EXPERIMENT NO-9

CN-C32-2103167

Aim :-

Use wireshark to understand the operation of TCP/IP layers.

- Ethernet layers: Frame header/Frame sized.
- Data link Layer :- MAC address ; ARP.
  (IP & MAC addressing)
- Network Layer: IP packet.
- Transport layer: TCP Paset, TCP, handshake segments etc.

Application Layer :- DHCP, FTP, HTP. header format.

Theory :-

Wireshark is a popular, open source network protocol analysis used for capturing and inspecting packets on a network. It is a powerful tool for network administrators, security professionals and students.

The objective of this experiment is to use wire shark, a network protocol analysis, to capture and analyze network traffic to understand the operation of various layer of TCP/IP protocol suite.

CN-682-2103164

1.) Ethernet layer.

This layer deals with frames, which are pack packets of data of data at the ethernet layer packets of data ethernet frames. One can observe the size of ethernet frames. one can observe the size of ethernet frames. One can observe the siz of ethernet frames. Ethernet frames have headers containing info rmation. like source & destination MAC address.

2.) Data link layer

The data link layer deal with MAC address Wireshark will you the MAC addresses of the addresses of the devics communicating in network. Users can capture ARP to packet to see how devices map, IP addresses to MAC addresses.

3.) Network Layer.

This layer involves a lot of processes. It involvs IP packets. Wireshark displays IP headers with information like source & destination IP address. ~~source~~ ICMP packet can be captured to observe network troubleshooting, messages, like ping request & replies.

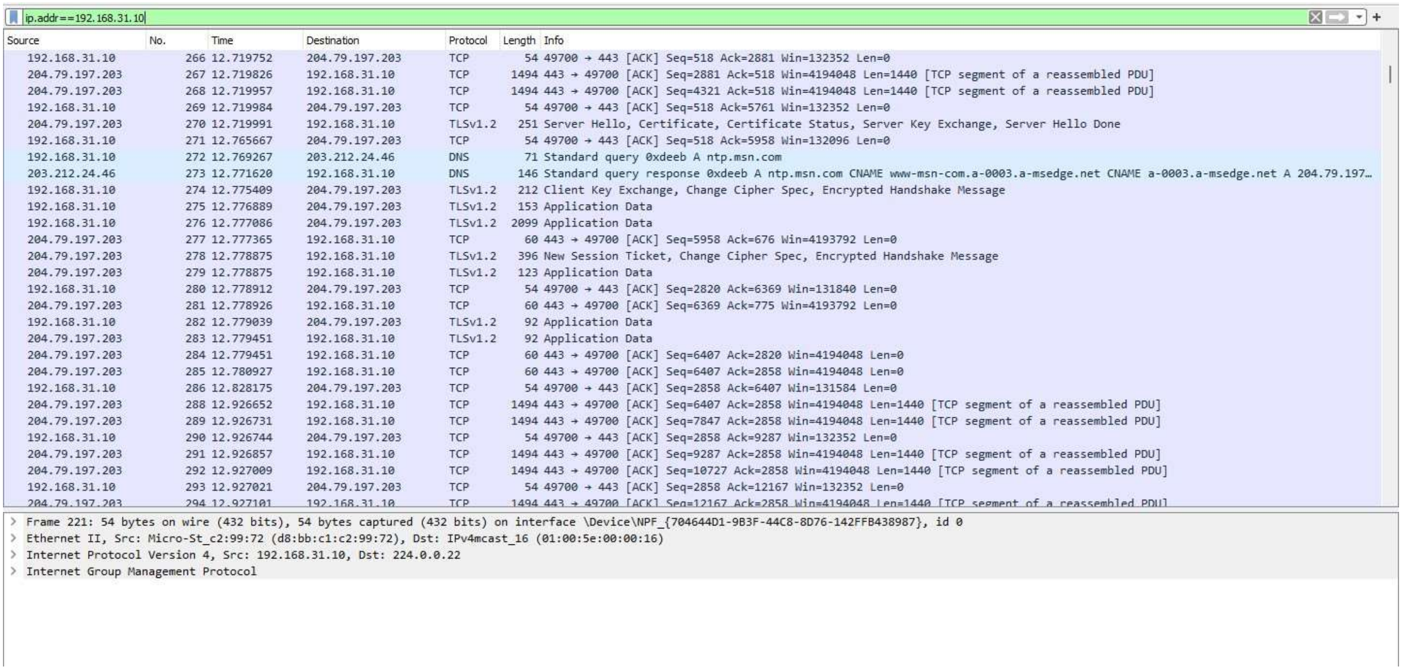
Transport layers :-

CN - C32 - 2103164

User can see which ports the used by application (eg:- web browsers, emails clients) for communication. By capturing TCP traffic, you can see three -way handshake process, which is how two devices establish a connect.

B+

1. Internet Protocol (IP)

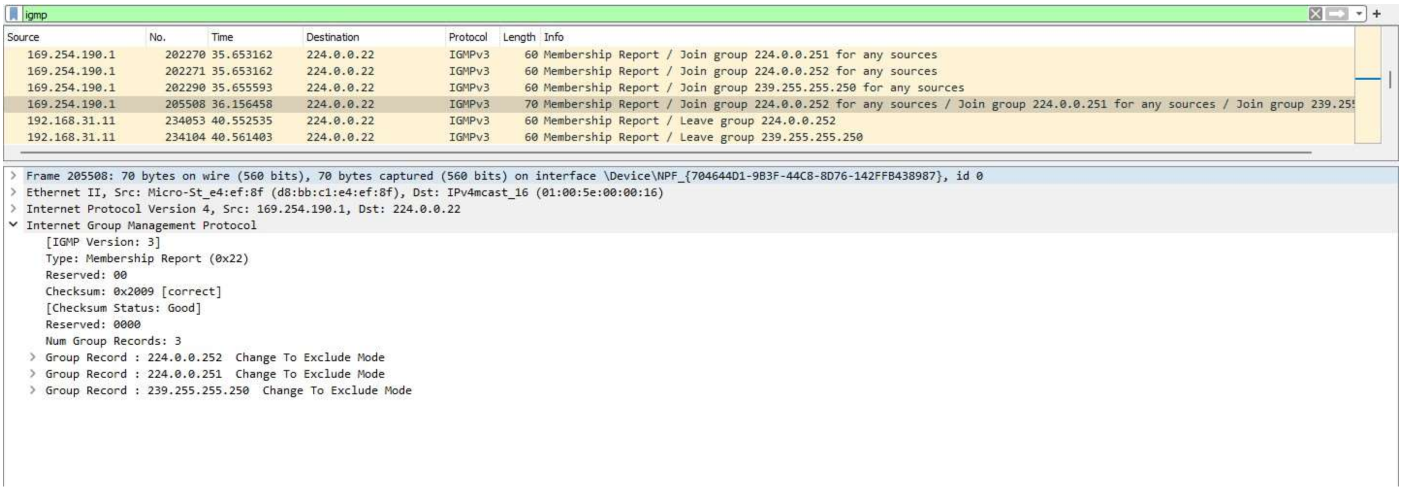


```
ip.addr==192.168.31.10

Source          No.    Time       Destination     Protocol Length Info
192.168.31.10     266 12.719752   204.79.197.203  TCP        54 49700 → 443 [ACK] Seq=518 Ack=2881 Win=132352 Len=0
204.79.197.203    267 12.719826   192.168.31.10   TCP      1494 443 → 49700 [ACK] Seq=2881 Ack=518 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
204.79.197.203    268 12.719957   192.168.31.10   TCP      1494 443 → 49700 [ACK] Seq=4321 Ack=518 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
192.168.31.10     269 12.719984   204.79.197.203  TCP        54 49700 → 443 [ACK] Seq=518 Ack=5761 Win=132352 Len=0
204.79.197.203    270 12.719991   192.168.31.10   TLSv1.2   251 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
192.168.31.10     271 12.765667   204.79.197.203  TCP        54 49700 → 443 [ACK] Seq=518 Ack=5958 Win=132096 Len=0
192.168.31.10     272 12.769267   203.212.24.46   DNS        71 Standard query 0xdeeb A ntp.msn.com
203.212.24.46     273 12.771620   192.168.31.10   DNS       146 Standard query response 0xdeeb A ntp.msn.com CNAME www-msn-com.a-0003.a-msedge.net CNAME a-0003.a-msedge.net A 204.79.197…
192.168.31.10     274 12.775409   204.79.197.203  TLSv1.2   212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
192.168.31.10     275 12.776889   204.79.197.203  TLSv1.2   153 Application Data
192.168.31.10     276 12.777086   204.79.197.203  TLSv1.2  2099 Application Data
204.79.197.203    277 12.777365   192.168.31.10   TCP        60 443 → 49700 [ACK] Seq=5958 Ack=676 Win=4193792 Len=0
204.79.197.203    278 12.778875   192.168.31.10   TLSv1.2   396 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
204.79.197.203    279 12.778875   192.168.31.10   TLSv1.2   123 Application Data
192.168.31.10     280 12.778912   204.79.197.203  TCP        54 49700 → 443 [ACK] Seq=2820 Ack=6369 Win=131840 Len=0
204.79.197.203    281 12.778926   192.168.31.10   TCP        60 443 → 49700 [ACK] Seq=6369 Ack=775 Win=4193792 Len=0
192.168.31.10     282 12.779039   204.79.197.203  TLSv1.2    92 Application Data
204.79.197.203    283 12.779451   192.168.31.10   TLSv1.2    92 Application Data
204.79.197.203    284 12.779451   192.168.31.10   TCP        60 443 → 49700 [ACK] Seq=6407 Ack=2820 Win=4194048 Len=0
204.79.197.203    285 12.780927   192.168.31.10   TCP        60 443 → 49700 [ACK] Seq=6407 Ack=2858 Win=4194048 Len=0
192.168.31.10     286 12.828175   204.79.197.203  TCP        54 49700 → 443 [ACK] Seq=2858 Ack=6407 Win=131584 Len=0
204.79.197.203    288 12.926652   192.168.31.10   TCP      1494 443 → 49700 [ACK] Seq=6407 Ack=2858 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
204.79.197.203    289 12.926731   192.168.31.10   TCP      1494 443 → 49700 [ACK] Seq=7847 Ack=2858 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
192.168.31.10     290 12.926744   204.79.197.203  TCP        54 49700 → 443 [ACK] Seq=2858 Ack=9287 Win=132352 Len=0
204.79.197.203    291 12.926857   192.168.31.10   TCP      1494 443 → 49700 [ACK] Seq=9287 Ack=2858 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
204.79.197.203    292 12.927009   192.168.31.10   TCP      1494 443 → 49700 [ACK] Seq=10727 Ack=2858 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
192.168.31.10     293 12.927021   204.79.197.203  TCP        54 49700 → 443 [ACK] Seq=2858 Ack=12167 Win=132352 Len=0
204.79.197.203    294 12.927101   192.168.31.10   TCP      1494 443 → 49700 [ACK] Seq=12167 Ack=2858 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]

> Frame 221: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{704644D1-9B3F-44C8-8D76-142FFB438987}, id 0
> Ethernet II, Src: Micro-St_c2:99:72 (d8:bb:c1:c2:99:72), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 224.0.0.22
> Internet Group Management Protocol
```

2. Internet Group Management Protocol (IGMP)

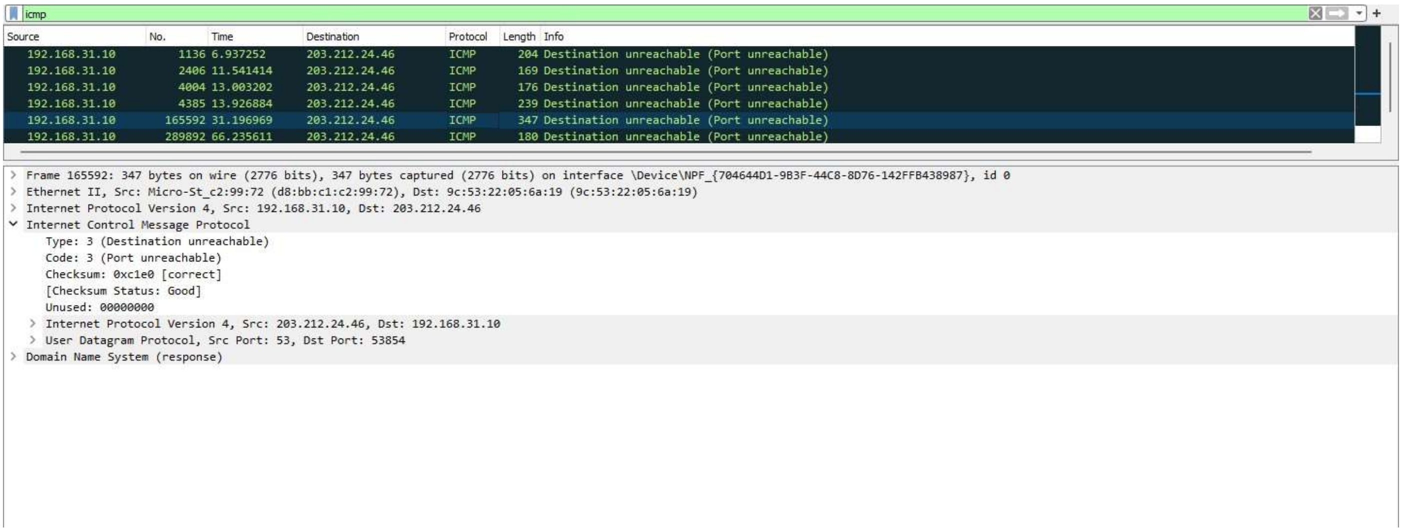


```
igmp

Source          No.     Time       Destination  Protocol Length Info
169.254.190.1    202270 35.653162  224.0.0.22   IGMPv3     60 Membership Report / Join group 224.0.0.251 for any sources
169.254.190.1    202271 35.653162  224.0.0.22   IGMPv3     60 Membership Report / Join group 224.0.0.252 for any sources
169.254.190.1    202290 35.655593  224.0.0.22   IGMPv3     60 Membership Report / Join group 239.255.255.250 for any sources
169.254.190.1    205508 36.156458  224.0.0.22   IGMPv3     70 Membership Report / Join group 224.0.0.252 for any sources / Join group 224.0.0.251 for any sources / Join group 239.25
192.168.31.11    234053 40.552535  224.0.0.22   IGMPv3     60 Membership Report / Leave group 224.0.0.252
192.168.31.11    234104 40.561403  224.0.0.22   IGMPv3     60 Membership Report / Leave group 239.255.255.250

> Frame 205508: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{704644D1-9B3F-44C8-8D76-142FFB438987}, id 0
> Ethernet II, Src: Micro-St_e4:ef:8f (d8:bb:c1:e4:ef:8f), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
> Internet Protocol Version 4, Src: 169.254.190.1, Dst: 224.0.0.22
v Internet Group Management Protocol
    [IGMP Version: 3]
    Type: Membership Report (0x22)
    Reserved: 00
    Checksum: 0x2009 [correct]
    [Checksum Status: Good]
    Reserved: 0000
    Num Group Records: 3
  > Group Record : 224.0.0.252  Change To Exclude Mode
  > Group Record : 224.0.0.251  Change To Exclude Mode
  > Group Record : 239.255.255.250  Change To Exclude Mode
```

3. Internet Control Message Protocol (ICMP)

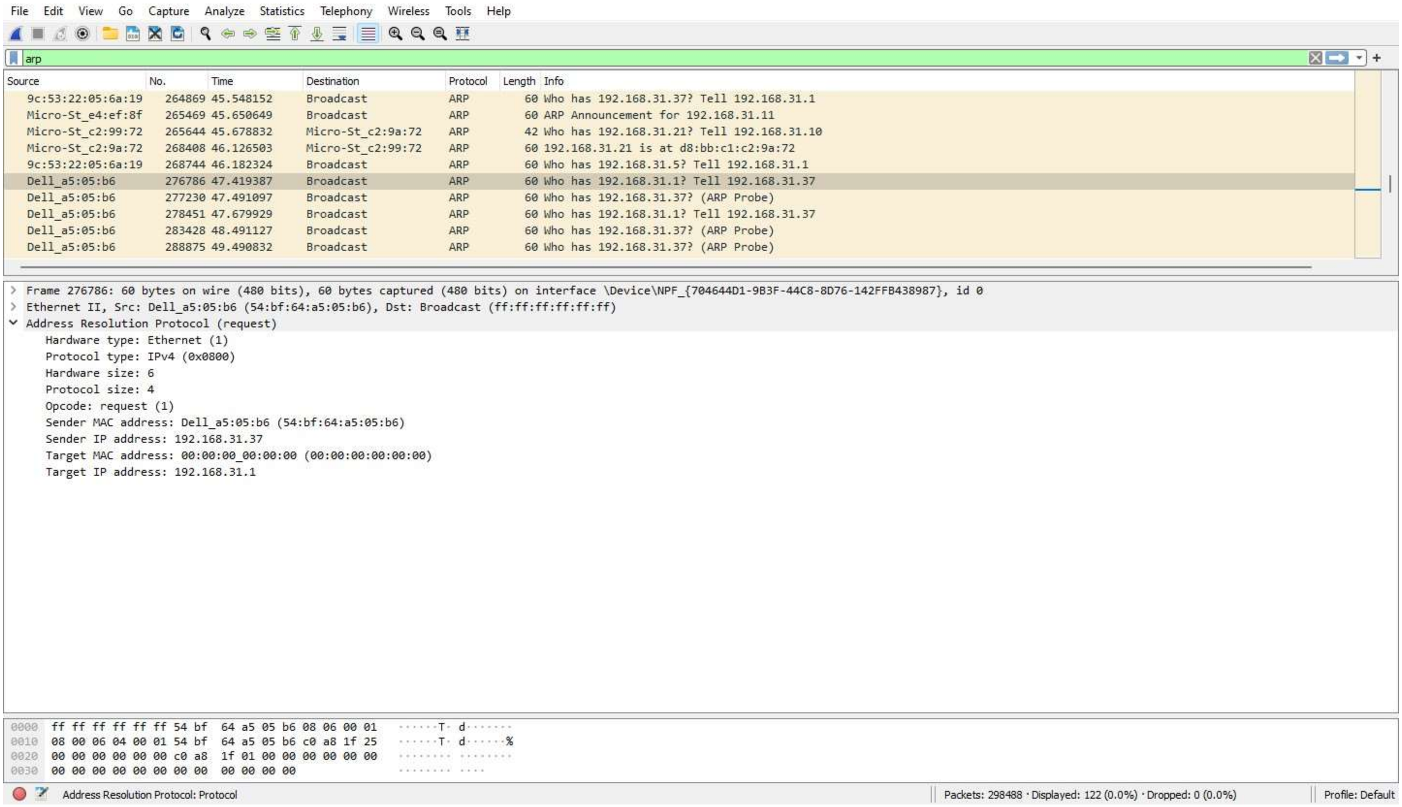


```
icmp

Source          No.     Time       Destination    Protocol Length Info
192.168.31.10      1136 6.937252   203.212.24.46  ICMP      204 Destination unreachable (Port unreachable)
192.168.31.10      2406 11.541414  203.212.24.46  ICMP      169 Destination unreachable (Port unreachable)
192.168.31.10      4004 13.003202  203.212.24.46  ICMP      176 Destination unreachable (Port unreachable)
192.168.31.10      4385 13.926884  203.212.24.46  ICMP      239 Destination unreachable (Port unreachable)
192.168.31.10    165592 31.196969  203.212.24.46  ICMP      347 Destination unreachable (Port unreachable)
192.168.31.10    289892 66.235611  203.212.24.46  ICMP      180 Destination unreachable (Port unreachable)

> Frame 165592: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface \Device\NPF_{704644D1-9B3F-44C8-8D76-142FFB438987}, id 0
> Ethernet II, Src: Micro-St_c2:99:72 (d8:bb:c1:c2:99:72), Dst: 9c:53:22:05:6a:19 (9c:53:22:05:6a:19)
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 203.212.24.46
v Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0xc1e0 [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 203.212.24.46, Dst: 192.168.31.10
  > User Datagram Protocol, Src Port: 53, Dst Port: 53854
> Domain Name System (response)
```

4. Address Resolution Protocol (ARP)



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
arp
```

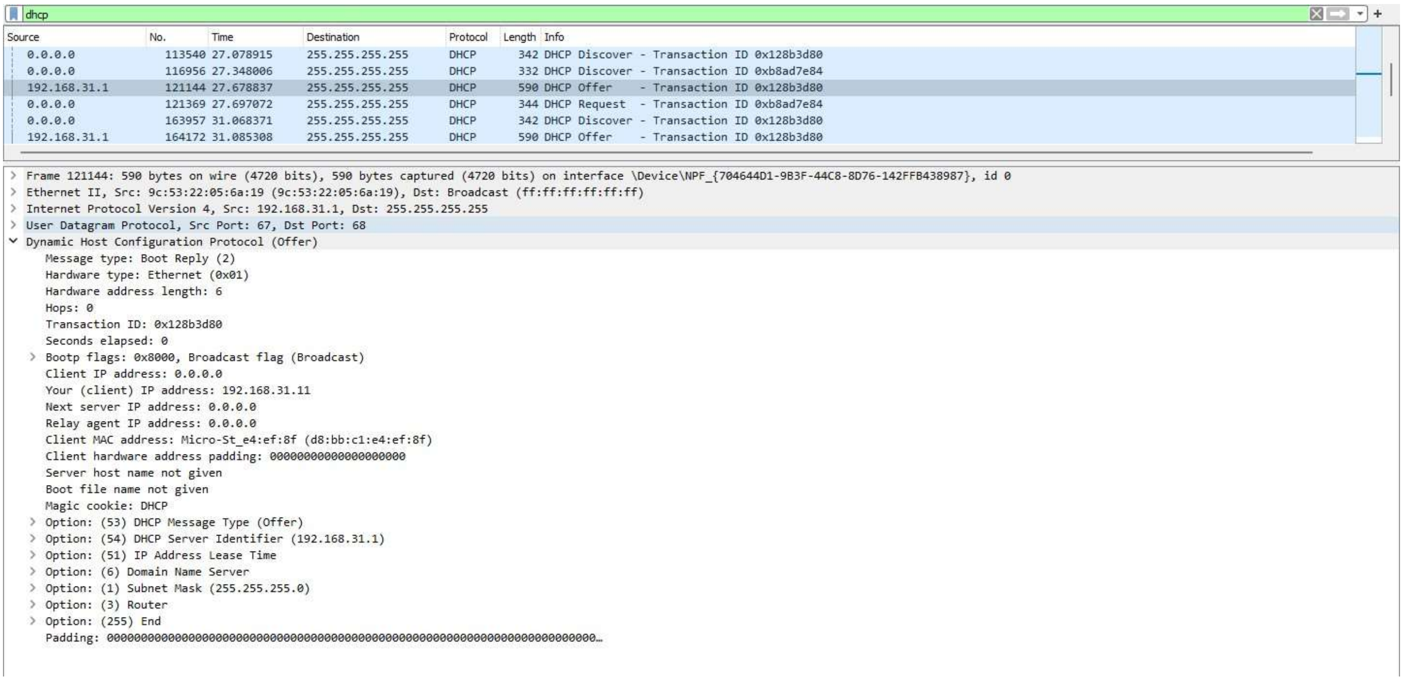
```
Source              No.    Time       Destination        Protocol  Length Info
  9c:53:22:05:6a:19  264869 45.548152  Broadcast          ARP       60 Who has 192.168.31.37? Tell 192.168.31.1
  Micro-St_e4:ef:8f  265469 45.650649  Broadcast          ARP       60 ARP Announcement for 192.168.31.11
  Micro-St_c2:99:72  265644 45.678832  Micro-St_c2:9a:72  ARP       42 Who has 192.168.31.21? Tell 192.168.31.10
  Micro-St_c2:9a:72  268408 46.126503  Micro-St_c2:99:72  ARP       60 192.168.31.21 is at d8:bb:c1:c2:9a:72
  9c:53:22:05:6a:19  268744 46.182324  Broadcast          ARP       60 Who has 192.168.31.5? Tell 192.168.31.1
  Dell_a5:05:b6      276786 47.419387  Broadcast          ARP       60 Who has 192.168.31.1? Tell 192.168.31.37
  Dell_a5:05:b6      277230 47.491097  Broadcast          ARP       60 Who has 192.168.31.37? (ARP Probe)
  Dell_a5:05:b6      278451 47.679929  Broadcast          ARP       60 Who has 192.168.31.1? Tell 192.168.31.37
  Dell_a5:05:b6      283428 48.491127  Broadcast          ARP       60 Who has 192.168.31.37? (ARP Probe)
  Dell_a5:05:b6      288875 49.490832  Broadcast          ARP       60 Who has 192.168.31.37? (ARP Probe)
```

```
> Frame 276786: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{704644D1-9B3F-44C8-8D76-142FFB438987}, id 0
> Ethernet II, Src: Dell_a5:05:b6 (54:bf:64:a5:05:b6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Dell_a5:05:b6 (54:bf:64:a5:05:b6)
    Sender IP address: 192.168.31.37
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.31.1
```

```
0000  ff ff ff ff ff ff 54 bf  64 a5 05 b6 08 06 00 01   ······T· d·······
0010  08 00 06 04 00 01 54 bf  64 a5 05 b6 c0 a8 1f 25   ······T· d······%
0020  00 00 00 00 00 00 c0 a8  1f 01 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Address Resolution Protocol: Protocol | Packets: 298488 · Displayed: 122 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

5. Dynamic Host Configuration Protocol (DHCP)

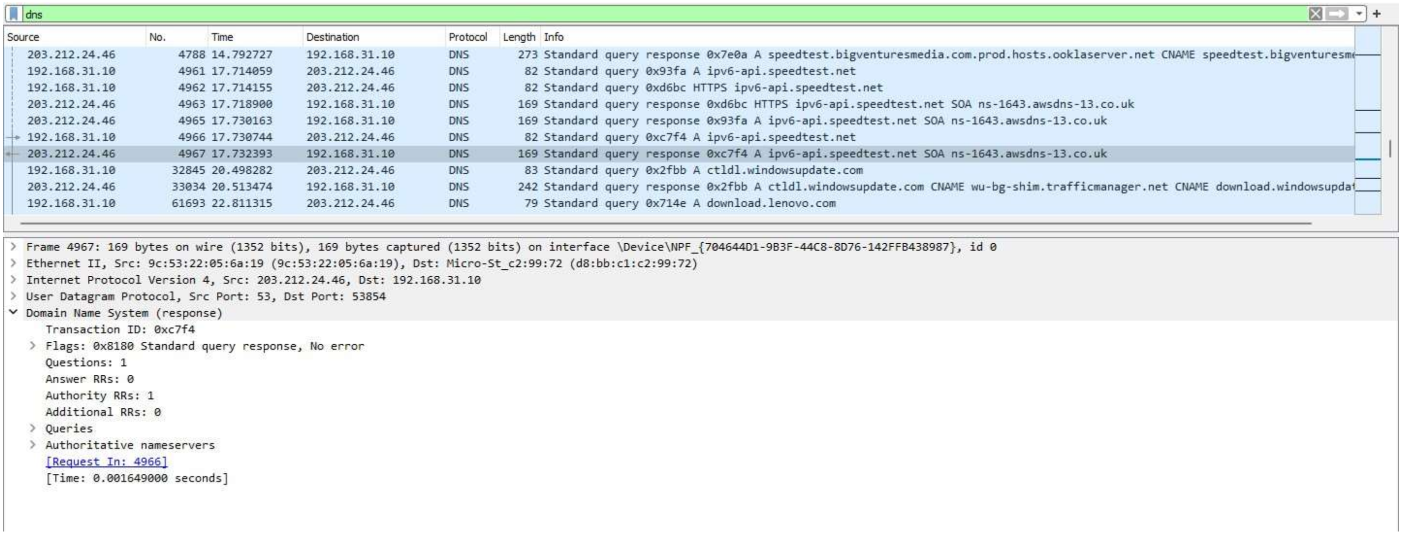


```
dhcp
```

```
Source          No.    Time       Destination      Protocol  Length Info
  0.0.0.0        113540 27.078915  255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x128b3d80
  0.0.0.0        116956 27.348006  255.255.255.255  DHCP      332 DHCP Discover - Transaction ID 0xb8ad7e84
  192.168.31.1   121144 27.678837  255.255.255.255  DHCP      590 DHCP Offer    - Transaction ID 0x128b3d80
  0.0.0.0        121369 27.697072  255.255.255.255  DHCP      344 DHCP Request  - Transaction ID 0xb8ad7e84
  0.0.0.0        163957 31.068371  255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x128b3d80
  192.168.31.1   164172 31.085308  255.255.255.255  DHCP      590 DHCP Offer    - Transaction ID 0x128b3d80
```

```
> Frame 121144: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{704644D1-9B3F-44C8-8D76-142FFB438987}, id 0
> Ethernet II, Src: 9c:53:22:05:6a:19 (9c:53:22:05:6a:19), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.31.1, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x128b3d80
    Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.31.11
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Micro-St_e4:ef:8f (d8:bb:c1:e4:ef:8f)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (192.168.31.1)
  > Option: (51) IP Address Lease Time
  > Option: (6) Domain Name Server
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000000000000000000000000000…
```

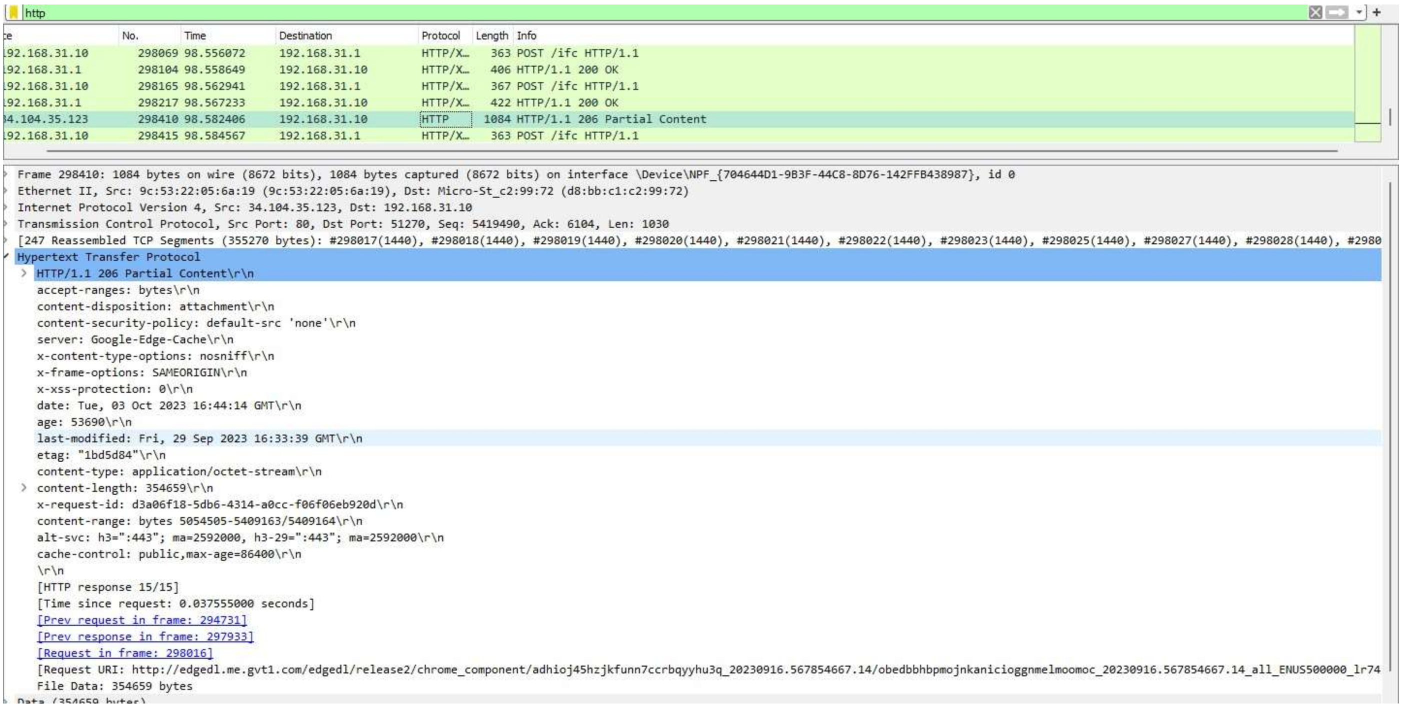
6. Domain Name System (DNS)



```
dns
Source          No.    Time       Destination     Protocol  Length Info
203.212.24.46     4788 14.792727  192.168.31.10   DNS        273 Standard query response 0x7e0a A speedtest.bigventuresmedia.com.prod.hosts.ooklaserver.net CNAME speedtest.bigventuresme
192.168.31.10     4961 17.714059  203.212.24.46   DNS         82 Standard query 0x93fa A ipv6-api.speedtest.net
192.168.31.10     4962 17.714155  203.212.24.46   DNS         82 Standard query 0xd6bc HTTPS ipv6-api.speedtest.net
203.212.24.46     4963 17.718900  192.168.31.10   DNS        169 Standard query response 0xd6bc HTTPS ipv6-api.speedtest.net SOA ns-1643.awsdns-13.co.uk
203.212.24.46     4965 17.730163  192.168.31.10   DNS        169 Standard query response 0x93fa A ipv6-api.speedtest.net SOA ns-1643.awsdns-13.co.uk
192.168.31.10     4966 17.730744  203.212.24.46   DNS         82 Standard query 0xc7f4 A ipv6-api.speedtest.net
203.212.24.46     4967 17.732393  192.168.31.10   DNS        169 Standard query response 0xc7f4 A ipv6-api.speedtest.net SOA ns-1643.awsdns-13.co.uk
192.168.31.10    32845 20.498282  203.212.24.46   DNS         83 Standard query 0x2fbb A ctldl.windowsupdate.com
203.212.24.46    33034 20.513474  192.168.31.10   DNS        242 Standard query response 0x2fbb A ctldl.windowsupdate.com CNAME wu-bg-shim.trafficmanager.net CNAME download.windowsupdat
192.168.31.10    61693 22.811315  203.212.24.46   DNS         79 Standard query 0x714e A download.lenovo.com
```

```
> Frame 4967: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits) on interface \Device\NPF_{704644D1-9B3F-44C8-8D76-142FFB438987}, id 0
> Ethernet II, Src: 9c:53:22:05:6a:19 (9c:53:22:05:6a:19), Dst: Micro-St_c2:99:72 (d8:bb:c1:c2:99:72)
> Internet Protocol Version 4, Src: 203.212.24.46, Dst: 192.168.31.10
> User Datagram Protocol, Src Port: 53, Dst Port: 53854
v Domain Name System (response)
    Transaction ID: 0xc7f4
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  > Queries
  > Authoritative nameservers
    [Request In: 4966]
    [Time: 0.001649000 seconds]
```

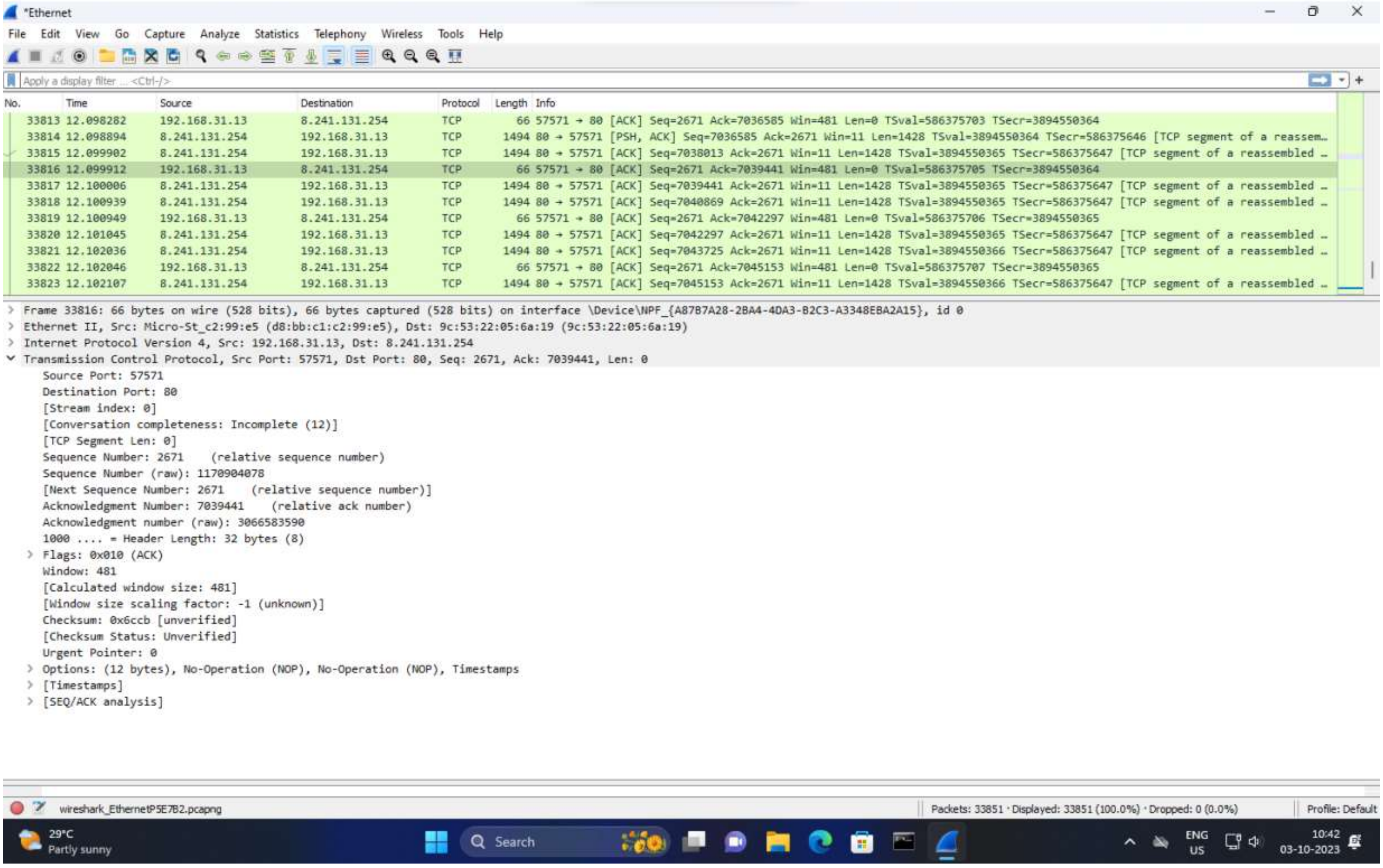
7. Hypertext Transfer Protocol (HTTP)



```
http
e               No.     Time       Destination     Protocol  Length Info
92.168.31.10     298069 98.556072  192.168.31.1    HTTP/X…    363 POST /ifc HTTP/1.1
92.168.31.1      298104 98.558649  192.168.31.10   HTTP/X…    406 HTTP/1.1 200 OK
92.168.31.10     298165 98.562941  192.168.31.1    HTTP/X…    367 POST /ifc HTTP/1.1
92.168.31.1      298217 98.567233  192.168.31.10   HTTP/X…    422 HTTP/1.1 200 OK
4.104.35.123     298410 98.582406  192.168.31.10   HTTP      1084 HTTP/1.1 206 Partial Content
92.168.31.10     298415 98.584567  192.168.31.1    HTTP/X…    363 POST /ifc HTTP/1.1
```

```
Frame 298410: 1084 bytes on wire (8672 bits), 1084 bytes captured (8672 bits) on interface \Device\NPF_{704644D1-9B3F-44C8-8D76-142FFB438987}, id 0
Ethernet II, Src: 9c:53:22:05:6a:19 (9c:53:22:05:6a:19), Dst: Micro-St_c2:99:72 (d8:bb:c1:c2:99:72)
Internet Protocol Version 4, Src: 34.104.35.123, Dst: 192.168.31.10
Transmission Control Protocol, Src Port: 80, Dst Port: 51270, Seq: 5419490, Ack: 6104, Len: 1030
[247 Reassembled TCP Segments (355270 bytes): #298017(1440), #298018(1440), #298019(1440), #298020(1440), #298021(1440), #298022(1440), #298023(1440), #298025(1440), #298027(1440), #298028(1440), #2980
Hypertext Transfer Protocol
  > HTTP/1.1 206 Partial Content\r\n
    accept-ranges: bytes\r\n
    content-disposition: attachment\r\n
    content-security-policy: default-src 'none'\r\n
    server: Google-Edge-Cache\r\n
    x-content-type-options: nosniff\r\n
    x-frame-options: SAMEORIGIN\r\n
    x-xss-protection: 0\r\n
    date: Tue, 03 Oct 2023 16:44:14 GMT\r\n
    age: 53690\r\n
    last-modified: Fri, 29 Sep 2023 16:33:39 GMT\r\n
    etag: "1bd5d84"\r\n
    content-type: application/octet-stream\r\n
  > content-length: 354659\r\n
    x-request-id: d3a06f18-5db6-4314-a0cc-f06f06eb920d\r\n
    content-range: bytes 5054505-5409163/5409164\r\n
    alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000\r\n
    cache-control: public,max-age=86400\r\n
    \r\n
    [HTTP response 15/15]
    [Time since request: 0.037555000 seconds]
    [Prev request in frame: 294731]
    [Prev response in frame: 297933]
    [Request in frame: 298016]
    [Request URI: http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/adhioj45hzjkfunn7ccrbqyyhu3q_20230916.567854667.14/obedbbhbpmojnkanicioggnmelmoomoc_20230916.567854667.14_all_ENUS500000_lr74
    File Data: 354659 bytes
Data (354659 bytes)
```

8. Transmission Control Protocol (TCP)

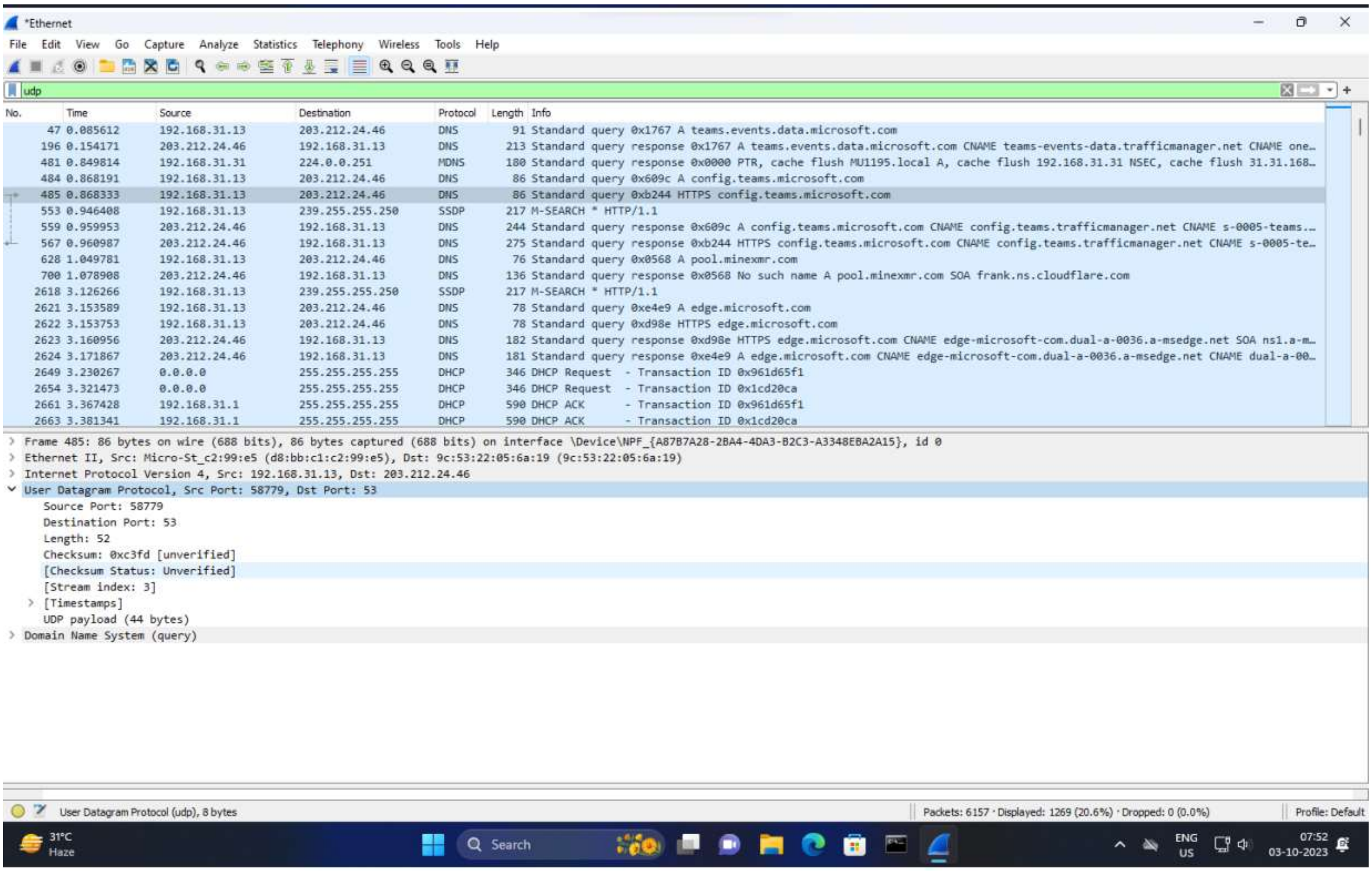

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
29°C
Partly sunny
Search
ENG
US
10:42
03-10-2023

```
No.   Time      Source          Destination     Protocol Length Info
33813 12.098282 192.168.31.13   8.241.131.254   TCP        66 57571 → 80 [ACK] Seq=2671 Ack=7036585 Win=481 Len=0 TSval=586375703 TSecr=3894550364
33814 12.098894 8.241.131.254   192.168.31.13   TCP      1494 80 → 57571 [PSH, ACK] Seq=7036585 Ack=2671 Win=11 Len=1428 TSval=3894550364 TSecr=586375646 [TCP segment of a reassem…
33815 12.099902 8.241.131.254   192.168.31.13   TCP      1494 80 → 57571 [ACK] Seq=7038013 Ack=2671 Win=11 Len=1428 TSval=3894550365 TSecr=586375647 [TCP segment of a reassembled …
33816 12.099912 192.168.31.13   8.241.131.254   TCP        66 57571 → 80 [ACK] Seq=2671 Ack=7039441 Win=481 Len=0 TSval=586375705 TSecr=3894550364
33817 12.100006 8.241.131.254   192.168.31.13   TCP      1494 80 → 57571 [ACK] Seq=7039441 Ack=2671 Win=11 Len=1428 TSval=3894550365 TSecr=586375647 [TCP segment of a reassembled …
33818 12.100939 8.241.131.254   192.168.31.13   TCP      1494 80 → 57571 [ACK] Seq=7040869 Ack=2671 Win=11 Len=1428 TSval=3894550365 TSecr=586375647 [TCP segment of a reassembled …
33819 12.100949 192.168.31.13   8.241.131.254   TCP        66 57571 → 80 [ACK] Seq=2671 Ack=7042297 Win=481 Len=0 TSval=586375706 TSecr=3894550365
33820 12.101045 8.241.131.254   192.168.31.13   TCP      1494 80 → 57571 [ACK] Seq=7042297 Ack=2671 Win=11 Len=1428 TSval=3894550365 TSecr=586375647 [TCP segment of a reassembled …
33821 12.102036 8.241.131.254   192.168.31.13   TCP      1494 80 → 57571 [ACK] Seq=7043725 Ack=2671 Win=11 Len=1428 TSval=3894550366 TSecr=586375647 [TCP segment of a reassembled …
33822 12.102046 192.168.31.13   8.241.131.254   TCP        66 57571 → 80 [ACK] Seq=2671 Ack=7045153 Win=481 Len=0 TSval=586375707 TSecr=3894550365
33823 12.102107 8.241.131.254   192.168.31.13   TCP      1494 80 → 57571 [ACK] Seq=7045153 Ack=2671 Win=11 Len=1428 TSval=3894550366 TSecr=586375647 [TCP segment of a reassembled …
```

```
> Frame 33816: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: Micro-St_c2:99:e5 (d8:bb:c1:c2:99:e5), Dst: 9c:53:22:05:6a:19 (9c:53:22:05:6a:19)
> Internet Protocol Version 4, Src: 192.168.31.13, Dst: 8.241.131.254
v Transmission Control Protocol, Src Port: 57571, Dst Port: 80, Seq: 2671, Ack: 7039441, Len: 0
    Source Port: 57571
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 0]
    Sequence Number: 2671    (relative sequence number)
    Sequence Number (raw): 1170904078
    [Next Sequence Number: 2671    (relative sequence number)]
    Acknowledgment Number: 7039441    (relative ack number)
    Acknowledgment number (raw): 3066583590
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
    Window: 481
    [Calculated window size: 481]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x6ccb [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
```

```
wireshark_EthernetP5E7B2.pcapng        Packets: 33851 · Displayed: 33851 (100.0%) · Dropped: 0 (0.0%)        Profile: Default
```

9. User Datagram Protocol (UDP)


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
31°C
Haze
Search
ENG
US
07:52
03-10-2023

```
udp
```

```
No.  Time     Source         Destination     Protocol Length Info
  47 0.085612 192.168.31.13  203.212.24.46   DNS       91 Standard query 0x1767 A teams.events.data.microsoft.com
 196 0.154171 203.212.24.46  192.168.31.13   DNS      213 Standard query response 0x1767 A teams.events.data.microsoft.com CNAME teams-events-data.trafficmanager.net CNAME one…
 481 0.849814 192.168.31.31  224.0.0.251     MDNS     180 Standard query response 0x0000 PTR, cache flush MU1195.local A, cache flush 192.168.31.31 NSEC, cache flush 31.31.168…
 484 0.868191 192.168.31.13  203.212.24.46   DNS       86 Standard query 0x609c A config.teams.microsoft.com
 485 0.868333 192.168.31.13  203.212.24.46   DNS       86 Standard query 0xb244 HTTPS config.teams.microsoft.com
 553 0.946408 192.168.31.13  239.255.255.250 SSDP     217 M-SEARCH * HTTP/1.1
 559 0.959953 203.212.24.46  192.168.31.13   DNS      244 Standard query response 0x609c A config.teams.microsoft.com CNAME config.teams.trafficmanager.net CNAME s-0005-teams.…
 567 0.960987 203.212.24.46  192.168.31.13   DNS      275 Standard query response 0xb244 HTTPS config.teams.microsoft.com CNAME config.teams.trafficmanager.net CNAME s-0005-te…
 628 1.049781 192.168.31.13  203.212.24.46   DNS       76 Standard query 0x0568 A pool.minexmr.com
 700 1.078908 203.212.24.46  192.168.31.13   DNS      136 Standard query response 0x0568 No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
2618 3.126266 192.168.31.13  239.255.255.250 SSDP     217 M-SEARCH * HTTP/1.1
2621 3.153589 192.168.31.13  203.212.24.46   DNS       78 Standard query 0xe4e9 A edge.microsoft.com
2622 3.153753 192.168.31.13  203.212.24.46   DNS       78 Standard query 0xd98e HTTPS edge.microsoft.com
2623 3.160956 203.212.24.46  192.168.31.13   DNS      182 Standard query response 0xd98e HTTPS edge.microsoft.com CNAME edge-microsoft-com.dual-a-0036.a-msedge.net SOA ns1.a-m…
2624 3.171867 203.212.24.46  192.168.31.13   DNS      181 Standard query response 0xe4e9 A edge.microsoft.com CNAME edge-microsoft-com.dual-a-0036.a-msedge.net CNAME dual-a-00…
2649 3.230267 0.0.0.0        255.255.255.255 DHCP     346 DHCP Request  - Transaction ID 0x961d65f1
2654 3.321473 0.0.0.0        255.255.255.255 DHCP     346 DHCP Request  - Transaction ID 0x1cd20ca
2661 3.367428 192.168.31.1   255.255.255.255 DHCP     590 DHCP ACK      - Transaction ID 0x961d65f1
2663 3.381341 192.168.31.1   255.255.255.255 DHCP     590 DHCP ACK      - Transaction ID 0x1cd20ca
```

```
> Frame 485: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: Micro-St_c2:99:e5 (d8:bb:c1:c2:99:e5), Dst: 9c:53:22:05:6a:19 (9c:53:22:05:6a:19)
> Internet Protocol Version 4, Src: 192.168.31.13, Dst: 203.212.24.46
v User Datagram Protocol, Src Port: 58779, Dst Port: 53
    Source Port: 58779
    Destination Port: 53
    Length: 52
    Checksum: 0xc3fd [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  > [Timestamps]
    UDP payload (44 bytes)
> Domain Name System (query)
```

```
User Datagram Protocol (udp), 8 bytes        Packets: 6157 · Displayed: 1269 (20.6%) · Dropped: 0 (0.0%)        Profile: Default
```