Date: 29/ 08/ 2025

Lab Practical #09:

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

Practical Assignment #09:

1. Explain usage of Wireshark tool.

- **Usage of Wireshark Tool:** Wireshark is the most widely used network protocol analyzer. It allows you to capture packets moving across a network in real time and then inspect their contents at a very detailed level.
- **Key Uses:**
- **Packet Capture:** Records all network traffic passing through an interface (wired, wireless, loopback).
- **Protocol Analysis:** Supports hundreds of protocols (HTTP, TCP, UDP, IP, ARP, DNS, FTP, SSL/TLS, etc.).
- **Troubleshooting:** Helps identify network issues such as latency, packet loss, retransmissions, or misconfigured systems.
- **Security Monitoring:** Detects suspicious traffic (malware communication, scanning, brute force attempts).
- **Learning/Education:** Excellent for students to understand how data moves across networks and how protocols interact.
- **Performance Tuning:** Analysis bandwidth usage, detects bottlenecks, and optimizes configurations.
- In simple words: Wireshark lets you “see” what’s happening inside your network packet by packet.

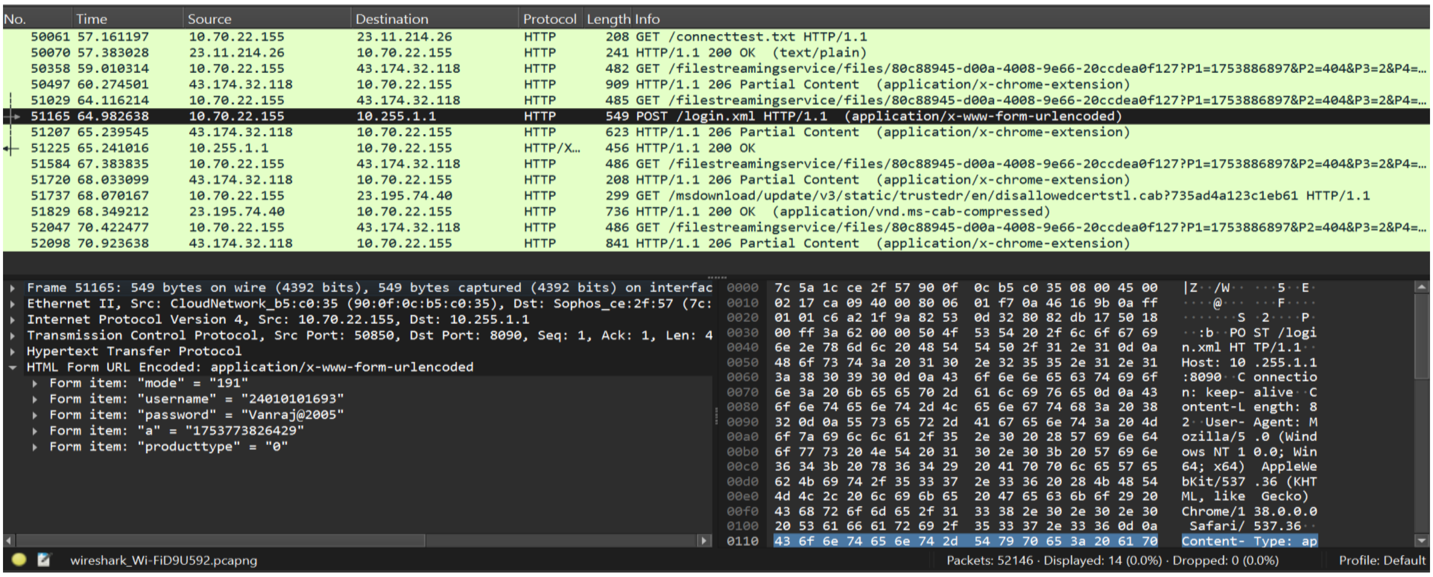
2. Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

- **Packet Capture & Header Analysis in Wireshark:** When you capture packets, Wireshark shows a breakdown at **three layers**:
- **Packet List Pane** – Summary of each captured packet (No., Time, Source, Destination, Protocol, Info).
- **Packet Details Pane** – Hierarchical breakdown of protocols in the packet.
- **Packet Bytes Pane** – Raw hex + ASCII data.

a) HTTP (Hypertext Transfer Protocol):

- Found under Application Layer.
- Wireshark shows Request/Response details:
- Request Method: GET, POST, etc.
- Host, User-Agent, Cookies.
- Response: Status code (200 OK, 404 Not Found).
- Example usage: Check what web resources are being request.

Date: 29/ 08/ 2025



```
No.    Time       Source          Destination     Protocol Length Info
 50061 57.161197  10.70.22.155    23.11.214.26    HTTP      208 GET /connecttest.txt HTTP/1.1
 50070 57.383028  23.11.214.26    10.70.22.155    HTTP      241 HTTP/1.1 200 OK  (text/plain)
 50358 59.010314  10.70.22.155    43.174.32.118   HTTP      482 GET /filestreamingservice/files/80c88945-d00a-4008-9e66-20ccdea0f127?P1=1753886897&P2=404&P3=2&P4=…
 50497 60.274501  43.174.32.118   10.70.22.155    HTTP      909 HTTP/1.1 206 Partial Content  (application/x-chrome-extension)
 51029 64.116214  10.70.22.155    43.174.32.118   HTTP      485 GET /filestreamingservice/files/80c88945-d00a-4008-9e66-20ccdea0f127?P1=1753886897&P2=404&P3=2&P4=…
 51165 64.982638  10.70.22.155    10.255.1.1      HTTP      549 POST /login.xml HTTP/1.1  (application/x-www-form-urlencoded)
 51207 65.239545  43.174.32.118   10.70.22.155    HTTP      623 HTTP/1.1 206 Partial Content  (application/x-chrome-extension)
 51225 65.241016  10.255.1.1      10.70.22.155    HTTP/X…   456 HTTP/1.1 200 OK
 51584 67.383835  10.70.22.155    43.174.32.118   HTTP      486 GET /filestreamingservice/files/80c88945-d00a-4008-9e66-20ccdea0f127?P1=1753886897&P2=404&P3=2&P4=…
 51720 68.033099  43.174.32.118   10.70.22.155    HTTP      208 HTTP/1.1 206 Partial Content  (application/x-chrome-extension)
 51737 68.070167  10.70.22.155    23.195.74.40    HTTP      299 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?735ad4a123c1eb61 HTTP/1.1
 51829 68.349212  23.195.74.40    10.70.22.155    HTTP      736 HTTP/1.1 200 OK  (application/vnd.ms-cab-compressed)
 52047 70.422477  10.70.22.155    43.174.32.118   HTTP      486 GET /filestreamingservice/files/80c88945-d00a-4008-9e66-20ccdea0f127?P1=1753886897&P2=404&P3=2&P4=…
 52098 70.923638  43.174.32.118   10.70.22.155    HTTP      841 HTTP/1.1 206 Partial Content  (application/x-chrome-extension)
```

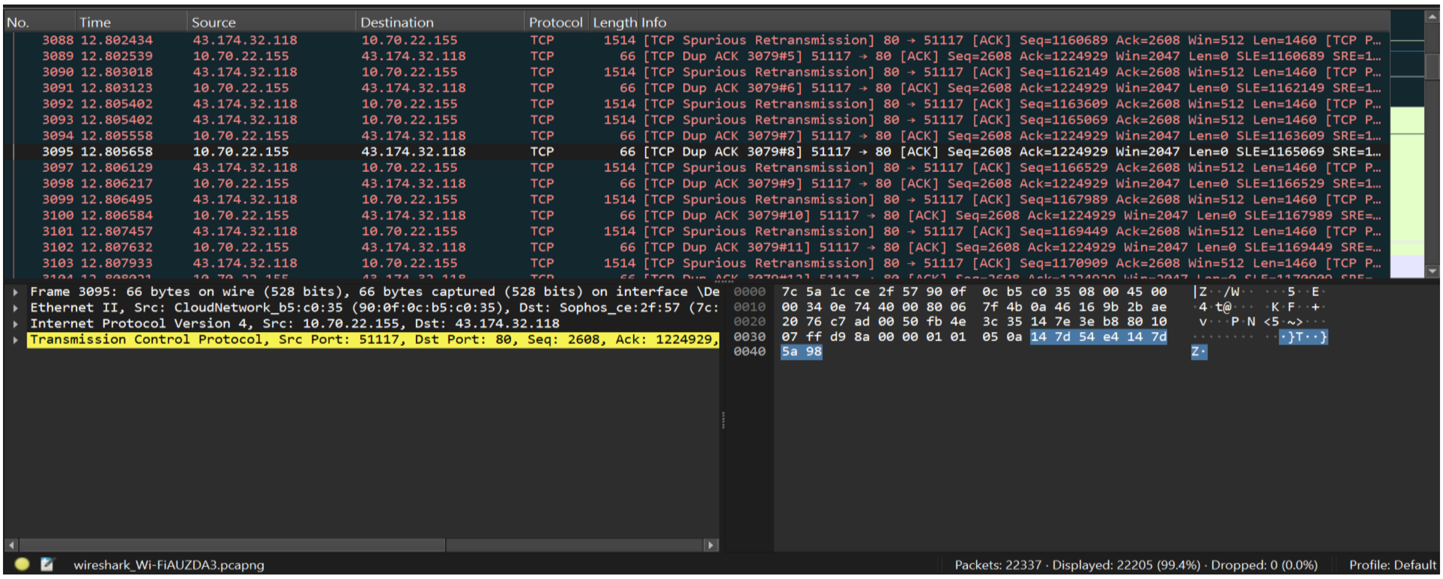
```
Frame 51165: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interfac
Ethernet II, Src: CloudNetwork_b5:c0:35 (90:0f:0c:b5:c0:35), Dst: Sophos_ce:2f:57 (7c:
Internet Protocol Version 4, Src: 10.70.22.155, Dst: 10.255.1.1
Transmission Control Protocol, Src Port: 50850, Dst Port: 8090, Seq: 1, Ack: 1, Len: 4
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "mode" = "191"
  Form item: "username" = "24010101693"
  Form item: "password" = "Vanraj@2005"
  Form item: "a" = "1753773826429"
  Form item: "producttype" = "0"
```

```
0000  7c 5a 1c ce 2f 57 90 0f  0c b5 c0 35 08 00 45 00   |Z··/W·· ···5··E·
0010  02 17 ca 09 40 00 80 06  01 f7 0a 46 16 9b 0a ff   ····@··· ···F····
0020  01 01 c6 a2 1f 9a 82 53  0d 32 80 82 db 17 50 18   ·······S ·2····P·
0030  00 ff 3a 62 00 00 50 4f  53 54 20 2f 6c 6f 67 69   ··:b··PO ST /logi
0040  6e 2e 78 6d 6c 20 48 54  54 50 2f 31 2e 31 0d 0a   n.xml HT TP/1.1··
0050  48 6f 73 74 3a 20 31 30  2e 32 35 35 2e 31 2e 31   Host: 10 .255.1.1
0060  3a 38 30 39 30 0d 0a 43  6f 6e 6e 65 63 74 69 6f   :8090··C onnectio
0070  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 43   n: keep- alive··C
0080  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 38   ontent-L ength: 8
0090  32 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   2··User- Agent: M
00a0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 57 69 6e 64   ozilla/5 .0 (Wind
00b0  6f 77 73 20 4e 54 20 31  30 2e 30 3b 20 57 69 6e   ows NT 1 0.0; Win
00c0  36 34 3b 20 78 36 34 29  20 41 70 70 6c 65 57 65   64; x64)  AppleWe
00d0  62 4b 69 74 2f 35 33 37  2e 33 36 20 28 4b 48 54   bKit/537 .36 (KHT
00e0  4d 4c 2c 20 6c 69 6b 65  20 47 65 63 6b 6f 29 20   ML, like  Gecko)
00f0  43 68 72 6f 6d 65 2f 31  33 38 2e 30 2e 30 2e 30   Chrome/1 38.0.0.0
0100  20 53 61 66 61 72 69 2f  35 33 37 2e 33 36 0d 0a    Safari/ 537.36··
0110  43 6f 6e 74 65 6e 74 2d  54 79 70 65 3a 20 61 70   Content- Type: ap
```

wireshark_Wi-FiD9U592.pcapng   Packets: 52146 · Displayed: 14 (0.0%) · Dropped: 0 (0.0%)   Profile: Default

b) TCP (Transmission Control Protocol):

- Found under Transport Layer.
- Fields you'll see in Wireshark:
- Source Port / Destination Port (e.g., 80 for HTTP, 443 for HTTPS).
- Sequence & Acknowledgment Numbers (for reliability).
- Flags (SYN, ACK, FIN, RST).
- Window Size (flow control).
- Example usage: Spot retransmissions, handshake problems, or dropped connections.



```
No.   Time       Source          Destination     Protocol Length Info
 3088 12.802434  43.174.32.118   10.70.22.155    TCP      1514 [TCP Spurious Retransmission] 80 → 51117 [ACK] Seq=1160689 Ack=2608 Win=512 Len=1460 [TCP P…
 3089 12.802539  10.70.22.155    43.174.32.118   TCP        66 [TCP Dup ACK 3079#5] 51117 → 80 [ACK] Seq=2608 Ack=1224929 Win=2047 Len=0 SLE=1160689 SRE=1…
 3090 12.803018  43.174.32.118   10.70.22.155    TCP      1514 [TCP Spurious Retransmission] 80 → 51117 [ACK] Seq=1162149 Ack=2608 Win=512 Len=1460 [TCP P…
 3091 12.803123  10.70.22.155    43.174.32.118   TCP        66 [TCP Dup ACK 3079#6] 51117 → 80 [ACK] Seq=2608 Ack=1224929 Win=2047 Len=0 SLE=1162149 SRE=1…
 3092 12.805402  43.174.32.118   10.70.22.155    TCP      1514 [TCP Spurious Retransmission] 80 → 51117 [ACK] Seq=1163609 Ack=2608 Win=512 Len=1460 [TCP P…
 3093 12.805402  43.174.32.118   10.70.22.155    TCP      1514 [TCP Spurious Retransmission] 80 → 51117 [ACK] Seq=1165069 Ack=2608 Win=512 Len=1460 [TCP P…
 3094 12.805558  10.70.22.155    43.174.32.118   TCP        66 [TCP Dup ACK 3079#7] 51117 → 80 [ACK] Seq=2608 Ack=1224929 Win=2047 Len=0 SLE=1163609 SRE=1…
 3095 12.805658  10.70.22.155    43.174.32.118   TCP        66 [TCP Dup ACK 3079#8] 51117 → 80 [ACK] Seq=2608 Ack=1224929 Win=2047 Len=0 SLE=1165069 SRE=1…
 3097 12.806129  43.174.32.118   10.70.22.155    TCP      1514 [TCP Spurious Retransmission] 80 → 51117 [ACK] Seq=1166529 Ack=2608 Win=512 Len=1460 [TCP P…
 3098 12.806217  10.70.22.155    43.174.32.118   TCP        66 [TCP Dup ACK 3079#9] 51117 → 80 [ACK] Seq=2608 Ack=1224929 Win=2047 Len=0 SLE=1166529 SRE=1…
 3099 12.806495  43.174.32.118   10.70.22.155    TCP      1514 [TCP Spurious Retransmission] 80 → 51117 [ACK] Seq=1167989 Ack=2608 Win=512 Len=1460 [TCP P…
 3100 12.806584  10.70.22.155    43.174.32.118   TCP        66 [TCP Dup ACK 3079#10] 51117 → 80 [ACK] Seq=2608 Ack=1224929 Win=2047 Len=0 SLE=1167989 SRE=…
 3101 12.807457  43.174.32.118   10.70.22.155    TCP      1514 [TCP Spurious Retransmission] 80 → 51117 [ACK] Seq=1169449 Ack=2608 Win=512 Len=1460 [TCP P…
 3102 12.807632  10.70.22.155    43.174.32.118   TCP        66 [TCP Dup ACK 3079#11] 51117 → 80 [ACK] Seq=2608 Ack=1224929 Win=2047 Len=0 SLE=1169449 SRE=…
 3103 12.807933  43.174.32.118   10.70.22.155    TCP      1514 [TCP Spurious Retransmission] 80 → 51117 [ACK] Seq=1170909 Ack=2608 Win=512 Len=1460 [TCP P…
```

```
Frame 3095: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \De
Ethernet II, Src: CloudNetwork_b5:c0:35 (90:0f:0c:b5:c0:35), Dst: Sophos_ce:2f:57 (7c:
Internet Protocol Version 4, Src: 10.70.22.155, Dst: 43.174.32.118
Transmission Control Protocol, Src Port: 51117, Dst Port: 80, Seq: 2608, Ack: 1224929,
```

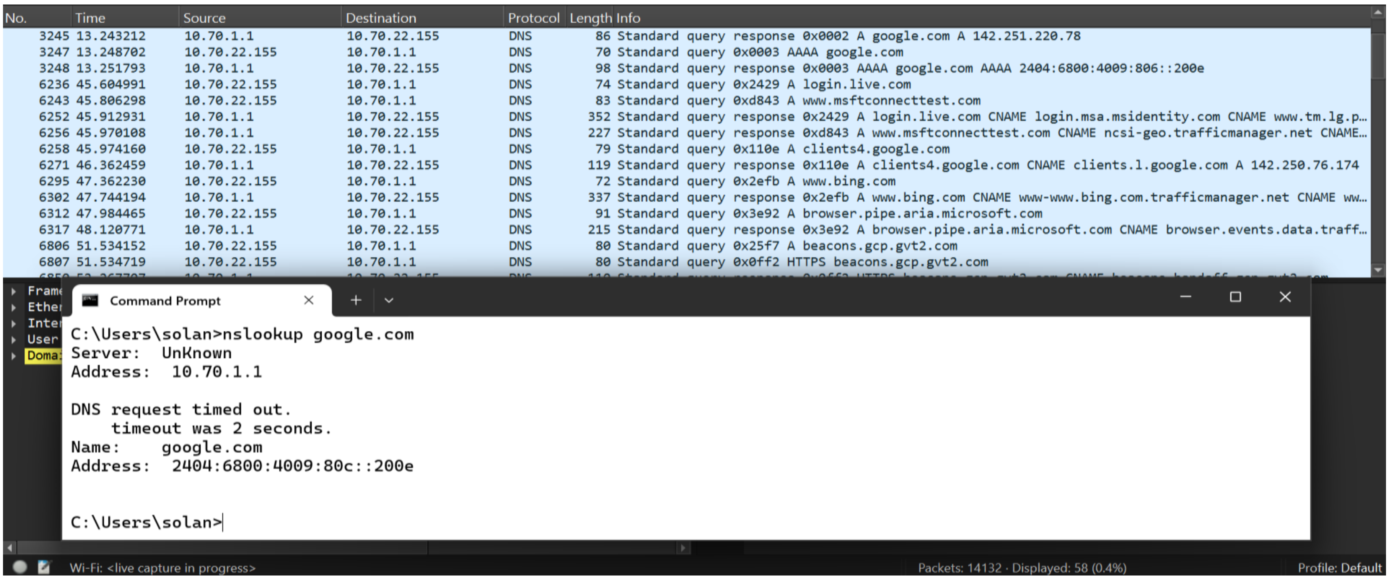
```
0000  7c 5a 1c ce 2f 57 90 0f  0c b5 c0 35 08 00 45 00   |Z··/W·· ···5··E·
0010  00 34 0e 74 40 00 80 06  7f 4b 0a 46 16 9b 2b ae   ·4·t@··· ·K·F··+·
0020  20 76 c7 ad 00 50 fb 4e  3c 35 14 7e 3e b8 80 10    v···P·N <5·~>···
0030  07 ff d9 8a 00 00 01 01  05 0a 14 7d 54 e4 14 7d   ········ ··}T··}
0040  5a 98                                              Z·
```

wireshark_Wi-FiAUZDA3.pcapng   Packets: 22337 · Displayed: 22205 (99.4%) · Dropped: 0 (0.0%)   Profile: Default

c) UDP (User Datagram Protocol):

- Also at **Transport Layer**, but simpler than TCP.

- Fields:
  - **Source Port / Destination Port** (e.g., 53 for DNS, 67/68 for DHCP).
  - **Length** (size of data).
  - **Checksum**.
- Example usage: Analyse lightweight communications like DNS queries or streaming.



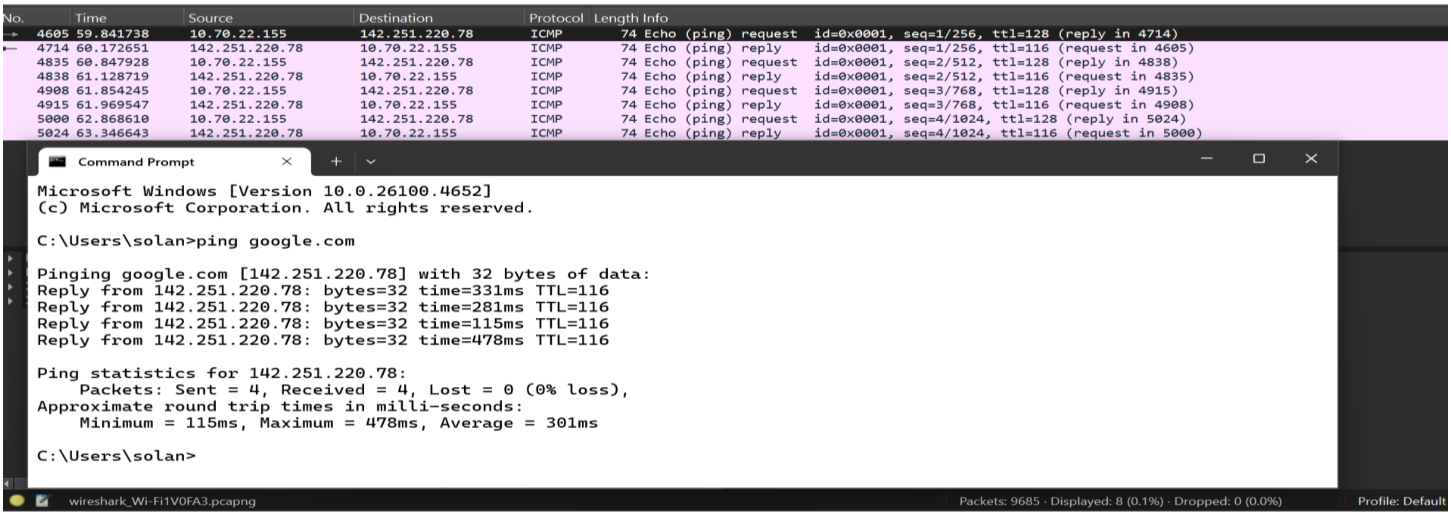
```
No.   Time      Source        Destination   Protocol Length Info
 3245 13.243212 10.70.1.1     10.70.22.155  DNS       86 Standard query response 0x0002 A google.com A 142.251.220.78
 3247 13.248702 10.70.22.155  10.70.1.1     DNS       70 Standard query 0x0003 AAAA google.com
 3248 13.251793 10.70.1.1     10.70.22.155  DNS       98 Standard query response 0x0003 AAAA google.com AAAA 2404:6800:4009:806::200e
 6236 45.604991 10.70.22.155  10.70.1.1     DNS       74 Standard query 0x2429 A login.live.com
 6243 45.806298 10.70.22.155  10.70.1.1     DNS       83 Standard query 0xd843 A www.msftconnecttest.com
 6252 45.912931 10.70.1.1     10.70.22.155  DNS      352 Standard query response 0x2429 A login.live.com CNAME login.msa.msidentity.com CNAME www.tm.lg.p…
 6256 45.970108 10.70.1.1     10.70.22.155  DNS      227 Standard query response 0xd843 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME…
 6258 45.974160 10.70.22.155  10.70.1.1     DNS       79 Standard query 0x110e A clients4.google.com
 6271 46.362459 10.70.1.1     10.70.22.155  DNS      119 Standard query response 0x110e A clients4.google.com CNAME clients.l.google.com A 142.250.76.174
 6295 47.362230 10.70.22.155  10.70.1.1     DNS       72 Standard query 0x2efb A www.bing.com
 6302 47.744194 10.70.1.1     10.70.22.155  DNS      337 Standard query response 0x2efb A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME ww…
 6312 47.984465 10.70.22.155  10.70.1.1     DNS       91 Standard query 0x3e92 A browser.pipe.aria.microsoft.com
 6317 48.120771 10.70.1.1     10.70.22.155  DNS      215 Standard query response 0x3e92 A browser.pipe.aria.microsoft.com CNAME browser.events.data.traff…
 6806 51.534152 10.70.22.155  10.70.1.1     DNS       80 Standard query 0x25f7 A beacons.gcp.gvt2.com
 6807 51.534719 10.70.22.155  10.70.1.1     DNS       80 Standard query 0x0ff2 HTTPS beacons.gcp.gvt2.com
```

```
C:\Users\solan>nslookup google.com
Server:  UnKnown
Address:  10.70.1.1

DNS request timed out.
    timeout was 2 seconds.
Name:    google.com
Address:  2404:6800:4009:80c::200e

C:\Users\solan>
```

Frame
Ether
Inte
User
Doma
Command Prompt
Wi-Fi: <live capture in progress>
Packets: 14132 · Displayed: 58 (0.4%)
Profile: Default

d) IP (Internet Protocol):

- Found under **Network Layer**.
- Fields:
- **Source IP / Destination IP**.
- **Version** (IPv4 / IPv6).
- **TTL (Time to Live)**.
- **Protocol** (shows whether it carries TCP, UDP, ICMP, etc.).
- **Header Checksum** (integrity).
- Example usage: Identify where traffic is coming from and going to.



```
No.   Time      Source          Destination     Protocol Length Info
 4605 59.841738 10.70.22.155    142.251.220.78  ICMP      74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 4714)
 4714 60.172651 142.251.220.78  10.70.22.155    ICMP      74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=116 (request in 4605)
 4835 60.847928 10.70.22.155    142.251.220.78  ICMP      74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 4838)
 4838 61.128719 142.251.220.78  10.70.22.155    ICMP      74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=116 (request in 4835)
 4908 61.854245 10.70.22.155    142.251.220.78  ICMP      74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply in 4915)
 4915 61.969547 142.251.220.78  10.70.22.155    ICMP      74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=116 (request in 4908)
 5000 62.868610 10.70.22.155    142.251.220.78  ICMP      74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 5024)
 5024 63.346643 142.251.220.78  10.70.22.155    ICMP      74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=116 (request in 5000)
```

```
Microsoft Windows [Version 10.0.26100.4652]
(c) Microsoft Corporation. All rights reserved.

C:\Users\solan>ping google.com

Pinging google.com [142.251.220.78] with 32 bytes of data:
Reply from 142.251.220.78: bytes=32 time=331ms TTL=116
Reply from 142.251.220.78: bytes=32 time=281ms TTL=116
Reply from 142.251.220.78: bytes=32 time=115ms TTL=116
Reply from 142.251.220.78: bytes=32 time=478ms TTL=116

Ping statistics for 142.251.220.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 115ms, Maximum = 478ms, Average = 301ms

C:\Users\solan>
```

Command Prompt
wireshark_Wi-Fi1V0FA3.pcapng
Packets: 9685 · Displayed: 8 (0.1%) · Dropped: 0 (0.0%)
Profile: Default