Date: 29/08 /2024

Lab Practical #08:

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

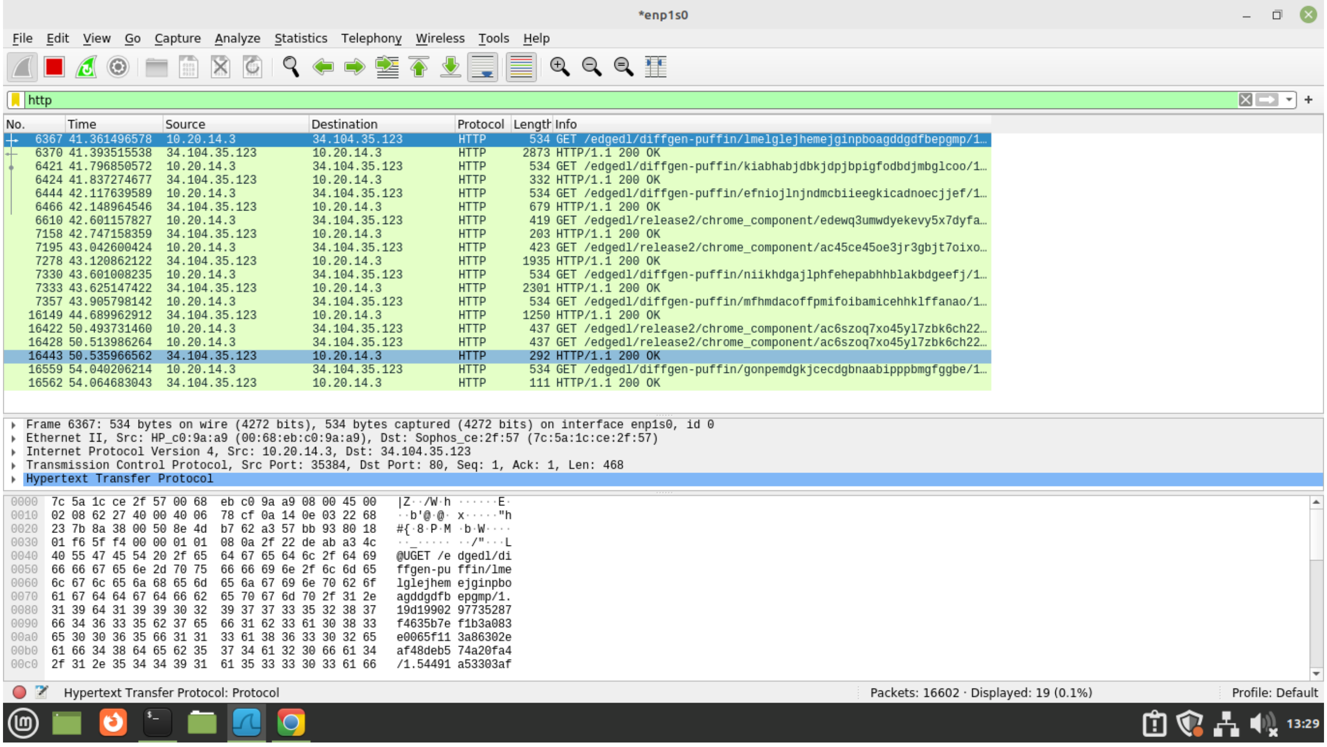
Practical Assignment #08:

1. Explain usage of Wireshark tool.

Wireshark is an open-source tool very widely used to traffic in a network in real time. It helps us to analyses the data packets flowing in the network thus providing valuable information about the network behavior and its performance as well as security.

Wireshark is a network analyzer that captures and examines network traffic. It operates by capturing packets from a network interface or reading packets from a capture file. It then decodes and analyzes these packets, providing detailed information about the protocols, conversations, and network behavior.

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



http

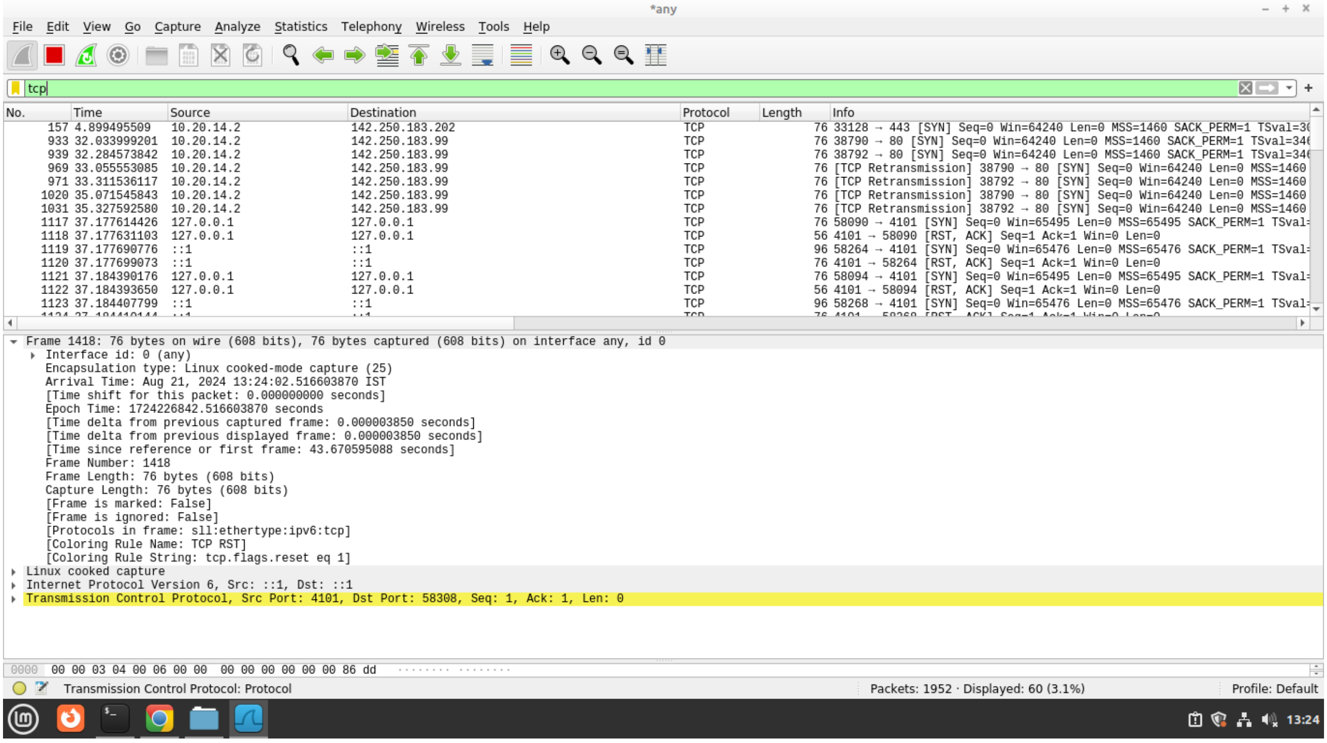
```
No.    Time          Source          Destination     Protocol Length Info
 6367 41.361496578  10.20.14.3      34.104.35.123   HTTP      534 GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1…
 6370 41.393515538  34.104.35.123   10.20.14.3      HTTP     2873 HTTP/1.1 200 OK
 6421 41.796850572  10.20.14.3      34.104.35.123   HTTP      534 GET /edgedl/diffgen-puffin/kiabhabjdbkjdpjbpigfodbdjmbglcoo/1…
 6424 41.837274677  34.104.35.123   10.20.14.3      HTTP      332 HTTP/1.1 200 OK
 6444 42.117639589  10.20.14.3      34.104.35.123   HTTP      534 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1…
 6466 42.148964546  34.104.35.123   10.20.14.3      HTTP      679 HTTP/1.1 200 OK
 6610 42.601157827  10.20.14.3      34.104.35.123   HTTP      419 GET /edgedl/release2/chrome_component/edewq3umwdyekevy5x7dyfa…
 7158 42.747158359  34.104.35.123   10.20.14.3      HTTP      203 HTTP/1.1 200 OK
 7195 43.042600424  10.20.14.3      34.104.35.123   HTTP      423 GET /edgedl/release2/chrome_component/ac45ce45oe3jr3gbjt7oixo…
 7278 43.120862122  34.104.35.123   10.20.14.3      HTTP     1935 HTTP/1.1 200 OK
 7330 43.601008235  10.20.14.3      34.104.35.123   HTTP      534 GET /edgedl/diffgen-puffin/niikhdgajlphfehepabhhblakbdgeefj/1…
 7333 43.625147422  34.104.35.123   10.20.14.3      HTTP     2301 HTTP/1.1 200 OK
 7357 43.905798142  10.20.14.3      34.104.35.123   HTTP      534 GET /edgedl/diffgen-puffin/mfhmdacoffpmifoibamicehhklffanao/1…
16149 44.689962912  34.104.35.123   10.20.14.3      HTTP     1250 HTTP/1.1 200 OK
16422 50.493731460  10.20.14.3      34.104.35.123   HTTP      437 GET /edgedl/release2/chrome_component/ac6szoq7xo45yl7zbk6ch22…
16428 50.513986264  10.20.14.3      34.104.35.123   HTTP      437 GET /edgedl/release2/chrome_component/ac6szoq7xo45yl7zbk6ch22…
16443 50.535966562  34.104.35.123   10.20.14.3      HTTP      292 HTTP/1.1 200 OK
16559 54.040206214  10.20.14.3      34.104.35.123   HTTP      534 GET /edgedl/diffgen-puffin/gonpemdgkjcecdgbnaabipppbmgfggbe/1…
16562 54.064683043  34.104.35.123   10.20.14.3      HTTP      111 HTTP/1.1 200 OK
```

```
Frame 6367: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface enp1s0, id 0
Ethernet II, Src: HP_c0:9a:a9 (00:68:eb:c0:9a:a9), Dst: Sophos_ce:2f:57 (7c:5a:1c:ce:2f:57)
Internet Protocol Version 4, Src: 10.20.14.3, Dst: 34.104.35.123
Transmission Control Protocol, Src Port: 35384, Dst Port: 80, Seq: 1, Ack: 1, Len: 468
Hypertext Transfer Protocol
```

```
0000  7c 5a 1c ce 2f 57 00 68  eb c0 9a a9 08 00 45 00   |Z··/W·h ······E·
0010  02 08 62 27 40 00 40 06  78 cf 0a 14 0e 03 22 68   ··b'@·@· x·····"h
0020  23 7b 8a 38 00 50 8e 4d  b7 62 a3 57 bb 93 80 18   #{·8·P·M ·b·W····
0030  01 f6 5f f4 00 00 01 01  08 0a 2f 22 de ab a3 4c   ··_····· ··/"···L
0040  40 55 47 45 54 20 2f 65  64 67 65 64 6c 2f 64 69   @UGET /e dgedl/di
0050  66 66 67 65 6e 2d 70 75  66 66 69 6e 2f 6c 6d 65   ffgen-pu ffin/lme
0060  6c 67 6c 65 6a 68 65 6d  65 6a 67 69 6e 70 62 6f   lglejhem ejginpbo
0070  61 67 64 64 67 64 66 62  65 70 67 6d 70 2f 31 2e   agddgdfb epgmp/1.
0080  31 39 64 31 39 39 30 32  39 37 37 33 35 32 38 37   19d19902 97735287
0090  66 34 36 33 35 62 37 65  66 31 62 33 61 30 38 33   f4635b7e f1b3a083
00a0  65 30 30 36 35 66 31 31  33 61 38 36 33 30 32 65   e0065f11 3a86302e
00b0  61 66 34 38 64 65 62 35  37 34 61 32 30 66 61 34   af48deb5 74a20fa4
00c0  2f 31 2e 35 34 34 39 31  61 35 33 33 30 33 61 66   /1.54491 a53303af
```

Hypertext Transfer Protocol: Protocol   Packets: 16602 · Displayed: 19 (0.1%)   Profile: Default

Date: 29/08 /2024


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

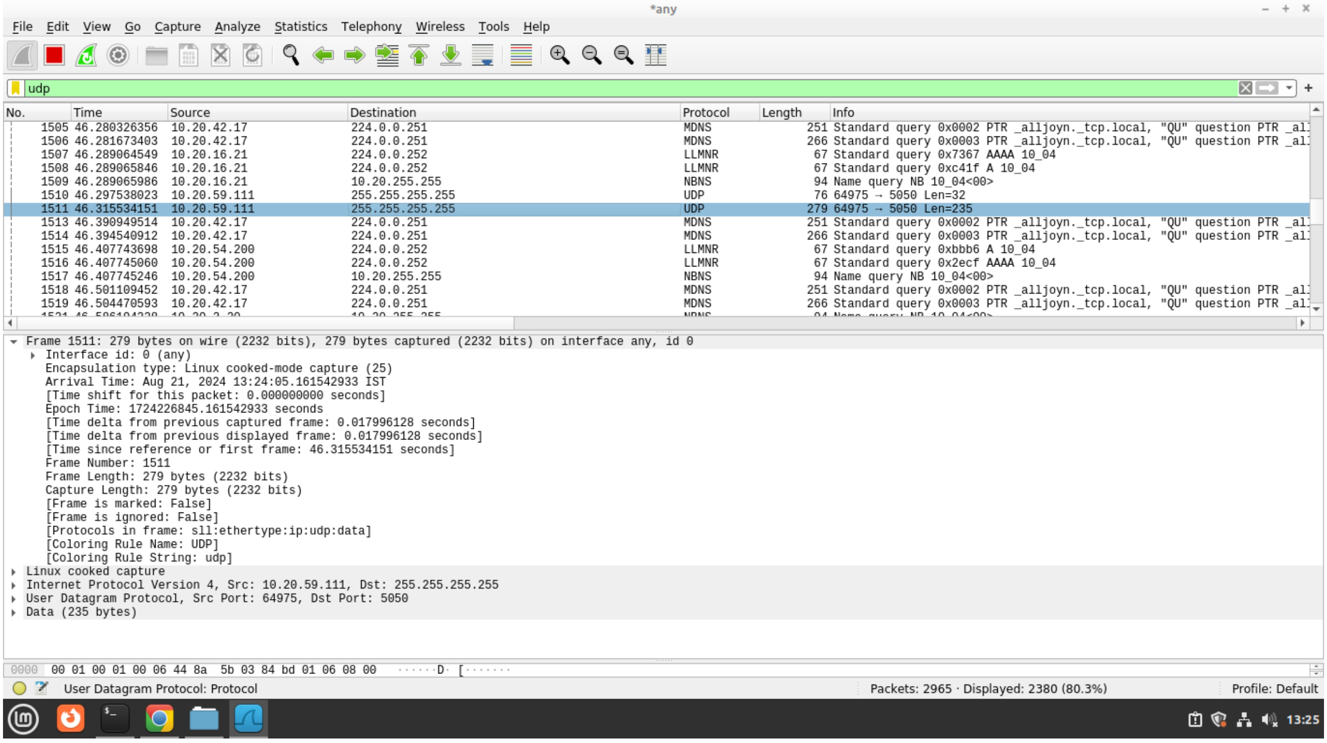
tcp

```
No.    Time          Source        Destination       Protocol  Length  Info
   157 4.899495509   10.20.14.2    142.250.183.202   TCP         76 33128 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3(
   933 32.033999201  10.20.14.2    142.250.183.99    TCP         76 38790 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=34(
   939 32.284573842  10.20.14.2    142.250.183.99    TCP         76 38792 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=34(
   969 33.055553085  10.20.14.2    142.250.183.99    TCP         76 [TCP Retransmission] 38790 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
   971 33.311536117  10.20.14.2    142.250.183.99    TCP         76 [TCP Retransmission] 38792 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
  1020 35.071545843  10.20.14.2    142.250.183.99    TCP         76 [TCP Retransmission] 38790 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
  1031 35.327592580  10.20.14.2    142.250.183.99    TCP         76 [TCP Retransmission] 38792 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
  1117 37.177614426  127.0.0.1     127.0.0.1         TCP         76 58090 → 4101 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=
  1118 37.177631103  127.0.0.1     127.0.0.1         TCP         56 4101 → 58090 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  1119 37.177690776  ::1           ::1               TCP         96 58264 → 4101 [SYN] Seq=0 Win=65476 Len=0 MSS=65476 SACK_PERM=1 TSval=
  1120 37.177699073  ::1           ::1               TCP         76 4101 → 58264 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  1121 37.184390176  127.0.0.1     127.0.0.1         TCP         76 58094 → 4101 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=
  1122 37.184393650  127.0.0.1     127.0.0.1         TCP         56 4101 → 58094 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  1123 37.184407799  ::1           ::1               TCP         96 58268 → 4101 [SYN] Seq=0 Win=65476 Len=0 MSS=65476 SACK_PERM=1 TSval=
```

```
Frame 1418: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
  Interface id: 0 (any)
  Encapsulation type: Linux cooked-mode capture (25)
  Arrival Time: Aug 21, 2024 13:24:02.516603870 IST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1724226842.516603870 seconds
  [Time delta from previous captured frame: 0.000003850 seconds]
  [Time delta from previous displayed frame: 0.000003850 seconds]
  [Time since reference or first frame: 43.670595088 seconds]
  Frame Number: 1418
  Frame Length: 76 bytes (608 bits)
  Capture Length: 76 bytes (608 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ethertype:ipv6:tcp]
  [Coloring Rule Name: TCP RST]
  [Coloring Rule String: tcp.flags.reset eq 1]
Linux cooked capture
Internet Protocol Version 6, Src: ::1, Dst: ::1
Transmission Control Protocol, Src Port: 4101, Dst Port: 58308, Seq: 1, Ack: 1, Len: 0

0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 86 dd   ········ ········
```

Transmission Control Protocol: Protocol   Packets: 1952 · Displayed: 60 (3.1%)   Profile: Default


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

udp

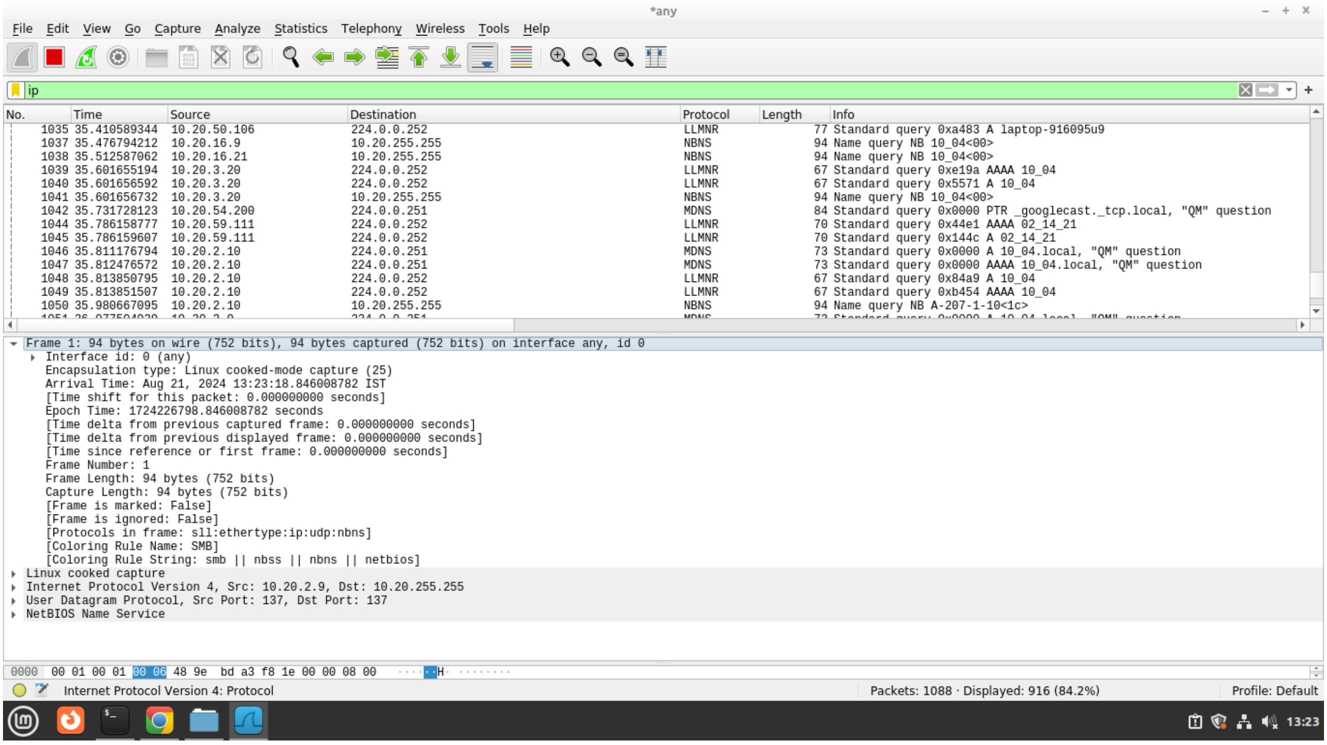
```
No.    Time          Source        Destination       Protocol  Length  Info
  1505 46.280326356  10.20.42.17   224.0.0.251       MDNS       251 Standard query 0x0002 PTR _alljoyn._tcp.local, "QU" question PTR _al]
  1506 46.281673403  10.20.42.17   224.0.0.251       MDNS       266 Standard query 0x0003 PTR _alljoyn._tcp.local, "QU" question PTR _al]
  1507 46.289064549  10.20.16.21   224.0.0.252       LLMNR       67 Standard query 0x7367 AAAA 10_04
  1508 46.289065846  10.20.16.21   224.0.0.252       LLMNR       67 Standard query 0xc41f A 10_04
  1509 46.289065986  10.20.16.21   10.20.255.255     NBNS        94 Name query NB 10_04<00>
  1510 46.297538023  10.20.59.111  255.255.255.255   UDP         76 64975 → 5050 Len=32
  1511 46.315534151  10.20.59.111  255.255.255.255   UDP        279 64975 → 5050 Len=235
  1513 46.390949514  10.20.42.17   224.0.0.251       MDNS       251 Standard query 0x0002 PTR _alljoyn._tcp.local, "QU" question PTR _al]
  1514 46.394540912  10.20.42.17   224.0.0.251       MDNS       266 Standard query 0x0003 PTR _alljoyn._tcp.local, "QU" question PTR _al]
  1515 46.407743698  10.20.54.200  224.0.0.252       LLMNR       67 Standard query 0xbbb6 A 10_04
  1516 46.407745060  10.20.54.200  224.0.0.252       LLMNR       67 Standard query 0x2ecf AAAA 10_04
  1517 46.407745246  10.20.54.200  10.20.255.255     NBNS        94 Name query NB 10_04<00>
  1518 46.501109452  10.20.42.17   224.0.0.251       MDNS       251 Standard query 0x0002 PTR _alljoyn._tcp.local, "QU" question PTR _al]
  1519 46.504470593  10.20.42.17   224.0.0.251       MDNS       266 Standard query 0x0003 PTR _alljoyn._tcp.local, "QU" question PTR _al]
```

```
Frame 1511: 279 bytes on wire (2232 bits), 279 bytes captured (2232 bits) on interface any, id 0
  Interface id: 0 (any)
  Encapsulation type: Linux cooked-mode capture (25)
  Arrival Time: Aug 21, 2024 13:24:05.161542933 IST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1724226845.161542933 seconds
  [Time delta from previous captured frame: 0.017996128 seconds]
  [Time delta from previous displayed frame: 0.017996128 seconds]
  [Time since reference or first frame: 46.315534151 seconds]
  Frame Number: 1511
  Frame Length: 279 bytes (2232 bits)
  Capture Length: 279 bytes (2232 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ethertype:ip:udp:data]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
Linux cooked capture
Internet Protocol Version 4, Src: 10.20.59.111, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 64975, Dst Port: 5050
Data (235 bytes)

0000  00 01 00 01 00 06 44 8a  5b 03 84 bd 01 06 08 00   ······D· [·······
```

User Datagram Protocol: Protocol   Packets: 2965 · Displayed: 2380 (80.3%)   Profile: Default

Date: 29/08 /2024



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

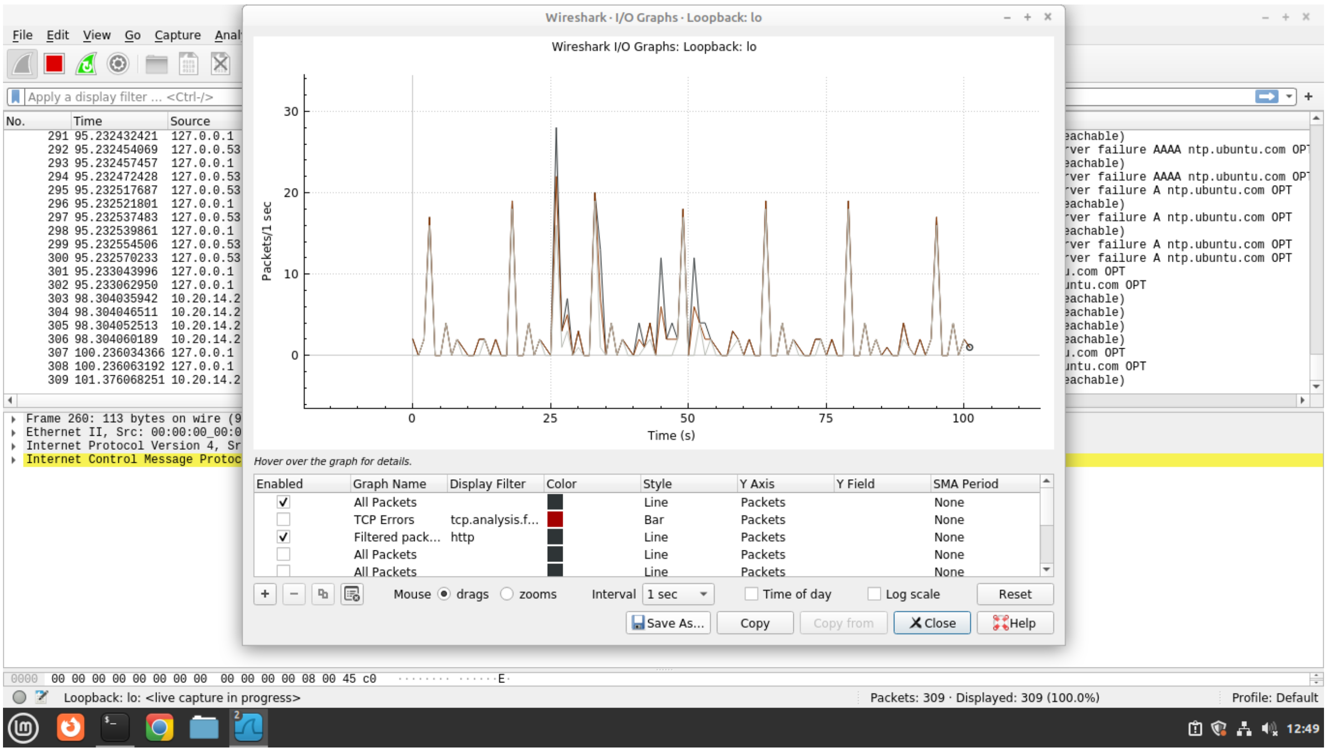
ip

```
No.  Time         Source         Destination    Protocol Length Info
1035 35.410589344 10.20.50.106   224.0.0.252    LLMNR    77 Standard query 0xa483 A laptop-916095u9
1037 35.476794212 10.20.16.9     10.20.255.255  NBNS     94 Name query NB 10_04<00>
1038 35.512587062 10.20.16.21    10.20.255.255  NBNS     94 Name query NB 10_04<00>
1039 35.601655194 10.20.3.20     224.0.0.252    LLMNR    67 Standard query 0xe19a AAAA 10_04
1040 35.601656592 10.20.3.20     224.0.0.252    LLMNR    67 Standard query 0x5571 A 10_04
1041 35.601656732 10.20.3.20     10.20.255.255  NBNS     94 Name query NB 10_04<00>
1042 35.731728123 10.20.54.200   224.0.0.251    MDNS     84 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
1044 35.786158777 10.20.59.111   224.0.0.252    LLMNR    70 Standard query 0x44e1 AAAA 02_14_21
1045 35.786159607 10.20.59.111   224.0.0.252    LLMNR    70 Standard query 0x144c A 02_14_21
1046 35.811176794 10.20.2.10     224.0.0.251    MDNS     73 Standard query 0x0000 A 10_04.local, "QM" question
1047 35.812476572 10.20.2.10     224.0.0.251    MDNS     73 Standard query 0x0000 AAAA 10_04.local, "QM" question
1048 35.813850795 10.20.2.10     224.0.0.252    LLMNR    67 Standard query 0x84a9 A 10_04
1049 35.813851507 10.20.2.10     224.0.0.252    LLMNR    67 Standard query 0xb454 AAAA 10_04
1050 35.980667095 10.20.2.10     10.20.255.255  NBNS     94 Name query NB A-207-1-10<1c>
```

```
Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface any, id 0
    Interface id: 0 (any)
    Encapsulation type: Linux cooked-mode capture (25)
    Arrival Time: Aug 21, 2024 13:23:18.846008782 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1724226798.846008782 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 94 bytes (752 bits)
    Capture Length: 94 bytes (752 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: sll:ethertype:ip:udp:nbns]
    [Coloring Rule Name: SMB]
    [Coloring Rule String: smb || nbss || nbns || netbios]
Linux cooked capture
Internet Protocol Version 4, Src: 10.20.2.9, Dst: 10.20.255.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
```

```
0000  00 01 00 01 00 06 48 9e  bd a3 f8 1e 00 00 08 00   ······H· ········
```

Internet Protocol Version 4: Protocol | Packets: 1088 · Displayed: 916 (84.2%) | Profile: Default



Wireshark · I/O Graphs · Loopback: lo
Wireshark I/O Graphs: Loopback: lo
30
20
10
0
Packets/1 sec
0
25
50
75
100
Time (s)
File Edit View Go Capture Anal
12:49

Apply a display filter ... <Ctrl-/>

```
No.  Time          Source
291 95.232432421  127.0.0.1
292 95.232454069  127.0.0.53
293 95.232457457  127.0.0.1
294 95.232472428  127.0.0.53
295 95.232517687  127.0.0.53
296 95.232521801  127.0.0.1
297 95.232537483  127.0.0.53
298 95.232539861  127.0.0.1
299 95.232554506  127.0.0.53
300 95.232570233  127.0.0.53
301 95.233043996  127.0.0.1
302 95.233062950  127.0.0.1
303 98.304035942  10.20.14.2
304 98.304046511  10.20.14.2
305 98.304052513  10.20.14.2
306 98.304060189  10.20.14.2
307 100.236034366 127.0.0.1
308 100.236063192 127.0.0.1
309 101.376068251 10.20.14.2
```

```
eachable)
rver failure AAAA ntp.ubuntu.com OP
eachable)
rver failure AAAA ntp.ubuntu.com OP
rver failure A ntp.ubuntu.com OPT
eachable)
rver failure A ntp.ubuntu.com OPT
eachable)
rver failure A ntp.ubuntu.com OPT
rver failure A ntp.ubuntu.com OPT
u.com OPT
untu.com OPT
eachable)
eachable)
eachable)
eachable)
u.com OPT
untu.com OPT
eachable)
```

```
Frame 260: 113 bytes on wire (9
Ethernet II, Src: 00:00:00_00:0
Internet Protocol Version 4, Sr
Internet Control Message Protoc
```

Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	All Packets		■	Line	Packets		None
□	TCP Errors	tcp.analysis.f...	🟥	Bar	Packets		None
☑	Filtered pack...	http	■	Line	Packets		None
□	All Packets		■	Line	Packets		None
□	All Packets		■	Line	Packets		None

Mouse ● drags ○ zooms | Interval 1 sec | □ Time of day | □ Log scale | Reset

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 c0   ········ ······E·
```

Loopback: lo: <live capture in progress> | Packets: 309 · Displayed: 309 (100.0%) | Profile: Default