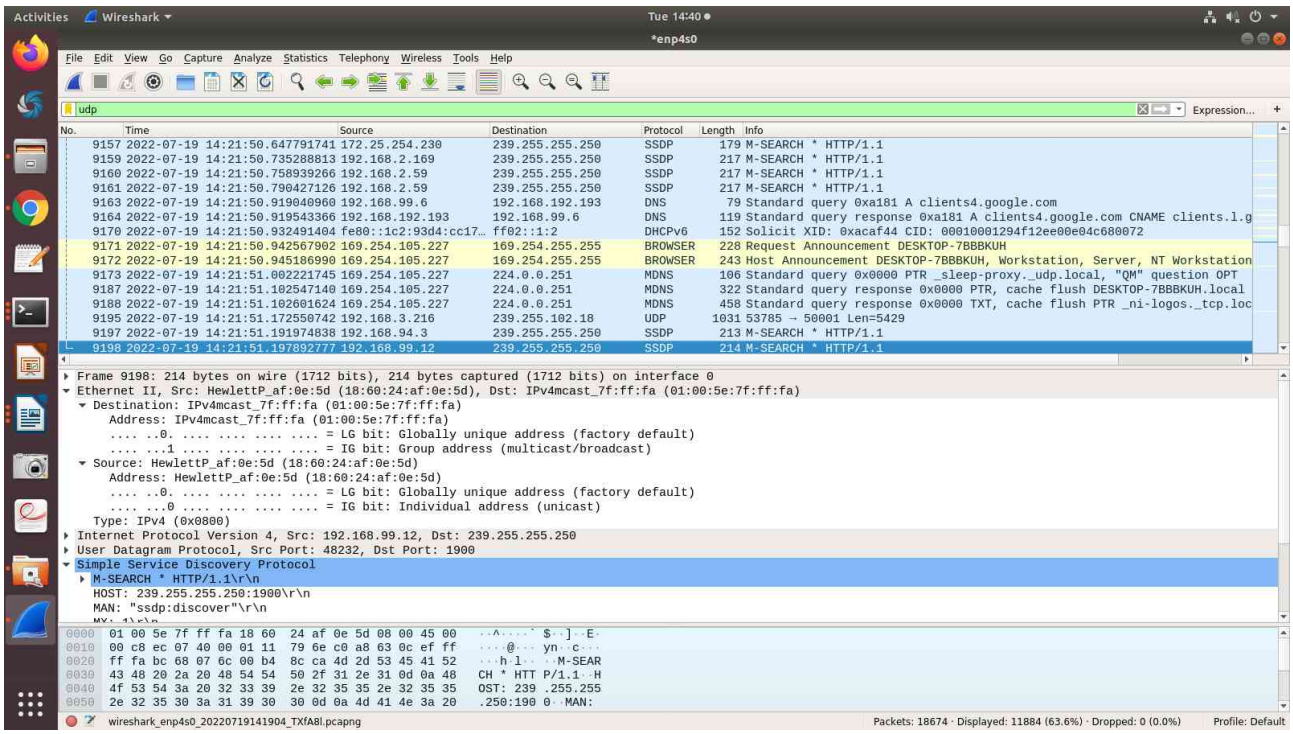



Activities
Wireshark
Tue 14:36
*enp4s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...
No. Time Source Destination Protocol Length Info
9163 2022-07-19 14:21:50.919040960 192.168.99.6 192.168.192.193 DNS 79 Standard query 0xa181 A clients4.google.com
9164 2022-07-19 14:21:50.919543366 192.168.192.193 192.168.99.6 DNS 119 Standard query response 0xa181 A clients4.google.com CNAME clients.l.google
12929 2022-07-19 14:22:59.844351721 192.168.99.6 192.168.192.193 DNS 89 Standard query 0xc085 A connectivity-check.ubuntu.com
12930 2022-07-19 14:22:59.844594358 192.168.99.6 192.168.192.193 DNS 89 Standard query 0xa2ea AAAA connectivity-check.ubuntu.com
12931 2022-07-19 14:22:59.844991056 192.168.192.193 192.168.99.6 DNS 137 Standard query response 0xc085 A connectivity-check.ubuntu.com A 35.232.111
12932 2022-07-19 14:22:59.845011554 192.168.192.193 192.168.99.6 DNS 89 Standard query response 0xa2ea AAAA connectivity-check.ubuntu.com
Frame 9163: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Ethernet II, Src: HewlettP_a9:23:a5 (18:60:24:a9:23:a5), Dst: Sophos_05:06:24 (c8:4f:86:05:06:24)
Destination: Sophos_05:06:24 (c8:4f:86:05:06:24)
Address: Sophos_05:06:24 (c8:4f:86:05:06:24)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: HewlettP_a9:23:a5 (18:60:24:a9:23:a5)
Address: HewlettP_a9:23:a5 (18:60:24:a9:23:a5)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.99.6, Dst: 192.168.192.193
User Datagram Protocol, Src Port: 54274, Dst Port: 53
Domain Name System (query)
0000 c8 4f 86 05 06 24 18 60 24 a9 23 a5 08 00 45 00 ·O···$·` $·#···E·
0010 00 41 6b 75 40 00 40 11 2a 1e c0 a8 63 06 c0 a8 ·Aku@·@· *···c···
0020 c0 c1 d4 02 00 35 00 2d a8 ff a1 81 01 00 00 01 ·····5·- ········
0030 00 00 00 00 00 00 08 63 6c 69 65 6e 74 73 34 06 ·······c lients4·
0040 67 6f 6f 67 6c 65 03 63 6f 6d 00 00 01 00 01 google·c om·····
Domain Name System: Protocol
Packets: 18674 · Displayed: 6 (0.0%) · Dropped: 0 (0.0%)
Profile: Default


Activities
Wireshark
Tue 14:37
*enp4s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src==192.168.99.6
Expression...
No. Time Source Destination Protocol Length Info
8501 2022-07-19 14:21:39.873755204 192.168.99.6 224.0.0.251 MDNS 196 Standard query response 0x0000 PTR, cache flush apsit-HP-280-G3-MT-252
8531 2022-07-19 14:21:40.386233254 192.168.99.6 224.0.0.251 MDNS 168 Standard query response 0x0000 PTR, cache flush apsit-HP-280-G3-MT-252
8546 2022-07-19 14:21:40.932011428 192.168.99.6 224.0.0.251 MDNS 168 Standard query response 0x0000 PTR, cache flush apsit-HP-280-G3-MT-252
8555 2022-07-19 14:21:41.060330418 192.168.99.6 224.0.0.251 MDNS 110 Standard query response 0x0000 AAAA, cache flush fe80::444e:1f4f:62c4:
8663 2022-07-19 14:21:43.246922921 192.168.99.6 224.0.0.251 MDNS 196 Standard query response 0x0000 PTR, cache flush apsit-HP-280-G3-MT-252
9081 2022-07-19 14:21:49.265226636 192.168.99.6 224.0.0.251 MDNS 168 Standard query response 0x0000 PTR, cache flush apsit-HP-280-G3-MT-252
9091 2022-07-19 14:21:49.454520342 192.168.99.6 192.168.192.193 TCP 54 50924 → 8090 [FIN, ACK] Seq=1 Ack=2 Win=237 Len=0
9092 2022-07-19 14:21:49.454888980 192.168.99.6 192.168.192.193 TCP 74 50926 → 8090 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=12
9094 2022-07-19 14:21:49.455481714 192.168.99.6 192.168.192.193 TCP 54 50926 → 8090 [ACK] Seq=1 Ack=1 Win=29312 Len=0
9095 2022-07-19 14:21:49.455785415 192.168.99.6 192.168.192.193 HTTP 459 GET /live?mode=192&username=20102014&a=1658220709452&producttype=0 HTT
9099 2022-07-19 14:21:49.456702627 192.168.99.6 192.168.192.193 TCP 54 50926 → 8090 [ACK] Seq=406 Ack=259 Win=30336 Len=0
9102 2022-07-19 14:21:49.660788147 192.168.99.6 192.168.192.193 TCP 54 [TCP Retransmission] 50924 → 8090 [FIN, ACK] Seq=1 Ack=2 Win=237 Len=0
9116 2022-07-19 14:21:49.868810116 192.168.99.6 192.168.192.193 TCP 54 [TCP Retransmission] 50924 → 8090 [FIN, ACK] Seq=1 Ack=2 Win=237 Len=0
9140 2022-07-19 14:21:50.280812033 192.168.99.6 192.168.192.193 TCP 54 [TCP Retransmission] 50924 → 8090 [FIN, ACK] Seq=1 Ack=2 Win=237 Len=0
9163 2022-07-19 14:21:50.919040960 192.168.99.6 192.168.192.193 DNS 79 Standard query 0xa181 A clients4.google.com
Frame 9163: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Ethernet II, Src: HewlettP_a9:23:a5 (18:60:24:a9:23:a5), Dst: Sophos_05:06:24 (c8:4f:86:05:06:24)
Destination: Sophos_05:06:24 (c8:4f:86:05:06:24)
Address: Sophos_05:06:24 (c8:4f:86:05:06:24)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: HewlettP_a9:23:a5 (18:60:24:a9:23:a5)
Address: HewlettP_a9:23:a5 (18:60:24:a9:23:a5)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.99.6, Dst: 192.168.192.193
User Datagram Protocol, Src Port: 54274, Dst Port: 53
Domain Name System (query)
0000 c8 4f 86 05 06 24 18 60 24 a9 23 a5 08 00 45 00 ·O···$·` $·#···E·
0010 00 41 6b 75 40 00 40 11 2a 1e c0 a8 63 06 c0 a8 ·Aku@·@· *···c···
0020 c0 c1 d4 02 00 35 00 2d a8 ff a1 81 01 00 00 01 ·····5·- ········
0030 00 00 00 00 00 00 08 63 6c 69 65 6e 74 73 34 06 ·······c lients4·
0040 67 6f 6f 67 6c 65 03 63 6f 6d 00 00 01 00 01 google·c om·····
wireshark_enp4s0_20220719141904_TXfA8l.pcapng
Packets: 18674 · Displayed: 331 (1.8%) · Dropped: 0 (0.0%)
Profile: Default


Activities
Wireshark
Tue 14:38
*enp4s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
No. Time Source Destination Protocol Length Info
9466 2022-07-19 14:21:55.438698925 192.168.99.6 192.168.192.193 ICMP 98 Echo (ping) request id=0x0e5f, seq=1/256, ttl=64 (reply in 9467)
9467 2022-07-19 14:21:55.439078102 192.168.192.193 192.168.99.6 ICMP 98 Echo (ping) reply id=0x0e5f, seq=1/256, ttl=64 (request in 9466)
9530 2022-07-19 14:21:56.456879515 192.168.99.6 192.168.192.193 ICMP 98 Echo (ping) request id=0x0e5f, seq=2/512, ttl=64 (reply in 9531)
9531 2022-07-19 14:21:56.457370691 192.168.192.193 192.168.99.6 ICMP 98 Echo (ping) reply id=0x0e5f, seq=2/512, ttl=64 (request in 9530)
9577 2022-07-19 14:21:57.480857557 192.168.99.6 192.168.192.193 ICMP 98 Echo (ping) request id=0x0e5f, seq=3/768, ttl=64 (reply in 9578)
9578 2022-07-19 14:21:57.481235613 192.168.192.193 192.168.99.6 ICMP 98 Echo (ping) reply id=0x0e5f, seq=3/768, ttl=64 (request in 9577)
9617 2022-07-19 14:21:58.504867638 192.168.99.6 192.168.192.193 ICMP 98 Echo (ping) request id=0x0e5f, seq=4/1024, ttl=64 (reply in 9618)
9618 2022-07-19 14:21:58.505209676 192.168.192.193 192.168.99.6 ICMP 98 Echo (ping) reply id=0x0e5f, seq=4/1024, ttl=64 (request in 9617)
9674 2022-07-19 14:21:59.528865295 192.168.99.6 192.168.192.193 ICMP 98 Echo (ping) request id=0x0e5f, seq=5/1280, ttl=64 (reply in 9675)
9675 2022-07-19 14:21:59.529240536 192.168.192.193 192.168.99.6 ICMP 98 Echo (ping) reply id=0x0e5f, seq=5/1280, ttl=64 (request in 9674)
9729 2022-07-19 14:22:00.552710225 192.168.99.6 192.168.192.193 ICMP 98 Echo (ping) request id=0x0e5f, seq=6/1536, ttl=64 (reply in 9730)
9730 2022-07-19 14:22:00.553032449 192.168.192.193 192.168.99.6 ICMP 98 Echo (ping) reply id=0x0e5f, seq=6/1536, ttl=64 (request in 9729)
9774 2022-07-19 14:22:01.576721428 192.168.99.6 192.168.192.193 ICMP 98 Echo (ping) request id=0x0e5f, seq=7/1792, ttl=64 (reply in 9775)
9775 2022-07-19 14:22:01.577127549 192.168.192.193 192.168.99.6 ICMP 98 Echo (ping) reply id=0x0e5f, seq=7/1792, ttl=64 (request in 9774)
9817 2022-07-19 14:22:02.600842787 192.168.99.6 192.168.192.193 ICMP 98 Echo (ping) request id=0x0e5f, seq=8/2048, ttl=64 (reply in 9818)
Frame 9466: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: HewlettP_a9:23:a5 (18:60:24:a9:23:a5), Dst: Sophos_05:06:24 (c8:4f:86:05:06:24)
Destination: Sophos_05:06:24 (c8:4f:86:05:06:24)
Address: Sophos_05:06:24 (c8:4f:86:05:06:24)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: HewlettP_a9:23:a5 (18:60:24:a9:23:a5)
Address: HewlettP_a9:23:a5 (18:60:24:a9:23:a5)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.99.6, Dst: 192.168.192.193
Internet Control Message Protocol
0000 c8 4f 86 05 06 24 18 60 24 a9 23 a5 08 00 45 00
0010 00 54 d3 ec 40 00 40 01 c1 a3 c0 a8 63 06 c0 a8
0020 c0 c1 08 00 0c 48 0e 5f 00 01 ab 70 d6 62 00 00
0030 00 00 96 b1 06 00 00 00 00 00 10 11 12 13 14 15
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
wireshark_enp4s0_20220719141904_TXfA8l.pcapng
Packets: 18674 · Displayed: 126 (0.7%) · Dropped: 0 (0.0%)
Profile: Default


Activities
Wireshark
Tue 14:39
*enp4s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst==192.168.99.6
Expression...
No. Time Source Destination Protocol Length Info
9093 2022-07-19 14:21:49.455425190 192.168.192.193 192.168.99.6 TCP 66 8090 → 50926 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM
9097 2022-07-19 14:21:49.456174562 192.168.192.193 192.168.99.6 TCP 60 8090 → 50926 [ACK] Seq=1 Ack=406 Win=30336 Len=0
9098 2022-07-19 14:21:49.456687453 192.168.192.193 192.168.99.6 HTTP/X… 312 HTTP/1.1 200 OK
9164 2022-07-19 14:21:50.919543366 192.168.192.193 192.168.99.6 DNS 119 Standard query response 0xa181 A clients4.google.com CNAME clients.l.g
9166 2022-07-19 14:21:50.920747297 142.251.42.46 192.168.99.6 TCP 66 443 → 38900 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=
9169 2022-07-19 14:21:50.921705025 142.251.42.46 192.168.99.6 TCP 60 443 → 38900 [ACK] Seq=1 Ack=599 Win=30464 Len=0
9176 2022-07-19 14:21:51.034512741 142.251.42.46 192.168.99.6 TLSv1.3 266 Server Hello, Change Cipher Spec, Application Data
9180 2022-07-19 14:21:51.046045350 142.251.42.46 192.168.99.6 TCP 60 443 → 38900 [ACK] Seq=213 Ack=663 Win=30464 Len=0
9182 2022-07-19 14:21:51.046214884 142.251.42.46 192.168.99.6 TCP 60 443 → 38900 [ACK] Seq=213 Ack=749 Win=30464 Len=0
9184 2022-07-19 14:21:51.046460958 142.251.42.46 192.168.99.6 TCP 60 443 → 38900 [ACK] Seq=213 Ack=980 Win=31616 Len=0
9185 2022-07-19 14:21:51.046479691 142.251.42.46 192.168.99.6 TCP 60 443 → 38900 [ACK] Seq=213 Ack=1024 Win=31616 Len=0
9191 2022-07-19 14:21:51.136878432 142.251.42.46 192.168.99.6 TLSv1.3 699 Application Data, Application Data, Application Data
9193 2022-07-19 14:21:51.137499300 142.251.42.46 192.168.99.6 TCP 60 443 → 38900 [ACK] Seq=858 Ack=1055 Win=31616 Len=0
9199 2022-07-19 14:21:51.220069841 142.251.42.46 192.168.99.6 TLSv1.3 1076 Application Data, Application Data, Application Data
9201 2022-07-19 14:21:51.222224106 142.251.42.46 192.168.99.6 TCP 60 443 → 38900 [ACK] Seq=1880 Ack=1094 Win=31616 Len=0
Frame 9201: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Sophos_05:06:24 (c8:4f:86:05:06:24), Dst: HewlettP_a9:23:a5 (18:60:24:a9:23:a5)
Destination: HewlettP_a9:23:a5 (18:60:24:a9:23:a5)
Address: HewlettP_a9:23:a5 (18:60:24:a9:23:a5)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Sophos_05:06:24 (c8:4f:86:05:06:24)
Address: Sophos_05:06:24 (c8:4f:86:05:06:24)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Padding: 000000000000
Internet Protocol Version 4, Src: 142.251.42.46, Dst: 192.168.99.6
Transmission Control Protocol, Src Port: 443, Dst Port: 38900, Seq: 1880, Ack: 1094, Len: 0
0000 18 60 24 a9 23 a5 c8 4f 86 05 06 24 08 00 45 00
0010 00 28 04 b7 40 00 40 06 59 41 8e fb 2a 2e c0 a8
0020 63 06 01 bb 97 f4 20 cb 47 8a f2 2b 3c 29 50 10
0030 00 f7 a1 ab 00 00 00 00 00 00 00 00
wireshark_enp4s0_20220719141904_TXfA8l.pcapng
Packets: 18674 · Displayed: 90 (0.5%) · Dropped: 0 (0.0%)
Profile: Default


Activities
Wireshark
Tue 14:40
*enp4s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
Expression...
No. Time Source Destination Protocol Length Info
9157 2022-07-19 14:21:50.647791741 172.25.254.230 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
9159 2022-07-19 14:21:50.735288813 192.168.2.169 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
9160 2022-07-19 14:21:50.758939266 192.168.2.59 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
9161 2022-07-19 14:21:50.790427126 192.168.2.59 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
9163 2022-07-19 14:21:50.919040960 192.168.99.6 192.168.192.193 DNS 79 Standard query 0xa181 A clients4.google.com
9164 2022-07-19 14:21:50.919543366 192.168.192.193 192.168.99.6 DNS 119 Standard query response 0xa181 A clients4.google.com CNAME clients.l.g
9170 2022-07-19 14:21:50.932491404 fe80::1c2:93d4:cc17… ff02::1:2 DHCPv6 152 Solicit XID: 0xacaf44 CID: 00010001294f12ee00e04c680072
9171 2022-07-19 14:21:50.942567902 169.254.105.227 169.254.255.255 BROWSER 228 Request Announcement DESKTOP-7BBBKUH
9172 2022-07-19 14:21:50.945186990 169.254.105.227 169.254.255.255 BROWSER 243 Host Announcement DESKTOP-7BBBKUH, Workstation, Server, NT Workstation
9173 2022-07-19 14:21:51.002221745 169.254.105.227 224.0.0.251 MDNS 106 Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question OPT
9187 2022-07-19 14:21:51.102547140 169.254.105.227 224.0.0.251 MDNS 322 Standard query response 0x0000 PTR, cache flush DESKTOP-7BBBKUH.local
9188 2022-07-19 14:21:51.102601624 169.254.105.227 224.0.0.251 MDNS 458 Standard query response 0x0000 TXT, cache flush PTR _ni-logos._tcp.loc
9195 2022-07-19 14:21:51.172550742 192.168.3.216 239.255.102.18 UDP 1031 53785 → 50001 Len=5429
9197 2022-07-19 14:21:51.191974838 192.168.94.3 239.255.255.250 SSDP 213 M-SEARCH * HTTP/1.1
9198 2022-07-19 14:21:51.197892777 192.168.99.12 239.255.255.250 SSDP 214 M-SEARCH * HTTP/1.1
Frame 9198: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0
Ethernet II, Src: HewlettP_af:0e:5d (18:60:24:af:0e:5d), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Destination: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Address: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
.... ..0. .... = LG bit: Globally unique address (factory default)
....1 .... = IG bit: Group address (multicast/broadcast)
Source: HewlettP_af:0e:5d (18:60:24:af:0e:5d)
Address: HewlettP_af:0e:5d (18:60:24:af:0e:5d)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.99.12, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 48232, Dst Port: 1900
Simple Service Discovery Protocol
M-SEARCH * HTTP/1.1\r\n
HOST: 239.255.255.250:1900\r\n
MAN: "ssdp:discover"\r\n
0000 01 00 5e 7f ff fa 18 60 24 af 0e 5d 08 00 45 00
0010 00 c8 ec 07 40 00 01 11 79 6e c0 a8 63 0c ef ff
0020 ff fa bc 68 07 6c 00 b4 8c ca 4d 2d 53 45 41 52
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20
wireshark_enp4s0_20220719141904_TXfA8l.pcapng
Packets: 18674 · Displayed: 11884 (63.6%) · Dropped: 0 (0.0%)
Profile: Default