Date: 22/08/2024

Lab Practical #08:

Study Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

Practical Assignment #08:

1. Explain usage of Wireshark tool.

Wireshark is a network protocol analyzer that captures and inspects data traveling across a network in real-time. It's an essential tool for network administrators, cybersecurity professionals, and developers for troubleshooting, analysis, and monitoring of network traffic

How to Use :

1. **Install Wireshark:** First, download and install Wireshark from the official website.
2. **Select a Network Interface:** When you open Wireshark, you'll see a list of network interfaces (like Wi-Fi, Ethernet). These represent the different connections your computer is using. Choose the one you want to monitor (e.g., your Wi-Fi connection).
3. **Start Capturing Packets:** Click the "Start Capturing Packets" button (the blue shark fin icon). Wireshark will begin recording all the network traffic passing through the selected interface.
4. **Analyze the Data:** As Wireshark captures packets, you'll see them listed in real-time with details like the source and destination IP addresses, protocols used, and data. You can stop the capture at any time to analyze the data more closely.
5. **Use Filters:** Wireshark lets you apply filters to narrow down the data. For example, you can filter by IP address, protocol, or even specific data within the packets.
6. **Save and Export:** Once you've captured the data you need, you can save it for future analysis or export it in various formats

Usage:

- **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
- **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
- **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.
- **Network Troubleshooting:** Identify and diagnose issues like slow network performance, packet loss, or connectivity problems by analyzing packet data.
- **Protocol Analysis:** Examine how specific protocols (e.g., HTTP, DNS, TCP) operate on the network, helping in debugging and understanding network communication.

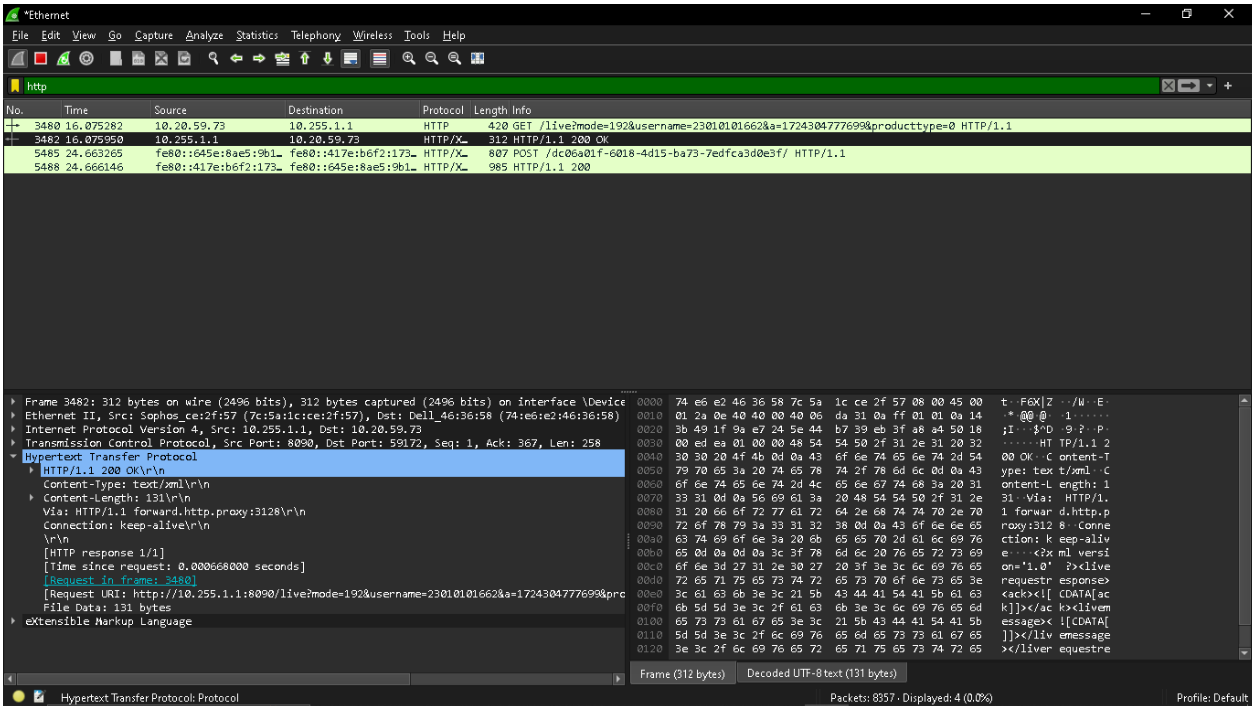
Date: 22/08/2024

- **Security Monitoring:** Detect unauthorized access, malware activity, or unusual traffic patterns that could indicate a security breach.
- **Application Performance Tuning:** Monitor and optimize the performance of networked applications by analyzing the communication between client and server.
- **VoIP Analysis:** Capture and analyze Voice over IP (VoIP) traffic to troubleshoot call quality issues and inspect SIP and RTP protocols.
- **Network Forensics:** Investigate network incidents, such as data breaches or cyberattacks, by reviewing captured packet data for evidence.
- **Learning and Education:** Study network protocols, packet structures, and traffic patterns to enhance your understanding of networking concepts.
- **Bandwidth Usage Analysis:** Monitor and analyze network bandwidth consumption to identify heavy bandwidth users or applications.
- **Network Mapping:** Visualize the flow of data across the network, helping in understanding network topology and device communication.
- **Compliance Auditing:** Ensure that network communications adhere to organizational policies and regulatory requirements by capturing and inspecting relevant traffic.

Date: 22/08/2024

2. Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

- **HTTP :**


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Frame (312 bytes)
Decoded UTF-8 text (131 bytes)
Hypertext Transfer Protocol: Protocol
Profile: Default

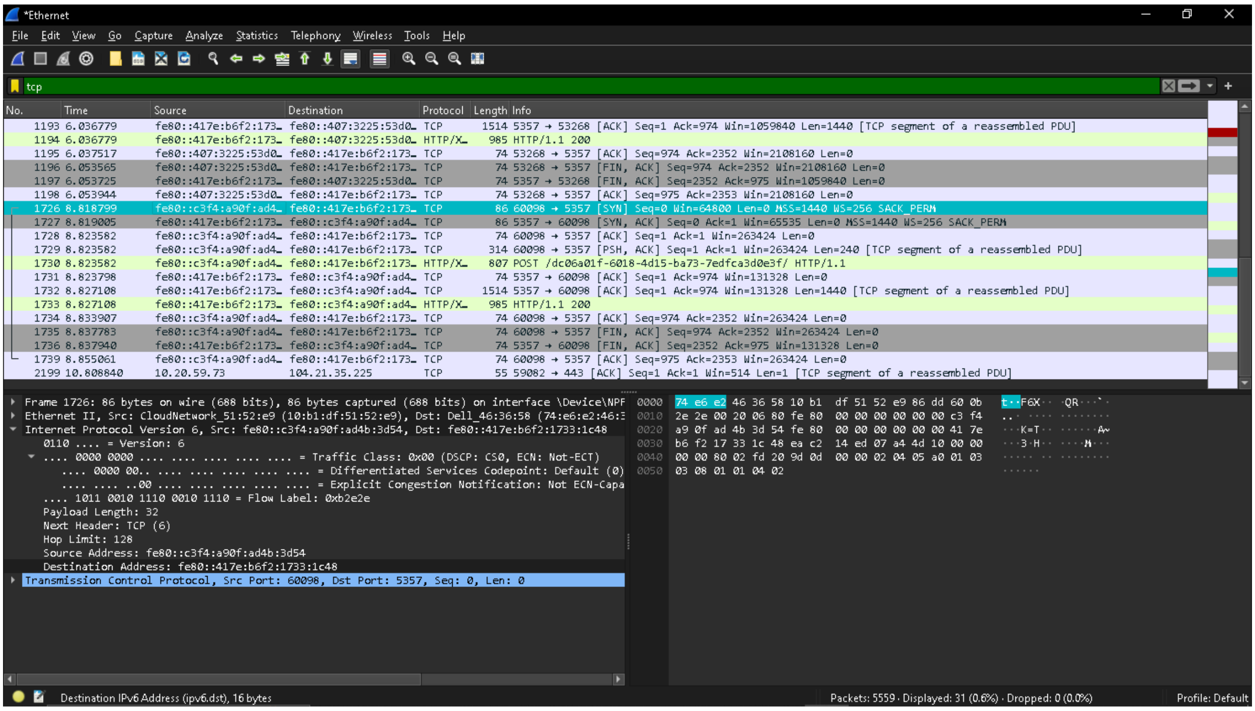
```
No.   Time       Source               Destination          Protocol  Length Info
3480 16.075282  10.20.59.73           10.255.1.1           HTTP       420 GET /live?mode=192&username=23010101662&a=1724304777699&producttype=0 HTTP/1.1
3482 16.075950  10.255.1.1            10.20.59.73          HTTP/X…    312 HTTP/1.1 200 OK
5485 24.663265  fe80::645e:8ae5:9b1…  fe80::417e:b6f2:173…  HTTP/X…    807 POST /dc06a01f-6018-4d15-ba73-7edfca3d0e3f/ HTTP/1.1
5488 24.666146  fe80::417e:b6f2:173…  fe80::645e:8ae5:9b1…  HTTP/X…    985 HTTP/1.1 200
```

```
Frame 3482: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface \Device
Ethernet II, Src: Sophos_ce:2f:57 (7c:5a:1c:ce:2f:57), Dst: Dell_46:36:58 (74:e6:e2:46:36:58)
Internet Protocol Version 4, Src: 10.255.1.1, Dst: 10.20.59.73
Transmission Control Protocol, Src Port: 8090, Dst Port: 59172, Seq: 1, Ack: 367, Len: 258
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Content-Type: text/xml\r\n
  Content-Length: 131\r\n
  Via: HTTP/1.1 forward.http.proxy:3128\r\n
  Connection: keep-alive\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.000668000 seconds]
  [Request in frame: 3480]
  [Request URI: http://10.255.1.1:8090/live?mode=192&username=23010101662&a=1724304777699&prc
  File Data: 131 bytes
eXtensible Markup Language
```

```
0000  74 e6 e2 46 36 58 7c 5a  1c ce 2f 57 08 00 45 00   t··F6X|Z ··/W··E·
0010  01 2a 0e 40 40 00 40 06  da 31 0a ff 01 01 0a 14   ·*·@@·@· ·1······
0020  3b 49 1f 9a e7 24 5e 44  b7 39 eb 3f a8 a4 50 18   ;I···$^D ·9·?··P·
0030  00 ed ea 01 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 54   00 OK··C ontent-T
0050  79 70 65 3a 20 74 65 78  74 2f 78 6d 6c 0d 0a 43   ype: tex t/xml··C
0060  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 31   ontent-L ength: 1
0070  33 31 0d 0a 56 69 61 3a  20 48 54 54 50 2f 31 2e   31··Via:  HTTP/1.
0080  31 20 66 6f 72 77 61 72  64 2e 68 74 74 70 2e 70   1 forwar d.http.p
0090  72 6f 78 79 3a 33 31 32  38 0d 0a 43 6f 6e 6e 65   roxy:312 8··Conne
00a0  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
00b0  65 0d 0a 0d 0a 3c 3f 78  6d 6c 20 76 65 72 73 69   e····<?x ml versi
00c0  6f 6e 3d 27 31 2e 30 27  20 3f 3e 3c 6c 69 76 65   on='1.0'  ?><live
00d0  72 65 71 75 65 73 74 72  65 73 70 6f 6e 73 65 3e   requestr esponse>
00e0  3c 61 63 6b 3e 3c 21 5b  43 44 41 54 41 5b 61 63   <ack><![ CDATA[ac
00f0  6b 5d 5d 3e 3c 2f 61 63  6b 3e 3c 6c 69 76 65 6d   k]]></ac k><livem
0100  65 73 73 61 67 65 3e 3c  21 5b 43 44 41 54 41 5b   essage>< ![CDATA[
0110  5d 5d 3e 3c 2f 6c 69 76  65 6d 65 73 73 61 67 65   ]]></liv emessage
0120  3e 3c 2f 6c 69 76 65 72  65 71 75 65 73 74 72 65   ></liver equestre
```

Packets: 8357 · Displayed: 4 (0.0%)

- **TCP :**


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Destination IPv6 Address (ipv6.dst), 16 bytes
Profile: Default

```
No.   Time       Source               Destination          Protocol  Length Info
1193 6.036779   fe80::417e:b6f2:173…  fe80::407:3225:53d0…  TCP       1514 5357 → 53268 [ACK] Seq=1 Ack=974 Win=1059840 Len=1440 [TCP segment of a reassembled PDU]
1194 6.036779   fe80::417e:b6f2:173…  fe80::407:3225:53d0…  HTTP/X…    985 HTTP/1.1 200
1195 6.037517   fe80::407:3225:53d0…  fe80::417e:b6f2:173…  TCP         74 53268 → 5357 [ACK] Seq=974 Ack=2352 Win=2108160 Len=0
1196 6.053565   fe80::407:3225:53d0…  fe80::417e:b6f2:173…  TCP         74 53268 → 5357 [FIN, ACK] Seq=974 Ack=2352 Win=2108160 Len=0
1197 6.053725   fe80::417e:b6f2:173…  fe80::407:3225:53d0…  TCP         74 5357 → 53268 [FIN, ACK] Seq=2352 Ack=975 Win=1059840 Len=0
1198 6.053944   fe80::407:3225:53d0…  fe80::417e:b6f2:173…  TCP         74 53268 → 5357 [ACK] Seq=975 Ack=2353 Win=2108160 Len=0
1726 8.818799   fe80::c3f4:a90f:ad4…  fe80::417e:b6f2:173…  TCP         86 60098 → 5357 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
1727 8.819005   fe80::417e:b6f2:173…  fe80::c3f4:a90f:ad4…  TCP         86 5357 → 60098 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
1728 8.823582   fe80::c3f4:a90f:ad4…  fe80::417e:b6f2:173…  TCP         74 60098 → 5357 [ACK] Seq=1 Ack=1 Win=263424 Len=0
1729 8.823582   fe80::c3f4:a90f:ad4…  fe80::417e:b6f2:173…  TCP        314 60098 → 5357 [PSH, ACK] Seq=1 Ack=1 Win=263424 Len=240 [TCP segment of a reassembled PDU]
1730 8.823582   fe80::c3f4:a90f:ad4…  fe80::417e:b6f2:173…  HTTP/X…    807 POST /dc06a01f-6018-4d15-ba73-7edfca3d0e3f/ HTTP/1.1
1731 8.823798   fe80::417e:b6f2:173…  fe80::c3f4:a90f:ad4…  TCP         74 5357 → 60098 [ACK] Seq=1 Ack=974 Win=131328 Len=0
1732 8.827108   fe80::417e:b6f2:173…  fe80::c3f4:a90f:ad4…  TCP       1514 5357 → 60098 [ACK] Seq=1 Ack=974 Win=131328 Len=1440 [TCP segment of a reassembled PDU]
1733 8.827108   fe80::417e:b6f2:173…  fe80::c3f4:a90f:ad4…  HTTP/X…    985 HTTP/1.1 200
1734 8.833907   fe80::c3f4:a90f:ad4…  fe80::417e:b6f2:173…  TCP         74 60098 → 5357 [ACK] Seq=974 Ack=2352 Win=263424 Len=0
1735 8.837783   fe80::c3f4:a90f:ad4…  fe80::417e:b6f2:173…  TCP         74 60098 → 5357 [FIN, ACK] Seq=974 Ack=2352 Win=263424 Len=0
1736 8.837940   fe80::417e:b6f2:173…  fe80::c3f4:a90f:ad4…  TCP         74 5357 → 60098 [FIN, ACK] Seq=2352 Ack=975 Win=131328 Len=0
1739 8.855061   fe80::c3f4:a90f:ad4…  fe80::417e:b6f2:173…  TCP         74 60098 → 5357 [ACK] Seq=975 Ack=2353 Win=263424 Len=0
2199 10.808840  10.20.59.73           104.21.35.225         TCP         55 59082 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
```

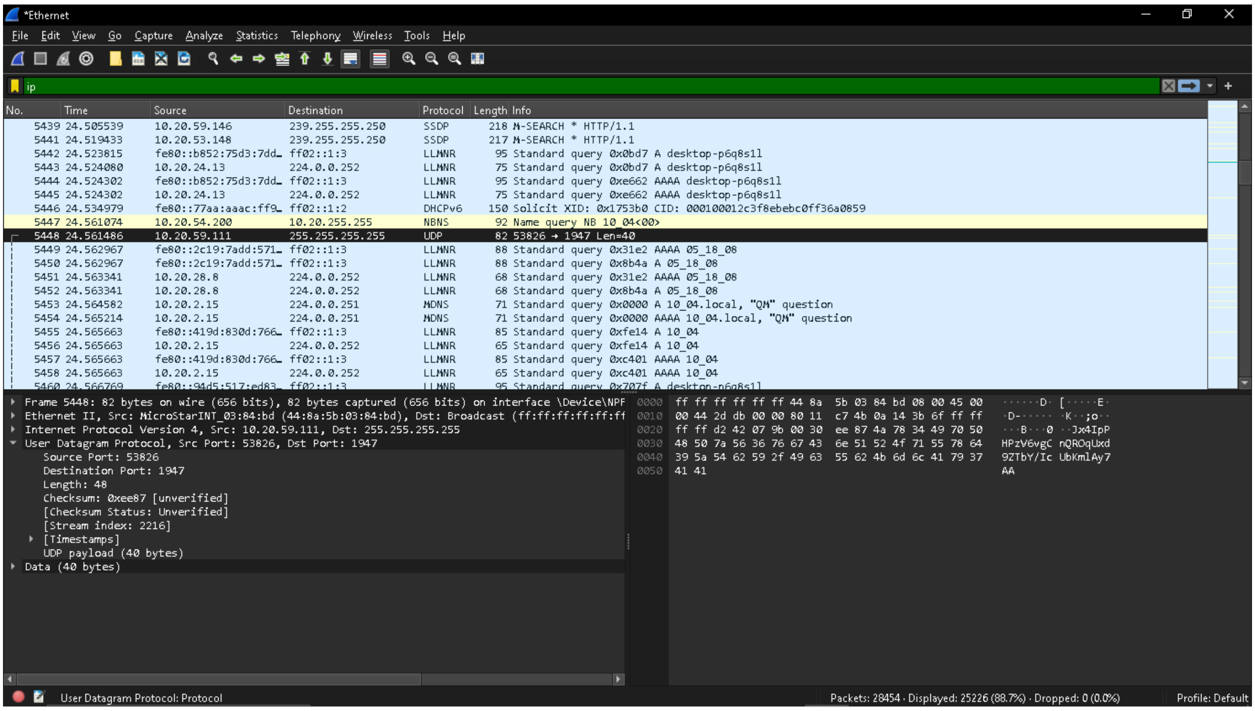
```
Frame 1726: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF
Ethernet II, Src: CloudNetwork_51:52:e9 (10:b1:df:51:52:e9), Dst: Dell_46:36:58 (74:e6:e2:46:3
Internet Protocol Version 6, Src: fe80::c3f4:a90f:ad4b:3d54, Dst: fe80::417e:b6f2:1733:1c48
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 00.. .... .... .... .... .... = Differentiated Services Codepoint: Default (0)
    .... .... ..00 .... .... .... .... .... = Explicit Congestion Notification: Not ECN-Capa
  .... 1011 0010 1110 0010 1110 = Flow Label: 0xb2e2e
  Payload Length: 32
  Next Header: TCP (6)
  Hop Limit: 128
  Source Address: fe80::c3f4:a90f:ad4b:3d54
  Destination Address: fe80::417e:b6f2:1733:1c48
Transmission Control Protocol, Src Port: 60098, Dst Port: 5357, Seq: 0, Len: 0
```

```
0000  74 e6 e2 46 36 58 10 b1  df 51 52 e9 86 dd 60 0b   t··F6X·· ·QR···`·
0010  2e 2e 00 20 06 80 fe 80  00 00 00 00 00 00 c3 f4   ..······ ········
0020  a9 0f ad 4b 3d 54 fe 80  00 00 00 00 00 00 41 7e   ···K=T·· ······A~
0030  b6 f2 17 33 1c 48 ea c2  14 ed 07 a4 4d 10 00 00   ···3·H·· ····M···
0040  00 00 80 02 fd 20 9d 0d  00 00 02 04 05 a0 01 03   ········ ········
0050  03 08 01 01 04 02                                   ······
```

Packets: 5559 · Displayed: 31 (0.6%) · Dropped: 0 (0.0%)

Date: 22/08/2024

- ## UDP :


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

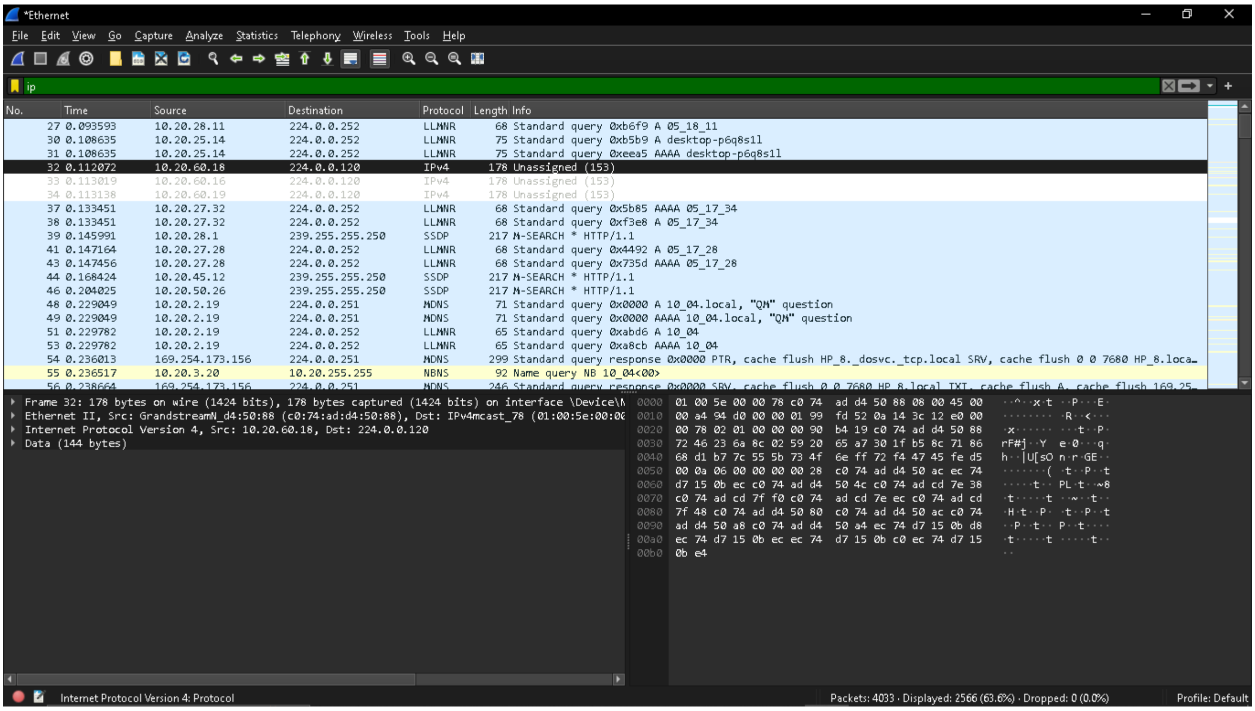
```
No.   Time      Source              Destination      Protocol Length Info
 5439 24.505539 10.20.59.146        239.255.255.250  SSDP     218 M-SEARCH * HTTP/1.1
 5441 24.519433 10.20.53.148        239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
 5442 24.523815 fe80::b852:75d3:7dd… ff02::1:3       LLMNR     95 Standard query 0x0bd7 A desktop-p6q8s1l
 5443 24.524080 10.20.24.13         224.0.0.252      LLMNR     75 Standard query 0x0bd7 A desktop-p6q8s1l
 5444 24.524302 fe80::b852:75d3:7dd… ff02::1:3       LLMNR     95 Standard query 0xe662 AAAA desktop-p6q8s1l
 5445 24.524302 10.20.24.13         224.0.0.252      LLMNR     75 Standard query 0xe662 AAAA desktop-p6q8s1l
 5446 24.534979 fe80::77aa:aaac:ff9… ff02::1:2       DHCPv6   150 Solicit XID: 0x1753b0 CID: 000100012c3f8ebebc0ff36a0859
 5447 24.561074 10.20.54.200        10.20.255.255    NBNS      92 Name query NB 10_04<00>
 5448 24.561486 10.20.59.111        255.255.255.255  UDP       82 53826 → 1947 Len=40
 5449 24.562967 fe80::2c19:7add:571… ff02::1:3       LLMNR     88 Standard query 0x31e2 AAAA 05_18_08
 5450 24.562967 fe80::2c19:7add:571… ff02::1:3       LLMNR     88 Standard query 0x8b4a A 05_18_08
 5451 24.563341 10.20.28.8          224.0.0.252      LLMNR     68 Standard query 0x31e2 AAAA 05_18_08
 5452 24.563341 10.20.28.8          224.0.0.252      LLMNR     68 Standard query 0x8b4a A 05_18_08
 5453 24.564582 10.20.2.15          224.0.0.251      MDNS      71 Standard query 0x0000 A 10_04.local, "QM" question
 5454 24.565214 10.20.2.15          224.0.0.251      MDNS      71 Standard query 0x0000 AAAA 10_04.local, "QM" question
 5455 24.565663 fe80::419d:830d:766… ff02::1:3       LLMNR     85 Standard query 0xfe14 A 10_04
 5456 24.565663 10.20.2.15          224.0.0.252      LLMNR     65 Standard query 0xfe14 A 10_04
 5457 24.565663 fe80::419d:830d:766… ff02::1:3       LLMNR     85 Standard query 0xc401 AAAA 10_04
 5458 24.565663 10.20.2.15          224.0.0.252      LLMNR     65 Standard query 0xc401 AAAA 10_04
 5460 24.566769 fe80::94d5:517:ed83… ff02::1:3       LLMNR     95 Standard query 0x707f A desktop-p6q8s1l
```

```
> Frame 5448: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF
> Ethernet II, Src: MicroStarINT_03:84:bd (44:8a:5b:03:84:bd), Dst: Broadcast (ff:ff:ff:ff:ff:ff
> Internet Protocol Version 4, Src: 10.20.59.111, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 53826, Dst Port: 1947
     Source Port: 53826
     Destination Port: 1947
     Length: 48
     Checksum: 0xee87 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 2216]
   > [Timestamps]
     UDP payload (40 bytes)
> Data (40 bytes)
```

```
0000  ff ff ff ff ff ff 44 8a  5b 03 84 bd 08 00 45 00   ······D· [·····E·
0010  00 44 2d db 00 00 80 11  c7 4b 0a 14 3b 6f ff ff   ·D-····· ·K··;o··
0020  ff ff d2 42 07 9b 00 30  ee 87 4a 78 34 49 70 50   ···B···0 ··Jx4IpP
0030  48 50 7a 56 36 76 67 43  6e 51 52 4f 71 55 78 64   HPzV6vgC nQROqUxd
0040  39 5a 54 62 59 2f 49 63  55 62 4b 6d 6c 41 79 37   9ZTbY/Ic UbKmlAy7
0050  41 41                                              AA
```

```
User Datagram Protocol: Protocol          Packets: 28454 · Displayed: 25226 (88.7%) · Dropped: 0 (0.0%)     Profile: Default
```

- ## IP :


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

```
No.   Time     Source           Destination      Protocol Length Info
   27 0.093593 10.20.28.11      224.0.0.252      LLMNR     68 Standard query 0xb6f9 A 05_18_11
   30 0.108635 10.20.25.14      224.0.0.252      LLMNR     75 Standard query 0xb5b9 A desktop-p6q8s1l
   31 0.108635 10.20.25.14      224.0.0.252      LLMNR     75 Standard query 0xeea5 AAAA desktop-p6q8s1l
   32 0.112072 10.20.60.18      224.0.0.120      IPv4     178 Unassigned (153)
   33 0.113019 10.20.60.16      224.0.0.120      IPv4     178 Unassigned (153)
   34 0.113138 10.20.60.19      224.0.0.120      IPv4     178 Unassigned (153)
   37 0.133451 10.20.27.32      224.0.0.252      LLMNR     68 Standard query 0x5b85 AAAA 05_17_34
   38 0.133451 10.20.27.32      224.0.0.252      LLMNR     68 Standard query 0xf3e8 A 05_17_34
   39 0.145991 10.20.28.1       239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
   41 0.147164 10.20.27.28      224.0.0.252      LLMNR     68 Standard query 0x4492 A 05_17_28
   43 0.147456 10.20.27.28      224.0.0.252      LLMNR     68 Standard query 0x735d AAAA 05_17_28
   44 0.168424 10.20.45.12      239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
   46 0.204025 10.20.50.26      239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
   48 0.229049 10.20.2.19       224.0.0.251      MDNS      71 Standard query 0x0000 A 10_04.local, "QM" question
   49 0.229049 10.20.2.19       224.0.0.251      MDNS      71 Standard query 0x0000 AAAA 10_04.local, "QM" question
   51 0.229782 10.20.2.19       224.0.0.252      LLMNR     65 Standard query 0xabd6 A 10_04
   53 0.229782 10.20.2.19       224.0.0.252      LLMNR     65 Standard query 0xa8cb AAAA 10_04
   54 0.236013 169.254.173.156  224.0.0.251      MDNS     299 Standard query response 0x0000 PTR, cache flush HP_8._dosvc._tcp.local SRV, cache flush 0 0 7680 HP_8.loca…
   55 0.236517 10.20.3.20       10.20.255.255    NBNS      92 Name query NB 10_04<00>
   56 0.238664 169.254.173.156  224.0.0.251      MDNS     246 Standard query response 0x0000 SRV, cache flush 0 0 7680 HP_8.local TXT, cache flush A, cache flush 169.25…
```

```
> Frame 32: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface \Device\N
> Ethernet II, Src: GrandstreamN_d4:50:88 (c0:74:ad:d4:50:88), Dst: IPv4mcast_78 (01:00:5e:00:00
> Internet Protocol Version 4, Src: 10.20.60.18, Dst: 224.0.0.120
> Data (144 bytes)
```

```
0000  01 00 5e 00 00 78 c0 74  ad d4 50 88 08 00 45 00   ··^··x·t ··P···E·
0010  00 a4 94 d0 00 00 01 99  fd 52 0a 14 3c 12 e0 00   ········ ·R··<···
0020  00 78 02 01 00 00 00 90  b4 19 c0 74 ad d4 50 88   ·x······ ···t··P·
0030  72 46 23 6a 8c 02 59 20  65 a7 30 1f b5 8c 71 86   rF#j··Y  e·0···q·
0040  68 d1 b7 7c 55 5b 73 4f  6e ff 72 f4 47 45 fe d5   h··|U[sO n·r·GE··
0050  00 0a 06 00 00 00 00 28  c0 74 ad d4 50 ac ec 74   ·······( ·t··P··t
0060  d7 15 0b ec c0 74 ad d4  50 4c c0 74 ad cd 7e 38   ·····t·· PL·t··~8
0070  c0 74 ad cd 7f f0 c0 74  ad cd 7e ec c0 74 ad cd   ·t·····t ··~··t··
0080  7f 48 c0 74 ad d4 50 80  c0 74 ad d4 50 ac c0 74   ·H·t··P· ·t··P··t
0090  ad d4 50 a8 c0 74 ad d4  50 a4 ec 74 d7 15 0b d8   ··P··t·· P··t····
00a0  ec 74 d7 15 0b ec ec 74  d7 15 0b c0 ec 74 d7 15   ·t·····t ·····t··
00b0  0b e4                                              ··
```

```
Internet Protocol Version 4: Protocol     Packets: 4033 · Displayed: 2566 (63.6%) · Dropped: 0 (0.0%)     Profile: Default
```