Experiment-5

Wireshark

AIM: Experiments on Packet capture tool

Packet Sniffer

● Sniffs messages being sent/received from/by your computer

● Store and display the contents of the various protocol fields in the messages.

DESCRIPTION:

WIRESHARK

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets. You can use Wireshark to inspect a suspicious program's network traffic, analyze the traffic flow on your network, or troubleshoot network problems.

What we can do with Wireshark:

□ Capture network traffic

□ Decode packet protocols using dissectors

□ Define filters – capture and display

□ Watch smart statistics

□ Analyze problems

□ Interactively browse that traffic

Wireshark used for:

□ Network administrators: troubleshoot network problems

□ Network security engineers: examine security problems

□ Developers: debug protocol implementations

□ People: learn network protocol internals Getting Wireshark

Wireshark can be downloaded for Windows or macOS from its official website. For Linux or another UNIX-like system, Wireshark will be found in its package repositories. For Ubuntu,Wireshark will be found in the Ubuntu Software Center.

Capturing Packets

After downloading and installing Wireshark, launch it and double-click the name of a network interface under Capture to start capturing packets on that interface As soon as you click the interface’s name, you’ll see the packets start to appear in real time.Wireshark captures each packet sent to or from your system. If you have promiscuous mode enabled—it’s enabled by default—you’ll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the ―Enable promiscuous mode on all interfaces‖ checkbox is activated at the bottom of this window. Click the red ―Stop‖ button near the top left corner of the window when you want to stop capturing traffic.

The ―Packet List‖ Pane

The packet list pane displays all the packets in the current capture file. The ―Packet List‖ pane Each line in the packet list corresponds to one packet in the capture file. If you select a line in this pane, more details will be displayed in the ―Packet Details‖ and ―Packet Bytes‖ panes.

The ―Packet Details‖ Pane

The packet details pane shows the current packet (selected in the ―Packet List‖ pane) in a more detailed form. This pane shows the protocols and protocol fields of the packet selected in the ―Packet List‖ pane. The protocols and fields of the packet shown in a tree which can be expanded And collapsed.

The ―Packet Bytes‖ Pane

The packet bytes pane shows the data of the current packet (selected in the ―Packet List‖ pane) in a hexdump style.

Color Coding

You’ll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.

Sample Captures:

If there’s nothing interesting on your own network to inspect, Wireshark’s wiki has you covered. The wiki contains a page of sample capture files that you can load and inspect. Click File > Open in Wireshark and browse for your downloaded file to open one. You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.

Filtering Packets

If you’re trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you’ll likely have a large amount of packets to sift through. That’s where Wireshark’s filters come in.

CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL

To filter, capture, view, packets in Wireshark Tool. Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save it.

Procedure1. Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph

2. Create a Filter to display only ARP packets and inspect the packets.

Procedure

3. Create a Filter to display only DNS packets and provide the flow graph.

4. Create a Filter to display only HTTP packets and inspect the packets

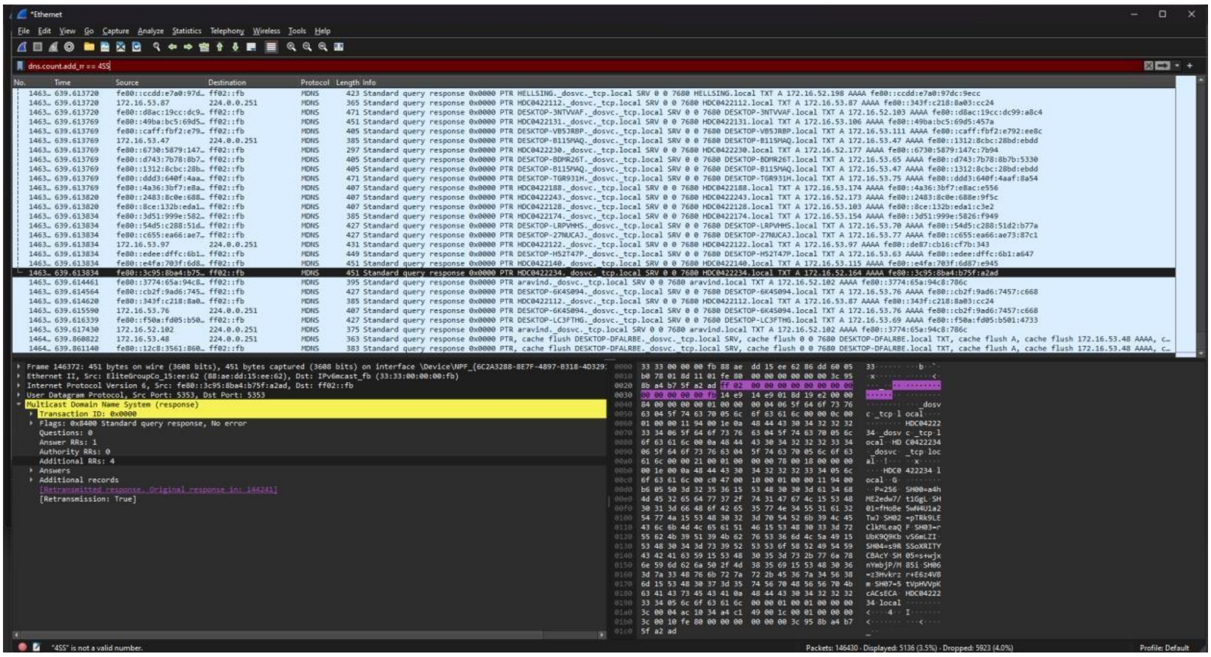
Procedure

5. Create a Filter to display only IP/ICMP packets and inspect the packets.

Procedure

6. Create a Filter to display only DHCP packets and inspect the packets.

Procedure :



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns.count.add_rr == 4SS
```

```
No.    Time        Source                Destination   Protocol Length Info
1463… 639.613720  fe80::ccdd:e7a0:97d…  ff02::fb      MDNS   423 Standard query response 0x0000 PTR HELLSING._dosvc._tcp.local SRV 0 0 7680 HELLSING.local TXT A 172.16.52.198 AAAA fe80::ccdd:e7a0:97dc:9ecc
1463… 639.613720  172.16.53.87          224.0.0.251   MDNS   365 Standard query response 0x0000 PTR HDC0422112._dosvc._tcp.local SRV 0 0 7680 HDC0422112.local TXT A 172.16.53.87 AAAA fe80::343f:c218:8a03:cc24
1463… 639.613720  fe80::d8ac:19cc:dc9…  ff02::fb      MDNS   471 Standard query response 0x0000 PTR DESKTOP-3NTVVAF._dosvc._tcp.local SRV 0 0 7680 DESKTOP-3NTVVAF.local TXT A 172.16.52.103 AAAA fe80::d8ac:19cc:dc99:a8c4
1463… 639.613769  fe80::49ba:bc5:69d5…  ff02::fb      MDNS   451 Standard query response 0x0000 PTR HDC0422131._dosvc._tcp.local SRV 0 0 7680 HDC0422131.local TXT A 172.16.53.106 AAAA fe80::49ba:bc5:69d5:457a
1463… 639.613769  fe80::caff:fbf2:e79…  ff02::fb      MDNS   405 Standard query response 0x0000 PTR DESKTOP-VB5JRBP._dosvc._tcp.local SRV 0 0 7680 DESKTOP-VB5JRBP.local TXT A 172.16.53.111 AAAA fe80::caff:fbf2:e792:ee8c
1463… 639.613769  172.16.53.47          224.0.0.251   MDNS   385 Standard query response 0x0000 PTR DESKTOP-B115MAQ._dosvc._tcp.local SRV 0 0 7680 DESKTOP-B115MAQ.local TXT A 172.16.53.47 AAAA fe80::1312:8cbc:28bd:ebdd
1463… 639.613769  fe80::6730:5879:147…  ff02::fb      MDNS   297 Standard query response 0x0000 PTR HDC0422230._dosvc._tcp.local SRV 0 0 7680 HDC0422230.local TXT A 172.16.52.177 AAAA fe80::6730:5879:147c:7b94
1463… 639.613769  fe80::d743:7b78:8b7…  ff02::fb      MDNS   405 Standard query response 0x0000 PTR DESKTOP-BDMR26T._dosvc._tcp.local SRV 0 0 7680 DESKTOP-BDMR26T.local TXT A 172.16.53.65 AAAA fe80::d743:7b78:8b7b:5330
1463… 639.613769  fe80::1312:8cbc:28b…  ff02::fb      MDNS   405 Standard query response 0x0000 PTR DESKTOP-B115MAQ._dosvc._tcp.local SRV 0 0 7680 DESKTOP-B115MAQ.local TXT A 172.16.53.47 AAAA fe80::1312:8cbc:28bd:ebdd
1463… 639.613769  fe80::ddd3:640f:4aa…  ff02::fb      MDNS   471 Standard query response 0x0000 PTR DESKTOP-TGR931H._dosvc._tcp.local SRV 0 0 7680 DESKTOP-TGR931H.local TXT A 172.16.53.75 AAAA fe80::ddd3:640f:4aaf:8a54
1463… 639.613769  fe80::4a36:3bf7:e8a…  ff02::fb      MDNS   407 Standard query response 0x0000 PTR HDC0422188._dosvc._tcp.local SRV 0 0 7680 HDC0422188.local TXT A 172.16.53.174 AAAA fe80::4a36:3bf7:e8ac:e556
1463… 639.613820  fe80::2483:8c0e:688…  ff02::fb      MDNS   407 Standard query response 0x0000 PTR HDC0422243._dosvc._tcp.local SRV 0 0 7680 HDC0422243.local TXT A 172.16.52.173 AAAA fe80::2483:8c0e:688e:9f5c
1463… 639.613820  fe80::8ce:132b:eda1…  ff02::fb      MDNS   407 Standard query response 0x0000 PTR HDC0422128._dosvc._tcp.local SRV 0 0 7680 HDC0422128.local TXT A 172.16.53.103 AAAA fe80::8ce:132b:eda1:c3e2
1463… 639.613834  fe80::3d51:999e:582…  ff02::fb      MDNS   385 Standard query response 0x0000 PTR HDC0422174._dosvc._tcp.local SRV 0 0 7680 HDC0422174.local TXT A 172.16.53.154 AAAA fe80::3d51:999e:5826:f949
1463… 639.613834  fe80::54d5:c288:51d…  ff02::fb      MDNS   427 Standard query response 0x0000 PTR DESKTOP-LRPVHHS._dosvc._tcp.local SRV 0 0 7680 DESKTOP-LRPVHHS.local TXT A 172.16.53.70 AAAA fe80::54d5:c288:51d2:b77a
1463… 639.613834  fe80::c655:ea66:ae7…  ff02::fb      MDNS   427 Standard query response 0x0000 PTR DESKTOP-27NUCAJ._dosvc._tcp.local SRV 0 0 7680 DESKTOP-27NUCAJ.local TXT A 172.16.53.77 AAAA fe80::c655:ea66:ae73:87c1
1463… 639.613834  172.16.53.97          224.0.0.251   MDNS   431 Standard query response 0x0000 PTR HDC0422122._dosvc._tcp.local SRV 0 0 7680 HDC0422122.local TXT A 172.16.53.97 AAAA fe80::de87:cb16:cf7b:343
1463… 639.613834  fe80::edee:dffc:6b1…  ff02::fb      MDNS   449 Standard query response 0x0000 PTR DESKTOP-H52T47P._dosvc._tcp.local SRV 0 0 7680 DESKTOP-H52T47P.local TXT A 172.16.53.63 AAAA fe80::edee:dffc:6b1:a647
1463… 639.613834  fe80::e4fa:703f:6d8…  ff02::fb      MDNS   451 Standard query response 0x0000 PTR HDC0422140._dosvc._tcp.local SRV 0 0 7680 HDC0422140.local TXT A 172.16.53.115 AAAA fe80::e4fa:703f:6d87:e945
1463… 639.613834  fe80::3c95:8ba4:b75…  ff02::fb      MDNS   451 Standard query response 0x0000 PTR HDC0422234._dosvc._tcp.local SRV 0 0 7680 HDC0422234.local TXT A 172.16.52.164 AAAA fe80::3c95:8ba4:b75f:a2ad
1463… 639.614461  fe80::3774:65a:94c8…  ff02::fb      MDNS   395 Standard query response 0x0000 PTR aravind._dosvc._tcp.local SRV 0 0 7680 aravind.local TXT A 172.16.52.102 AAAA fe80::3774:65a:94c8:786c
1463… 639.614564  fe80::cb2f:9ad6:745…  ff02::fb      MDNS   427 Standard query response 0x0000 PTR DESKTOP-6K4S094._dosvc._tcp.local SRV 0 0 7680 DESKTOP-6K4S094.local TXT A 172.16.53.76 AAAA fe80::cb2f:9ad6:7457:c668
1463… 639.614620  fe80::343f:c218:8a0…  ff02::fb      MDNS   385 Standard query response 0x0000 PTR HDC0422112._dosvc._tcp.local SRV 0 0 7680 HDC0422112.local TXT A 172.16.53.87 AAAA fe80::343f:c218:8a03:cc24
1463… 639.615590  172.16.53.76          224.0.0.251   MDNS   407 Standard query response 0x0000 PTR DESKTOP-6K4S094._dosvc._tcp.local SRV 0 0 7680 DESKTOP-6K4S094.local TXT A 172.16.53.76 AAAA fe80::cb2f:9ad6:7457:c668
1463… 639.616339  fe80::f50a:fd05:b50…  ff02::fb      MDNS   427 Standard query response 0x0000 PTR DESKTOP-LC3FTHG._dosvc._tcp.local SRV 0 0 7680 DESKTOP-LC3FTHG.local TXT A 172.16.53.69 AAAA fe80::f50a:fd05:b501:4733
1463… 639.617430  172.16.52.102         224.0.0.251   MDNS   375 Standard query response 0x0000 PTR aravind._dosvc._tcp.local SRV 0 0 7680 aravind.local TXT A 172.16.52.102 AAAA fe80::3774:65a:94c8:786c
1464… 639.860822  172.16.53.48          224.0.0.251   MDNS   363 Standard query response 0x0000 PTR, cache flush DESKTOP-DFALRBE._dosvc._tcp.local SRV, cache flush 0 0 7680 DESKTOP-DFALRBE.local TXT, cache flush A, cache flush 172.16.53.48 AAAA, c…
1464… 639.861140  fe80::12c8:3561:860…  ff02::fb      MDNS   383 Standard query response 0x0000 PTR, cache flush DESKTOP-DFALRBE._dosvc._tcp.local SRV, cache flush 0 0 7680 DESKTOP-DFALRBE.local TXT, cache flush A, cache flush 172.16.53.48 AAAA, c…
```

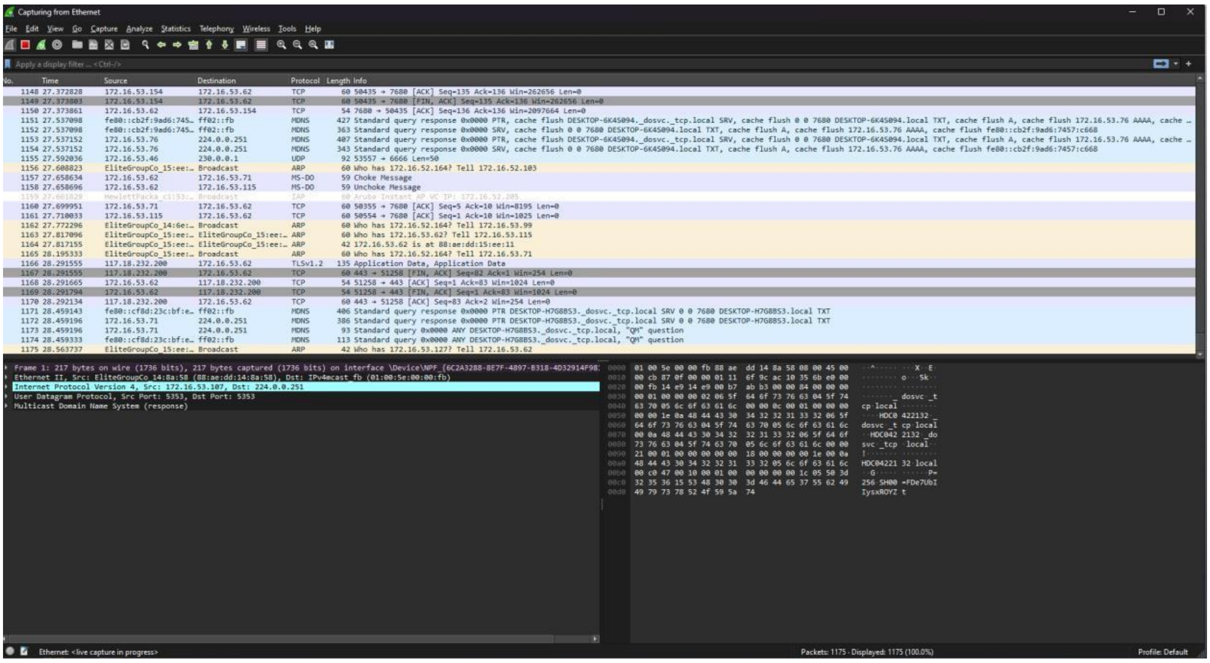
```
> Frame 146372: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface \Device\NPF_{6C2A3288-8E7F-4897-B318-4D329
> Ethernet II, Src: EliteGroupCo_15:ee:62 (88:ae:dd:15:ee:62), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
> Internet Protocol Version 6, Src: fe80::3c95:8ba4:b75f:a2ad, Dst: ff02::fb
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
v Multicast Domain Name System (response)
  > Transaction ID: 0x0000
  > Flags: 0x8400 Standard query response, No error
    Questions: 0
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 4
  > Answers
  > Additional records
    [Retransmitted response. Original response in: 144241]
    [Retransmission: True]
```

```
0000  33 33 00 00 00 fb 88 ae  dd 15 ee 62 86 dd 60 05   33·······b··`·
0010  b0 78 01 8d 11 01 fe 80  00 00 00 00 00 00 3c 95   ·x············<·
0020  8b a4 b7 5f a2 ad ff 02  00 00 00 00 00 00 00 00   ···_············
0030  00 00 00 00 00 fb 14 e9  14 e9 01 8d 19 e2 00 00   ················
0040  84 00 00 00 00 01 00 00  00 04 06 5f 64 6f 73 76   ···········_dosv
0050  63 04 5f 74 63 70 05 6c  6f 63 61 6c 00 00 0c 00   c·_tcp·l ocal····
0060  01 00 00 11 94 00 1e 0a  48 44 43 30 34 32 32 32   ········ HDC04222
0070  33 34 06 5f 64 6f 73 76  63 04 5f 74 63 70 05 6c   34·_dosv c·_tcp·l
0080  6f 63 61 6c 00 0a 48 44  43 30 34 32 32 32 33 34   ocal··HD C0422234
0090  06 5f 64 6f 73 76 63 04  5f 74 63 70 05 6c 6f 63   ·_dosvc· _tcp·loc
00a0  61 6c 00 00 21 00 01 00  00 00 78 00 18 00 00 00   al··!··· ··x·····
00b0  00 1e 00 0a 48 44 43 30  34 32 32 32 33 34 05 6c   ····HDC0 422234·l
00c0  6f 63 61 6c 00 c0 47 00  10 00 01 00 00 11 94 00   ocal··G· ········
00d0  b6 05 50 3d 32 35 36 15  53 48 30 30 3d 61 34 68   ··P=256· SH00=a4h
00e0  4d 45 32 65 64 77 37 2f  74 31 47 67 4c 15 53 48   ME2edw7/ t1GgL·SH
00f0  30 31 3d 66 48 6f 42 65  35 77 4e 34 55 31 61 32   01=fHoBe 5wN4U1a2
0100  54 77 4a 15 53 48 30 32  3d 70 54 52 6b 39 4c 45   TwJ·SH02 =pTRk9LE
0110  43 6c 6b 4d 4c 65 61 51  46 15 53 48 30 33 3d 72   ClkMLeaQ F·SH03=r
0120  55 62 4b 39 51 39 4b 62  76 53 36 6d 4c 5a 49 15   UbK9Q9Kb vS6mLZI·
0130  53 48 30 34 3d 73 39 52  53 53 6f 58 52 49 54 59   SH04=s9R SSoXRITY
0140  43 42 41 63 59 15 53 48  30 35 3d 73 2b 77 6a 78   CBAcY·SH 05=s+wjx
0150  6e 59 6d 62 6a 50 2f 4d  38 35 69 15 53 48 30 36   nYmbjP/M 85i·SH06
0160  3d 7a 33 48 76 6b 72 7a  72 2b 45 36 7a 34 56 38   =z3Hvkrz r+E6z4V8
0170  6d 15 53 48 30 37 3d 35  74 56 70 48 56 56 70 4b   m·SH07=5 tVpHVVpK
0180  63 41 43 73 45 43 41 0a  48 44 43 30 34 32 32 32   cACsECA· HDC04222
0190  33 34 05 6c 6f 63 61 6c  00 00 01 00 01 00 00 00   34·local ········
01a0  3c 00 04 ac 10 34 a4 c1  49 00 1c 00 01 00 00 00   <····4·· I·······
01b0  3c 00 10 fe 80 00 00 00  00 00 00 3c 95 8b a4 b7   <······· ···<····
01c0  5f a2 ad                                           _··
```

"4SS" is not a valid number.

Packets: 146430 · Displayed: 5136 (3.5%) · Dropped: 5923 (4.0%)

Profile: Default



Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time       Source                Destination           Protocol Length Info
1148 27.372828  172.16.53.154         172.16.53.62          TCP       60 50435 → 7680 [ACK] Seq=135 Ack=136 Win=262656 Len=0
1149 27.373803  172.16.53.154         172.16.53.62          TCP       60 50435 → 7680 [FIN, ACK] Seq=135 Ack=136 Win=262656 Len=0
1150 27.373861  172.16.53.62          172.16.53.154         TCP       54 7680 → 50435 [ACK] Seq=136 Ack=136 Win=2097664 Len=0
1151 27.537098  fe80::cb2f:9ad6:745…  ff02::fb              MDNS     427 Standard query response 0x0000 PTR, cache flush DESKTOP-6K4S094._dosvc._tcp.local SRV, cache flush 0 0 7680 DESKTOP-6K4S094.local TXT, cache flush A, cache flush 172.16.53.76 AAAA, cache …
1152 27.537098  fe80::cb2f:9ad6:745…  ff02::fb              MDNS     363 Standard query response 0x0000 SRV, cache flush 0 0 7680 DESKTOP-6K4S094.local TXT, cache flush A, cache flush 172.16.53.76 AAAA, cache flush fe80::cb2f:9ad6:7457:c668
1153 27.537152  172.16.53.76          224.0.0.251           MDNS     407 Standard query response 0x0000 PTR, cache flush DESKTOP-6K4S094._dosvc._tcp.local SRV, cache flush 0 0 7680 DESKTOP-6K4S094.local TXT, cache flush A, cache flush 172.16.53.76 AAAA, cache …
1154 27.537152  172.16.53.76          224.0.0.251           MDNS     343 Standard query response 0x0000 SRV, cache flush 0 0 7680 DESKTOP-6K4S094.local TXT, cache flush A, cache flush 172.16.53.76 AAAA, cache flush fe80::cb2f:9ad6:7457:c668
1155 27.592036  172.16.53.46          230.0.0.1             UDP       92 53557 → 6666 Len=50
1156 27.608823  EliteGroupCo_15:ee:…  Broadcast             ARP       60 Who has 172.16.52.164? Tell 172.16.52.103
1157 27.658634  172.16.53.62          172.16.53.71          MS-DO     59 Choke Message
1158 27.658696  172.16.53.62          172.16.53.115         MS-DO     59 Unchoke Message
1159 27.661828  HewlettPacka_c1:53:…  Broadcast             IAP       60 Aruba Instant AP VC IP: 172.16.52.205
1160 27.699951  172.16.53.71          172.16.53.62          TCP       60 50355 → 7680 [ACK] Seq=5 Ack=10 Win=8195 Len=0
1161 27.710033  172.16.53.115         172.16.53.62          TCP       60 50554 → 7680 [ACK] Seq=1 Ack=10 Win=1025 Len=0
1162 27.772296  EliteGroupCo_14:6e:…  Broadcast             ARP       60 Who has 172.16.52.164? Tell 172.16.53.99
1163 27.817096  EliteGroupCo_15:ee:…  EliteGroupCo_15:ee:…  ARP       60 Who has 172.16.53.62? Tell 172.16.53.115
1164 27.817155  EliteGroupCo_15:ee:…  EliteGroupCo_15:ee:…  ARP       42 172.16.53.62 is at 88:ae:dd:15:ee:11
1165 28.195333  EliteGroupCo_15:ee:…  Broadcast             ARP       60 Who has 172.16.52.164? Tell 172.16.53.71
1166 28.291555  117.18.232.200        172.16.53.62          TLSv1.2  135 Application Data, Application Data
1167 28.291555  117.18.232.200        172.16.53.62          TCP       60 443 → 51258 [FIN, ACK] Seq=82 Ack=1 Win=254 Len=0
1168 28.291665  172.16.53.62          117.18.232.200        TCP       54 51258 → 443 [ACK] Seq=1 Ack=83 Win=1024 Len=0
1169 28.291794  172.16.53.62          117.18.232.200        TCP       54 51258 → 443 [FIN, ACK] Seq=1 Ack=83 Win=1024 Len=0
1170 28.292134  117.18.232.200        172.16.53.62          TCP       60 443 → 51258 [ACK] Seq=83 Ack=2 Win=254 Len=0
1171 28.459143  fe80::cf8d:23c:bf:e…  ff02::fb              MDNS     406 Standard query response 0x0000 PTR DESKTOP-H7G8BS3._dosvc._tcp.local SRV 0 0 7680 DESKTOP-H7G8BS3.local TXT
1172 28.459196  172.16.53.71          224.0.0.251           MDNS     386 Standard query response 0x0000 PTR DESKTOP-H7G8BS3._dosvc._tcp.local SRV 0 0 7680 DESKTOP-H7G8BS3.local TXT
1173 28.459196  172.16.53.71          224.0.0.251           MDNS      93 Standard query 0x0000 ANY DESKTOP-H7G8BS3._dosvc._tcp.local, "QM" question
1174 28.459333  fe80::cf8d:23c:bf:e…  ff02::fb              MDNS     113 Standard query 0x0000 ANY DESKTOP-H7G8BS3._dosvc._tcp.local, "QM" question
1175 28.563737  EliteGroupCo_15:ee:…  Broadcast             ARP       42 Who has 172.16.53.127? Tell 172.16.53.62
```

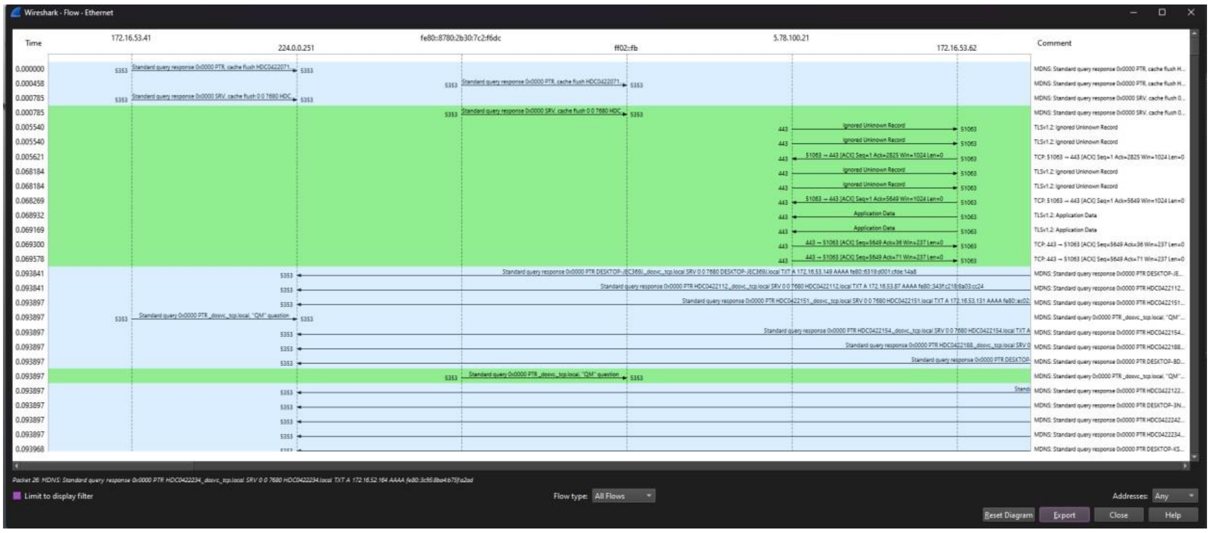
```
> Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{6C2A3288-8E7F-4897-B318-4D32914F98
> Ethernet II, Src: EliteGroupCo_14:8a:58 (88:ae:dd:14:8a:58), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 172.16.53.107, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (response)
```

```
0000  01 00 5e 00 00 fb 88 ae  dd 14 8a 58 08 00 45 00   ··^····· ···X··E·
0010  00 cb 87 0f 00 00 01 11  6f 9c ac 10 35 6b e0 00   ········ o···5k··
0020  00 fb 14 e9 14 e9 00 b7  ab b3 00 00 84 00 00 00   ········ ········
0030  00 01 00 00 00 02 06 5f  64 6f 73 76 63 04 5f 74   ·······_ dosvc·_t
0040  63 70 05 6c 6f 63 61 6c  00 00 0c 00 01 00 00 00   cp·local ········
0050  00 00 1e 0a 48 44 43 30  34 32 32 31 33 32 06 5f   ····HDC0 422132·_
0060  64 6f 73 76 63 04 5f 74  63 70 05 6c 6f 63 61 6c   dosvc·_t cp·local
0070  00 0a 48 44 43 30 34 32  32 31 33 32 06 5f 64 6f   ··HDC042 2132·_do
0080  73 76 63 04 5f 74 63 70  05 6c 6f 63 61 6c 00 00   svc·_tcp ·local··
0090  21 00 01 00 00 00 00 00  18 00 00 00 00 1e 00 0a   !······· ········
00a0  48 44 43 30 34 32 32 31  33 32 05 6c 6f 63 61 6c   HDC04221 32·local
00b0  00 c0 47 00 10 00 01 00  00 00 00 00 1c 05 50 3d   ··G····· ······P=
00c0  32 35 36 15 53 48 30 30  3d 46 44 65 37 55 62 49   256·SH00 =FDe7UbI
00d0  49 79 73 78 52 4f 59 5a  74                        IysxROYZ t
```

Ethernet: <live capture in progress>

Packets: 1175 · Displayed: 1175 (100.0%)

Profile: Default



```
Time      Comment
0.000000  MDNS: Standard query response 0x0000 PTR, cache flush H...
0.000458  MDNS: Standard query response 0x0000 PTR, cache flush H...
0.000785  MDNS: Standard query response 0x0000 SRV, cache flush 0...
0.000785  MDNS: Standard query response 0x0000 SRV, cache flush 0...
0.005540  TLSv1.2: Ignored Unknown Record
0.005540  TLSv1.2: Ignored Unknown Record
0.005621  TCP: 51063 → 443 [ACK] Seq=1 Ack=2825 Win=1024 Len=0
0.068184  TLSv1.2: Ignored Unknown Record
0.068184  TLSv1.2: Ignored Unknown Record
0.068269  TCP: 51063 → 443 [ACK] Seq=1 Ack=5649 Win=1024 Len=0
0.068932  TLSv1.2: Application Data
0.069169  TLSv1.2: Application Data
0.069300  TCP: 443 → 51063 [ACK] Seq=5649 Ack=36 Win=237 Len=0
0.069578  TCP: 443 → 51063 [ACK] Seq=5649 Ack=71 Win=237 Len=0
0.093841  MDNS: Standard query response 0x0000 PTR DESKTOP-JE...
0.093841  MDNS: Standard query response 0x0000 PTR HDC0422112...
0.093897  MDNS: Standard query response 0x0000 PTR HDC0422151...
0.093897  MDNS: Standard query 0x0000 PTR _dosvc._tcp.local, "QM"...
0.093897  MDNS: Standard query response 0x0000 PTR HDC0422154...
0.093897  MDNS: Standard query response 0x0000 PTR HDC0422188...
0.093897  MDNS: Standard query response 0x0000 PTR DESKTOP-BD...
0.093897  MDNS: Standard query 0x0000 PTR _dosvc._tcp.local, "QM"...
0.093897  MDNS: Standard query response 0x0000 PTR HDC0422122...
0.093897  MDNS: Standard query response 0x0000 PTR DESKTOP-3N...
0.093897  MDNS: Standard query response 0x0000 PTR HDC0422242...
0.093897  MDNS: Standard query response 0x0000 PTR HDC0422234...
0.093968  MDNS: Standard query response 0x0000 PTR DESKTOP-KS...
```

```
Packet 26: MDNS: Standard query response 0x0000 PTR HDC0422234._dosvc._tcp.local SRV 0 0 7680 HDC0422234.local TXT A 172.16.52.164 AAAA fe80::3c95:8ba4:b75f:a2ad
```

RESULT:

The Experiments on Packet capture tool has been executed successfully.