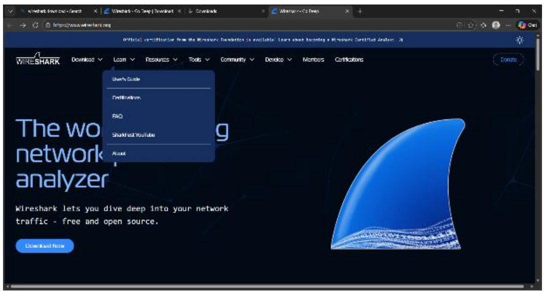
Task -03

Networking Basics for Cyber Security

1. Learn basic networking concepts (IP, MAC, DNS, TCP/UDP).

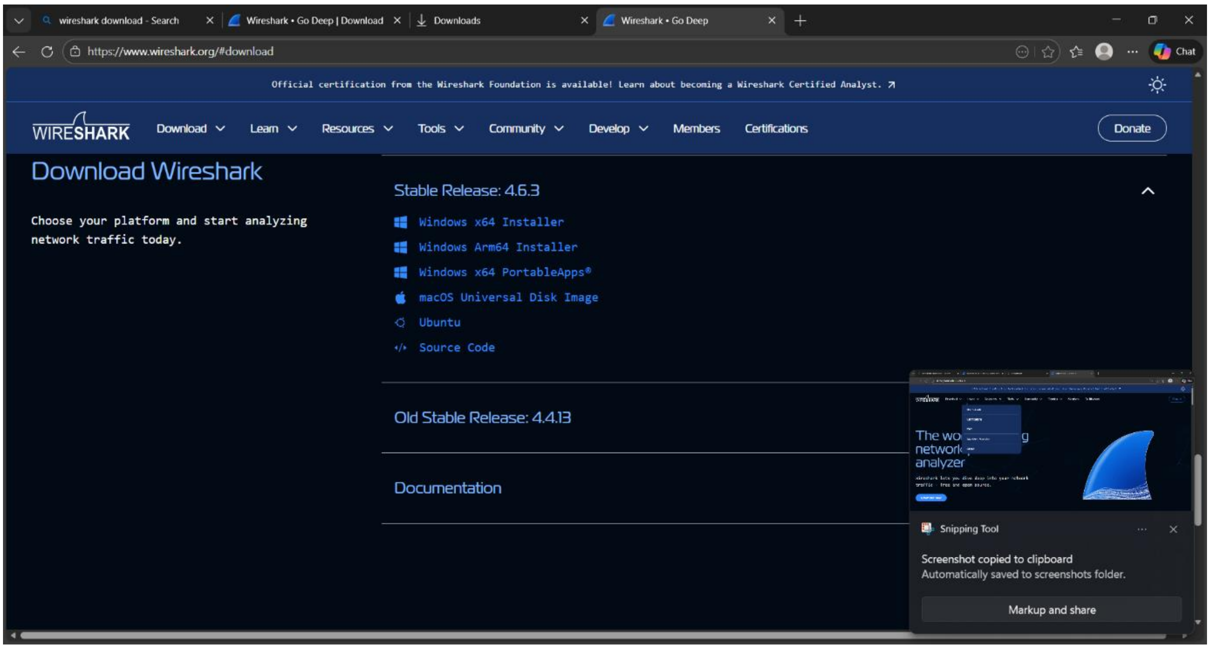
- **IP Address** – Identifies a device on a network
- **MAC Address** – Physical address of network device
- **DNS** – Converts domain names into IP addresses
- **TCP** – Reliable, connection-based protocol
- **UDP** – Fast, connectionless protocol

2. Install Wireshark and capture live network traffic



The wo g network analyzer

Wireshark lets you dive deep into your network traffic - free and open source.



Official certification from the Wireshark Foundation is available! Learn about becoming a Wireshark Certified Analyst.

Download Wireshark

Choose your platform and start analyzing network traffic today.

Stable Release: 4.6.3

- Windows x64 Installer
- Windows Arm64 Installer
- Windows x64 PortableApps®
- macOS Universal Disk Image
- Ubuntu
- Source Code

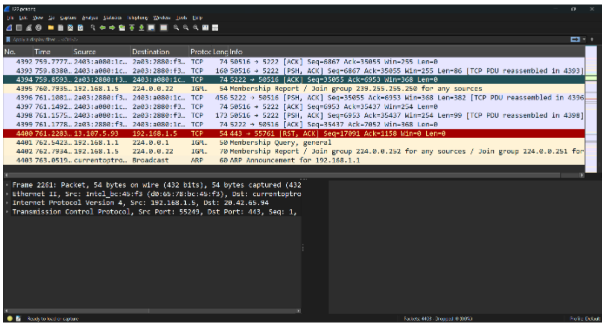
Old Stable Release: 4.4.13

Documentation

Snipping Tool

Screenshot copied to clipboard
Automatically saved to screenshots folder.

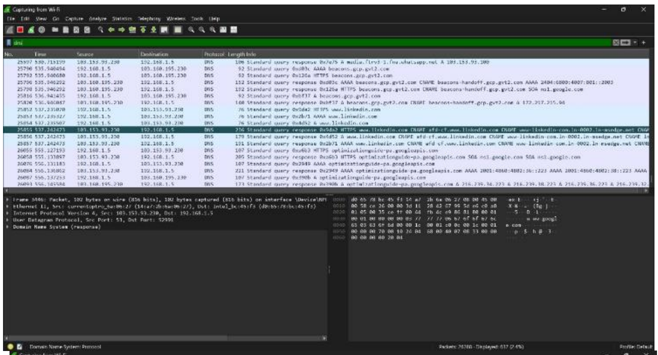
Markup and share



```
No.  Time         Source             Destination        Protoc Leng Info
4392 759.7777...  2403:a080:1c...    2a03:2880:f3...    TCP      74 50516 → 5222 [ACK] Seq=6867 Ack=35055 Win=255 Len=0
4393 759.8380...  2403:a080:1c...    2a03:2880:f3...    TCP     160 50516 → 5222 [PSH, ACK] Seq=6867 Ack=35055 Win=255 Len=86 [TCP PDU reassembled in 4393]
4394 759.8593...  2a03:2880:f3...    2403:a080:1c...    TCP      74 5222 → 50516 [ACK] Seq=35055 Ack=6953 Win=368 Len=0
4395 760.7935...  192.168.1.5        224.0.0.22         IGM.     54 Membership Report / Join group 239.255.255.250 for any sources
4396 761.1081...  2a03:2880:f3...    2403:a080:1c...    TCP     456 5222 → 50516 [PSH, ACK] Seq=35055 Ack=6953 Win=368 Len=382 [TCP PDU reassembled in 4396
4397 761.1492...  2403:a080:1c...    2a03:2880:f3...    TCP      74 50516 → 5222 [ACK] Seq=6953 Ack=35437 Win=254 Len=0
4398 761.1575...  2403:a080:1c...    2a03:2880:f3...    TCP     173 50516 → 5222 [PSH, ACK] Seq=6953 Ack=35437 Win=254 Len=99 [TCP PDU reassembled in 4398]
4399 761.1778...  2a03:2880:f3...    2403:a080:1c...    TCP      74 5222 → 50516 [ACK] Seq=35437 Ack=7052 Win=368 Len=0
4400 761.2283...  13.107.5.93        192.168.1.5        TCP      54 443 → 55761 [RST, ACK] Seq=17091 Ack=1158 Win=0 Len=0
4401 762.5423...  192.168.1.1        224.0.0.1          IGM.     50 Membership Query, general
4402 762.7934...  192.168.1.5        224.0.0.22         IGM.     70 Membership Report / Join group 224.0.0.252 for any sources / Join group 224.0.0.251 for
4403 763.0519...  currentoptro...    Broadcast          ARP      60 ARP Announcement for 192.168.1.1

› Frame 2261: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432
› Ethernet II, Src: Intel_bc:45:f3 (d0:65:78:bc:45:f3), Dst: currentoptro
› Internet Protocol Version 4, Src: 192.168.1.5, Dst: 20.42.65.94
› Transmission Control Protocol, Src Port: 55249, Dst Port: 443, Seq: 1,
```

3. Filter packets by protocol (HTTP, DNS, TCP).



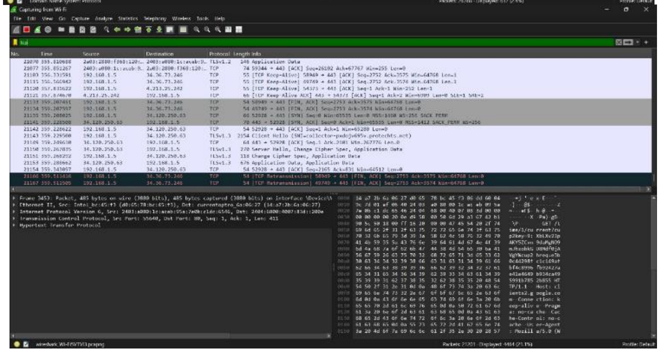
```
No.   Time        Source            Destination       Protocol Length Info
25597 530.715199  103.153.93.230    192.168.1.5       DNS      106 Standard query response 0x7e75 A media.ftrv3-1.fna.whatsapp.net A 103.153.93.100
25790 535.940494  192.168.1.5       103.160.195.230   DNS       92 Standard query 0xd03c AAAA beacons.gcp.gvt2.com
25792 535.940680  192.168.1.5       103.160.195.230   DNS       92 Standard query 0x126a HTTPS beacons.gcp.gvt2.com
25796 535.946292  103.160.195.230   192.168.1.5       DNS      152 Standard query response 0xd03c AAAA beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com AAAA 2404:6800:4007:801::2003
25798 535.946292  103.160.195.230   192.168.1.5       DNS      152 Standard query response 0x126a HTTPS beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com SOA ns1.google.com
25816 536.941455  192.168.1.5       103.160.195.230   DNS       92 Standard query 0xbf37 A beacons.gcp.gvt2.com
25820 536.946047  103.160.195.230   192.168.1.5       DNS      148 Standard query response 0xbf37 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 172.217.215.94
25852 537.235070  192.168.1.5       103.153.93.230    DNS       76 Standard query 0x9da2 HTTPS www.linkedin.com
25853 537.235327  192.168.1.5       103.153.93.230    DNS       76 Standard query 0x2b71 AAAA www.linkedin.com
25854 537.235507  192.168.1.5       103.153.93.230    DNS       76 Standard query 0x4d52 A www.linkedin.com
25855 537.242473  103.153.93.230    192.168.1.5       DNS      236 Standard query response 0x9da2 HTTPS www.linkedin.com CNAME afd-cf.www.linkedin.com CNAME www-linkedin-com.l-0002.l-msedge.net CNAM
25856 537.242473  103.153.93.230    192.168.1.5       DNS      179 Standard query response 0x4d52 A www.linkedin.com CNAME afd-cf.www.linkedin.com CNAME www-linkedin-com.l-0002.l-msedge.net CNAME l
25857 537.242473  103.153.93.230    192.168.1.5       DNS      191 Standard query response 0x2b71 AAAA www.linkedin.com CNAME afd-cf.www.linkedin.com CNAME www-linkedin-com.l-0002.l-msedge.net CNAME
26055 555.127193  192.168.1.5       103.153.93.230    DNS      107 Standard query 0xa6b3 HTTPS optimizationguide-pa.googleapis.com
26058 555.133897  103.153.93.230    192.168.1.5       DNS      205 Standard query response 0xa6b3 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com SOA ns1.google.com
26076 556.131183  192.168.1.5       103.153.93.230    DNS      107 Standard query 0x2949 AAAA optimizationguide-pa.googleapis.com
26084 556.136802  103.153.93.230    192.168.1.5       DNS      221 Standard query response 0x2949 AAAA optimizationguide-pa.googleapis.com AAAA 2001:4860:4802:36::223 AAAA 2001:4860:4802:38::223 AAAA
26087 556.137253  192.168.1.5       103.160.195.230   DNS      107 Standard query 0x390b A optimizationguide-pa.googleapis.com
26093 556.145594  103.160.195.230   192.168.1.5       DNS      173 Standard query response 0x390b A optimizationguide-pa.googleapis.com A 216.239.34.223 A 216.239.38.223 A 216.239.36.223 A 216.239.32.

› Frame 3446: Packet, 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF
› Ethernet II, Src: currentoptro_6a:06:27 (14:a7:2b:6a:06:27), Dst: Intel_bc:45:f3 (d0:65:78:bc:45:f3)
› Internet Protocol Version 4, Src: 103.153.93.230, Dst: 192.168.1.5
› User Datagram Protocol, Src Port: 53, Dst Port: 52991
› Domain Name System (response)

Domain Name System: Protocol                Packets: 26288 · Displayed: 617 (2.4%)
```

*DNS

-

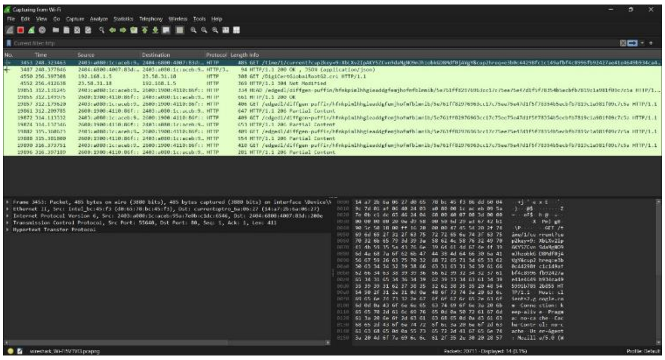


```
No.   Time        Source              Destination         Protocol Length Info
21070 355.810688  2a03:2880:f368:120:...  2403:a080:1c:aceb:9...  TLSv1.2  146 Application Data
21077 355.851267  2403:a080:1c:aceb:9...  2a03:2880:f368:120:...  TCP       74 59344 → 443 [ACK] Seq=26102 Ack=67767 Win=255 Len=0
21103 356.331591  192.168.1.5         34.36.73.246        TCP       55 [TCP Keep-Alive] 58949 → 443 [ACK] Seq=2752 Ack=3575 Win=64768 Len=1
21115 356.560942  192.168.1.5         34.36.73.246        TCP       55 [TCP Keep-Alive] 49749 → 443 [ACK] Seq=2752 Ack=3574 Win=64768 Len=1
21120 357.831622  192.168.1.5         4.213.25.242        TCP       55 [TCP Keep-Alive] 54373 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
21121 357.874670  4.213.25.242        192.168.1.5         TCP       66 [TCP Keep-Alive ACK] 443 → 54373 [ACK] Seq=1 Ack=2 Win=6909 Len=0 SLE=1 SRE=2
21133 359.207451  192.168.1.5         34.36.73.246        TCP       54 58949 → 443 [FIN, ACK] Seq=2753 Ack=3575 Win=64768 Len=0
21134 359.207597  192.168.1.5         34.36.73.246        TCP       54 49749 → 443 [FIN, ACK] Seq=2753 Ack=3574 Win=64768 Len=0
21135 359.208025  192.168.1.5         34.120.250.63       TCP       66 52928 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
21141 359.228508  34.120.250.63       192.168.1.5         TCP       70 443 → 52928 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
21142 359.228622  192.168.1.5         34.120.250.63       TCP       54 52928 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
21143 359.229500  192.168.1.5         34.120.250.63       TLSv1.3 2154 Client Hello (SNI=collector-pxdojv695v.protechts.net)
21149 359.249610  34.120.250.63       192.168.1.5         TCP       64 443 → 52928 [ACK] Seq=1 Ack=2101 Win=267776 Len=0
21150 359.267835  34.120.250.63       192.168.1.5         TLSv1.3  270 Server Hello, Change Cipher Spec, Application Data
21151 359.268292  192.168.1.5         34.120.250.63       TLSv1.3  118 Change Cipher Spec, Application Data
21153 359.288662  34.120.250.63       192.168.1.5         TLSv1.3  676 Application Data, Application Data
21154 359.343057  192.168.1.5         34.120.250.63       TCP       54 52928 → 443 [ACK] Seq=2165 Ack=831 Win=64512 Len=0
21166 359.511416  192.168.1.5         34.36.73.246        TCP       54 [TCP Retransmission] 58949 → 443 [FIN, ACK] Seq=2753 Ack=3575 Win=64768 Len=0
21167 359.512505  192.168.1.5         34.36.73.246        TCP       54 [TCP Retransmission] 49749 → 443 [FIN, ACK] Seq=2753 Ack=3574 Win=64768 Len=0

› Frame 3453: Packet, 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface \Device\N
› Ethernet II, Src: Intel_bc:45:f3 (d0:65:78:bc:45:f3), Dst: currentoptro_6a:06:27 (14:a7:2b:6a:06:27)
› Internet Protocol Version 6, Src: 2403:a080:1c:aceb:95a:7e0b:c1dc:6546, Dst: 2404:6800:4007:83d::200e
› Transmission Control Protocol, Src Port: 55640, Dst Port: 80, Seq: 1, Ack: 1, Len: 411
› Hypertext Transfer Protocol

wireshark_Wi-FiSVTV31.pcapng                Packets: 2201 · Displayed: 4484 (21.1%)
```

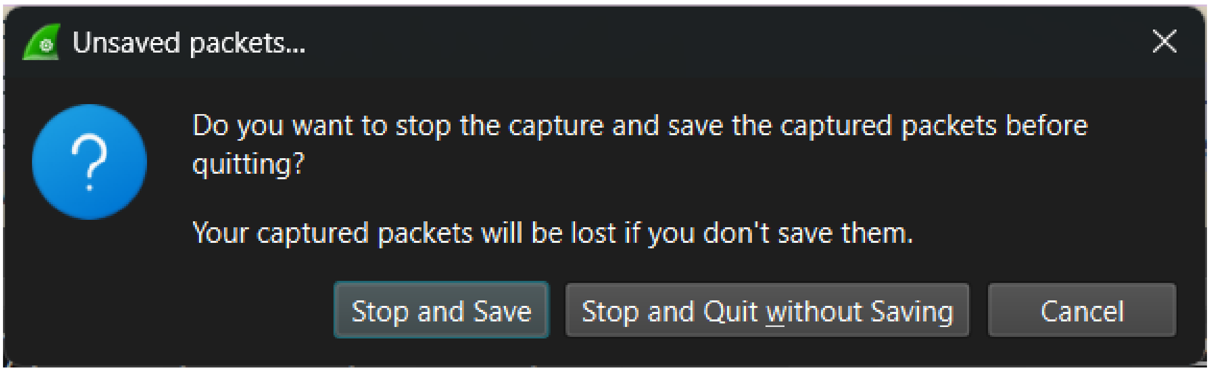
*TCP



```
No.   Time        Source                  Destination             Protocol Length Info
3453  248.323463  2403:a080:1c:aceb:9...  2404:6800:4007:83d:...  HTTP     485 GET /time/1/current?cup2key=9:XbLXv2IpAKY57Cvn9daMgN09mJhzobkGD0Mdf0jAVgY&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca4...
3487  248.377846  2404:6800:4007:83d:...  2403:a080:1c:aceb:9...  HTTP/J...  94 HTTP/1.1 200 OK , JSON (application/json)
4550  256.397308  192.168.1.5             23.58.31.18             HTTP     308 GET /DigiCertGlobalRootG2.crl HTTP/1.1
4552  256.412638  23.58.31.18             192.168.1.5             HTTP     369 HTTP/1.1 304 Not Modified
19851 312.131245  2403:a080:1c:aceb:9...  2600:1900:4110:86f::    HTTP     334 HEAD /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/5e761ff8297698dcc17c75ee75e47d1f5f78354b5ecbfb7819c1a981f09c7c5a HTTP/1...
19855 312.149975  2600:1900:4110:86f::    2403:a080:1c:aceb:9...  HTTP     661 HTTP/1.1 200 OK
19857 312.179620  2403:a080:1c:aceb:9...  2600:1900:4110:86f::    HTTP     406 GET /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/5e761ff8297698dcc17c75ee75e47d1f5f78354b5ecbfb7819c1a981f09c7c5a HTTP/1.1
19861 312.209785  2600:1900:4110:86f::    2403:a080:1c:aceb:9...  HTTP     647 HTTP/1.1 206 Partial Content
19872 314.113332  2403:a080:1c:aceb:9...  2600:1900:4110:86f::    HTTP     409 GET /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/5e761ff8297698dcc17c75ee75e47d1f5f78354b5ecbfb7819c1a981f09c7c5a HTTP/1.1
19874 314.137346  2600:1900:4110:86f::    2403:a080:1c:aceb:9...  HTTP     651 HTTP/1.1 206 Partial Content
19882 315.360673  2403:a080:1c:aceb:9...  2600:1900:4110:86f::    HTTP     409 GET /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/5e761ff8297698dcc17c75ee75e47d1f5f78354b5ecbfb7819c1a981f09c7c5a HTTP/1.1
19888 315.381800  2600:1900:4110:86f::    2403:a080:1c:aceb:9...  HTTP     554 HTTP/1.1 206 Partial Content
19890 316.373751  2403:a080:1c:aceb:9...  2600:1900:4110:86f::    HTTP     410 GET /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/5e761ff8297698dcc17c75ee75e47d1f5f78354b5ecbfb7819c1a981f09c7c5a HTTP/1.1
19896 316.397189  2600:1900:4110:86f::    2403:a080:1c:aceb:9...  HTTP     281 HTTP/1.1 206 Partial Content

› Frame 3453: Packet, 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface \Device\N
› Ethernet II, Src: Intel_bc:45:f3 (d0:65:78:bc:45:f3), Dst: currentoptro_6a:06:27 (14:a7:2b:6a:06:27)
› Internet Protocol Version 6, Src: 2403:a080:1c:aceb:95a:7e0b:c1dc:6546, Dst: 2404:6800:4007:83d::200e
› Transmission Control Protocol, Src Port: 55640, Dst Port: 80, Seq: 1, Ack: 1, Len: 411
› Hypertext Transfer Protocol
```

*HTTP



Do you want to stop the capture and save the captured packets before quitting?

Your captured packets will be lost if you don't save them.

4. Observe three-way TCP handshake.

TCP 3-WAY HANDSHAKE

The TCP 3-Way Handshake is a three-step process (SYN, SYN-ACK, ACK) used by the Transmission Control Protocol (TCP) to reliably establish a connection between a client and server, ensuring both are ready to communicate and agree on initial sequence numbers before data transfer begins, forming a full-duplex connection for secure and synchronized data exchange.

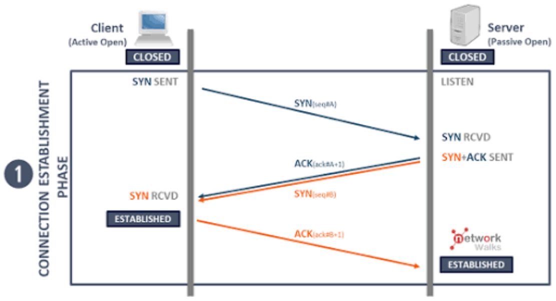
The Three Steps:

1. **SYN**

(Synchronize):

- The client sends a TCP segment with the **SYN flag** set to 1, indicating a request to start a connection.
- It includes an initial sequence number (ISN) to track data flow.

2. **SYN-ACK (Synchronize-Acknowledge):**
   - The server receives the SYN, sets both the **SYN and ACK flags**, and sends it back.
   - The ACK number confirms receipt of the client's SYN (incremented by 1), and the server sends its own ISN.
3. **ACK (Acknowledge):**
   - The client receives the SYN-ACK and sends a final segment with the **ACK flag** set.
   - This acknowledges the server's ISN, completing the handshake.



5. Identify plain-text traffic vs encrypted traffic

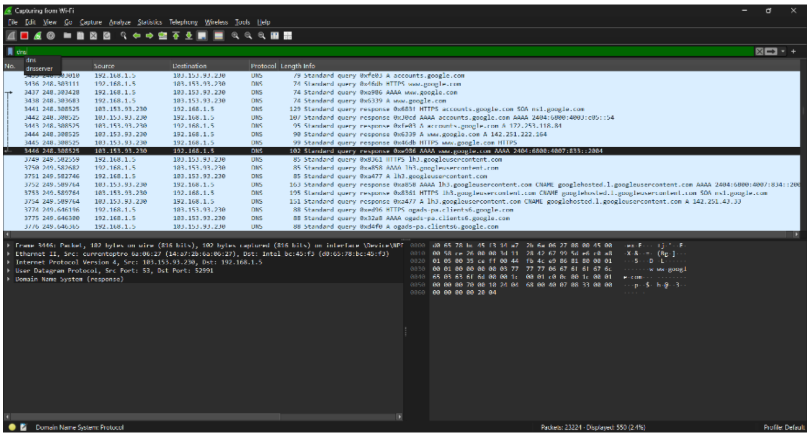
Plain-text traffic

- **Definition**: Original, readable data (cleartext) that hasn't been altered or hidden.
- **Appearance**: You can see the actual content (e.g., HTTP requests/responses, emails, clear FTP) in network traffic analysis tools.
- **Examples**: Basic HTTP, Telnet, unencrypted email (SMTP/POP3 without TLS).
- **Identification**: Direct inspection of packet payloads.

Encrypted Traffic

- **Definition**: Plaintext data transformed into ciphertext (scrambled data) by encryption algorithms.
- **Appearance**: Appears as random-looking binary data (ciphertext) in packet captures, making content inspection impossible.
- **Examples**: HTTPS (web), FTPS, SSH, VPNs, encrypted DNS (DoH).
- **Identification (Metadata & Behavior)**:
    - **Protocols**: Look for TLS/SSL handshake packets (e.g., ServerHello, ClientHello).
    - **Metadata**: Source/destination IPs, ports (443 for HTTPS), flow duration, packet sizes, inter-arrival times.
    - **Statistical Analysis**: High entropy (randomness) in payloads, indicating encryption.
    - **Patterns**: Specific patterns in handshake data or flow sequences can reveal application types (e.g., browser, malware).

6.Capture DNS queries and analyze them.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
dns
dnsserver
Domain Name System Protocol
Profile: Default

```
No.  Time         Source          Destination     Protocol Length Info
[illegible] 248.303010 192.168.1.5 103.153.93.230 DNS  79 Standard query 0xfe03 A accounts.google.com
3436 248.303111   192.168.1.5     103.153.93.230  DNS      74 Standard query 0x46db HTTPS www.google.com
3437 248.303428   192.168.1.5     103.153.93.230  DNS      74 Standard query 0xe986 AAAA www.google.com
3438 248.303683   192.168.1.5     103.153.93.230  DNS      74 Standard query 0x6339 A www.google.com
3441 248.308525   103.153.93.230  192.168.1.5     DNS     129 Standard query response 0x6831 HTTPS accounts.google.com SOA ns1.google.com
3442 248.308525   103.153.93.230  192.168.1.5     DNS     107 Standard query response 0x30cd AAAA accounts.google.com AAAA 2404:6800:4003:c05::54
3443 248.308525   103.153.93.230  192.168.1.5     DNS      95 Standard query response 0xfe03 A accounts.google.com A 172.253.118.84
3444 248.308525   103.153.93.230  192.168.1.5     DNS      90 Standard query response 0x6339 A www.google.com A 142.251.222.164
3445 248.308525   103.153.93.230  192.168.1.5     DNS      99 Standard query response 0x46db HTTPS www.google.com HTTPS
3446 248.308525   103.153.93.230  192.168.1.5     DNS     102 Standard query response 0xe986 AAAA www.google.com AAAA 2404:6800:4007:833::2004
3749 249.582559   192.168.1.5     103.153.93.230  DNS      85 Standard query 0x8361 HTTPS lh3.googleusercontent.com
3750 249.582682   192.168.1.5     103.153.93.230  DNS      85 Standard query 0xa858 AAAA lh3.googleusercontent.com
3751 249.582746   192.168.1.5     103.153.93.230  DNS      85 Standard query 0xa477 A lh3.googleusercontent.com
3752 249.589764   103.153.93.230  192.168.1.5     DNS     163 Standard query response 0xa858 AAAA lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com AAAA 2404:6800:4007:834::200
3753 249.589764   103.153.93.230  192.168.1.5     DNS     195 Standard query response 0x8361 HTTPS lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com SOA ns1.google.com
3754 249.589764   103.153.93.230  192.168.1.5     DNS     151 Standard query response 0xa477 A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 142.251.43.33
3774 249.646196   192.168.1.5     103.153.93.230  DNS      88 Standard query 0xed96 HTTPS ogads-pa.clients6.google.com
3775 249.646300   192.168.1.5     103.153.93.230  DNS      88 Standard query 0x32a8 AAAA ogads-pa.clients6.google.com
3776 249.646365   192.168.1.5     103.153.93.230  DNS      88 Standard query 0xd4f0 A ogads-pa.clients6.google.com

> Frame 3446: Packet, 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF
> Ethernet II, Src: currentoptro 6a:06:27 (14:a7:2b:6a:06:27), Dst: Intel bc:45:f3 (d0:65:78:bc:45:f3)
> Internet Protocol Version 4, Src: 103.153.93.230, Dst: 192.168.1.5
> User Datagram Protocol, Src Port: 53, Dst Port: 52991
> Domain Name System (response)

0000  d0 65 78 bc 45 f3 14 a7  2b 6a 06 27 08 00 45 00   ·ex·E···+j·'··E·
0010  00 58 ce 26 00 00 3d 11  28 42 67 99 5d e6 c0 a8   ·X·&··=·(Bg·]···
0020  01 05 00 35 ce ff 00 44  fb 4c e9 86 81 80 00 01   ···5···D·L······
0030  00 01 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······www·googl
0040  65 03 63 6f 6d 00 00 1c  00 01 c0 0c 00 1c 00 01   e·com···········
0050  00 00 00 70 00 10 24 04  68 00 40 07 08 33 00 00   ···p··$·h·@··3··
0060  00 00 00 00 20 04                                  ···· ·

Packets: 23224 · Displayed: 550 (2.4%)
```

7.Save packet captures for analysis.

NETWORK ANALYZER.pcapng

8.Write observations in simple language.

1. The client sent a **SYN** packet to initiate the connection.
2. The server responded with a **SYN-ACK** packet to acknowledge the request.
3. The client replied with an **ACK** packet, completing the handshake.
   This establishes a reliable TCP connection between client and server.