Date: 01 / 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.**
2. **Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)**

Date: 01 / 08 / 2025

1. Explain usage of Wireshark tool.

Wireshark is a widely used network protocol analyzer that allows capturing and inspecting data packets traveling across a network. It is mainly used by network administrators, cybersecurity professionals, and students to analyze network traffic in detail.

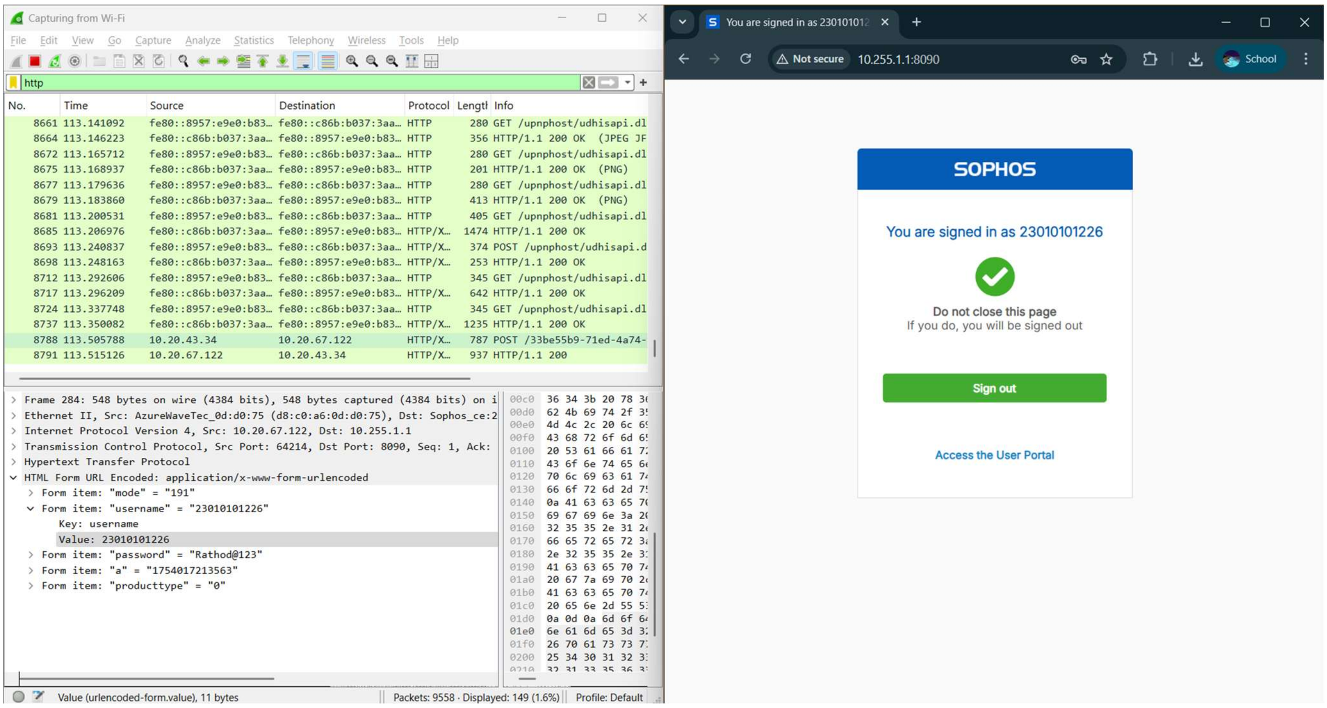
Main Usages:

1. **Capturing Network Traffic**
   - Wireshark captures live packets from network interfaces (e.g., Ethernet, Wi-Fi).
   - Each packet is displayed with details like source IP, destination IP, protocol, size, and time.
2. **Protocol Analysis**
   - It supports hundreds of protocols such as TCP, UDP, HTTP, DNS, etc.
   - Wireshark decodes packet structures, helping to understand how communication takes place.
3. **Troubleshooting Network Issues**
   - Helps in finding network delays, packet loss, retransmissions, and routing errors.
   - Used to identify performance bottlenecks in a network.
4. **Security and Forensics**
   - Detects suspicious activity like port scans, malware communication, or unauthorized access.
   - Assists in forensic analysis after cyberattacks by analyzing saved capture files (.pcap).
5. **Filtering and Searching**
   - Provides strong filters for focusing on specific traffic.
     - Example: ip.addr == 192.168.1.5 (traffic of a particular IP).
     - Example: http (only HTTP traffic).
6. **Learning and Education**
   - Useful for students to study how network protocols (like TCP 3-way handshake) work.
   - Helps visualize encrypted vs. unencrypted communication.
7. **Export and Reporting**
   - Captures can be saved for later analysis in .pcap format.
   - Generates useful reports such as protocol hierarchy and endpoint conversations.

Date: 01 / 08 / 2025

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

- **HTTP**


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

http

```
No.     Time       Source                Destination           Protocol Lengtl Info
   8661 113.141092 fe80::8957:e9e0:b83… fe80::c86b:b037:3aa… HTTP      280 GET /upnphost/udhisapi.dl
   8664 113.146223 fe80::c86b:b037:3aa… fe80::8957:e9e0:b83… HTTP      356 HTTP/1.1 200 OK  (JPEG JF
   8672 113.165712 fe80::8957:e9e0:b83… fe80::c86b:b037:3aa… HTTP      280 GET /upnphost/udhisapi.dl
   8675 113.168937 fe80::c86b:b037:3aa… fe80::8957:e9e0:b83… HTTP      201 HTTP/1.1 200 OK  (PNG)
   8677 113.179636 fe80::8957:e9e0:b83… fe80::c86b:b037:3aa… HTTP      280 GET /upnphost/udhisapi.dl
   8679 113.183860 fe80::c86b:b037:3aa… fe80::8957:e9e0:b83… HTTP      413 HTTP/1.1 200 OK  (PNG)
   8681 113.200531 fe80::8957:e9e0:b83… fe80::c86b:b037:3aa… HTTP      405 GET /upnphost/udhisapi.dl
   8685 113.206976 fe80::c86b:b037:3aa… fe80::8957:e9e0:b83… HTTP/X…  1474 HTTP/1.1 200 OK
   8693 113.240837 fe80::8957:e9e0:b83… fe80::c86b:b037:3aa… HTTP/X…   374 POST /upnphost/udhisapi.d
   8698 113.248163 fe80::c86b:b037:3aa… fe80::8957:e9e0:b83… HTTP/X…   253 HTTP/1.1 200 OK
   8712 113.292606 fe80::8957:e9e0:b83… fe80::c86b:b037:3aa… HTTP      345 GET /upnphost/udhisapi.dl
   8717 113.296209 fe80::c86b:b037:3aa… fe80::8957:e9e0:b83… HTTP/X…   642 HTTP/1.1 200 OK
   8724 113.337748 fe80::8957:e9e0:b83… fe80::c86b:b037:3aa… HTTP      345 GET /upnphost/udhisapi.dl
   8737 113.350082 fe80::c86b:b037:3aa… fe80::8957:e9e0:b83… HTTP/X…  1235 HTTP/1.1 200 OK
   8788 113.505788 10.20.43.34          10.20.67.122         HTTP/X…   787 POST /33be55b9-71ed-4a74-
   8791 113.515126 10.20.67.122         10.20.43.34          HTTP/X…   937 HTTP/1.1 200
```

```
> Frame 284: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits) on i
> Ethernet II, Src: AzureWaveTec_0d:d0:75 (d8:c0:a6:0d:d0:75), Dst: Sophos_ce:2
> Internet Protocol Version 4, Src: 10.20.67.122, Dst: 10.255.1.1
> Transmission Control Protocol, Src Port: 64214, Dst Port: 8090, Seq: 1, Ack:
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "mode" = "191"
  v Form item: "username" = "23010101226"
      Key: username
      Value: 23010101226
  > Form item: "password" = "Rathod@123"
  > Form item: "a" = "1754017213563"
  > Form item: "producttype" = "0"
```

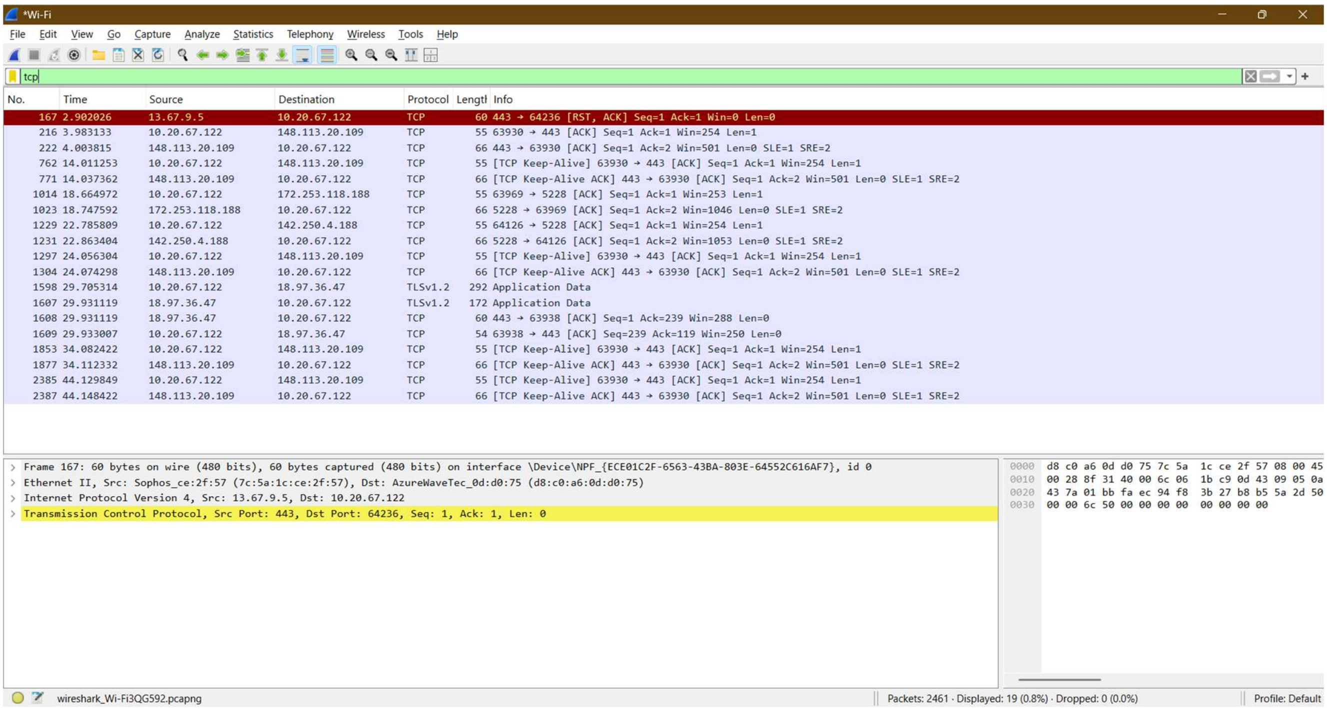
```
00c0  36 34 3b 20 78 3
00d0  62 4b 69 74 2f 3
00e0  4d 4c 2c 20 6c 6
00f0  43 68 72 6f 6d 6
0100  20 53 61 66 61 7
0110  43 6f 6e 74 65 6
0120  70 6c 69 63 61 7
0130  66 6f 72 6d 2d 7
0140  0a 41 63 63 65 7
0150  69 67 69 6e 3a 2
0160  32 35 35 2e 31 2
0170  66 65 72 65 72 3
0180  2e 32 35 35 2e 3
0190  41 63 63 65 70 7
01a0  20 67 7a 69 70 2
01b0  41 63 63 65 70 7
01c0  20 65 6e 2d 55 5
01d0  0a 0d 0a 6d 6f 6
01e0  6e 61 6d 65 3d 3
01f0  26 70 61 73 73 7
0200  25 34 30 31 32 3
```

Value (urlencoded-form.value), 11 bytes | Packets: 9558 · Displayed: 149 (1.6%) | Profile: Default

You are signed in as 23010101226

Do not close this page
If you do, you will be signed out

- **TCP**


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

tcp

```
No.    Time      Source          Destination     Protocol Lengtl Info
   167 2.902026  13.67.9.5       10.20.67.122    TCP        60 443 → 64236 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   216 3.983133  10.20.67.122    148.113.20.109  TCP        55 63930 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
   222 4.003815  148.113.20.109  10.20.67.122    TCP        66 443 → 63930 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
   762 14.011253 10.20.67.122    148.113.20.109  TCP        55 [TCP Keep-Alive] 63930 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
   771 14.037362 148.113.20.109  10.20.67.122    TCP        66 [TCP Keep-Alive ACK] 443 → 63930 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
  1014 18.664972 10.20.67.122    172.253.118.188 TCP        55 63969 → 5228 [ACK] Seq=1 Ack=1 Win=253 Len=1
  1023 18.747592 172.253.118.188 10.20.67.122    TCP        66 5228 → 63969 [ACK] Seq=1 Ack=2 Win=1046 Len=0 SLE=1 SRE=2
  1229 22.785809 10.20.67.122    142.250.4.188   TCP        55 64126 → 5228 [ACK] Seq=1 Ack=1 Win=254 Len=1
  1231 22.863404 142.250.4.188   10.20.67.122    TCP        66 5228 → 64126 [ACK] Seq=1 Ack=2 Win=1053 Len=0 SLE=1 SRE=2
  1297 24.056304 10.20.67.122    148.113.20.109  TCP        55 [TCP Keep-Alive] 63930 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
  1304 24.074298 148.113.20.109  10.20.67.122    TCP        66 [TCP Keep-Alive ACK] 443 → 63930 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
  1598 29.705314 10.20.67.122    18.97.36.47     TLSv1.2   292 Application Data
  1607 29.931119 18.97.36.47     10.20.67.122    TLSv1.2   172 Application Data
  1608 29.931119 18.97.36.47     10.20.67.122    TCP        60 443 → 63938 [ACK] Seq=1 Ack=239 Win=288 Len=0
  1609 29.933007 10.20.67.122    18.97.36.47     TCP        54 63938 → 443 [ACK] Seq=239 Ack=119 Win=250 Len=0
  1853 34.082422 10.20.67.122    148.113.20.109  TCP        55 [TCP Keep-Alive] 63930 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
  1877 34.112332 148.113.20.109  10.20.67.122    TCP        66 [TCP Keep-Alive ACK] 443 → 63930 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
  2385 44.129849 10.20.67.122    148.113.20.109  TCP        55 [TCP Keep-Alive] 63930 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
  2387 44.148422 148.113.20.109  10.20.67.122    TCP        66 [TCP Keep-Alive ACK] 443 → 63930 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
```

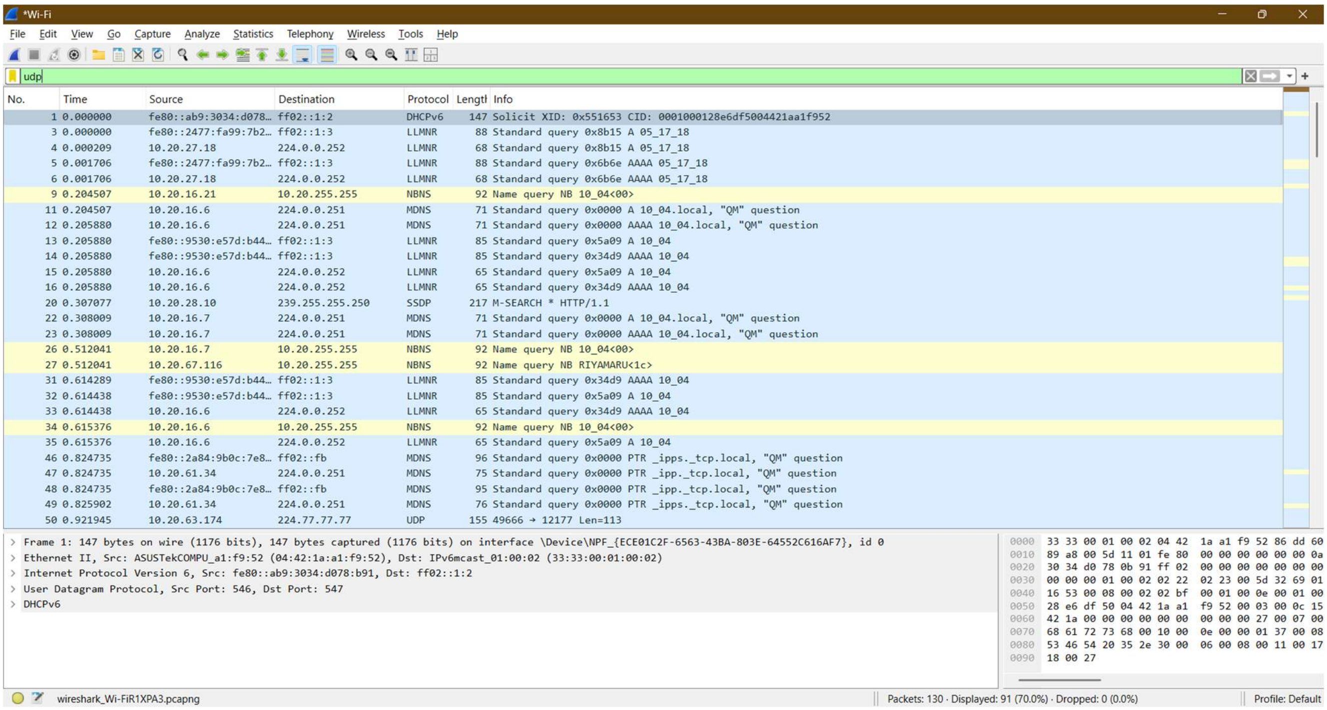
```
> Frame 167: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{ECE01C2F-6563-43BA-803E-64552C616AF7}, id 0
> Ethernet II, Src: Sophos_ce:2f:57 (7c:5a:1c:ce:2f:57), Dst: AzureWaveTec_0d:d0:75 (d8:c0:a6:0d:d0:75)
> Internet Protocol Version 4, Src: 13.67.9.5, Dst: 10.20.67.122
> Transmission Control Protocol, Src Port: 443, Dst Port: 64236, Seq: 1, Ack: 1, Len: 0
```

```
0000  d8 c0 a6 0d d0 75 7c 5a  1c ce 2f 57 08 00 45
0010  00 28 8f 31 40 00 6c 06  1b c9 0d 43 09 05 0a
0020  43 7a 01 bb fa ec 94 f8  3b 27 b8 b5 5a 2d 50
0030  00 00 6c 50 00 00 00 00  00 00 00 00
```

wireshark_Wi-Fi3QG592.pcapng | Packets: 2461 · Displayed: 19 (0.8%) · Dropped: 0 (0.0%) | Profile: Default

Date: 01 / 08 / 2025

- ## UDP


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

udp

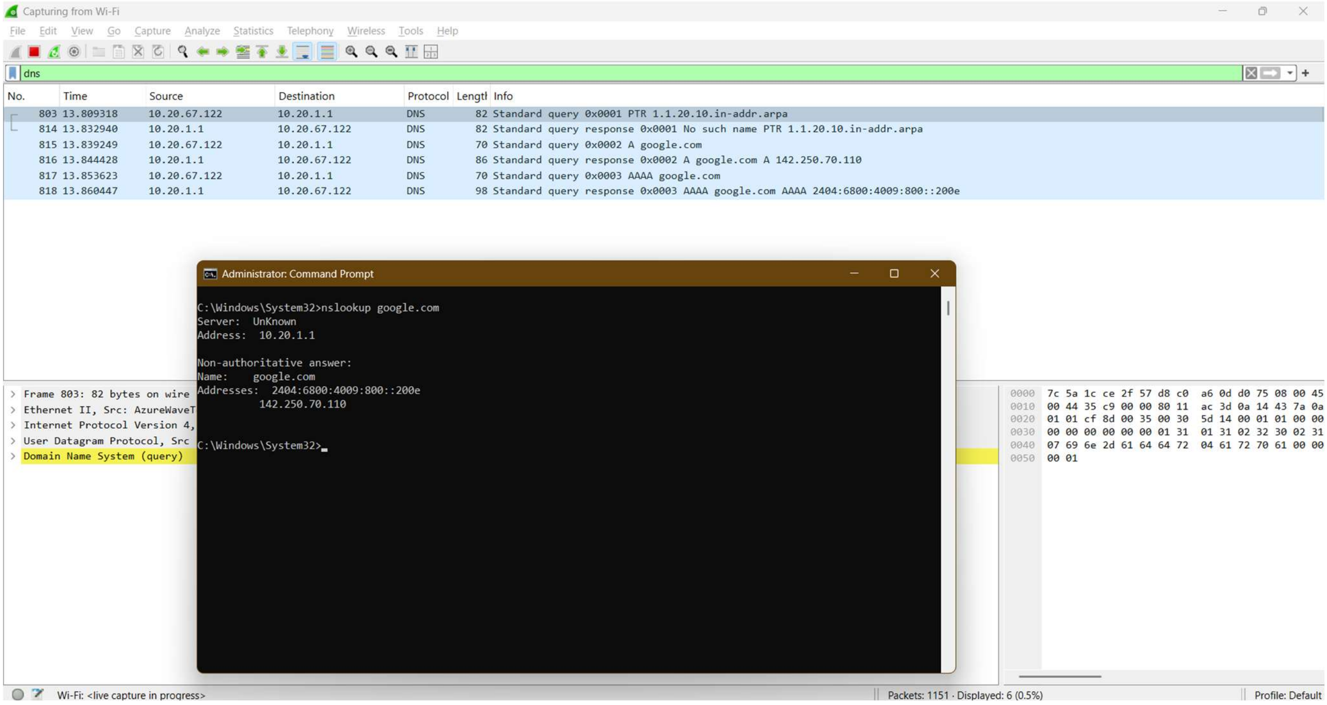
```
No.  Time      Source                Destination      Protocol Lengtl Info
   1 0.000000  fe80::ab9:3034:d078…  ff02::1:2        DHCPv6   147 Solicit XID: 0x551653 CID: 0001000128e6df5004421aa1f952
   3 0.000000  fe80::2477:fa99:7b2…  ff02::1:3        LLMNR     88 Standard query 0x8b15 A 05_17_18
   4 0.000209  10.20.27.18           224.0.0.252      LLMNR     68 Standard query 0x8b15 A 05_17_18
   5 0.001706  fe80::2477:fa99:7b2…  ff02::1:3        LLMNR     88 Standard query 0x6b6e AAAA 05_17_18
   6 0.001706  10.20.27.18           224.0.0.252      LLMNR     68 Standard query 0x6b6e AAAA 05_17_18
   9 0.204507  10.20.16.21           10.20.255.255    NBNS      92 Name query NB 10_04<00>
  11 0.204507  10.20.16.6            224.0.0.251      MDNS      71 Standard query 0x0000 A 10_04.local, "QM" question
  12 0.205880  10.20.16.6            224.0.0.251      MDNS      71 Standard query 0x0000 AAAA 10_04.local, "QM" question
  13 0.205880  fe80::9530:e57d:b44…  ff02::1:3        LLMNR     85 Standard query 0x5a09 A 10_04
  14 0.205880  fe80::9530:e57d:b44…  ff02::1:3        LLMNR     85 Standard query 0x34d9 AAAA 10_04
  15 0.205880  10.20.16.6            224.0.0.252      LLMNR     65 Standard query 0x5a09 A 10_04
  16 0.205880  10.20.16.6            224.0.0.252      LLMNR     65 Standard query 0x34d9 AAAA 10_04
  20 0.307077  10.20.28.10           239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
  22 0.308009  10.20.16.7            224.0.0.251      MDNS      71 Standard query 0x0000 A 10_04.local, "QM" question
  23 0.308009  10.20.16.7            224.0.0.251      MDNS      71 Standard query 0x0000 AAAA 10_04.local, "QM" question
  26 0.512041  10.20.16.7            10.20.255.255    NBNS      92 Name query NB 10_04<00>
  27 0.512041  10.20.67.116          10.20.255.255    NBNS      92 Name query NB RIYAMARU<1c>
  31 0.614289  fe80::9530:e57d:b44…  ff02::1:3        LLMNR     85 Standard query 0x34d9 AAAA 10_04
  32 0.614438  fe80::9530:e57d:b44…  ff02::1:3        LLMNR     85 Standard query 0x5a09 A 10_04
  33 0.614438  10.20.16.6            224.0.0.252      LLMNR     65 Standard query 0x34d9 AAAA 10_04
  34 0.615376  10.20.16.6            10.20.255.255    NBNS      92 Name query NB 10_04<00>
  35 0.615376  10.20.16.6            224.0.0.252      LLMNR     65 Standard query 0x5a09 A 10_04
  46 0.824735  fe80::2a84:9b0c:7e8…  ff02::fb         MDNS      96 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question
  47 0.824735  10.20.61.34           224.0.0.251      MDNS      75 Standard query 0x0000 PTR _ipp._tcp.local, "QM" question
  48 0.824735  fe80::2a84:9b0c:7e8…  ff02::fb         MDNS      95 Standard query 0x0000 PTR _ipp._tcp.local, "QM" question
  49 0.825902  10.20.61.34           224.0.0.251      MDNS      76 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question
  50 0.921945  10.20.63.174          224.77.77.77     UDP      155 49666 → 12177 Len=113
```

```
> Frame 1: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface \Device\NPF_{ECE01C2F-6563-43BA-803E-64552C616AF7}, id 0
> Ethernet II, Src: ASUSTekCOMPU_a1:f9:52 (04:42:1a:a1:f9:52), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
> Internet Protocol Version 6, Src: fe80::ab9:3034:d078:b91, Dst: ff02::1:2
> User Datagram Protocol, Src Port: 546, Dst Port: 547
> DHCPv6
```

```
0000  33 33 00 01 00 02 04 42  1a a1 f9 52 86 dd 60
0010  89 a8 00 5d 11 01 fe 80  00 00 00 00 00 00 0a
0020  30 34 d0 78 0b 91 ff 02  00 00 00 00 00 00 00
0030  00 00 00 01 00 02 02 22  02 23 00 5d 32 69 01
0040  16 53 00 08 00 02 02 bf  00 01 00 0e 00 01 00
0050  28 e6 df 50 04 42 1a a1  f9 52 00 03 00 0c 15
0060  42 1a 00 00 00 00 00 00  00 00 00 27 00 07 00
0070  68 61 72 73 68 00 10 00  0e 00 00 01 37 00 08
0080  53 46 54 20 35 2e 30 00  06 00 08 00 11 00 17
0090  18 00 27
```

wireshark_Wi-FiR1XPA3.pcapng | Packets: 130 · Displayed: 91 (70.0%) · Dropped: 0 (0.0%) | Profile: Default

- ## DNS


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Administrator: Command Prompt

dns

```
No.  Time       Source        Destination   Protocol Lengtl Info
 803 13.809318  10.20.67.122  10.20.1.1     DNS      82 Standard query 0x0001 PTR 1.1.20.10.in-addr.arpa
 814 13.832940  10.20.1.1     10.20.67.122  DNS      82 Standard query response 0x0001 No such name PTR 1.1.20.10.in-addr.arpa
 815 13.839249  10.20.67.122  10.20.1.1     DNS      70 Standard query 0x0002 A google.com
 816 13.844428  10.20.1.1     10.20.67.122  DNS      86 Standard query response 0x0002 A google.com A 142.250.70.110
 817 13.853623  10.20.67.122  10.20.1.1     DNS      70 Standard query 0x0003 AAAA google.com
 818 13.860447  10.20.1.1     10.20.67.122  DNS      98 Standard query response 0x0003 AAAA google.com AAAA 2404:6800:4009:800::200e
```

```
C:\Windows\System32>nslookup google.com
Server:  UnKnown
Address:  10.20.1.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:800::200e
          142.250.70.110


C:\Windows\System32>_
```

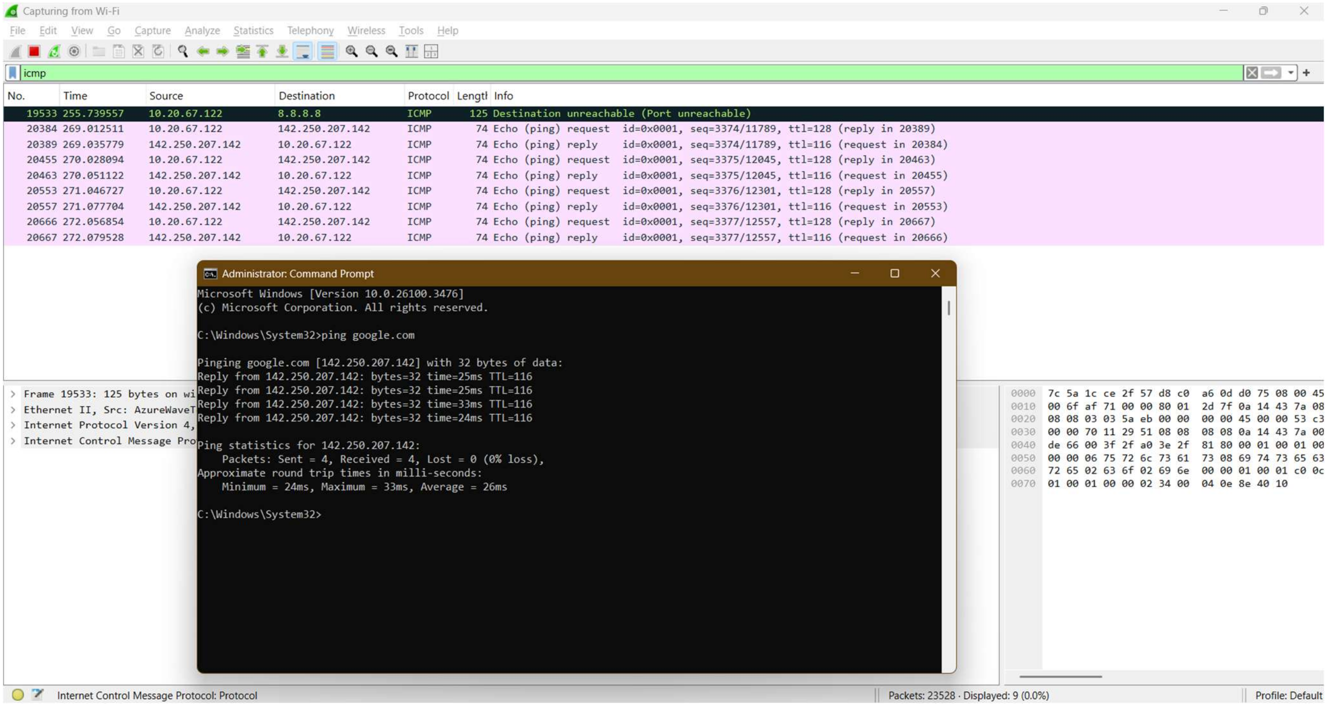
```
> Frame 803: 82 bytes on wire
> Ethernet II, Src: AzureWaveT
> Internet Protocol Version 4,
> User Datagram Protocol, Src
> Domain Name System (query)
```

```
0000  7c 5a 1c ce 2f 57 d8 c0  a6 0d d0 75 08 00 45
0010  00 44 35 c9 00 00 80 11  ac 3d 0a 14 43 7a 0a
0020  01 01 cf 8d 00 35 00 30  5d 14 00 01 01 00 00
0030  00 00 00 00 00 00 01 31  01 31 02 32 30 02 31
0040  07 69 6e 2d 61 64 64 72  04 61 72 70 61 00 00
0050  00 01
```

Wi-Fi: <live capture in progress> | Packets: 1151 · Displayed: 6 (0.5%) | Profile: Default

Date: 01 / 08 / 2025

- ## ICMP


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.   Time        Source          Destination     Protocol Lengtl Info
19533 255.739557  10.20.67.122    8.8.8.8         ICMP     125 Destination unreachable (Port unreachable)
20384 269.012511  10.20.67.122    142.250.207.142 ICMP      74 Echo (ping) request  id=0x0001, seq=3374/11789, ttl=128 (reply in 20389)
20389 269.035779  142.250.207.142 10.20.67.122    ICMP      74 Echo (ping) reply    id=0x0001, seq=3374/11789, ttl=116 (request in 20384)
20455 270.028094  10.20.67.122    142.250.207.142 ICMP      74 Echo (ping) request  id=0x0001, seq=3375/12045, ttl=128 (reply in 20463)
20463 270.051122  142.250.207.142 10.20.67.122    ICMP      74 Echo (ping) reply    id=0x0001, seq=3375/12045, ttl=116 (request in 20455)
20553 271.046727  10.20.67.122    142.250.207.142 ICMP      74 Echo (ping) request  id=0x0001, seq=3376/12301, ttl=128 (reply in 20557)
20557 271.077704  142.250.207.142 10.20.67.122    ICMP      74 Echo (ping) reply    id=0x0001, seq=3376/12301, ttl=116 (request in 20553)
20666 272.056854  10.20.67.122    142.250.207.142 ICMP      74 Echo (ping) request  id=0x0001, seq=3377/12557, ttl=128 (reply in 20667)
20667 272.079528  142.250.207.142 10.20.67.122    ICMP      74 Echo (ping) reply    id=0x0001, seq=3377/12557, ttl=116 (request in 20666)
```

```
> Frame 19533: 125 bytes on wi
> Ethernet II, Src: AzureWaveT
> Internet Protocol Version 4,
> Internet Control Message Pro
```

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.26100.3476]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ping google.com

Pinging google.com [142.250.207.142] with 32 bytes of data:
Reply from 142.250.207.142: bytes=32 time=25ms TTL=116
Reply from 142.250.207.142: bytes=32 time=25ms TTL=116
Reply from 142.250.207.142: bytes=32 time=33ms TTL=116
Reply from 142.250.207.142: bytes=32 time=24ms TTL=116

Ping statistics for 142.250.207.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 33ms, Average = 26ms

C:\Windows\System32>
```

```
0000  7c 5a 1c ce 2f 57 d8 c0  a6 0d d0 75 08 00 45
0010  00 6f af 71 00 00 80 01  2d 7f 0a 14 43 7a 08
0020  08 08 03 03 5a eb 00 00  00 00 45 00 00 53 c3
0030  00 00 70 11 29 51 08 08  08 08 0a 14 43 7a 00
0040  de 66 00 3f 2f a0 3e 2f  81 80 00 01 00 01 00
0050  00 00 06 75 72 6c 73 61  73 08 69 74 73 65 63
0060  72 65 02 63 6f 02 69 6e  00 00 01 00 01 c0 0c
0070  01 00 01 00 00 02 34 00  04 0e 8e 40 10
```

Internet Control Message Protocol: Protocol

Packets: 23528 · Displayed: 9 (0.0%)

Profile: Default