

CNS: EXPERIMENT - 8

Aim:

Study of packet sniffer tools Wireshark :-

- a. Observer performance in promiscuous as well as non-promiscuous mode.
- b. Show the packets can be traced based on different filters
Port Filters, Address Filters, Protocol Filters, String Filters

Theory:

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Applications of wireshark:-

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- QA engineers use it to verify network applications
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

OUTPUT

Promiscuous Mode:

The screenshot shows Wireshark in Promiscuous Mode capturing traffic on the Ethernet II interface. The packet list displays various protocols including LLNMR, MDNS, and ARP. The packet details pane shows the structure of a frame, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Multicast Domain Name System (query). The packet bytes pane shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|-----------|------------------------|-------------|----------|--------|---|
| 74298 | 93.264120 | fe80::37c4:1265:a27... | ff02::1:3 | LLNMR | 95 | Standard query 0x21b1 AAAA desktop-13mq5is |
| 74299 | 93.264120 | 192.168.45.164 | 224.0.0.252 | LLNMR | 75 | Standard query 0xf0ca A desktop-13mq5is |
| 74300 | 93.264120 | 192.168.45.164 | 224.0.0.252 | LLNMR | 75 | Standard query 0x21b1 AAAA desktop-13mq5is |
| 74301 | 93.264195 | 192.168.45.164 | 224.0.0.251 | MDNS | 81 | Standard query 0x0000 A desktop-13mq5is.local, "QM" question |
| 74302 | 93.264835 | fe80::37c4:1265:a27... | ff02::fb | MDNS | 101 | Standard query 0x0000 A desktop-13mq5is.local, "QM" question |
| 74303 | 93.264851 | 192.168.41.190 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 74304 | 93.265414 | fe80::941c:c745:76b... | ff02::fb | MDNS | 74 | Standard query response 0x0000 |
| 74305 | 93.265660 | 192.168.45.164 | 224.0.0.251 | MDNS | 81 | Standard query 0x0000 AAAA desktop-13mq5is.local, "QU" question |
| 74306 | 93.265897 | 192.168.45.164 | 224.0.0.251 | MDNS | 81 | Standard query 0x0000 A desktop-13mq5is.local, "QM" question |
| 74307 | 93.266314 | fe80::37c4:1265:a27... | ff02::fb | MDNS | 101 | Standard query 0x0000 A desktop-13mq5is.local, "QM" question |
| 74308 | 93.266591 | 192.168.41.190 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 74309 | 93.266591 | 192.168.41.190 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 74310 | 93.266775 | 192.168.45.164 | 224.0.0.251 | MDNS | 81 | Standard query 0x0000 AAAA desktop-13mq5is.local, "QU" question |
| 74311 | 93.266810 | fe80::941c:c745:76b... | ff02::fb | MDNS | 74 | Standard query response 0x0000 |
| 74312 | 93.267218 | fe80::37c4:1265:a27... | ff02::fb | MDNS | 101 | Standard query 0x0000 AAAA desktop-13mq5is.local, "QU" question |
| 74313 | 93.267494 | 192.168.41.190 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 74314 | 93.267670 | fe80::37c4:1265:a27... | ff02::fb | MDNS | 101 | Standard query 0x0000 AAAA desktop-13mq5is.local, "QU" question |
| 74315 | 93.267942 | fe80::941c:c745:76b... | ff02::fb | MDNS | 74 | Standard query response 0x0000 |
| 74316 | 93.268220 | fe80::941c:c745:76b... | ff02::fb | MDNS | 74 | Standard query response 0x0000 |
| 74317 | 93.293744 | HonHaiPr_86:49:81 | Broadcast | ARP | 60 | Who has 192.168.32.20? Tell 192.168.33.77 |

> Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 10
> Ethernet II, Src: HonHaiPr_8d:20:d7 (f4:6b:8c:8d:20:d7), Dst: IPv4mcast_fb (01:00:00:00:00:00)
> Internet Protocol Version 4, Src: 10.3.3.1, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)

Ethernet: <live capture in progress> | Packets: 74317 · Displayed: 74317 (100.0%) | Profile: Default

Non Promiscuous Mode:

The screenshot shows Wireshark in Non Promiscuous Mode capturing traffic on the Ethernet II interface. The packet list displays various protocols including MDNS, ARP, and LLNMR. The packet details pane shows the structure of a frame, including Ethernet II, Address Resolution Protocol, and Multicast Domain Name System (query). The packet bytes pane shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|----------|-------------------|-------------|----------|--------|---|
| 1622 | 7.842564 | 192.168.41.190 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 1623 | 7.843254 | 192.168.45.164 | 224.0.0.251 | MDNS | 81 | Standard query 0x0000 A desktop-13mq5is.local, "QM" question |
| 1624 | 7.843974 | 192.168.41.190 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 1625 | 7.851087 | HonHaiPr_8d:20:83 | Broadcast | ARP | 60 | Who has 192.168.32.20? Tell 192.168.47.5 |
| 1626 | 7.851280 | 192.168.42.71 | 224.0.0.252 | LLNMR | 69 | Standard query 0x606d AAAA extc410-1 |
| 1627 | 7.851280 | 192.168.42.71 | 224.0.0.252 | LLNMR | 69 | Standard query 0xea30 A extc410-1 |
| 1628 | 7.853902 | 192.168.45.208 | 224.0.0.251 | MDNS | 429 | Standard query response 0x0000 PTR DESKTOP-8DHG11A._dosvc._tcp.local SRV 0 0 7680 DESKTP... |
| 1629 | 7.854307 | 192.168.45.208 | 224.0.0.251 | MDNS | 365 | Standard query response 0x0000 SRV 0 0 7680 DESKTOP-8DHG11A.local TXT A 192.168.45.208 ... |
| 1630 | 7.862003 | 192.168.32.193 | 224.0.0.251 | MDNS | 298 | Standard query response 0x0000 PTR DESKTOP-DNDJ502._dosvc._tcp.local SRV 0 0 7680 DESKTP... |
| 1631 | 7.862651 | 192.168.32.193 | 224.0.0.251 | MDNS | 93 | Standard query 0x0000 ANY DESKTOP-DNDJ502._dosvc._tcp.local, "QM" question |
| 1632 | 7.863501 | 192.168.41.190 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 1633 | 7.868593 | HonHaiPr_86:45:64 | Broadcast | ARP | 60 | Who has 192.168.37.218? Tell 192.168.44.72 |
| 1634 | 7.872433 | HonHaiPr_86:4d:06 | Broadcast | ARP | 60 | Who has 192.168.37.143? Tell 192.168.46.119 |
| 1635 | 7.882312 | HonHaiPr_8b:3a:ab | Broadcast | ARP | 60 | Who has 192.168.32.170? Tell 192.168.42.71 |
| 1636 | 7.882312 | HonHaiPr_8b:3a:ab | Broadcast | ARP | 60 | Who has 192.168.33.107? Tell 192.168.42.71 |
| 1637 | 7.883050 | HonHaiPr_8b:3a:ab | Broadcast | ARP | 60 | Who has 192.168.46.244? Tell 192.168.42.71 |
| 1638 | 7.896158 | Dell_22:8e:e0 | Broadcast | ARP | 60 | Who has 192.168.32.20? Tell 192.168.47.169 |
| 1639 | 7.899630 | Sophos_fc:00:05 | Broadcast | ARP | 60 | Who has 192.168.32.71? Tell 192.168.32.1 |
| 1640 | 7.904592 | HonHaiPr_86:4d:d8 | Broadcast | ARP | 60 | Who has 192.168.32.20? Tell 192.168.33.136 |
| 1641 | 7.935144 | HonHaiPr_86:49:50 | Broadcast | ARP | 60 | Who has 192.168.38.93? Tell 192.168.46.218 |
| 1642 | 7.943504 | HonHaiPr_84:00:d8 | Broadcast | ARP | 60 | Who has 192.168.32.20? Tell 192.168.44.102 |

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 10
> Ethernet II, Src: HonHaiPr_86:45:2d (f4:6b:8c:86:45:2d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

Ethernet: <live capture in progress> | Packets: 1737 · Displayed: 1737 (100.0%) | Profile: Default

Port Filters:

tcp.port ≥ 1024 && tcp.port ≤ 65535

Wireshark packet capture showing a filtered list of TCP connections. The filter is **tcp.port ≥ 1024 && tcp.port ≤ 65535**. The packet list shows various TCP segments, including a spurious retransmission and a duplicate ACK. The packet details pane shows the structure of a TCP segment, including the header and application data.

Address Filter:

ip.addr = 142.251.42.68

Wireshark packet capture showing a filtered list of packets to and from 142.251.42.68. The filter is **ip.addr == 142.251.42.68**. The packet list shows various protocols, including TCP, TLS, and ICMP. The packet details pane shows the structure of a TCP segment, including the header and application data.

Protocol Filters:

udp

Wireshark interface showing a filter 'udp' applied. The packet list displays various MDNS and BROWSER messages. The packet details pane shows the structure of a Multicast Domain Name System (response) packet.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---------|------------|------------------------|----------------|----------|--------|--|
| 4205... | 364.272211 | fe80::941c:c745:76b... | ff02::fb | MDNS | 74 | Standard query response 0x0000 |
| 4205... | 364.272623 | 192.168.41.190 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 4205... | 364.272623 | fe80::941c:c745:76b... | ff02::fb | MDNS | 74 | Standard query response 0x0000 |
| 4205... | 364.272807 | 192.168.41.213 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 4205... | 364.272807 | fe80::a0ba:bdd6:f36... | ff02::fb | MDNS | 74 | Standard query response 0x0000 |
| 4205... | 364.301097 | 192.168.46.179 | 192.168.47.255 | BROWSER | 243 | Host Announcement AIDS211-7, Workstation, Server, SQL Server, NT Workstation |
| 4205... | 364.302916 | 192.168.34.145 | 224.0.0.251 | MDNS | 81 | Standard query 0x0000 A desktop-d3eggf6.local, "QM" question |
| 4205... | 364.303068 | 192.168.46.151 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 4205... | 364.303068 | 192.168.41.213 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 4205... | 364.303564 | fe80::d3ef:a563:fec... | ff02::fb | MDNS | 101 | Standard query 0x0000 A desktop-d3eggf6.local, "QM" question |
| 4205... | 364.303564 | 192.168.41.190 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 4205... | 364.303855 | fe80::941c:c745:76b... | ff02::fb | MDNS | 74 | Standard query response 0x0000 |
| 4205... | 364.303864 | fe80::a0ba:bdd6:f36... | ff02::fb | MDNS | 74 | Standard query response 0x0000 |
| 4205... | 364.304190 | 192.168.34.145 | 224.0.0.251 | MDNS | 81 | Standard query 0x0000 AAAA desktop-d3eggf6.local, "QM" question |
| 4205... | 364.304247 | 192.168.46.151 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 4205... | 364.304531 | 192.168.41.190 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 4205... | 364.304552 | fe80::d3ef:a563:fec... | ff02::fb | MDNS | 101 | Standard query 0x0000 AAAA desktop-d3eggf6.local, "QM" question |
| 4205... | 364.304873 | 192.168.41.213 | 224.0.0.251 | MDNS | 60 | Standard query response 0x0000 |
| 4205... | 364.304991 | fe80::941c:c745:76b... | ff02::fb | MDNS | 74 | Standard query response 0x0000 |
| 4205... | 364.306028 | fe80::a0ba:bdd6:f36... | ff02::fb | MDNS | 74 | Standard query response 0x0000 |

Frame 17408: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface...
Ethernet II, Src: Dell_a9:98:af (e4:54:e8:a9:98:af), Dst: IPv6mcast_fb (33:33:00:00:00:00)
Internet Protocol Version 6, Src: fe80::6585:946d:ab35:54a4, Dst: ff02::fb
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (response)

String Filter:

tcp contains "HTTP"

Wireshark interface showing a filter 'tcp contains HTTP' applied. The packet list displays various TCP segments. The packet details pane shows the structure of a TCP segment of a reassembled PDU.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|-----------|----------------|----------------|----------|--------|--|
| 8544 | 3.410679 | 202.94.162.202 | 192.168.37.241 | TCP | 1514 | 80 → 49874 [ACK] Seq=1 Ack=1 Win=254 Len=1460 [TCP segment of a reassembled PDU] |
| 11057 | 6.787383 | 202.94.162.202 | 192.168.37.241 | TCP | 1514 | 80 → 49874 [ACK] Seq=11473 Ack=519 Win=262 Len=1460 [TCP segment of a reassembled PDU] |
| 12420 | 7.918049 | 202.94.162.202 | 192.168.37.241 | TCP | 1514 | 80 → 49874 [ACK] Seq=27997 Ack=1037 Win=270 Len=1460 [TCP segment of a reassembled PDU] |
| 13953 | 9.055668 | 202.94.162.202 | 192.168.37.241 | TCP | 1514 | 80 → 49874 [ACK] Seq=39091 Ack=1555 Win=279 Len=1460 [TCP segment of a reassembled PDU] |
| 18009 | 11.320875 | 202.94.162.202 | 192.168.37.241 | TCP | 1514 | 80 → 49874 [ACK] Seq=60716 Ack=2074 Win=287 Len=1460 [TCP segment of a reassembled PDU] |
| 19512 | 12.449778 | 202.94.162.202 | 192.168.37.241 | TCP | 1514 | 80 → 49874 [ACK] Seq=108050 Ack=2594 Win=296 Len=1460 [TCP segment of a reassembled PDU] |
| 21343 | 13.573140 | 202.94.162.202 | 192.168.37.241 | TCP | 1514 | 80 → 49874 [ACK] Seq=191324 Ack=3114 Win=304 Len=1460 [TCP segment of a reassembled PDU] |
| 21977 | 14.693950 | 202.94.162.202 | 192.168.37.241 | TCP | 1514 | 80 → 49874 [ACK] Seq=336862 Ack=3634 Win=312 Len=1460 [TCP segment of a reassembled PDU] |
| 22721 | 15.819029 | 202.94.162.202 | 192.168.37.241 | TCP | 1514 | 80 → 49874 [ACK] Seq=682947 Ack=4155 Win=321 Len=1460 [TCP segment of a reassembled PDU] |
| 23932 | 16.931075 | 202.94.162.202 | 192.168.37.241 | TCP | 1514 | 80 → 49874 [ACK] Seq=1443491 Ack=4677 Win=329 Len=1460 [TCP segment of a reassembled PDU] |
| 26285 | 18.055327 | 202.94.162.202 | 192.168.37.241 | TCP | 1514 | 80 → 49874 [ACK] Seq=2948407 Ack=5199 Win=337 Len=1460 [TCP segment of a reassembled PDU] |
| 27837 | 19.182113 | 202.94.162.202 | 192.168.37.241 | TCP | 1514 | 80 → 49874 [ACK] Seq=5895636 Ack=5722 Win=346 Len=1460 [TCP segment of a reassembled PDU] |
| 30092 | 20.313126 | 202.94.162.202 | 192.168.37.241 | TCP | 1514 | 80 → 49874 [ACK] Seq=11776420 Ack=6246 Win=354 Len=1460 [TCP segment of a reassembled PDU] |
| 31391 | 20.933168 | 34.104.35.123 | 192.168.37.241 | TCP | 743 | 80 → 49785 [PSH, ACK] Seq=1 Ack=1 Win=329 Len=689 [TCP segment of a reassembled PDU] |
| 31608 | 21.347981 | 199.232.46.172 | 192.168.37.241 | HTTP | 486 | HTTP/1.1 304 Not Modified |
| 31729 | 21.437197 | 199.232.46.172 | 192.168.37.241 | TCP | 1514 | 80 → 49886 [ACK] Seq=433 Ack=479 Win=31360 Len=1460 [TCP segment of a reassembled PDU] |
| 35052 | 25.010482 | 34.104.35.123 | 192.168.37.241 | TCP | 1514 | 80 → 49785 [ACK] Seq=690 Ack=333 Win=337 Len=1460 [TCP segment of a reassembled PDU] |
| 38303 | 28.649387 | 199.232.46.172 | 192.168.37.241 | TCP | 1514 | 80 → 49893 [ACK] Seq=1 Ack=197 Win=30336 Len=1460 [TCP segment of a reassembled PDU] |
| 38469 | 29.071176 | 34.104.35.123 | 192.168.37.241 | TCP | 1514 | 80 → 49785 [ACK] Seq=7145 Ack=669 Win=346 Len=1460 [TCP segment of a reassembled PDU] |
| 40208 | 31.116660 | 34.104.35.123 | 192.168.37.241 | TCP | 1514 | 80 → 49785 [ACK] Seq=16980 Ack=1006 Win=354 Len=1460 [TCP segment of a reassembled PDU] |

Frame 13953: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on...
Ethernet II, Src: Sophos_fc:00:05 (c8:4f:86:fc:00:05), Dst: Dell_ad:1b:fd (8c:ec:4...)
Internet Protocol Version 4, Src: 202.94.162.202, Dst: 192.168.37.241
Transmission Control Protocol, Src Port: 80, Dst Port: 49874, Seq: 39091, Ack: 155...