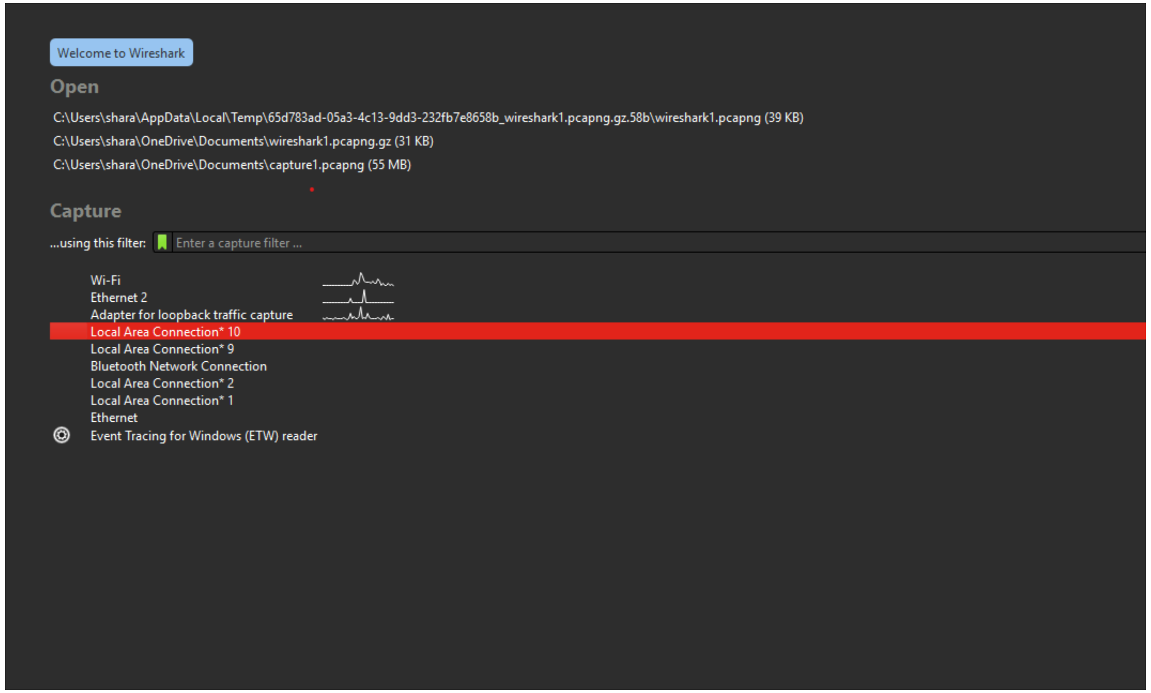
TASK 5: CAPTURING AND ANALYZING NETWORK TRAFFIC USING WIRESHARK

STEP 1: Install wireshark

- Go to official website of wireshark and download the latest version of wireshark

STEP 2: Start capturing the network using wireshark

- Search wireshark in your search bar and open it



Open

C:\Users\shara\AppData\Local\Temp\65d783ad-05a3-4c13-9dd3-232fb7e8658b_wireshark1.pcapng.gz.58b\wireshark1.pcapng (39 KB)
C:\Users\shara\OneDrive\Documents\wireshark1.pcapng.gz (31 KB)
C:\Users\shara\OneDrive\Documents\capture1.pcapng (55 MB)

Capture

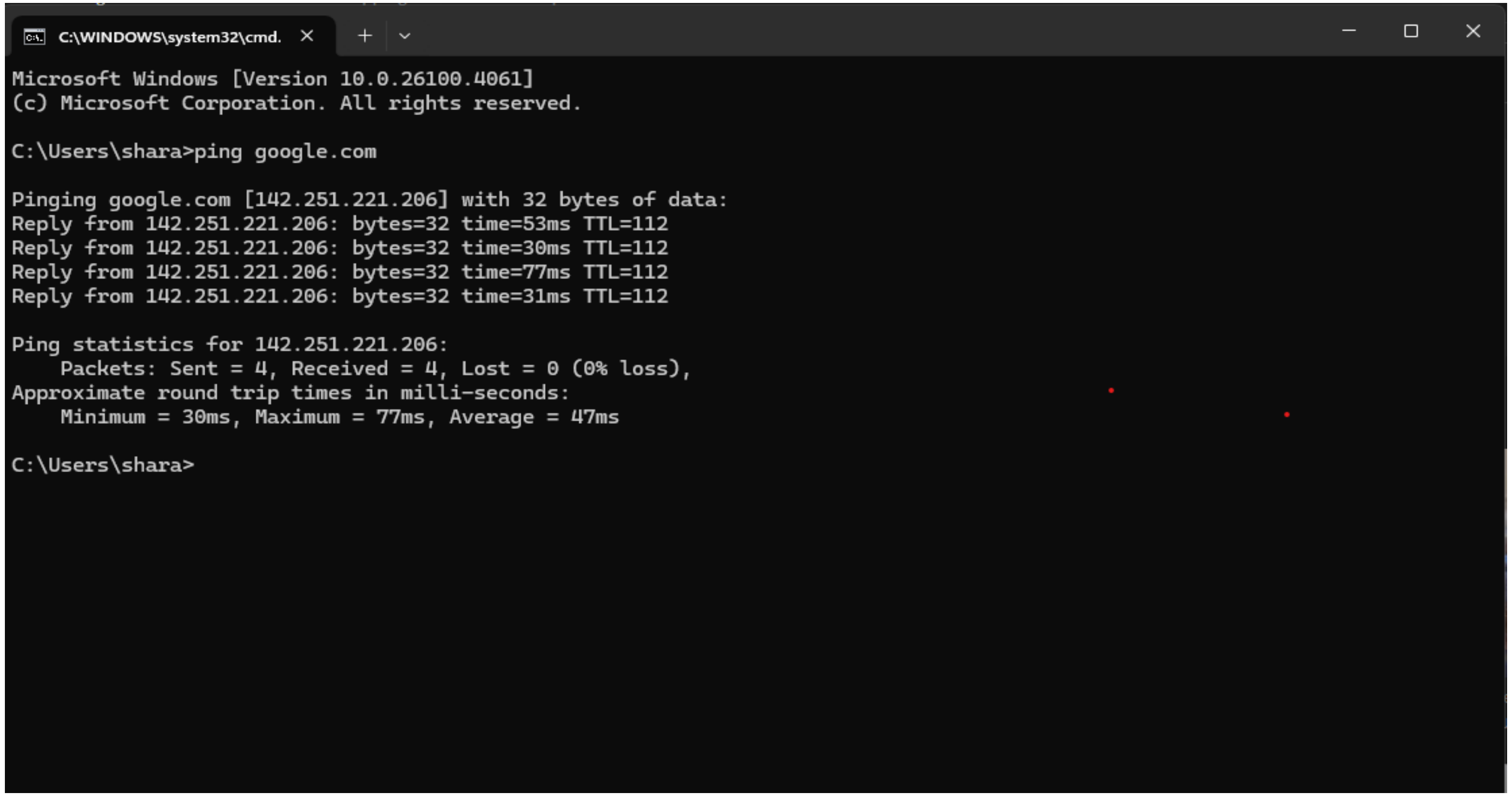
...using this filter:

Wi-Fi
Ethernet 2
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Bluetooth Network Connection
Local Area Connection* 2
Local Area Connection* 1
Ethernet
Event Tracing for Windows (ETW) reader

- select the network connected to your device(eg : ethernet, wifi…….)
- Double-click on that interface to start capturing

STEP 3: Browse a website or ping a Server to generate traffic

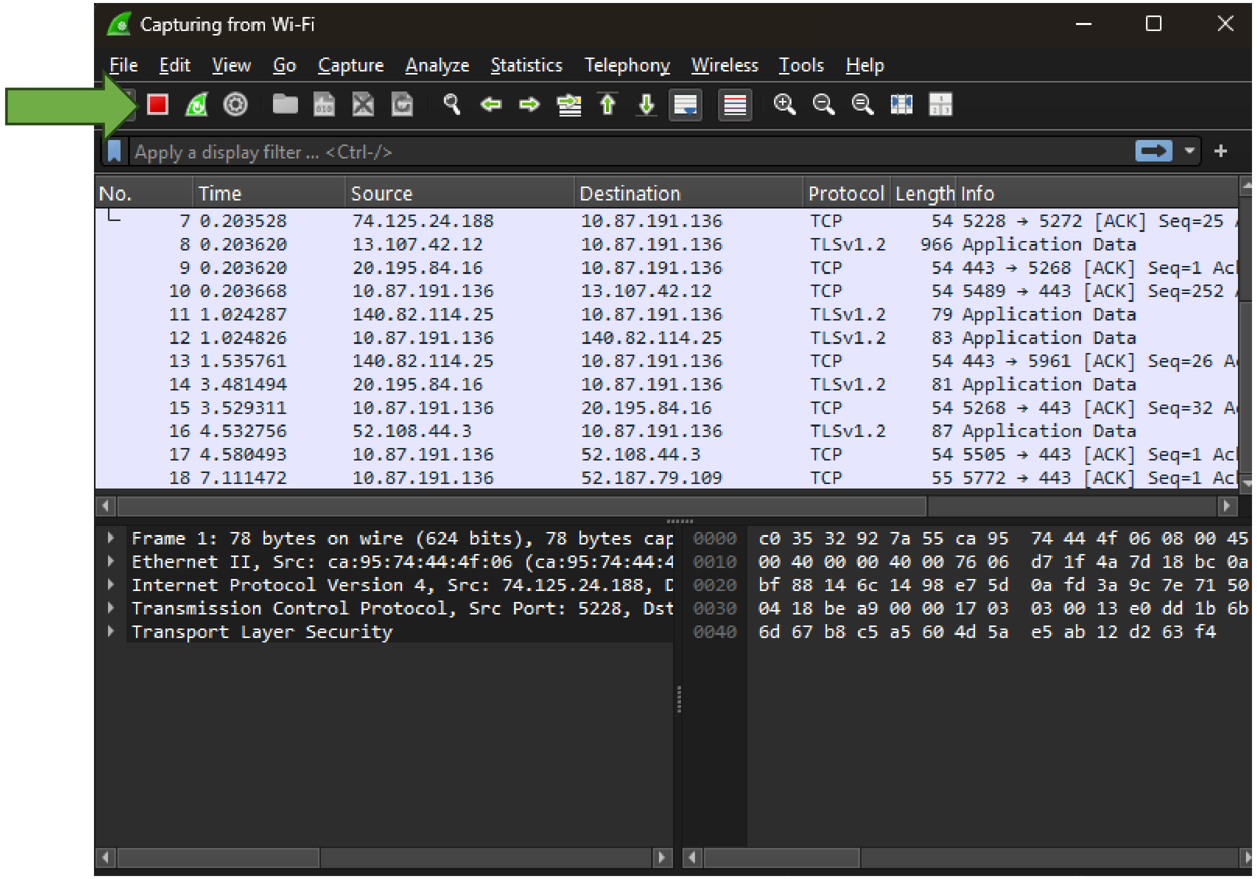
- While wireshark is capturing the network,open your web browser and start searching any wbsites
- Alternatively, open your command prompt and type ping (searched website)(eg: ping google.com)



```
Microsoft Windows [Version 10.0.26100.4061]
(c) Microsoft Corporation. All rights reserved.

C:\Users\shara>ping google.com

Pinging google.com [142.251.221.206] with 32 bytes of data:
Reply from 142.251.221.206: bytes=32 time=53ms TTL=112
Reply from 142.251.221.206: bytes=32 time=30ms TTL=112
Reply from 142.251.221.206: bytes=32 time=77ms TTL=112
Reply from 142.251.221.206: bytes=32 time=31ms TTL=112

Ping statistics for 142.251.221.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 77ms, Average = 47ms

C:\Users\shara>
```

STEEP 4: Stop capturing after a min:

- In wireshark , click the red square ”stop capturing the packets”


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

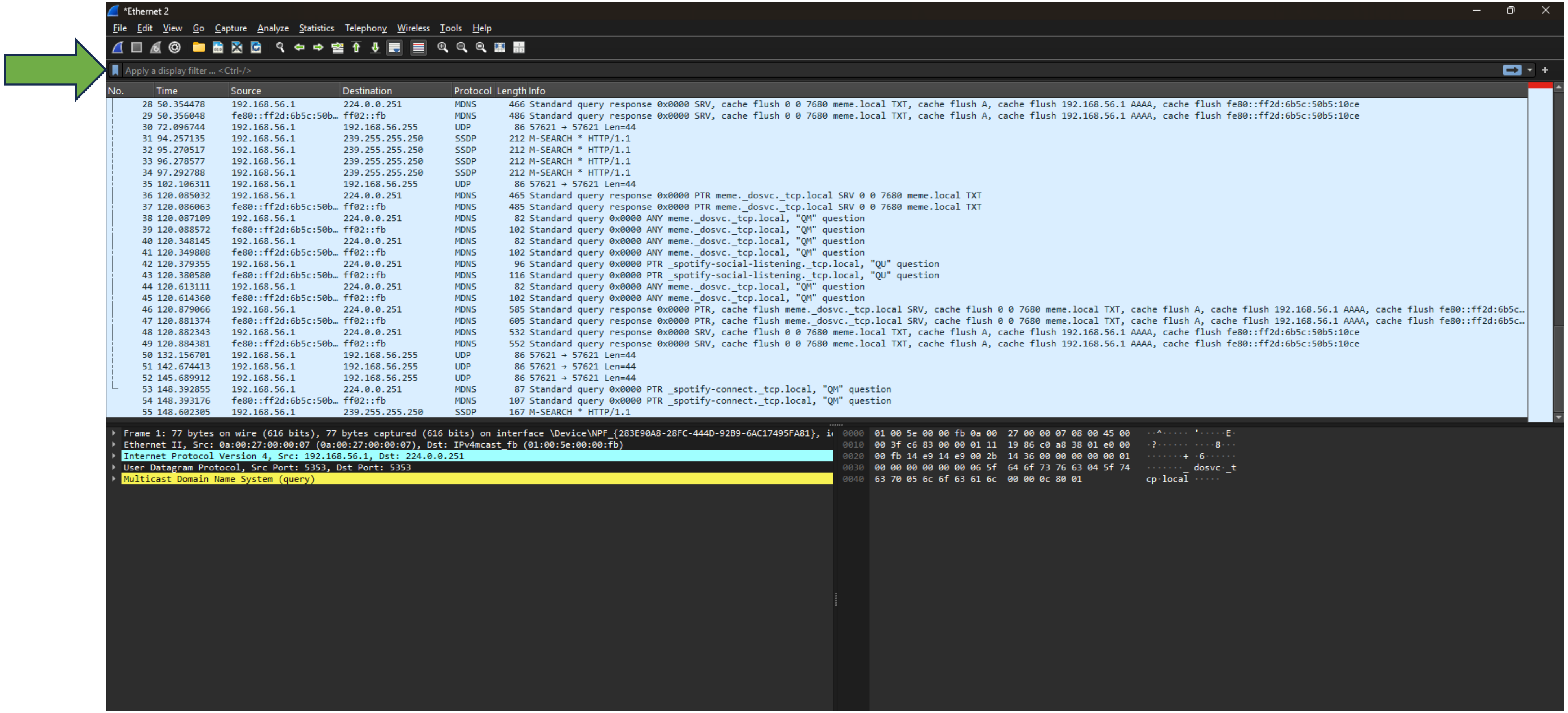
```
No.   Time      Source          Destination     Protocol Length Info
    7 0.203528  74.125.24.188   10.87.191.136   TCP        54 5228 → 5272 [ACK] Seq=25 A
    8 0.203620  13.107.42.12    10.87.191.136   TLSv1.2   966 Application Data
    9 0.203620  20.195.84.16    10.87.191.136   TCP        54 443 → 5268 [ACK] Seq=1 Ack
   10 0.203668  10.87.191.136   13.107.42.12    TCP        54 5489 → 443 [ACK] Seq=252 A
   11 1.024287  140.82.114.25   10.87.191.136   TLSv1.2    79 Application Data
   12 1.024826  10.87.191.136   140.82.114.25   TLSv1.2    83 Application Data
   13 1.535761  140.82.114.25   10.87.191.136   TCP        54 443 → 5961 [ACK] Seq=26 Ac
   14 3.481494  20.195.84.16    10.87.191.136   TLSv1.2    81 Application Data
   15 3.529311  10.87.191.136   20.195.84.16    TCP        54 5268 → 443 [ACK] Seq=32 Ac
   16 4.532756  52.108.44.3     10.87.191.136   TLSv1.2    87 Application Data
   17 4.580493  10.87.191.136   52.108.44.3     TCP        54 5505 → 443 [ACK] Seq=1 Ack
   18 7.111472  10.87.191.136   52.187.79.109   TCP        55 5772 → 443 [ACK] Seq=1 Ack
```

```
> Frame 1: 78 bytes on wire (624 bits), 78 bytes cap
> Ethernet II, Src: ca:95:74:44:4f:06 (ca:95:74:44:4
> Internet Protocol Version 4, Src: 74.125.24.188, D
> Transmission Control Protocol, Src Port: 5228, Dst
> Transport Layer Security
```

```
0000  c0 35 32 92 7a 55 ca 95  74 44 4f 06 08 00 45
0010  00 40 00 00 40 00 76 06  d7 1f 4a 7d 18 bc 0a
0020  bf 88 14 6c 14 98 e7 5d  0a fd 3a 9c 7e 71 50
0030  04 18 be a9 00 00 17 03  03 00 13 e0 dd 1b 6b
0040  6d 67 b8 c5 a5 60 4d 5a  e5 ab 12 d2 63 f4
```

PART 2: analyze the captured packets.

- In the filter bar at the top of wireshark, you can type the protocols we want to analyze.

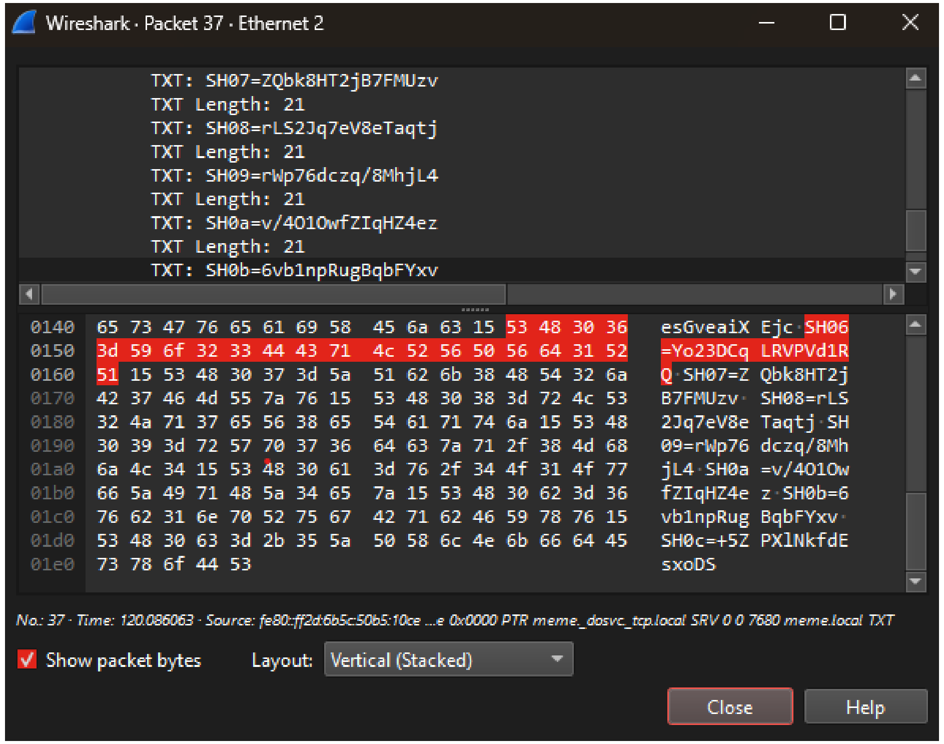


```
No.  Time        Source                   Destination      Protocol Length Info
  28 50.354478   192.168.56.1             224.0.0.251      MDNS     466 Standard query response 0x0000 SRV, cache flush 0 0 7680 meme.local TXT, cache flush A, cache flush 192.168.56.1 AAAA, cache flush fe80::ff2d:6b5c:50b5:10ce
  29 50.356048   fe80::ff2d:6b5c:50b…     ff02::fb         MDNS     486 Standard query response 0x0000 SRV, cache flush 0 0 7680 meme.local TXT, cache flush A, cache flush 192.168.56.1 AAAA, cache flush fe80::ff2d:6b5c:50b5:10ce
  30 72.096744   192.168.56.1             192.168.56.255   UDP       86 57621 → 57621 Len=44
  31 94.257135   192.168.56.1             239.255.255.250  SSDP     212 M-SEARCH * HTTP/1.1
  32 95.270517   192.168.56.1             239.255.255.250  SSDP     212 M-SEARCH * HTTP/1.1
  33 96.278577   192.168.56.1             239.255.255.250  SSDP     212 M-SEARCH * HTTP/1.1
  34 97.292788   192.168.56.1             239.255.255.250  SSDP     212 M-SEARCH * HTTP/1.1
  35 102.106311  192.168.56.1             192.168.56.255   UDP       86 57621 → 57621 Len=44
  36 120.085032  192.168.56.1             224.0.0.251      MDNS     465 Standard query response 0x0000 PTR meme._dosvc._tcp.local SRV 0 0 7680 meme.local TXT
  37 120.086063  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS     485 Standard query response 0x0000 PTR meme._dosvc._tcp.local SRV 0 0 7680 meme.local TXT
  38 120.087109  192.168.56.1             224.0.0.251      MDNS      82 Standard query 0x0000 ANY meme._dosvc._tcp.local, "QM" question
  39 120.088572  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS     102 Standard query 0x0000 ANY meme._dosvc._tcp.local, "QM" question
  40 120.348145  192.168.56.1             224.0.0.251      MDNS      82 Standard query 0x0000 ANY meme._dosvc._tcp.local, "QM" question
  41 120.349808  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS     102 Standard query 0x0000 ANY meme._dosvc._tcp.local, "QM" question
  42 120.379355  192.168.56.1             224.0.0.251      MDNS      96 Standard query 0x0000 PTR _spotify-social-listening._tcp.local, "QU" question
  43 120.380580  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS     116 Standard query 0x0000 PTR _spotify-social-listening._tcp.local, "QU" question
  44 120.613111  192.168.56.1             224.0.0.251      MDNS      82 Standard query 0x0000 ANY meme._dosvc._tcp.local, "QM" question
  45 120.614360  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS     102 Standard query 0x0000 ANY meme._dosvc._tcp.local, "QM" question
  46 120.879066  192.168.56.1             224.0.0.251      MDNS     585 Standard query response 0x0000 PTR, cache flush meme._dosvc._tcp.local SRV, cache flush 0 0 7680 meme.local TXT, cache flush A, cache flush 192.168.56.1 AAAA, cache flush fe80::ff2d:6b5c…
  47 120.881374  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS     605 Standard query response 0x0000 PTR, cache flush meme._dosvc._tcp.local SRV, cache flush 0 0 7680 meme.local TXT, cache flush A, cache flush 192.168.56.1 AAAA, cache flush fe80::ff2d:6b5c…
  48 120.882343  192.168.56.1             224.0.0.251      MDNS     532 Standard query response 0x0000 SRV, cache flush 0 0 7680 meme.local TXT, cache flush A, cache flush 192.168.56.1 AAAA, cache flush fe80::ff2d:6b5c:50b5:10ce
  49 120.884381  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS     552 Standard query response 0x0000 SRV, cache flush 0 0 7680 meme.local TXT, cache flush A, cache flush 192.168.56.1 AAAA, cache flush fe80::ff2d:6b5c:50b5:10ce
  50 132.156701  192.168.56.1             192.168.56.255   UDP       86 57621 → 57621 Len=44
  51 142.674413  192.168.56.1             192.168.56.255   UDP       86 57621 → 57621 Len=44
  52 145.689912  192.168.56.1             192.168.56.255   UDP       86 57621 → 57621 Len=44
  53 148.392855  192.168.56.1             224.0.0.251      MDNS      87 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
  54 148.393176  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS     107 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
  55 148.602305  192.168.56.1             239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
```

```
Frame 1: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{283E90A8-28FC-444D-92B9-6AC17495FA81}, i
Ethernet II, Src: 0a:00:27:00:00:07 (0a:00:27:00:00:07), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.56.1, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
```

```
0000  01 00 5e 00 00 fb 0a 00  27 00 00 07 08 00 45 00   ··^·····'·····E·
0010  00 3f c6 83 00 00 01 11  19 86 c0 a8 38 01 e0 00   ·?··········8···
0020  00 fb 14 e9 14 e9 00 2b  14 36 00 00 00 00 00 01   ·······+·6······
0030  00 00 00 00 00 00 06 5f  64 6f 73 76 63 04 5f 74   ·······_dosvc·_t
0040  63 70 05 6c 6f 63 61 6c  00 00 0c 80 01            cp·local·····
```

- Identify atleast 3 different Protocols in the capture
- Look at the protocols and study the usage of the selected protocols



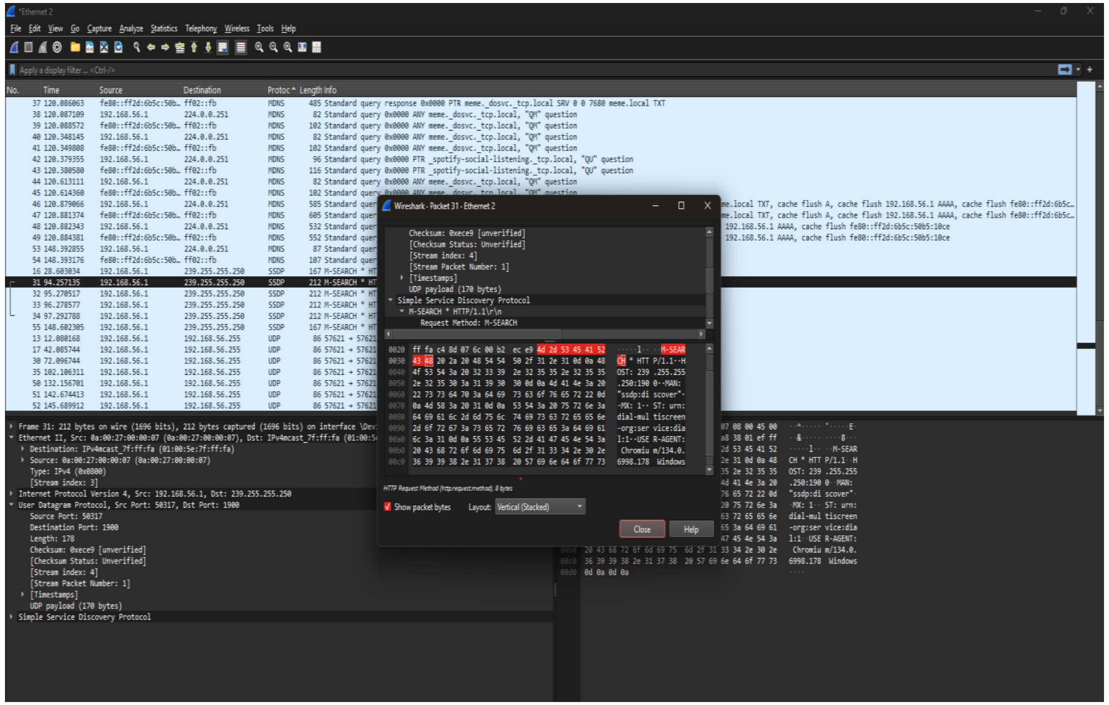
Wireshark · Packet 37 · Ethernet 2

```
        TXT: SH07=ZQbk8HT2jB7FMUzv
        TXT Length: 21
        TXT: SH08=rLS2Jq7eV8eTaqtj
        TXT Length: 21
        TXT: SH09=rWp76dczq/8MhjL4
        TXT Length: 21
        TXT: SH0a=v/4O1OwfZIqHZ4ez
        TXT Length: 21
        TXT: SH0b=6vb1npRugBqbFYxv
```

```
0140  65 73 47 76 65 61 69 58  45 6a 63 15 53 48 30 36   esGveaiX Ejc·SH06
0150  3d 59 6f 32 33 44 43 71  4c 52 56 50 56 64 31 52   =Yo23DCq LRVPVd1R
0160  51 15 53 48 30 37 3d 5a  51 62 6b 38 48 54 32 6a   Q·SH07=Z Qbk8HT2j
0170  42 37 46 4d 55 7a 76 15  53 48 30 38 3d 72 4c 53   B7FMUzv· SH08=rLS
0180  32 4a 71 37 65 56 38 65  54 61 71 74 6a 15 53 48   2Jq7eV8e Taqtj·SH
0190  30 39 3d 72 57 70 37 36  64 63 7a 71 2f 38 4d 68   09=rWp76 dczq/8Mh
01a0  6a 4c 34 15 53 48 30 61  3d 76 2f 34 4f 31 4f 77   jL4·SH0a =v/4O1Ow
01b0  66 5a 49 71 48 5a 34 65  7a 15 53 48 30 62 3d 36   fZIqHZ4e z·SH0b=6
01c0  76 62 31 6e 70 52 75 67  42 71 62 46 59 78 76 15   vb1npRug BqbFYxv·
01d0  53 48 30 63 3d 2b 35 5a  50 58 6c 4e 6b 66 64 45   SH0c=+5Z PXlNkfdE
01e0  73 78 6f 44 53                                     sxoDS
```

No.: 37 · Time: 120.086063 · Source: fe80::ff2d:6b5c:50b5:10ce …e 0x0000 PTR meme_dosvc_tcp.local SRV 0 0 7680 meme.local TXT

☑ Show packet bytes   Layout: Vertical (Stacked)



*Ethernet 2

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

```
No. Time        Source                   Destination      Protoc Length Info
 37 120.086063  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS   485 Standard query response 0x0000 PTR meme._dosvc._tcp.local SRV 0 0 7680 meme.local TXT
 38 120.087109  192.168.56.1             224.0.0.251      MDNS    82 Standard query 0x0000 ANY meme._dosvc._tcp.local, "QM" question
 39 120.088572  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS   102 Standard query 0x0000 ANY meme._dosvc._tcp.local, "QM" question
 40 120.348145  192.168.56.1             224.0.0.251      MDNS    82 Standard query 0x0000 ANY meme._dosvc._tcp.local, "QM" question
 41 120.349808  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS   102 Standard query 0x0000 ANY meme._dosvc._tcp.local, "QM" question
 42 120.379355  192.168.56.1             224.0.0.251      MDNS    96 Standard query 0x0000 PTR _spotify-social-listening._tcp.local, "QU" question
 43 120.380580  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS   116 Standard query 0x0000 PTR _spotify-social-listening._tcp.local, "QU" question
 44 120.613111  192.168.56.1             224.0.0.251      MDNS    82 Standard query 0x0000 ANY meme._dosvc._tcp.local, "QM" question
 45 120.614360  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS   102 Standard query 0x0000 ANY meme._dosvc._tcp.local, "QM" question
 46 120.879066  192.168.56.1             224.0.0.251      MDNS   585 Standard quer… me.local TXT, cache flush A, cache flush 192.168.56.1 AAAA, cache flush fe80::ff2d:6b5c…
 47 120.881374  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS   605 Standard quer… me.local TXT, cache flush A, cache flush 192.168.56.1 AAAA, cache flush fe80::ff2d:6b5c…
 48 120.882343  192.168.56.1             224.0.0.251      MDNS   532 Standard quer… 192.168.56.1 AAAA, cache flush fe80::ff2d:6b5c:50b5:10ce
 49 120.884381  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS   552 Standard quer… 192.168.56.1 AAAA, cache flush fe80::ff2d:6b5c:50b5:10ce
 53 148.392855  192.168.56.1             224.0.0.251      MDNS    87 Standard quer
 54 148.393176  fe80::ff2d:6b5c:50b…     ff02::fb         MDNS   107 Standard quer
 16 28.603034   192.168.56.1             239.255.255.250  SSDP   167 M-SEARCH * HT
 31 94.257135   192.168.56.1             239.255.255.250  SSDP   212 M-SEARCH * HT
 32 95.270517   192.168.56.1             239.255.255.250  SSDP   212 M-SEARCH * HT
 33 96.278577   192.168.56.1             239.255.255.250  SSDP   212 M-SEARCH * HT
 34 97.292788   192.168.56.1             239.255.255.250  SSDP   212 M-SEARCH * HT
 55 148.602305  192.168.56.1             239.255.255.250  SSDP   167 M-SEARCH * HT
 13 12.080168   192.168.56.1             192.168.56.255   UDP     86 57621 → 57621
 17 42.085744   192.168.56.1             192.168.56.255   UDP     86 57621 → 57621
 30 72.096744   192.168.56.1             192.168.56.255   UDP     86 57621 → 57621
 35 102.106311  192.168.56.1             192.168.56.255   UDP     86 57621 → 57621
 50 132.156701  192.168.56.1             192.168.56.255   UDP     86 57621 → 57621
 51 142.674413  192.168.56.1             192.168.56.255   UDP     86 57621 → 57621
 52 145.689912  192.168.56.1             192.168.56.255   UDP     86 57621 → 57621
```

```
▸ Frame 31: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits) on interface \Dev
▾ Ethernet II, Src: 0a:00:27:00:00:07 (0a:00:27:00:00:07), Dst: IPv4mcast_7f:ff:fa (01:00:5e
  ▸ Destination: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
  ▸ Source: 0a:00:27:00:00:07 (0a:00:27:00:00:07)
    Type: IPv4 (0x0800)
    [Stream index: 3]
▸ Internet Protocol Version 4, Src: 192.168.56.1, Dst: 239.255.255.250
▾ User Datagram Protocol, Src Port: 50317, Dst Port: 1900
    Source Port: 50317
    Destination Port: 1900
    Length: 178
    Checksum: 0xece9 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
    [Stream Packet Number: 1]
  ▸ [Timestamps]
    UDP payload (170 bytes)
▸ Simple Service Discovery Protocol
```

Wireshark · Packet 31 · Ethernet 2

```
    Checksum: 0xece9 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
    [Stream Packet Number: 1]
  ▸ [Timestamps]
    UDP payload (170 bytes)
▾ Simple Service Discovery Protocol
  ▾ M-SEARCH * HTTP/1.1\r\n
      Request Method: M-SEARCH
```

```
0020  ff fa c4 8d 07 6c 00 b2  ec e9 4d 2d 53 45 41 52   ·····l·· ··M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN:
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX: 1·· ST: urn:
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65 65 6e   dial-mul tiscreen
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64 69 61   -org:ser vice:dia
00a0  6c 3a 31 0d 0a 55 53 45  52 2d 41 47 45 4e 54 3a   l:1··USE R-AGENT:
00b0  20 43 68 72 6f 6d 69 75  6d 2f 31 33 34 2e 30 2e    Chromiu m/134.0.
00c0  36 39 39 38 2e 31 37 38  20 57 69 6e 64 6f 77 73   6998.178  Windows
```

HTTP Request Method (http.request.method), 8 bytes

☑ Show packet bytes   Layout: Vertical (Stacked)

From my reference , I can clearly say'

- MDNS(Multicast DNS): Used for name resolution within small local network
- SSDP(Simple Service Discovery Protocol):used for finding services on a local network
- UDP(User Datagram Protocol):It is a transport layer protocol, to transfer data with speed and low latency

(And many more……)

By searching the findings in depth we can understand clearly about the protocols, and their usage etc.