Name: **Shrey Pendurkar**
Class: **D15C**
Batch: **C**
Roll No: **64**

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).

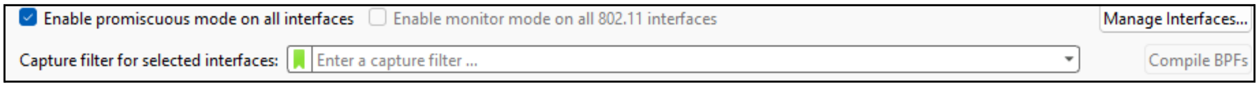
In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

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

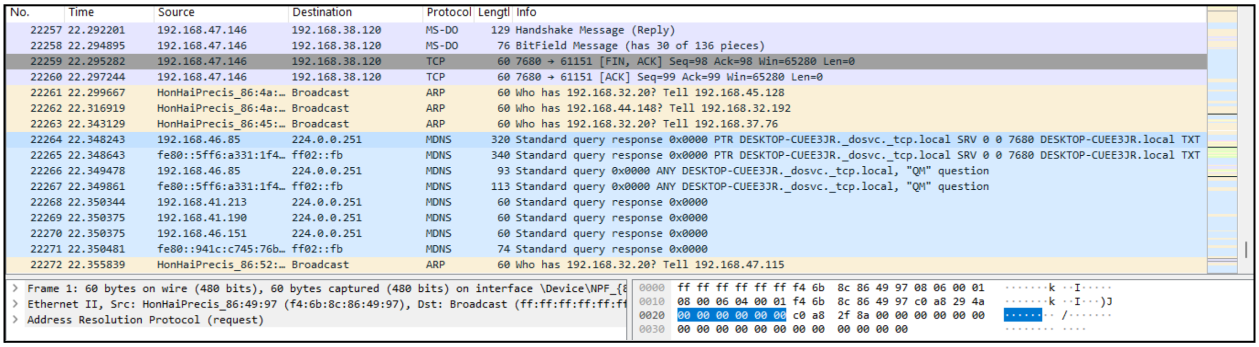
Output:

1) Promiscuous mode:



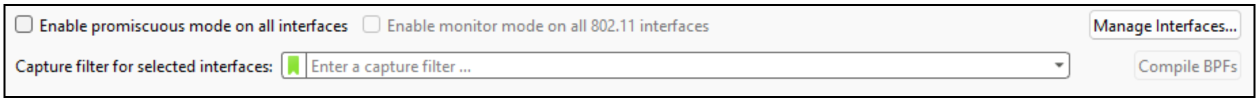
☑ Enable promiscuous mode on all interfaces ☐ Enable monitor mode on all 802.11 interfaces

Capture filter for selected interfaces:



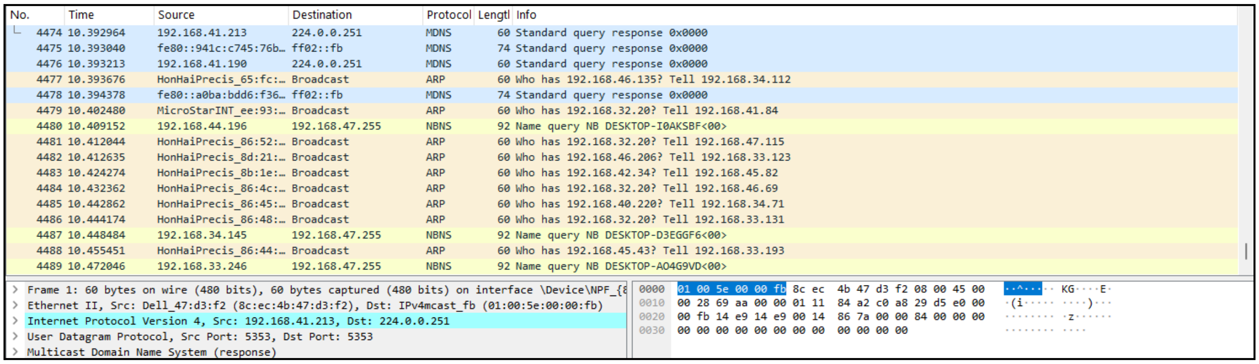
```
No.   Time      Source                 Destination     Protocol Lengtl Info
22257 22.292201 192.168.47.146         192.168.38.120  MS-DO    129 Handshake Message (Reply)
22258 22.294895 192.168.47.146         192.168.38.120  MS-DO     76 BitField Message (has 30 of 136 pieces)
22259 22.295282 192.168.47.146         192.168.38.120  TCP       60 7680 → 61151 [FIN, ACK] Seq=98 Ack=98 Win=65280 Len=0
22260 22.297244 192.168.47.146         192.168.38.120  TCP       60 7680 → 61151 [ACK] Seq=99 Ack=99 Win=65280 Len=0
22261 22.299667 HonHaiPrecis_86:4a:…   Broadcast       ARP       60 Who has 192.168.32.20? Tell 192.168.45.128
22262 22.316919 HonHaiPrecis_86:4a:…   Broadcast       ARP       60 Who has 192.168.44.148? Tell 192.168.32.192
22263 22.343129 HonHaiPrecis_86:45:…   Broadcast       ARP       60 Who has 192.168.32.20? Tell 192.168.37.76
22264 22.348243 192.168.46.85          224.0.0.251     MDNS     320 Standard query response 0x0000 PTR DESKTOP-CUEE3JR._dosvc._tcp.local SRV 0 0 7680 DESKTOP-CUEE3JR.local TXT
22265 22.348643 fe80::5ff6:a331:1f4…   ff02::fb        MDNS     340 Standard query response 0x0000 PTR DESKTOP-CUEE3JR._dosvc._tcp.local SRV 0 0 7680 DESKTOP-CUEE3JR.local TXT
22266 22.349478 192.168.46.85          224.0.0.251     MDNS      93 Standard query 0x0000 ANY DESKTOP-CUEE3JR._dosvc._tcp.local, "QM" question
22267 22.349861 fe80::5ff6:a331:1f4…   ff02::fb        MDNS     113 Standard query 0x0000 ANY DESKTOP-CUEE3JR._dosvc._tcp.local, "QM" question
22268 22.350344 192.168.41.213         224.0.0.251     MDNS      60 Standard query response 0x0000
22269 22.350375 192.168.41.190         224.0.0.251     MDNS      60 Standard query response 0x0000
22270 22.350375 192.168.46.151         224.0.0.251     MDNS      60 Standard query response 0x0000
22271 22.350481 fe80::941c:c745:76b…   ff02::fb        MDNS      74 Standard query response 0x0000
22272 22.355839 HonHaiPrecis_86:52:…   Broadcast       ARP       60 Who has 192.168.32.20? Tell 192.168.47.115

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{8
> Ethernet II, Src: HonHaiPrecis_86:49:97 (f4:6b:8c:86:49:97), Dst: Broadcast (ff:ff:ff:ff:ff:ff
> Address Resolution Protocol (request)

0000  ff ff ff ff ff ff f4 6b  8c 86 49 97 08 06 00 01   ······k ··I·····
0010  08 00 06 04 00 01 f4 6b  8c 86 49 97 c0 a8 29 4a   ······k ··I···)J
0020  00 00 00 00 00 00 c0 a8  2f 8a 00 00 00 00 00 00   ········ /·······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

2) Non-promiscuous mode:



☐ Enable promiscuous mode on all interfaces ☐ Enable monitor mode on all 802.11 interfaces

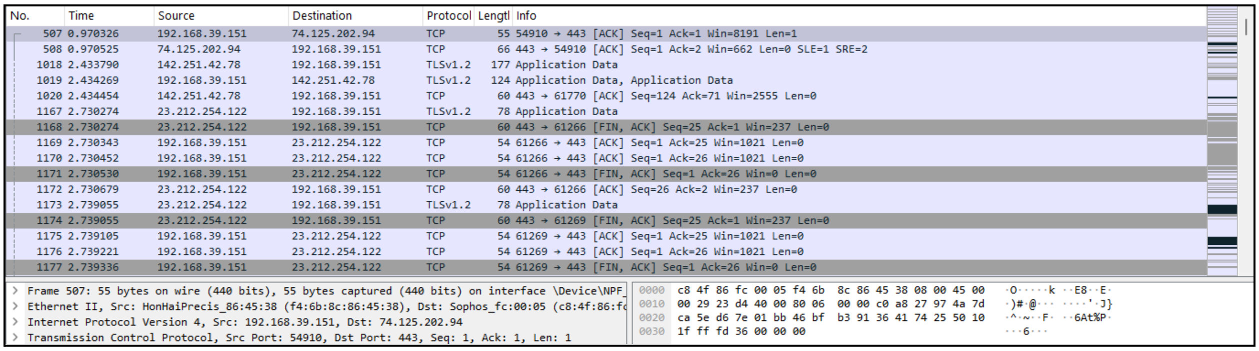
Capture filter for selected interfaces: Enter a capture filter …



```
No.  Time      Source                 Destination     Protocol Lengtl Info
4474 10.392964 192.168.41.213         224.0.0.251     MDNS     60 Standard query response 0x0000
4475 10.393040 fe80::941c:c745:76b…   ff02::fb        MDNS     74 Standard query response 0x0000
4476 10.393213 192.168.41.190         224.0.0.251     MDNS     60 Standard query response 0x0000
4477 10.393676 HonHaiPrecis_65:fc:…   Broadcast       ARP      60 Who has 192.168.46.135? Tell 192.168.34.112
4478 10.394378 fe80::a0ba:bdd6:f36…   ff02::fb        MDNS     74 Standard query response 0x0000
4479 10.402480 MicroStarINT_ee:93:…   Broadcast       ARP      60 Who has 192.168.32.20? Tell 192.168.41.84
4480 10.409152 192.168.44.196         192.168.47.255  NBNS     92 Name query NB DESKTOP-I0AKSBF<00>
4481 10.412044 HonHaiPrecis_86:52:…   Broadcast       ARP      60 Who has 192.168.32.20? Tell 192.168.47.115
4482 10.412635 HonHaiPrecis_8d:21:…   Broadcast       ARP      60 Who has 192.168.46.206? Tell 192.168.33.123
4483 10.424274 HonHaiPrecis_8b:1e:…   Broadcast       ARP      60 Who has 192.168.42.34? Tell 192.168.45.82
4484 10.432362 HonHaiPrecis_86:4c:…   Broadcast       ARP      60 Who has 192.168.32.20? Tell 192.168.46.69
4485 10.442862 HonHaiPrecis_86:45:…   Broadcast       ARP      60 Who has 192.168.40.220? Tell 192.168.34.71
4486 10.444174 HonHaiPrecis_86:48:…   Broadcast       ARP      60 Who has 192.168.32.20? Tell 192.168.33.131
4487 10.448484 192.168.34.145         192.168.47.255  NBNS     92 Name query NB DESKTOP-D3EGGF6<00>
4488 10.455451 HonHaiPrecis_86:44:…   Broadcast       ARP      60 Who has 192.168.45.43? Tell 192.168.33.193
4489 10.472046 192.168.33.246         192.168.47.255  NBNS     92 Name query NB DESKTOP-AO4G9VD<00>

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{8
> Ethernet II, Src: Dell_47:d3:f2 (8c:ec:4b:47:d3:f2), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 192.168.41.213, 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 8c ec  4b 47 d3 f2 08 00 45 00   ··^····· KG····E·
0010  00 28 69 aa 00 00 01 11  84 a2 c0 a8 29 d5 e0 00   ·(i····· ····)···
0020  00 fb 14 e9 14 e9 00 14  86 7a 00 00 84 00 00 00   ········ ·z······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

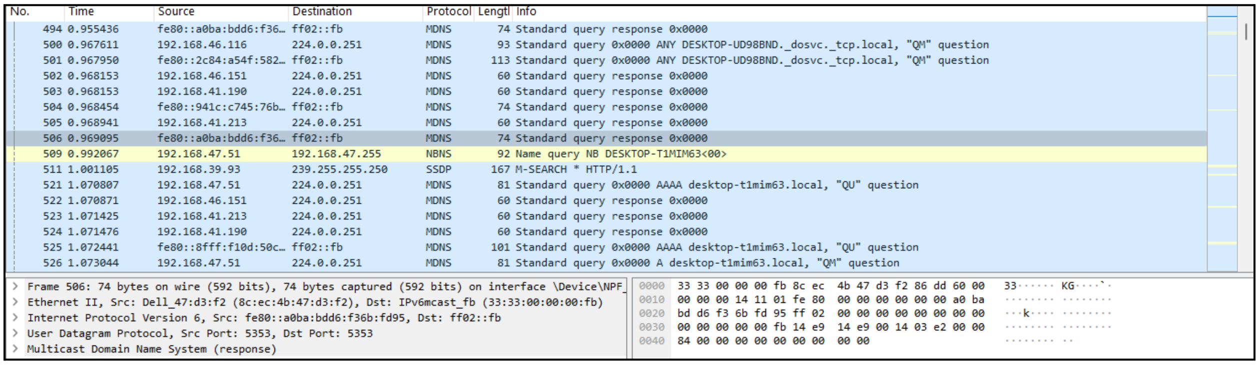
3) Protocol Filters:

a) TCP



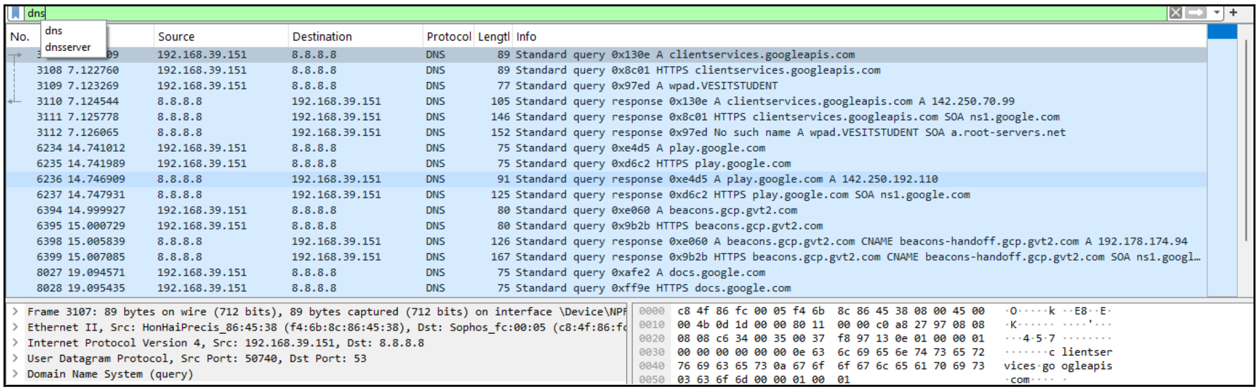
```
No.  Time     Source          Destination     Protocol Lengtl Info
 507 0.970326 192.168.39.151  74.125.202.94   TCP       55 54910 → 443 [ACK] Seq=1 Ack=1 Win=8191 Len=1
 508 0.970525 74.125.202.94   192.168.39.151  TCP       66 443 → 54910 [ACK] Seq=1 Ack=2 Win=662 Len=0 SLE=1 SRE=2
1018 2.433790 142.251.42.78   192.168.39.151  TLSv1.2  177 Application Data
1019 2.434269 192.168.39.151  142.251.42.78   TLSv1.2  124 Application Data, Application Data
1020 2.434454 142.251.42.78   192.168.39.151  TCP       60 443 → 61770 [ACK] Seq=124 Ack=71 Win=2555 Len=0
1167 2.730274 23.212.254.122  192.168.39.151  TLSv1.2   78 Application Data
1168 2.730274 23.212.254.122  192.168.39.151  TCP       60 443 → 61266 [FIN, ACK] Seq=25 Ack=1 Win=237 Len=0
1169 2.730343 192.168.39.151  23.212.254.122  TCP       54 61266 → 443 [ACK] Seq=1 Ack=25 Win=1021 Len=0
1170 2.730452 192.168.39.151  23.212.254.122  TCP       54 61266 → 443 [ACK] Seq=1 Ack=26 Win=1021 Len=0
1171 2.730530 192.168.39.151  23.212.254.122  TCP       54 61266 → 443 [FIN, ACK] Seq=1 Ack=26 Win=0 Len=0
1172 2.730679 23.212.254.122  192.168.39.151  TCP       60 443 → 61266 [ACK] Seq=26 Ack=2 Win=237 Len=0
1173 2.739055 23.212.254.122  192.168.39.151  TLSv1.2   78 Application Data
1174 2.739055 23.212.254.122  192.168.39.151  TCP       60 443 → 61269 [FIN, ACK] Seq=25 Ack=1 Win=237 Len=0
1175 2.739105 192.168.39.151  23.212.254.122  TCP       54 61269 → 443 [ACK] Seq=1 Ack=25 Win=1021 Len=0
1176 2.739221 192.168.39.151  23.212.254.122  TCP       54 61269 → 443 [ACK] Seq=1 Ack=26 Win=1021 Len=0
1177 2.739336 192.168.39.151  23.212.254.122  TCP       54 61269 → 443 [FIN, ACK] Seq=1 Ack=26 Win=0 Len=0

> Frame 507: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_
> Ethernet II, Src: HonHaiPrecis_86:45:38 (f4:6b:8c:86:45:38), Dst: Sophos_fc:00:05 (c8:4f:86:fc
> Internet Protocol Version 4, Src: 192.168.39.151, Dst: 74.125.202.94
> Transmission Control Protocol, Src Port: 54910, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

0000  c8 4f 86 fc 00 05 f4 6b  8c 86 45 38 08 00 45 00   ·O·····k ··E8··E·
0010  00 29 23 d4 40 00 80 06  00 00 c0 a8 27 97 4a 7d   ·)#·@··· ····'·J}
0020  ca 5e d6 7e 01 bb 46 bf  b3 91 36 41 74 25 50 10   ·^·~··F· ··6At%P·
0030  1f ff fd 36 00 00 00                               ···6···
```

b) UDP



```
No.   Time       Source                  Destination       Protocol Lengtl Info
  494 0.955436   fe80::a0ba:bdd6:f36…  ff02::fb          MDNS       74 Standard query response 0x0000
  500 0.967611   192.168.46.116        224.0.0.251       MDNS       93 Standard query 0x0000 ANY DESKTOP-UD98BND._dosvc._tcp.local, "QM" question
  501 0.967950   fe80::2c84:a54f:582…  ff02::fb          MDNS      113 Standard query 0x0000 ANY DESKTOP-UD98BND._dosvc._tcp.local, "QM" question
  502 0.968153   192.168.46.151        224.0.0.251       MDNS       60 Standard query response 0x0000
  503 0.968153   192.168.41.190        224.0.0.251       MDNS       60 Standard query response 0x0000
  504 0.968454   fe80::941c:c745:76b…  ff02::fb          MDNS       74 Standard query response 0x0000
  505 0.968941   192.168.41.213        224.0.0.251       MDNS       60 Standard query response 0x0000
  506 0.969095   fe80::a0ba:bdd6:f36…  ff02::fb          MDNS       74 Standard query response 0x0000
  509 0.992067   192.168.47.51         192.168.47.255    NBNS       92 Name query NB DESKTOP-T1MIM63<00>
  511 1.001105   192.168.39.93         239.255.255.250   SSDP      167 M-SEARCH * HTTP/1.1
  521 1.070807   192.168.47.51         224.0.0.251       MDNS       81 Standard query 0x0000 AAAA desktop-t1mim63.local, "QU" question
  522 1.070871   192.168.46.151        224.0.0.251       MDNS       60 Standard query response 0x0000
  523 1.071425   192.168.41.213        224.0.0.251       MDNS       60 Standard query response 0x0000
  524 1.071476   192.168.41.190        224.0.0.251       MDNS       60 Standard query response 0x0000
  525 1.072441   fe80::8fff:f10d:50c…  ff02::fb          MDNS      101 Standard query 0x0000 AAAA desktop-t1mim63.local, "QU" question
  526 1.073044   192.168.47.51         224.0.0.251       MDNS       81 Standard query 0x0000 A desktop-t1mim63.local, "QM" question

> Frame 506: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_
> Ethernet II, Src: Dell_47:d3:f2 (8c:ec:4b:47:d3:f2), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
> Internet Protocol Version 6, Src: fe80::a0ba:bdd6:f36b:fd95, Dst: ff02::fb
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (response)

0000  33 33 00 00 00 fb 8c ec  4b 47 d3 f2 86 dd 60 00   33······ KG····`·
0010  00 00 00 14 11 01 fe 80  00 00 00 00 00 00 a0 ba   ········ ········
0020  bd d6 f3 6b fd 95 ff 02  00 00 00 00 00 00 00 00   ···k···· ········
0030  00 00 00 00 00 fb 14 e9  14 e9 00 14 03 e2 00 00   ········ ········
0040  84 00 00 00 00 00 00 00  00 00                     ········ ··
```

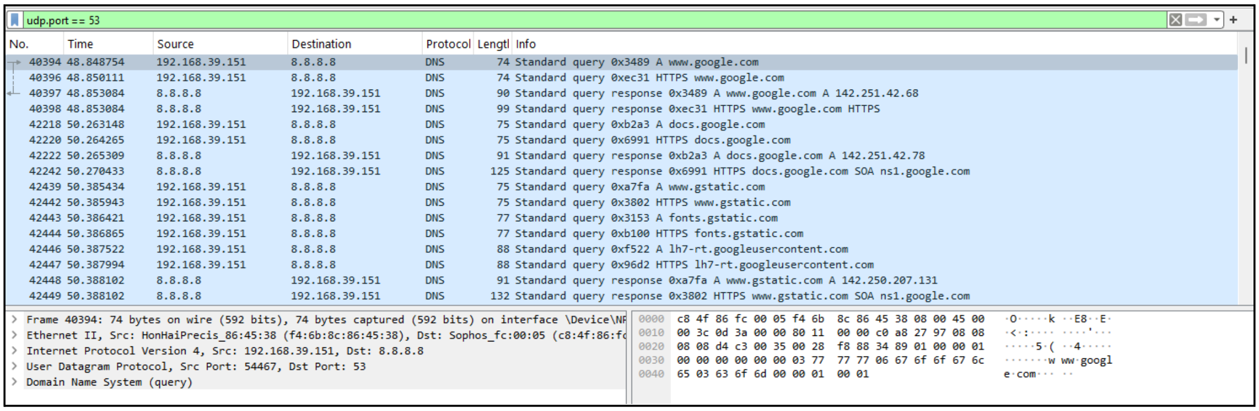
c) DNS



```
dns
No.   dns          Source           Destination       Protocol Lengtl Info
3     dnsserver 09 192.168.39.151   8.8.8.8           DNS        89 Standard query 0x130e A clientservices.googleapis.com
 3108 7.122760     192.168.39.151   8.8.8.8           DNS        89 Standard query 0x8c01 HTTPS clientservices.googleapis.com
 3109 7.123269     192.168.39.151   8.8.8.8           DNS        77 Standard query 0x97ed A wpad.VESITSTUDENT
 3110 7.124544     8.8.8.8          192.168.39.151    DNS       105 Standard query response 0x130e A clientservices.googleapis.com A 142.250.70.99
 3111 7.125778     8.8.8.8          192.168.39.151    DNS       146 Standard query response 0x8c01 HTTPS clientservices.googleapis.com SOA ns1.google.com
 3112 7.126065     8.8.8.8          192.168.39.151    DNS       152 Standard query response 0x97ed No such name A wpad.VESITSTUDENT SOA a.root-servers.net
 6234 14.741012    192.168.39.151   8.8.8.8           DNS        75 Standard query 0xe4d5 A play.google.com
 6235 14.741989    192.168.39.151   8.8.8.8           DNS        75 Standard query 0xd6c2 HTTPS play.google.com
 6236 14.746909    8.8.8.8          192.168.39.151    DNS        91 Standard query response 0xe4d5 A play.google.com A 142.250.192.110
 6237 14.747931    8.8.8.8          192.168.39.151    DNS       125 Standard query response 0xd6c2 HTTPS play.google.com SOA ns1.google.com
 6394 14.999927    192.168.39.151   8.8.8.8           DNS        80 Standard query 0xe060 A beacons.gcp.gvt2.com
 6395 15.000729    192.168.39.151   8.8.8.8           DNS        80 Standard query 0x9b2b HTTPS beacons.gcp.gvt2.com
 6398 15.005839    8.8.8.8          192.168.39.151    DNS       126 Standard query response 0xe060 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 192.178.174.94
 6399 15.007085    8.8.8.8          192.168.39.151    DNS       167 Standard query response 0x9b2b HTTPS beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com SOA ns1.googl…
 8027 19.094571    192.168.39.151   8.8.8.8           DNS        75 Standard query 0xafe2 A docs.google.com
 8028 19.095435    192.168.39.151   8.8.8.8           DNS        75 Standard query 0xff9e HTTPS docs.google.com

> Frame 3107: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF
> Ethernet II, Src: HonHaiPrecis_86:45:38 (f4:6b:8c:86:45:38), Dst: Sophos_fc:00:05 (c8:4f:86:fc
> Internet Protocol Version 4, Src: 192.168.39.151, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 50740, Dst Port: 53
> Domain Name System (query)

0000  c8 4f 86 fc 00 05 f4 6b  8c 86 45 38 08 00 45 00   ·O·····k ··E8··E·
0010  00 4b 0d 1d 00 00 80 11  00 00 c0 a8 27 97 08 08   ·K······ ····'···
0020  08 08 c6 34 00 35 00 37  f8 97 13 0e 01 00 00 01   ···4·5·7 ········
0030  00 00 00 00 00 00 0e 63  6c 69 65 6e 74 73 65 72   ·······c lientser
0040  76 69 63 65 73 0a 67 6f  6f 67 6c 65 61 70 69 73   vices·go ogleapis
0050  03 63 6f 6d 00 00 01 00  01                        ·com···· ·
```

4) Port filters:

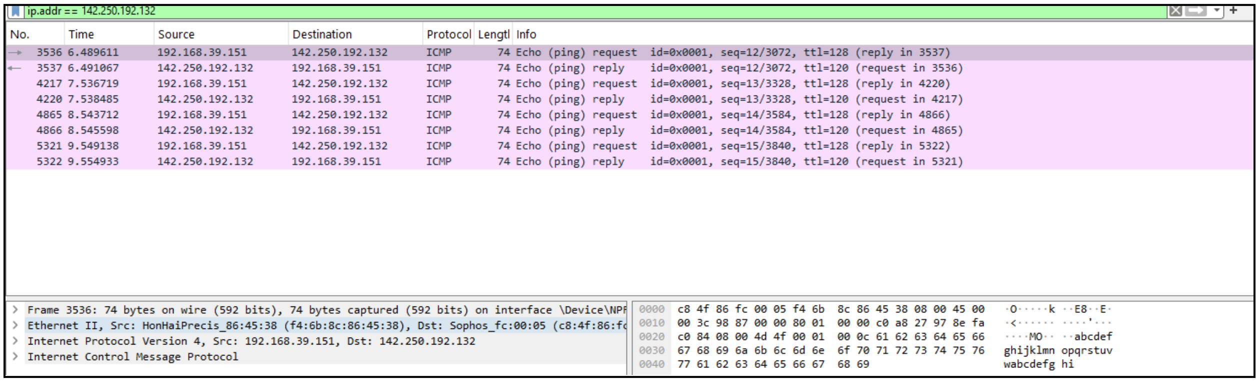
udp.port == 53



```
udp.port == 53
No.    Time        Source           Destination       Protocol Lengtl Info
 40394 48.848754   192.168.39.151   8.8.8.8           DNS        74 Standard query 0x3489 A www.google.com
 40396 48.850111   192.168.39.151   8.8.8.8           DNS        74 Standard query 0xec31 HTTPS www.google.com
 40397 48.853084   8.8.8.8          192.168.39.151    DNS        90 Standard query response 0x3489 A www.google.com A 142.251.42.68
 40398 48.853084   8.8.8.8          192.168.39.151    DNS        99 Standard query response 0xec31 HTTPS www.google.com HTTPS
 42218 50.263148   192.168.39.151   8.8.8.8           DNS        75 Standard query 0xb2a3 A docs.google.com
 42220 50.264265   192.168.39.151   8.8.8.8           DNS        75 Standard query 0x6991 HTTPS docs.google.com
 42222 50.265309   8.8.8.8          192.168.39.151    DNS        91 Standard query response 0xb2a3 A docs.google.com A 142.251.42.78
 42242 50.270433   8.8.8.8          192.168.39.151    DNS       125 Standard query response 0x6991 HTTPS docs.google.com SOA ns1.google.com
 42439 50.385434   192.168.39.151   8.8.8.8           DNS        75 Standard query 0xa7fa A www.gstatic.com
 42442 50.385943   192.168.39.151   8.8.8.8           DNS        75 Standard query 0x3802 HTTPS www.gstatic.com
 42443 50.386421   192.168.39.151   8.8.8.8           DNS        77 Standard query 0x3153 A fonts.gstatic.com
 42444 50.386865   192.168.39.151   8.8.8.8           DNS        77 Standard query 0xb100 HTTPS fonts.gstatic.com
 42446 50.387522   192.168.39.151   8.8.8.8           DNS        88 Standard query 0xf522 A lh7-rt.googleusercontent.com
 42447 50.387994   192.168.39.151   8.8.8.8           DNS        88 Standard query 0x96d2 HTTPS lh7-rt.googleusercontent.com
 42448 50.388102   8.8.8.8          192.168.39.151    DNS        91 Standard query response 0xa7fa A www.gstatic.com A 142.250.207.131
 42449 50.388102   8.8.8.8          192.168.39.151    DNS       132 Standard query response 0x3802 HTTPS www.gstatic.com SOA ns1.google.com

> Frame 40394: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NF
> Ethernet II, Src: HonHaiPrecis_86:45:38 (f4:6b:8c:86:45:38), Dst: Sophos_fc:00:05 (c8:4f:86:fc
> Internet Protocol Version 4, Src: 192.168.39.151, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 54467, Dst Port: 53
> Domain Name System (query)

0000  c8 4f 86 fc 00 05 f4 6b  8c 86 45 38 08 00 45 00   ·O·····k ··E8··E·
0010  00 3c 0d 3a 00 00 80 11  00 00 c0 a8 27 97 08 08   ·<·:···· ····'···
0020  08 08 d4 c3 00 35 00 28  f8 88 34 89 01 00 00 01   ·····5·( ··4·····
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 01  00 01                     e·com··· ··
```

5) Address Filters:

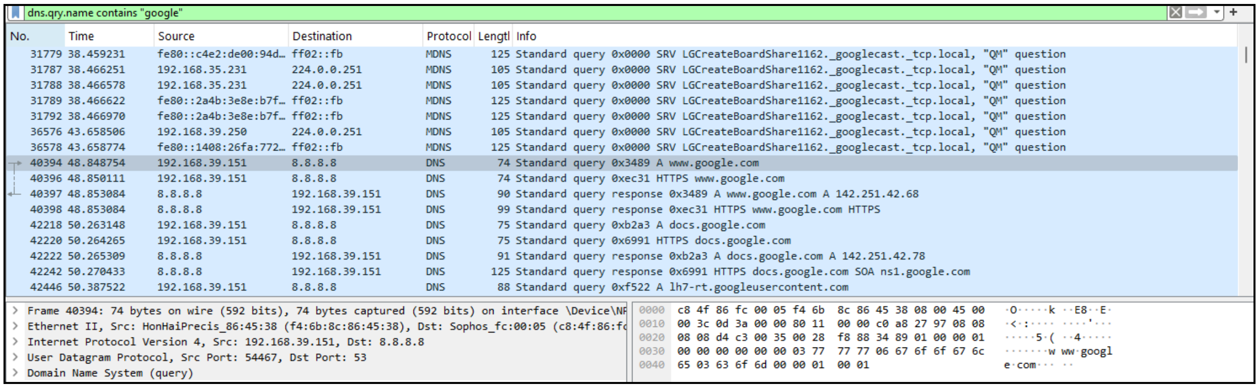
ip.addr == 142.250.192.132



```
ip.addr == 142.250.192.132

No.    Time      Source           Destination      Protocol Lengtl Info
 3536 6.489611   192.168.39.151   142.250.192.132  ICMP       74 Echo (ping) request  id=0x0001, seq=12/3072, ttl=128 (reply in 3537)
 3537 6.491067   142.250.192.132  192.168.39.151   ICMP       74 Echo (ping) reply    id=0x0001, seq=12/3072, ttl=120 (request in 3536)
 4217 7.536719   192.168.39.151   142.250.192.132  ICMP       74 Echo (ping) request  id=0x0001, seq=13/3328, ttl=128 (reply in 4220)
 4220 7.538485   142.250.192.132  192.168.39.151   ICMP       74 Echo (ping) reply    id=0x0001, seq=13/3328, ttl=120 (request in 4217)
 4865 8.543712   192.168.39.151   142.250.192.132  ICMP       74 Echo (ping) request  id=0x0001, seq=14/3584, ttl=128 (reply in 4866)
 4866 8.545598   142.250.192.132  192.168.39.151   ICMP       74 Echo (ping) reply    id=0x0001, seq=14/3584, ttl=120 (request in 4865)
 5321 9.549138   192.168.39.151   142.250.192.132  ICMP       74 Echo (ping) request  id=0x0001, seq=15/3840, ttl=128 (reply in 5322)
 5322 9.554933   142.250.192.132  192.168.39.151   ICMP       74 Echo (ping) reply    id=0x0001, seq=15/3840, ttl=120 (request in 5321)

> Frame 3536: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF
> Ethernet II, Src: HonHaiPrecis_86:45:38 (f4:6b:8c:86:45:38), Dst: Sophos_fc:00:05 (c8:4f:86:fc
> Internet Protocol Version 4, Src: 192.168.39.151, Dst: 142.250.192.132
> Internet Control Message Protocol

0000  c8 4f 86 fc 00 05 f4 6b  8c 86 45 38 08 00 45 00   ·O·····k ··E8··E·
0010  00 3c 98 87 00 00 80 01  00 00 c0 a8 27 97 8e fa   ·<······ ····'···
0020  c0 84 08 00 4d 4f 00 01  00 0c 61 62 63 64 65 66   ····MO·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

6) String Filter:

dns.qry.name contains “google”



```
dns.qry.name contains "google"

No.    Time       Source              Destination      Protocol Lengtl Info
 31779 38.459231  fe80::c4e2:de00:94d… ff02::fb        MDNS      125 Standard query 0x0000 SRV LGCreateBoardShare1162._googlecast._tcp.local, "QM" question
 31787 38.466251  192.168.35.231      224.0.0.251      MDNS      105 Standard query 0x0000 SRV LGCreateBoardShare1162._googlecast._tcp.local, "QM" question
 31788 38.466578  192.168.35.231      224.0.0.251      MDNS      105 Standard query 0x0000 SRV LGCreateBoardShare1162._googlecast._tcp.local, "QM" question
 31789 38.466622  fe80::2a4b:3e8e:b7f… ff02::fb        MDNS      125 Standard query 0x0000 SRV LGCreateBoardShare1162._googlecast._tcp.local, "QM" question
 31792 38.466970  fe80::2a4b:3e8e:b7f… ff02::fb        MDNS      125 Standard query 0x0000 SRV LGCreateBoardShare1162._googlecast._tcp.local, "QM" question
 36576 43.658506  192.168.39.250      224.0.0.251      MDNS      105 Standard query 0x0000 SRV LGCreateBoardShare1162._googlecast._tcp.local, "QM" question
 36578 43.658774  fe80::1408:26fa:772… ff02::fb        MDNS      125 Standard query 0x0000 SRV LGCreateBoardShare1162._googlecast._tcp.local, "QM" question
 40394 48.848754  192.168.39.151      8.8.8.8          DNS        74 Standard query 0x3489 A www.google.com
 40396 48.850111  192.168.39.151      8.8.8.8          DNS        74 Standard query 0xec31 HTTPS www.google.com
 40397 48.853084  8.8.8.8             192.168.39.151   DNS        90 Standard query response 0x3489 A www.google.com A 142.251.42.68
 40398 48.853084  8.8.8.8             192.168.39.151   DNS        99 Standard query response 0xec31 HTTPS www.google.com HTTPS
 42218 50.263148  192.168.39.151      8.8.8.8          DNS        75 Standard query 0xb2a3 A docs.google.com
 42220 50.264265  192.168.39.151      8.8.8.8          DNS        75 Standard query 0x6991 HTTPS docs.google.com
 42222 50.265309  8.8.8.8             192.168.39.151   DNS        91 Standard query response 0xb2a3 A docs.google.com A 142.251.42.78
 42242 50.270433  8.8.8.8             192.168.39.151   DNS       125 Standard query response 0x6991 HTTPS docs.google.com SOA ns1.google.com
 42446 50.387522  192.168.39.151      8.8.8.8          DNS        88 Standard query 0xf522 A lh7-rt.googleusercontent.com

> Frame 40394: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NF
> Ethernet II, Src: HonHaiPrecis_86:45:38 (f4:6b:8c:86:45:38), Dst: Sophos_fc:00:05 (c8:4f:86:fc
> Internet Protocol Version 4, Src: 192.168.39.151, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 54467, Dst Port: 53
> Domain Name System (query)

0000  c8 4f 86 fc 00 05 f4 6b  8c 86 45 38 08 00 45 00   ·O·····k ··E8··E·
0010  00 3c 0d 3a 00 00 80 11  00 00 c0 a8 27 97 08 08   ·<·:···· ····'···
0020  08 08 d4 c3 00 35 00 28  f8 88 34 89 01 00 00 01   ·····5·( ··4·····
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 01  00 01                     e·com··· ··
```

Conclusion:

The experiment demonstrates the effectiveness of Wireshark as a network packet analyzer, showcasing its ability to capture and analyze network traffic in both promiscuous and non-promiscuous modes using various filtering techniques. By applying protocol, port, address, and string filters, packets related to specific protocols, ports, addresses, and data content were isolated and examined. This experiment highlights Wireshark’s utility in real-world scenarios for network troubleshooting, security analysis, application testing, and protocol debugging, making it an essential tool for network professionals and learners alike.