

## EXPERIMENT -5

## AIM Experiments on Packet capture tool: Wireshark

## Packet Sniffer

- Sniffs messages being sent/received from/by your computer
- Store and display the contents of the various protocol fields in the messages
- Passive program
  - never sends packets itself
  - no packets addressed to it
  - receives a copy of all packets (sent/received)

## Packet Sniffer Structure Diagnostic Tools

- Tcpdump
  - E.g. `tcpdump -enx host 10.129.41.2 -w exe3.out`
- Wireshark
  - `wireshark -r exe3.out`

### Packet 1(ARP):

[illegible]

### Packet 2(TCP):

```

45 0.073250 172.16.53.104 172.16.53.137 TCP 66 60700 → 7600 [FIN, Seq=1046440] Len=0 HSI=1400 is=256 SACK_FIRH
141 0.133113 172.16.53.137 172.16.53.104 TCP 66 52183 → 7600 [ACK, Seq=1046440] Len=0 HSI=1400 is=256 SACK_FIRH
140 0.182338 172.16.53.104 172.16.53.137 TCP 66 7600 → 52183 [SYN, ACK, Seq=8 Ack=1, HSI=1400 is=256 SACK_FIRH]
149 0.182338 172.16.53.104 172.16.53.137 TCP 66 52183 → 7600 [ACK, Seq=8 Ack=1, HSI=1400 is=256 SACK_FIRH]
141 0.188347 172.16.53.91 172.16.53.60 MS-DOS 129 Handshake Message (Request)
149 0.188354 172.16.53.91 172.16.53.91 MS-DOS 129 Handshake Message (Reply)
151 0.188403 172.16.53.91 172.16.53.60 MS-DOS 97 Bitfield Message (has 34 of 384 pieces)
151 0.188475 172.16.53.91 172.16.53.91 MS-DOS 97 Bitfield Message (has 33 of 384 pieces)
152 0.188487 172.16.53.91 172.16.53.91 TCP 54 7600 → 52183 [FIN, ACK, Seq=1046440] Len=0 HSI=1400 is=256 SACK_FIRH
152 0.188516 172.16.53.91 172.16.53.60 TCP 66 52183 → 7600 [ACK, Seq=1046440] Len=0 HSI=1400 is=256 SACK_FIRH
154 0.188616 172.16.53.91 172.16.53.60 TCP 66 52183 → 7600 [FIN, ACK, Seq=1046440] Len=0 HSI=1400 is=256 SACK_FIRH
155 0.188565 172.16.53.91 172.16.53.91 TCP 54 7600 → 52183 [ACK, Seq=120 Ack=120] HSI=207604 Len=0
156 0.188574 172.16.53.91 172.16.53.60 TCP 54 59624 → 7600 [ACK, Seq=76 Ack=76] HSI=1400 is=256 SACK_FIRH
280 0.238797 172.16.52.58 172.16.52.58 TCP 66 7600 → 59624 [ACK, Seq=8 Ack=8, HSI=1400 is=256 SACK_FIRH]
282 0.238798 172.16.52.58 172.16.52.58 TCP 54 59624 → 7600 [ACK, Seq=76 Ack=76] HSI=1400 is=256 SACK_FIRH
282 0.239139 172.16.53.104 172.16.52.58 MS-DOS 129 Handshake Message (Request)
284 0.240045 172.16.52.58 172.16.52.58 MS-DOS 129 Handshake Message (Reply)
284 0.240045 172.16.52.58 172.16.52.58 TCP 66 7600 → 59624 [FIN, ACK, Seq=76 Ack=76] HSI=207620 Len=0
280 0.240075 172.16.53.104 172.16.52.58 TCP 54 59624 → 7600 [ACK, Seq=76 Ack=76] HSI=207620 Len=0
280 0.240088 172.16.53.104 172.16.52.58 TCP 54 59624 → 7600 [FIN, ACK, Seq=76 Ack=76] HSI=207620 Len=0
280 0.240162 172.16.52.58 172.16.53.60 TCP 66 7600 → 59624 [ACK, Seq=77 Ack=77] HSI=207720 Len=0
282 0.279286 172.16.53.104 172.16.53.137 TCP 66 [TCP Retransmission] 60700 → 7600 [SYN, Seq=1046440] Len=0 HSI=1400 is=256 SACK_FIRH
535 0.304166 172.16.53.104 172.16.53.137 TCP 66 [TCP Retransmission] 60700 → 7600 [SYN, Seq=1046440] Len=0 HSI=1400 is=256 SACK_FIRH
1090 13.497578 172.16.53.104 172.251.175.138 150.0.0.0 application Data
1102 13.133215 172.251.175.188 172.16.53.60 TCP 66 5228 → 50874 [ACK, Seq=1 Ack=2] HSI=200 Len=0
1102 13.133215 172.251.175.188 172.16.53.60 0.0.0.0.0.0 application Data

```

### Packet 3(MDNS):

No.	Time	Source	Destination	Protocol	Length	Info
2153	19.423169	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	76	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2154	19.423169	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	96	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2155	19.423777	172.16.53.191	224.0.0.251	ICMPv6	76	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2156	19.423777	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	96	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2157	19.424382	172.16.53.191	224.0.0.251	ICMPv6	76	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2158	19.424382	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	96	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2159	19.424782	172.16.53.191	224.0.0.251	ICMPv6	76	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2160	19.425091	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	96	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2161	19.425267	172.16.53.191	224.0.0.251	ICMPv6	76	Standard query 0x0000 AAAA h0c422178.local, "Q" question
2162	19.425750	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	96	Standard query 0x0000 AAAA h0c422178.local, "Q" question
2163	19.425750	172.16.53.191	224.0.0.251	ICMPv6	76	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2164	19.426071	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	96	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2165	19.426470	172.16.53.191	224.0.0.251	ICMPv6	76	Standard query 0x0000 AAAA h0c422201.local, "Q" question
2166	19.426470	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	96	Standard query 0x0000 AAAA h0c422201.local, "Q" question
2167	19.426791	172.16.53.191	224.0.0.251	ICMPv6	76	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2168	19.426791	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	96	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2169	19.427079	172.16.53.191	224.0.0.251	ICMPv6	76	Standard query 0x0000 AAAA h0c422201.local, "Q" question
2170	19.427551	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	96	Standard query 0x0000 AAAA h0c422201.local, "Q" question
2171	19.427547	172.16.53.191	224.0.0.251	ICMPv6	76	Standard query 0x0000 AAAA h0c422178.local, "Q" question
2172	19.428066	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	96	Standard query 0x0000 AAAA h0c422178.local, "Q" question
2173	19.428100	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	96	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2174	19.428645	172.16.53.191	224.0.0.251	ICMPv6	76	Standard query 0x0000 AAAA h0c422183.local, "Q" question
2175	19.428823	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	96	Standard query 0x0000 AAAA h0c422183.local, "Q" question
2176	19.429489	172.16.53.191	224.0.0.251	ICMPv6	76	Standard query 0x0000 AAAA h0c422166.local, "Q" question
2177	19.429489	fe80::83be:5045:542c::ff02:1b	224.0.0.251	ICMPv6	96	Standard query 0x0000 AAAA h0c422166.local, "Q" question
* Frame 20: 28 bytes on wire (608 bits), 85 bytes captured (608 bits) on interface Vbice\NPF_{7FA435C5-9403-410F-BD95-E06B228E78A3}, Ethernet II, Src: E1158d904c315e1efc (88aae1dd15e1efc), Dst: Trunkcast_Fc (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: 5522, Dst Port: 5555						
* Multicast Domain Name System (query)						

## Packet 4(QUIC):

No.	Time	Source	Destination	Protocol	Length	Info
4474	35.188623	172.16.53.68	142.250.195.78	QUIC	1876	Protected Payload (QUIC), DCID=elbe5d79e458d885
4475	35.188885	172.16.53.68	142.250.195.78	QUIC	888	Protected Payload (QUIC), DCID=elbe5d79e458d885
4476	35.189248	142.250.195.78	172.16.53.68	QUIC	162	Protected Payload (QUIC)
4477	35.189589	172.16.53.68	142.250.195.78	QUIC	75	Protected Payload (QUIC), DCID=elbe5d79e458d885
4478	35.190889	142.250.195.78	172.16.53.68	QUIC	67	Protected Payload (QUIC)
4479	35.190889	142.250.195.78	172.16.53.68	QUIC	67	Protected Payload (QUIC)
4481	35.191579	142.250.195.78	172.16.53.68	QUIC	71	Protected Payload (QUIC)
4482	35.191579	142.250.195.78	172.16.53.68	QUIC	67	Protected Payload (QUIC)
4483	35.192052	172.16.53.68	142.250.195.78	QUIC	75	Protected Payload (QUIC), DCID=elbe5d79e458d885
4485	35.193987	142.250.195.78	172.16.53.68	QUIC	71	Protected Payload (QUIC)
4486	35.193987	142.250.195.78	172.16.53.68	QUIC	67	Protected Payload (QUIC)
4487	35.193987	142.250.195.78	172.16.53.68	QUIC	71	Protected Payload (QUIC)
4488	35.194487	142.250.195.78	172.16.53.68	QUIC	71	Protected Payload (QUIC)
4489	35.194925	172.16.53.68	142.250.195.78	QUIC	75	Protected Payload (QUIC), DCID=elbe5d79e458d885
4491	35.308880	142.250.195.78	172.16.53.68	QUIC	884	Protected Payload (QUIC)
4492	35.308570	142.250.195.78	172.16.53.68	QUIC	662	Protected Payload (QUIC)
4493	35.308100	142.250.195.78	172.16.53.68	QUIC	200	Protected Payload (QUIC)
4494	35.308362	172.16.53.68	142.250.195.78	QUIC	80	Protected Payload (QUIC), DCID=elbe5d79e458d885
4495	35.308526	142.250.195.78	172.16.53.68	QUIC	196	Protected Payload (QUIC)
4496	35.308416	172.16.53.68	142.250.195.78	QUIC	75	Protected Payload (QUIC), DCID=elbe5d79e458d885
4500	35.311835	142.250.195.78	172.16.53.68	QUIC	66	Protected Payload (QUIC)
4505	35.361532	142.250.195.78	172.16.53.68	QUIC	664	Protected Payload (QUIC)
4506	35.361394	142.250.195.78	172.16.53.68	QUIC	70	Protected Payload (QUIC), DCID=elbe5d79e458d885
4507	35.361584	172.16.53.68	142.250.195.78	QUIC	77	Protected Payload (QUIC)
4509	35.361681	142.250.195.78	172.16.53.68	QUIC	60	Protected Payload (QUIC)
* Frame 182: 1292 bytes on wire (40336 bits), 1292 bytes captured (40336 bits) on interface Vbice\NPF_{7FA435C5-9403-410F-BD95-E06B228E78A3}, Ethernet II, Src: E1158d904c315e1efc (88aae1dd15e1efc), Dst: Sophos_cf1be13e (7c5a1c1cf1be13e)						
* Internet Protocol Version 4, Src: 172.16.53.68, Dst: 142.250.183.227						
* User Datagram Protocol, Src Port: 56087, Dst Port: 443						
* QUIC 1E7F						

## Packet 5(LLMNR):

No.	Time	Source	Destination	Protocol	Length	Info
291	3.728093	172.16.53.191	224.0.0.252	LLMNR	70	Standard query 0x3e4c A h0c422142
292	3.730214	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3e4c A h0c422142
293	3.738214	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3e0b AAAA h0c422142
294	3.738085	172.16.53.191	224.0.0.252	LLMNR	70	Standard query 0x3e0b AAAA h0c422142
300	3.732288	172.16.53.191	224.0.0.252	LLMNR	70	Standard query 0x3e04 A h0c422166
304	3.732280	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3e04 A h0c422166
306	3.732772	172.16.53.191	224.0.0.252	LLMNR	70	Standard query 0x3f0b AAAA h0c422166
307	3.732772	172.16.53.191	224.0.0.252	LLMNR	70	Standard query 0x3f0b AAAA h0c422166
308	3.732778	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3f0b AAAA h0c422166
309	3.732778	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3f0b AAAA h0c422166
312	3.733325	172.16.53.191	224.0.0.252	LLMNR	70	Standard query 0x3f0c AAAA h0c422183
313	3.733382	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3f0c AAAA h0c422183
314	3.733382	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3f0c AAAA h0c422183
317	3.733953	172.16.53.191	224.0.0.252	LLMNR	70	Standard query 0x3e03 A h0c422201
319	3.733754	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3e03 A h0c422201
321	3.733954	172.16.53.191	224.0.0.252	LLMNR	70	Standard query 0x3e15 AAAA h0c422201
332	3.730780	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3e95 A h0c422178
333	3.730683	172.16.53.191	224.0.0.252	LLMNR	70	Standard query 0x3e95 A h0c422178
335	3.732759	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3e0f AAAA h0c422178
336	3.733124	172.16.53.191	224.0.0.252	LLMNR	70	Standard query 0x3e0f AAAA h0c422178
364	4.143183	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3e4c A h0c422142
366	4.143183	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3e4c A h0c422142
367	4.143183	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3e0b AAAA h0c422166
368	4.143183	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3f0b AAAA h0c422166
371	4.143183	fe80::83be:5045:542c::ff02:1b	224.0.0.252	LLMNR	90	Standard query 0x3e04 A h0c422166
* Frame 291: 70 bytes on wire (1680 bits), 70 bytes captured (1680 bits) on interface Vbice\NPF_{7FA435C5-9403-410F-BD95-E06B228E78A3}, Ethernet II, Src: E1158d904c315e1efc (88aae1dd15e1efc), Dst: Trunkcast_Fc (01:00:5e:00:00:00)						
* Internet Protocol Version 4, Src: 172.16.53.191, Dst: 224.0.0.252						
* User Datagram Protocol, Src Port: 56272, Dst Port: 5555						
* Link-local Multicast Name Resolution (query)						

## RESULT: -

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

