CYBER SECURITY INTERNSHIP

Task 3

Networking Basics for Cyber Security

JASHMI KS

Networking basics in cyber security refer to the fundamental concepts that explain how data is transmitted, addressed, and protected over a network. These concepts include IP addresses and MAC addresses for identifying devices, DNS for translating domain names into IP addresses, TCP and UDP for data transmission, and packets as small units of data exchanged between systems. Understanding these basics helps cybersecurity professionals monitor network traffic, detect insecure communication, and identify potential threats using tools like packet sniffers.

IP Address

- IP (Internet Protocol) address uniquely identifies a device on a network.
- Example: 192.168.1.1
- Used to locate devices and route data.

MAC Address

- MAC (Media Access Control) address is a physical address of a network interface.
- Example: 00:1A:2B:3C:4D:5E
- Used within the local network.

DNS (Domain Name System)

- Converts domain names into IP addresses.
- Example: google.com → 142.250.195.78
- Acts like the phonebook of the internet.

TCP (Transmission Control Protocol)

- Connection-oriented and reliable.
- Ensures data delivery, order, and error correction.
- Used in: HTTP, HTTPS, FTP, Email.

UDP (User Datagram Protocol)

- Connectionless and faster.
- No guarantee of delivery.
- Used in: Video streaming, VoIP, Online games.

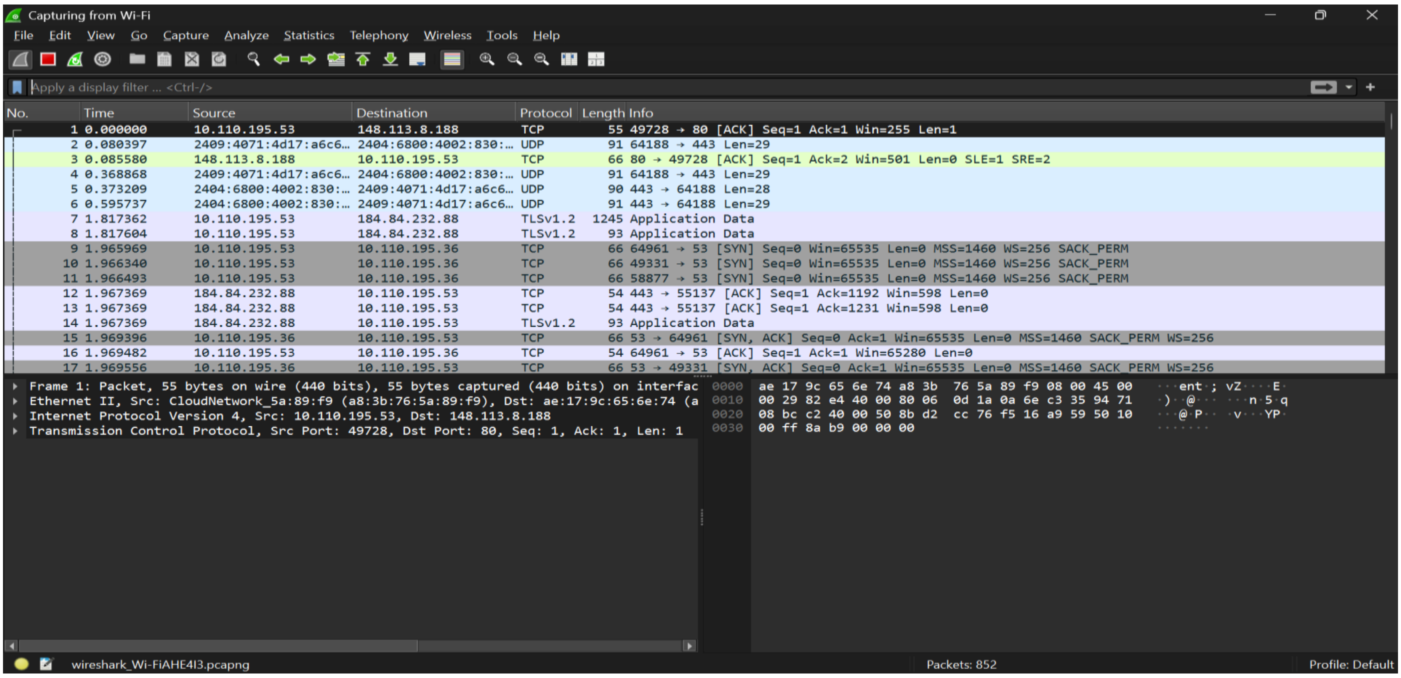
Wireshark

Wireshark is a free and open-source network protocol analyzer used to capture and inspect network traffic in real time. It helps engineers, analysts, and security professionals understand what is happening inside a network at the packet level.

- Captures live network traffic across multiple interfaces
- Provides deep visibility into protocols and packet structure
- Helps troubleshoot network issues and analyze performance
- Essential for security investigations and protocol debugging

Filter Packets by Protocol (HTTP, DNS, TCP)

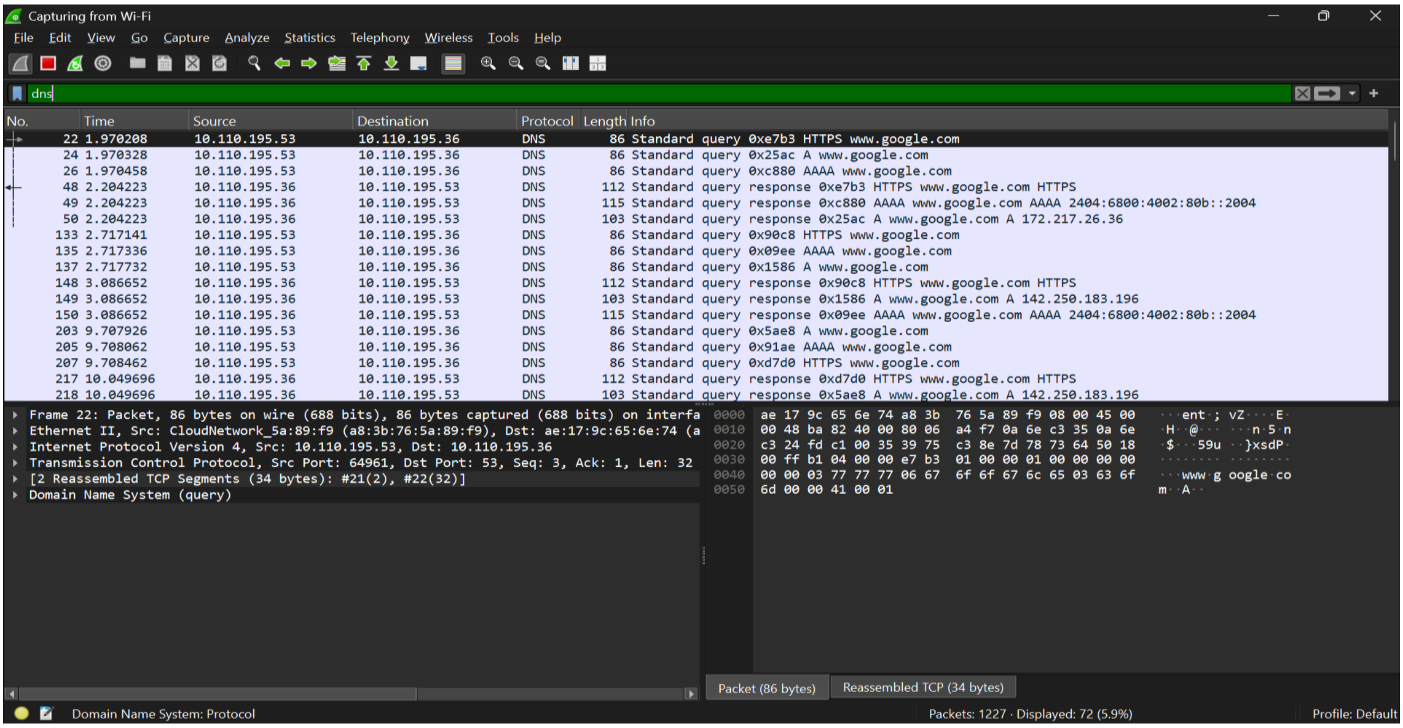
Packet filtering is the process of displaying specific types of network packets from a captured data set. By filtering packets based on protocols such as HTTP, DNS, and TCP, network traffic can be analyzed more efficiently. This helps in understanding protocol behavior and identifying relevant communication in a network.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
wireshark_Wi-FiAHE4I3.pcapng
Packets: 852
Profile: Default

```
No.    Time      Source               Destination          Protocol Length Info
     1 0.000000  10.110.195.53        148.113.8.188        TCP        55 49728 → 80 [ACK] Seq=1 Ack=1 Win=255 Len=1
     2 0.080397  2409:4071:4d17:a6c6… 2404:6800:4002:830:… UDP        91 64188 → 443 Len=29
     3 0.085580  148.113.8.188        10.110.195.53        TCP        66 80 → 49728 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
     4 0.368868  2409:4071:4d17:a6c6… 2404:6800:4002:830:… UDP        91 64188 → 443 Len=29
     5 0.373209  2404:6800:4002:830:… 2409:4071:4d17:a6c6… UDP        90 443 → 64188 Len=28
     6 0.595737  2404:6800:4002:830:… 2409:4071:4d17:a6c6… UDP        91 443 → 64188 Len=29
     7 1.817362  10.110.195.53        184.84.232.88        TLSv1.2  1245 Application Data
     8 1.817604  10.110.195.53        184.84.232.88        TLSv1.2    93 Application Data
     9 1.965969  10.110.195.53        10.110.195.36        TCP        66 64961 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
    10 1.966340  10.110.195.53        10.110.195.36        TCP        66 49331 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
    11 1.966493  10.110.195.53        10.110.195.36        TCP        66 58877 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
    12 1.967369  184.84.232.88        10.110.195.53        TCP        54 443 → 55137 [ACK] Seq=1 Ack=1192 Win=598 Len=0
    13 1.967369  184.84.232.88        10.110.195.53        TCP        54 443 → 55137 [ACK] Seq=1 Ack=1231 Win=598 Len=0
    14 1.967369  184.84.232.88        10.110.195.53        TLSv1.2    93 Application Data
    15 1.969396  10.110.195.36        10.110.195.53        TCP        66 53 → 64961 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=256
    16 1.969482  10.110.195.53        10.110.195.36        TCP        54 64961 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
    17 1.969556  10.110.195.36        10.110.195.53        TCP        66 53 → 49331 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=256
```

```
▸ Frame 1: Packet, 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interfac
▸ Ethernet II, Src: CloudNetwork_5a:89:f9 (a8:3b:76:5a:89:f9), Dst: ae:17:9c:65:6e:74 (a
▸ Internet Protocol Version 4, Src: 10.110.195.53, Dst: 148.113.8.188
▸ Transmission Control Protocol, Src Port: 49728, Dst Port: 80, Seq: 1, Ack: 1, Len: 1
```

```
0000  ae 17 9c 65 6e 74 a8 3b  76 5a 89 f9 08 00 45 00   ···ent·; vZ····E·
0010  00 29 82 e4 40 00 80 06  0d 1a 0a 6e c3 35 94 71   ·)··@··· ···n·5·q
0020  08 bc c2 40 00 50 8b d2  cc 76 f5 16 a9 59 50 10   ···@·P·· ·v···YP·
0030  00 ff 8a b9 00 00 00                               ·······
```

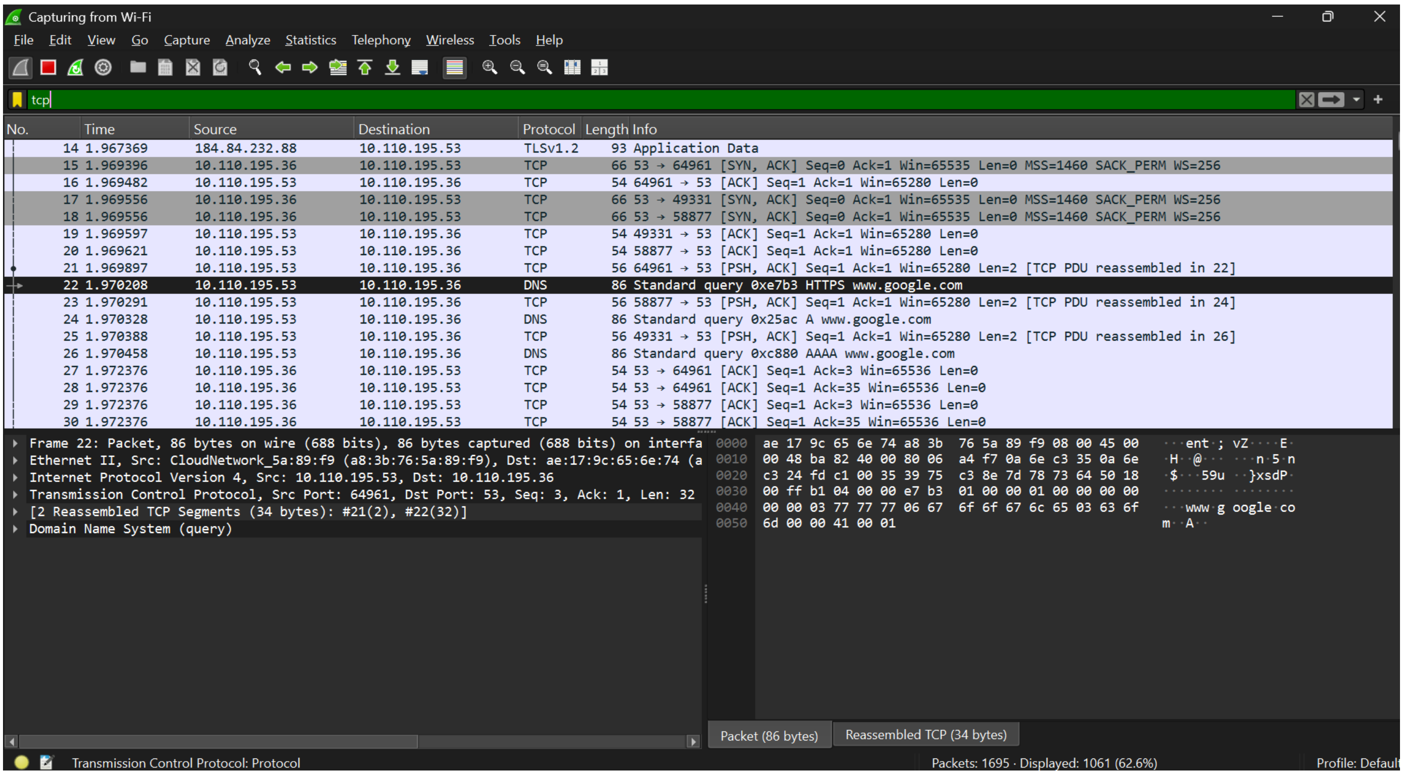

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet (86 bytes)
Reassembled TCP (34 bytes)
Domain Name System: Protocol
Packets: 1227 · Displayed: 72 (5.9%)
Profile: Default

dns

```
No.    Time      Source               Destination          Protocol Length Info
    22 1.970208  10.110.195.53        10.110.195.36        DNS        86 Standard query 0xe7b3 HTTPS www.google.com
    24 1.970328  10.110.195.53        10.110.195.36        DNS        86 Standard query 0x25ac A www.google.com
    26 1.970458  10.110.195.53        10.110.195.36        DNS        86 Standard query 0xc880 AAAA www.google.com
    48 2.204223  10.110.195.36        10.110.195.53        DNS       112 Standard query response 0xe7b3 HTTPS www.google.com HTTPS
    49 2.204223  10.110.195.36        10.110.195.53        DNS       115 Standard query response 0xc880 AAAA www.google.com AAAA 2404:6800:4002:80b::2004
    50 2.204223  10.110.195.36        10.110.195.53        DNS       103 Standard query response 0x25ac A www.google.com A 172.217.26.36
   133 2.717141  10.110.195.53        10.110.195.36        DNS        86 Standard query 0x90c8 HTTPS www.google.com
   135 2.717336  10.110.195.53        10.110.195.36        DNS        86 Standard query 0x09ee AAAA www.google.com
   137 2.717732  10.110.195.53        10.110.195.36        DNS        86 Standard query 0x1586 A www.google.com
   148 3.086652  10.110.195.36        10.110.195.53        DNS       112 Standard query response 0x90c8 HTTPS www.google.com HTTPS
   149 3.086652  10.110.195.36        10.110.195.53        DNS       103 Standard query response 0x1586 A www.google.com A 142.250.183.196
   150 3.086652  10.110.195.36        10.110.195.53        DNS       115 Standard query response 0x09ee AAAA www.google.com AAAA 2404:6800:4002:80b::2004
   203 9.707926  10.110.195.53        10.110.195.36        DNS        86 Standard query 0x5ae8 A www.google.com
   205 9.708062  10.110.195.53        10.110.195.36        DNS        86 Standard query 0x91ae AAAA www.google.com
   207 9.708462  10.110.195.53        10.110.195.36        DNS        86 Standard query 0xd7d0 HTTPS www.google.com
   217 10.049696 10.110.195.36        10.110.195.53        DNS       112 Standard query response 0xd7d0 HTTPS www.google.com HTTPS
   218 10.049696 10.110.195.36        10.110.195.53        DNS       103 Standard query response 0x5ae8 A www.google.com A 142.250.183.196
```

```
▸ Frame 22: Packet, 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interfa
▸ Ethernet II, Src: CloudNetwork_5a:89:f9 (a8:3b:76:5a:89:f9), Dst: ae:17:9c:65:6e:74 (a
▸ Internet Protocol Version 4, Src: 10.110.195.53, Dst: 10.110.195.36
▸ Transmission Control Protocol, Src Port: 64961, Dst Port: 53, Seq: 3, Ack: 1, Len: 32
▸ [2 Reassembled TCP Segments (34 bytes): #21(2), #22(32)]
▸ Domain Name System (query)
```

```
0000  ae 17 9c 65 6e 74 a8 3b  76 5a 89 f9 08 00 45 00   ···ent·; vZ····E·
0010  00 48 ba 82 40 00 80 06  a4 f7 0a 6e c3 35 0a 6e   ·H··@··· ···n·5·n
0020  c3 24 fd c1 00 35 39 75  c3 8e 7d 78 73 64 50 18   ·$···59u ··}xsdP·
0030  00 ff b1 04 00 00 e7 b3  01 00 00 01 00 00 00 00   ········ ········
0040  00 00 03 77 77 77 06 67  6f 6f 67 6c 65 03 63 6f   ···www·g oogle·co
0050  6d 00 00 41 00 01                                  m··A··
```


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Packet (86 bytes)
Reassembled TCP (34 bytes)
Profile: Default

```
No.   Time      Source          Destination     Protocol Length Info
   14 1.967369  184.84.232.88   10.110.195.53   TLSv1.2    93 Application Data
   15 1.969396  10.110.195.36   10.110.195.53   TCP        66 53 → 64961 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=256
   16 1.969482  10.110.195.53   10.110.195.36   TCP        54 64961 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
   17 1.969556  10.110.195.36   10.110.195.53   TCP        66 53 → 49331 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=256
   18 1.969556  10.110.195.36   10.110.195.53   TCP        66 53 → 58877 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=256
   19 1.969597  10.110.195.53   10.110.195.36   TCP        54 49331 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
   20 1.969621  10.110.195.53   10.110.195.36   TCP        54 58877 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
   21 1.969897  10.110.195.53   10.110.195.36   TCP        56 64961 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in 22]
   22 1.970208  10.110.195.53   10.110.195.36   DNS        86 Standard query 0xe7b3 HTTPS www.google.com
   23 1.970291  10.110.195.53   10.110.195.36   TCP        56 58877 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in 24]
   24 1.970328  10.110.195.53   10.110.195.36   DNS        86 Standard query 0x25ac A www.google.com
   25 1.970388  10.110.195.53   10.110.195.36   TCP        56 49331 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in 26]
   26 1.970458  10.110.195.53   10.110.195.36   DNS        86 Standard query 0xc880 AAAA www.google.com
   27 1.972376  10.110.195.36   10.110.195.53   TCP        54 53 → 64961 [ACK] Seq=1 Ack=3 Win=65536 Len=0
   28 1.972376  10.110.195.36   10.110.195.53   TCP        54 53 → 64961 [ACK] Seq=1 Ack=35 Win=65536 Len=0
   29 1.972376  10.110.195.36   10.110.195.53   TCP        54 53 → 58877 [ACK] Seq=1 Ack=3 Win=65536 Len=0
   30 1.972376  10.110.195.36   10.110.195.53   TCP        54 53 → 58877 [ACK] Seq=1 Ack=35 Win=65536 Len=0
```

```
Frame 22: Packet, 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interfa
Ethernet II, Src: CloudNetwork_5a:89:f9 (a8:3b:76:5a:89:f9), Dst: ae:17:9c:65:6e:74 (a
Internet Protocol Version 4, Src: 10.110.195.53, Dst: 10.110.195.36
Transmission Control Protocol, Src Port: 64961, Dst Port: 53, Seq: 3, Ack: 1, Len: 32
[2 Reassembled TCP Segments (34 bytes): #21(2), #22(32)]
Domain Name System (query)
```

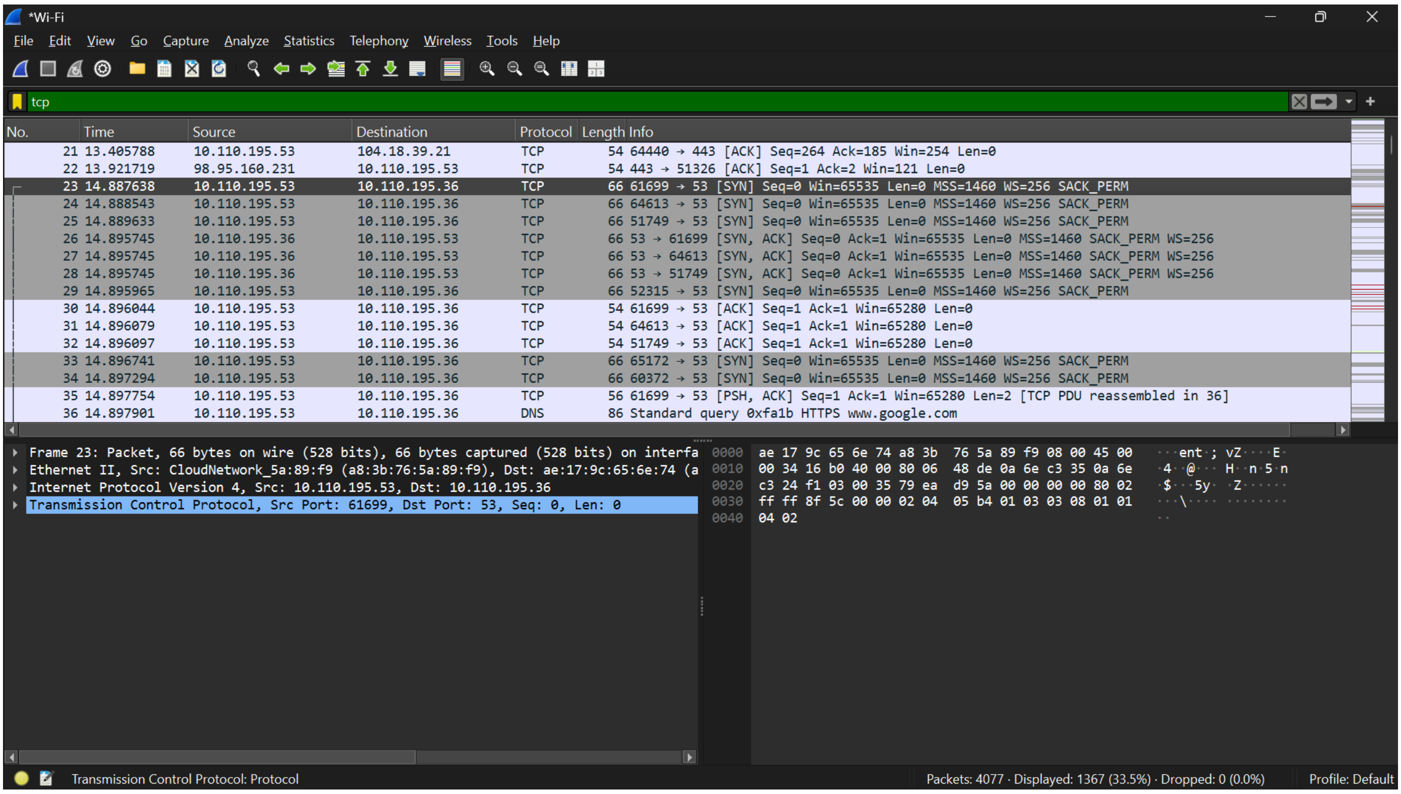
```
0000  ae 17 9c 65 6e 74 a8 3b  76 5a 89 f9 08 00 45 00   ···ent·; vZ····E·
0010  00 48 ba 82 40 00 80 06  a4 f7 0a 6e c3 35 0a 6e   ·H··@··· ···n·5·n
0020  c3 24 fd c1 00 35 39 75  c3 8e 7d 78 73 64 50 18   ·$···59u ··}xsdP·
0030  00 ff b1 04 00 00 e7 b3  01 00 00 01 00 00 00 00   ········ ········
0040  00 00 03 77 77 77 06 67  6f 6f 67 6c 65 03 63 6f   ···www·g oogle·co
0050  6d 00 00 41 00 01                                  m··A··
```

Transmission Control Protocol: Protocol

Packets: 1695 · Displayed: 1061 (62.6%)

Three-Way TCP Handshake

The TCP three-way handshake is a connection establishment mechanism used to initiate reliable communication between two devices. It consists of three stages that confirm both the sender and receiver are ready for data transmission before the connection is established.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Profile: Default

```
No.   Time       Source          Destination     Protocol Length Info
   21 13.405788  10.110.195.53   104.18.39.21    TCP        54 64440 → 443 [ACK] Seq=264 Ack=185 Win=254 Len=0
   22 13.921719  98.95.160.231   10.110.195.53   TCP        54 443 → 51326 [ACK] Seq=1 Ack=2 Win=121 Len=0
   23 14.887638  10.110.195.53   10.110.195.36   TCP        66 61699 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   24 14.888543  10.110.195.53   10.110.195.36   TCP        66 64613 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   25 14.889633  10.110.195.53   10.110.195.36   TCP        66 51749 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   26 14.895745  10.110.195.36   10.110.195.53   TCP        66 53 → 61699 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=256
   27 14.895745  10.110.195.36   10.110.195.53   TCP        66 53 → 64613 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=256
   28 14.895745  10.110.195.36   10.110.195.53   TCP        66 53 → 51749 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=256
   29 14.895965  10.110.195.53   10.110.195.36   TCP        66 52315 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   30 14.896044  10.110.195.53   10.110.195.36   TCP        54 61699 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
   31 14.896079  10.110.195.53   10.110.195.36   TCP        54 64613 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
   32 14.896097  10.110.195.53   10.110.195.36   TCP        54 51749 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
   33 14.896741  10.110.195.53   10.110.195.36   TCP        66 65172 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   34 14.897294  10.110.195.53   10.110.195.36   TCP        66 60372 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   35 14.897754  10.110.195.53   10.110.195.36   TCP        56 61699 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in 36]
   36 14.897901  10.110.195.53   10.110.195.36   DNS        86 Standard query 0xfa1b HTTPS www.google.com
```

```
Frame 23: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interfa
Ethernet II, Src: CloudNetwork_5a:89:f9 (a8:3b:76:5a:89:f9), Dst: ae:17:9c:65:6e:74 (a
Internet Protocol Version 4, Src: 10.110.195.53, Dst: 10.110.195.36
Transmission Control Protocol, Src Port: 61699, Dst Port: 53, Seq: 0, Len: 0
```

```
0000  ae 17 9c 65 6e 74 a8 3b  76 5a 89 f9 08 00 45 00   ···ent·; vZ····E·
0010  00 34 16 b0 40 00 80 06  48 de 0a 6e c3 35 0a 6e   ·4··@··· H··n·5·n
0020  c3 24 f1 03 00 35 79 ea  d9 5a 00 00 00 00 80 02   ·$···5y· ·Z······
0030  ff ff 8f 5c 00 00 02 04  05 b4 01 03 03 08 01 01   ···\···· ········
0040  04 02                                              ··
```

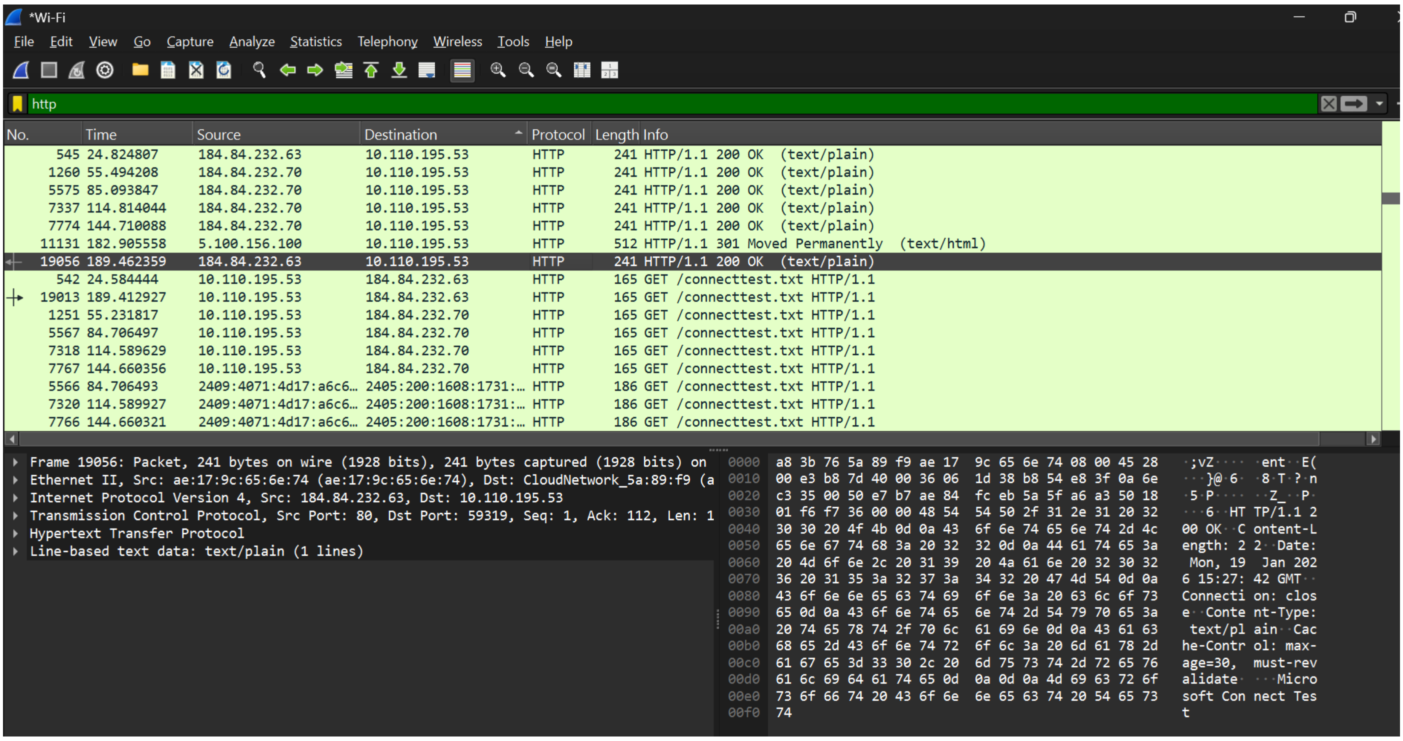
Transmission Control Protocol: Protocol

Packets: 4077 · Displayed: 1367 (33.5%) · Dropped: 0 (0.0%)

Plain-Text Traffic vs Encrypted Traffic

Plain-text traffic transmits data in a readable format without encryption, making it vulnerable to interception. Encrypted traffic protects data by encoding it into an unreadable form, ensuring secure communication. Identifying these traffic types is essential for assessing network security.

Plain-text traffic

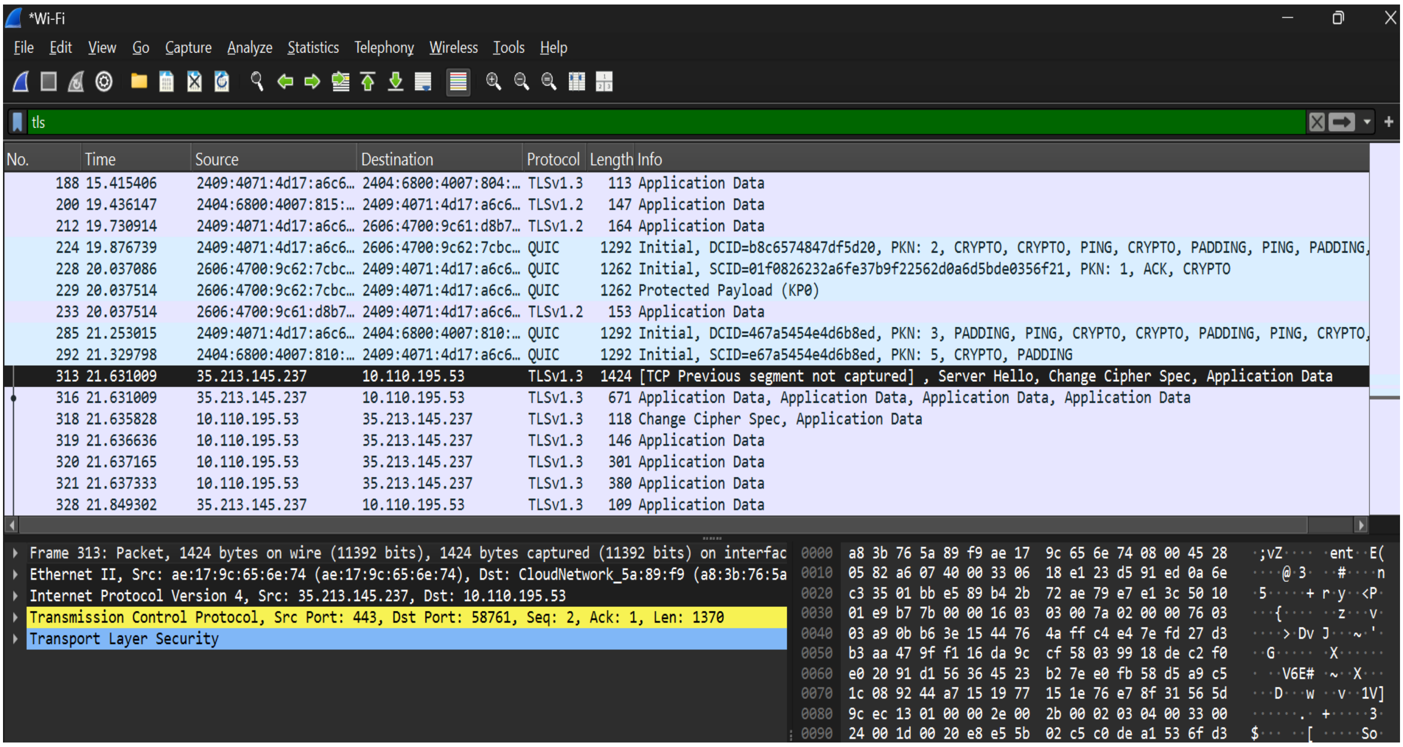

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time        Source                Destination           Protocol Length Info
  545 24.824807    184.84.232.63         10.110.195.53         HTTP      241 HTTP/1.1 200 OK  (text/plain)
 1260 55.494208    184.84.232.70         10.110.195.53         HTTP      241 HTTP/1.1 200 OK  (text/plain)
 5575 85.093847    184.84.232.70         10.110.195.53         HTTP      241 HTTP/1.1 200 OK  (text/plain)
 7337 114.814044   184.84.232.70         10.110.195.53         HTTP      241 HTTP/1.1 200 OK  (text/plain)
 7774 144.710088   184.84.232.70         10.110.195.53         HTTP      241 HTTP/1.1 200 OK  (text/plain)
11131 182.905558   5.100.156.100         10.110.195.53         HTTP      512 HTTP/1.1 301 Moved Permanently  (text/html)
19056 189.462359   184.84.232.63         10.110.195.53         HTTP      241 HTTP/1.1 200 OK  (text/plain)
  542 24.584444    10.110.195.53         184.84.232.63         HTTP      165 GET /connecttest.txt HTTP/1.1
19013 189.412927   10.110.195.53         184.84.232.63         HTTP      165 GET /connecttest.txt HTTP/1.1
 1251 55.231817    10.110.195.53         184.84.232.70         HTTP      165 GET /connecttest.txt HTTP/1.1
 5567 84.706497    10.110.195.53         184.84.232.70         HTTP      165 GET /connecttest.txt HTTP/1.1
 7318 114.589629   10.110.195.53         184.84.232.70         HTTP      165 GET /connecttest.txt HTTP/1.1
 7767 144.660356   10.110.195.53         184.84.232.70         HTTP      165 GET /connecttest.txt HTTP/1.1
 5566 84.706493    2409:4071:4d17:a6c6…  2405:200:1608:1731:…  HTTP      186 GET /connecttest.txt HTTP/1.1
 7320 114.589927   2409:4071:4d17:a6c6…  2405:200:1608:1731:…  HTTP      186 GET /connecttest.txt HTTP/1.1
 7766 144.660321   2409:4071:4d17:a6c6…  2405:200:1608:1731:…  HTTP      186 GET /connecttest.txt HTTP/1.1
```

```
▸ Frame 19056: Packet, 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on
▸ Ethernet II, Src: ae:17:9c:65:6e:74 (ae:17:9c:65:6e:74), Dst: CloudNetwork_5a:89:f9 (a
▸ Internet Protocol Version 4, Src: 184.84.232.63, Dst: 10.110.195.53
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 59319, Seq: 1, Ack: 112, Len: 1
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/plain (1 lines)
```

```
0000  a8 3b 76 5a 89 f9 ae 17  9c 65 6e 74 08 00 45 28   ·;vZ····  ·ent··E(
0010  00 e3 b8 7d 40 00 36 06  1d 38 b8 54 e8 3f 0a 6e   ···}@·6·  ·8·T·?·n
0020  c3 35 00 50 e7 b7 ae 84  fc eb 5a 5f a6 a3 50 18   ·5·P····  ··Z_··P·
0030  01 f6 f7 36 00 00 48 54  54 50 2f 31 2e 31 20 32   ···6··HT  TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   00 OK··C  ontent-L
0050  65 6e 67 74 68 3a 20 32  32 0d 0a 44 61 74 65 3a   ength: 2  2··Date:
0060  20 4d 6f 6e 2c 20 31 39  20 4a 61 6e 20 32 30 32    Mon, 19   Jan 202
0070  36 20 31 35 3a 32 37 3a  34 32 20 47 4d 54 0d 0a   6 15:27:  42 GMT··
0080  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 63 6c 6f 73   Connecti  on: clos
0090  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   e··Conte  nt-Type:
00a0  20 74 65 78 74 2f 70 6c  61 69 6e 0d 0a 43 61 63    text/pl  ain··Cac
00b0  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6d 61 78 2d   he-Contr  ol: max-
00c0  61 67 65 3d 33 30 2c 20  6d 75 73 74 2d 72 65 76   age=30,   must-rev
00d0  61 6c 69 64 61 74 65 0d  0a 0d 0a 4d 69 63 72 6f   alidate·  ···Micro
00e0  73 6f 66 74 20 43 6f 6e  6e 65 63 74 20 54 65 73   soft Con  nect Tes
00f0  74                                                 t
```

Encrypted traffic


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls

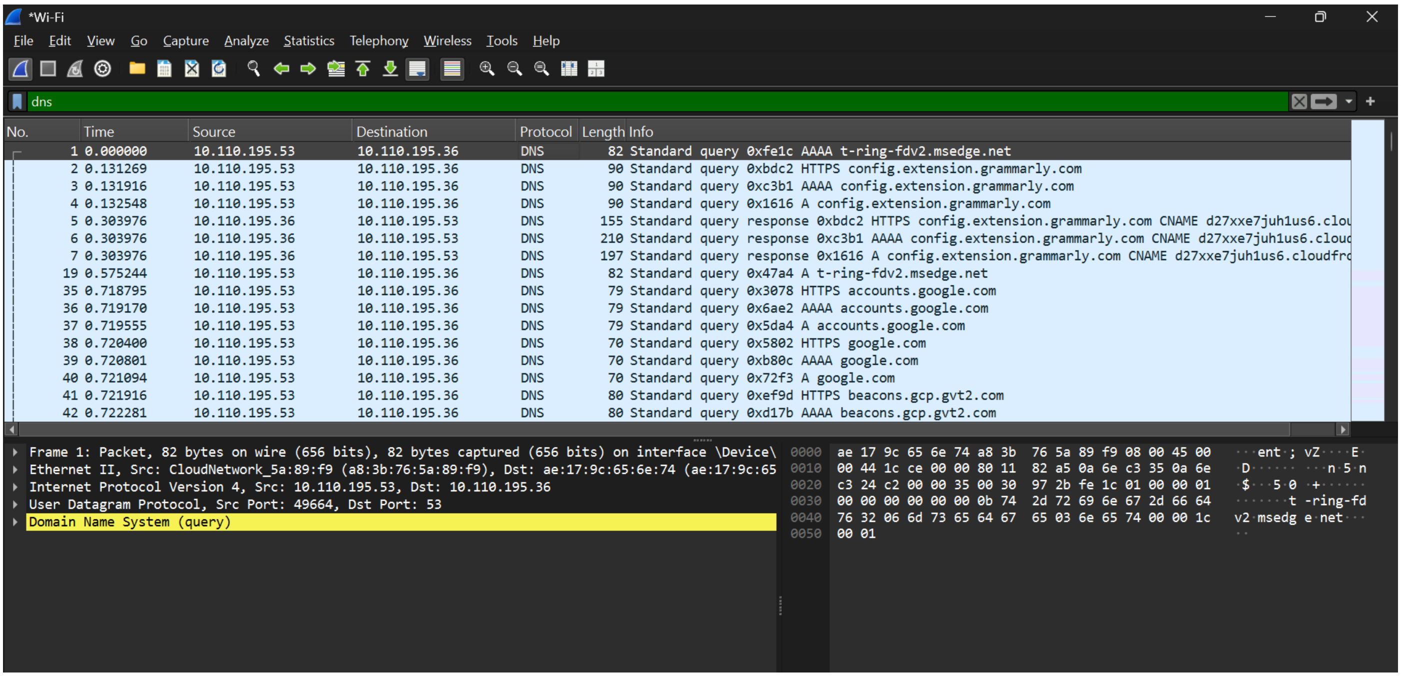
```
No.  Time        Source                Destination           Protocol Length Info
188 15.415406    2409:4071:4d17:a6c6…  2404:6800:4007:804:…  TLSv1.3   113 Application Data
200 19.436147    2404:6800:4007:815:…  2409:4071:4d17:a6c6…  TLSv1.2   147 Application Data
212 19.730914    2409:4071:4d17:a6c6…  2606:4700:9c61:d8b7…  TLSv1.2   164 Application Data
224 19.876739    2409:4071:4d17:a6c6…  2606:4700:9c62:7cbc…  QUIC     1292 Initial, DCID=b8c6574847df5d20, PKN: 2, CRYPTO, CRYPTO, PING, CRYPTO, PADDING, PING, PADDING,
228 20.037086    2606:4700:9c62:7cbc…  2409:4071:4d17:a6c6…  QUIC     1262 Initial, SCID=01f0826232a6fe37b9f22562d0a6d5bde0356f21, PKN: 1, ACK, CRYPTO
229 20.037514    2606:4700:9c62:7cbc…  2409:4071:4d17:a6c6…  QUIC     1262 Protected Payload (KP0)
233 20.037514    2606:4700:9c61:d8b7…  2409:4071:4d17:a6c6…  TLSv1.2   153 Application Data
285 21.253015    2409:4071:4d17:a6c6…  2404:6800:4007:810:…  QUIC     1292 Initial, DCID=467a5454e4d6b8ed, PKN: 3, PADDING, PING, CRYPTO, CRYPTO, PADDING, PING, CRYPTO,
292 21.329798    2404:6800:4007:810:…  2409:4071:4d17:a6c6…  QUIC     1292 Initial, SCID=e67a5454e4d6b8ed, PKN: 5, CRYPTO, PADDING
313 21.631009    35.213.145.237        10.110.195.53         TLSv1.3  1424 [TCP Previous segment not captured] , Server Hello, Change Cipher Spec, Application Data
316 21.631009    35.213.145.237        10.110.195.53         TLSv1.3   671 Application Data, Application Data, Application Data, Application Data
318 21.635828    10.110.195.53         35.213.145.237        TLSv1.3   118 Change Cipher Spec, Application Data
319 21.636636    10.110.195.53         35.213.145.237        TLSv1.3   146 Application Data
320 21.637165    10.110.195.53         35.213.145.237        TLSv1.3   301 Application Data
321 21.637333    10.110.195.53         35.213.145.237        TLSv1.3   380 Application Data
328 21.849302    35.213.145.237        10.110.195.53         TLSv1.3   109 Application Data
```

```
▸ Frame 313: Packet, 1424 bytes on wire (11392 bits), 1424 bytes captured (11392 bits) on interfac
▸ Ethernet II, Src: ae:17:9c:65:6e:74 (ae:17:9c:65:6e:74), Dst: CloudNetwork_5a:89:f9 (a8:3b:76:5a
▸ Internet Protocol Version 4, Src: 35.213.145.237, Dst: 10.110.195.53
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 58761, Seq: 2, Ack: 1, Len: 1370
▸ Transport Layer Security
```

```
0000  a8 3b 76 5a 89 f9 ae 17  9c 65 6e 74 08 00 45 28   ·;vZ····  ·ent··E(
0010  05 82 a6 07 40 00 33 06  18 e1 23 d5 91 ed 0a 6e   ····@·3·  ··#····n
0020  c3 35 01 bb e5 89 b4 2b  72 ae 79 e7 e1 3c 50 10   ·5·····+  r·y··<P·
0030  01 e9 b7 7b 00 00 16 03  03 00 7a 02 00 00 76 03   ···{····  ··z···v·
0040  03 a9 0b b6 3e 15 44 76  4a ff c4 e4 7e fd 27 d3   ····>·Dv  J···~·'·
0050  b3 aa 47 9f f1 16 da 9c  cf 58 03 99 18 de c2 f0   ··G·····  ·X······
0060  e0 20 91 d1 56 36 45 23  b2 7e e0 fb 58 d5 a9 c5   · ··V6E#  ·~··X···
0070  1c 08 92 44 a7 15 19 77  15 1e 76 e7 8f 31 56 5d   ···D···w  ··v··1V]
0080  9c ec 13 01 00 00 2e 00  2b 00 02 03 04 00 33 00   ······.·  +·····3·
0090  24 00 1d 00 20 e8 e5 5b  02 c5 c0 de a1 53 6f d3   $··· ··[  ·····So·
```

DNS Queries

DNS queries are requests used to resolve domain names into IP addresses. Analyzing DNS traffic helps in understanding domain access patterns and identifying suspicious or malicious domain requests.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns
```

```
No.   Time       Source          Destination     Protocol Length Info
    1 0.000000   10.110.195.53   10.110.195.36   DNS         82 Standard query 0xfe1c AAAA t-ring-fdv2.msedge.net
    2 0.131269   10.110.195.53   10.110.195.36   DNS         90 Standard query 0xbdc2 HTTPS config.extension.grammarly.com
    3 0.131916   10.110.195.53   10.110.195.36   DNS         90 Standard query 0xc3b1 AAAA config.extension.grammarly.com
    4 0.132548   10.110.195.53   10.110.195.36   DNS         90 Standard query 0x1616 A config.extension.grammarly.com
    5 0.303976   10.110.195.36   10.110.195.53   DNS        155 Standard query response 0xbdc2 HTTPS config.extension.grammarly.com CNAME d27xxe7juh1us6.clou
    6 0.303976   10.110.195.36   10.110.195.53   DNS        210 Standard query response 0xc3b1 AAAA config.extension.grammarly.com CNAME d27xxe7juh1us6.clou
    7 0.303976   10.110.195.36   10.110.195.53   DNS        197 Standard query response 0x1616 A config.extension.grammarly.com CNAME d27xxe7juh1us6.cloudfr
   19 0.575244   10.110.195.53   10.110.195.36   DNS         82 Standard query 0x47a4 A t-ring-fdv2.msedge.net
   35 0.718795   10.110.195.53   10.110.195.36   DNS         79 Standard query 0x3078 HTTPS accounts.google.com
   36 0.719170   10.110.195.53   10.110.195.36   DNS         79 Standard query 0x6ae2 AAAA accounts.google.com
   37 0.719555   10.110.195.53   10.110.195.36   DNS         79 Standard query 0x5da4 A accounts.google.com
   38 0.720400   10.110.195.53   10.110.195.36   DNS         70 Standard query 0x5802 HTTPS google.com
   39 0.720801   10.110.195.53   10.110.195.36   DNS         70 Standard query 0xb80c AAAA google.com
   40 0.721094   10.110.195.53   10.110.195.36   DNS         70 Standard query 0x72f3 A google.com
   41 0.721916   10.110.195.53   10.110.195.36   DNS         80 Standard query 0xef9d HTTPS beacons.gcp.gvt2.com
   42 0.722281   10.110.195.53   10.110.195.36   DNS         80 Standard query 0xd17b AAAA beacons.gcp.gvt2.com
```

```
Frame 1: Packet, 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\
Ethernet II, Src: CloudNetwork_5a:89:f9 (a8:3b:76:5a:89:f9), Dst: ae:17:9c:65:6e:74 (ae:17:9c:65
Internet Protocol Version 4, Src: 10.110.195.53, Dst: 10.110.195.36
User Datagram Protocol, Src Port: 49664, Dst Port: 53
Domain Name System (query)
```

```
0000  ae 17 9c 65 6e 74 a8 3b  76 5a 89 f9 08 00 45 00   ···ent·; vZ····E·
0010  00 44 1c ce 00 00 80 11  82 a5 0a 6e c3 35 0a 6e   ·D······ ···n·5·n
0020  c3 24 c2 00 00 35 00 30  97 2b fe 1c 01 00 00 01   ·$···5·0 ·+······
0030  00 00 00 00 00 00 0b 74  2d 72 69 6e 67 2d 66 64   ·······t -ring-fd
0040  76 32 06 6d 73 65 64 67  65 03 6e 65 74 00 00 1c   v2·msedg e·net···
0050  00 01                                              ··
```

Packet Captures for Analysis

Saving packet captures allows network traffic data to be preserved for future analysis and reporting. These files are useful for reviewing network behavior and conducting forensic investigations.

I have learned the basics of networking in cybersecurity, including IP and MAC addresses, DNS, and TCP/UDP protocols. I also learned how to use Wireshark to capture and analyze network traffic, filter packets, understand the difference between plain-text and encrypted traffic, and save packet captures for future analysis.