Date: 24/02/2025

Lab Practical 11:

Wireshark is a widely used, opensource network analyzer that can capture and display real-time details of network traffic. It is particularly useful for troubleshooting network issues, analyzing network protocols and ensuring network security.

Key features of Wireshark

1. It has a great GUI as well as a conventional CLI(T Shark).
2. It offers network monitoring on almost all types of network standards (ethernet, wlan, Bluetooth etc)
3. It is open-source with a large community of backers and developers.
4. All the necessary components for monitoring, analyzing and documenting the network traffic are present. It is free to use.

Installing and Setting Up Wireshark:

For Linux:

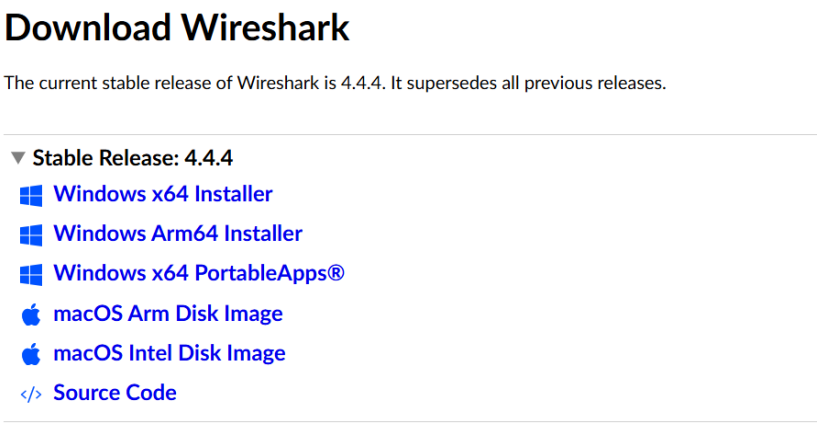
Wireshark is pre-installed on Kali Linux, but if you need to install it on other Linux distributions, you can use the following command:

```
sudo apt-get update
sudo apt-get install wireshark
sudo wireshark
```

For Windows & mac:

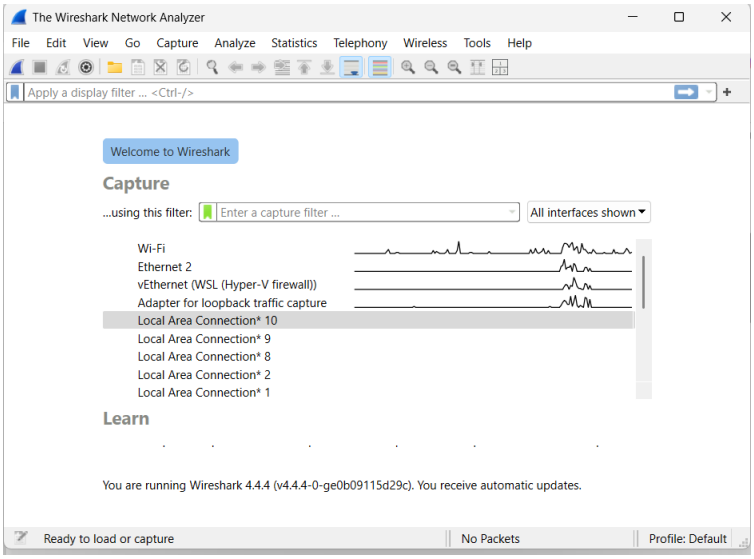
Download the installer from following site install it.

https://www.wireshark.org/download.html

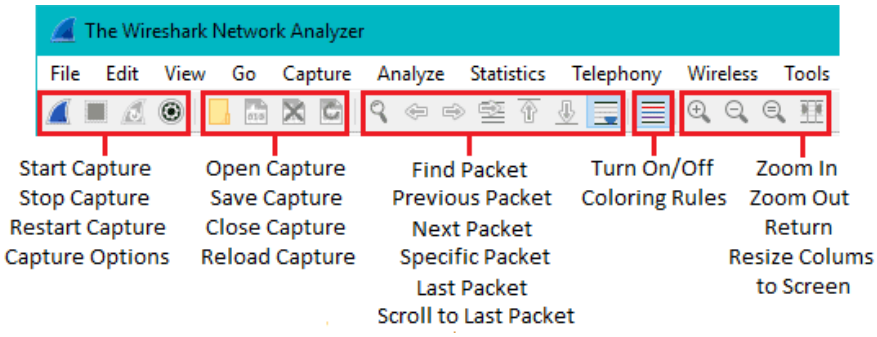


Date: 24/02/2025

Home Screen:

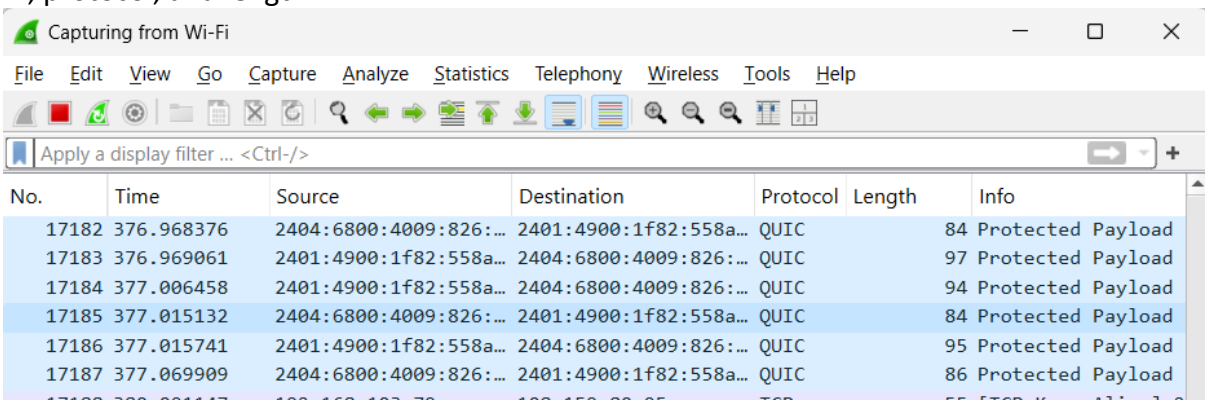


Basic Controls:



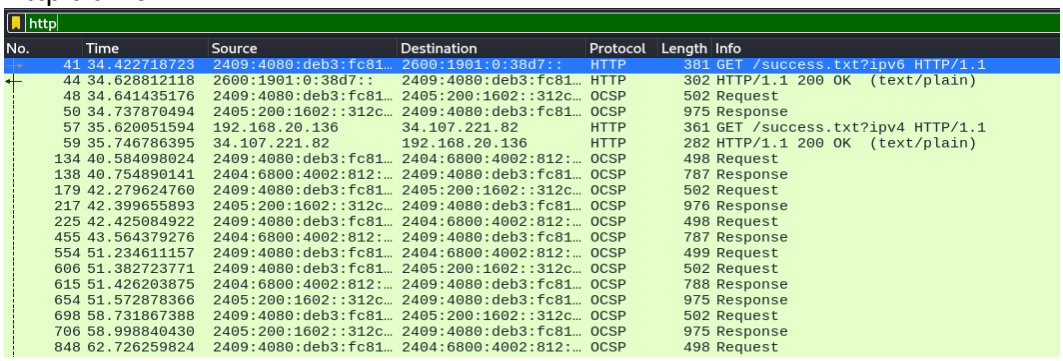
Examine the Packet List:

1. **Packet Details:** Each packet in the capture is listed with a timestamp, source IP, destination IP, protocol, and length.

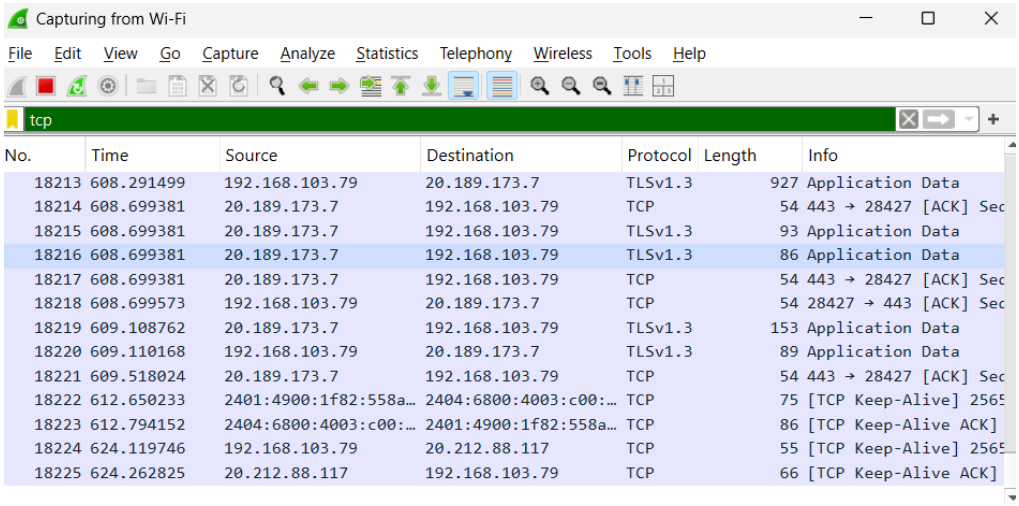


Date: 24/02/2025

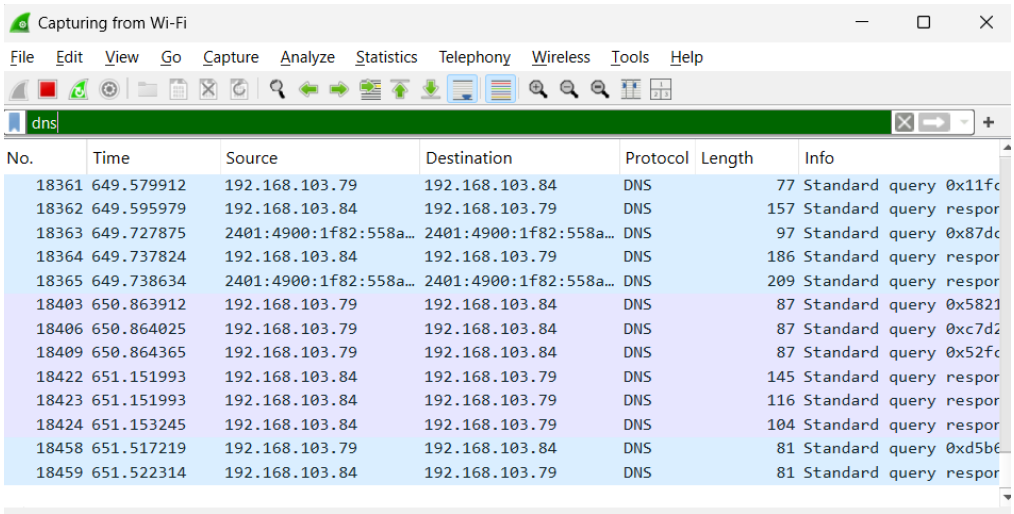
2. **Filtering Packets:** Use the filter bar to isolate specific protocols or traffic.
   - Http traffic



   - TCP traffic

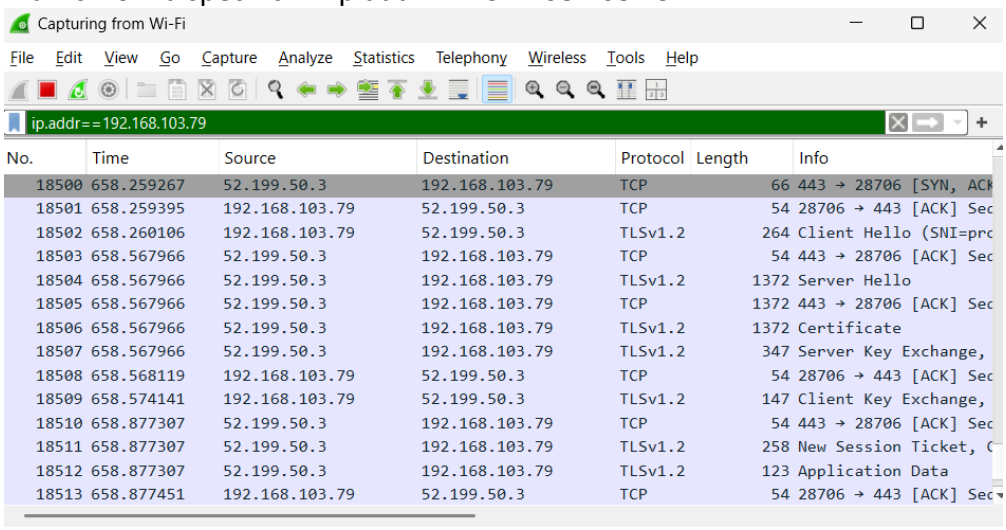


   - DNS traffic

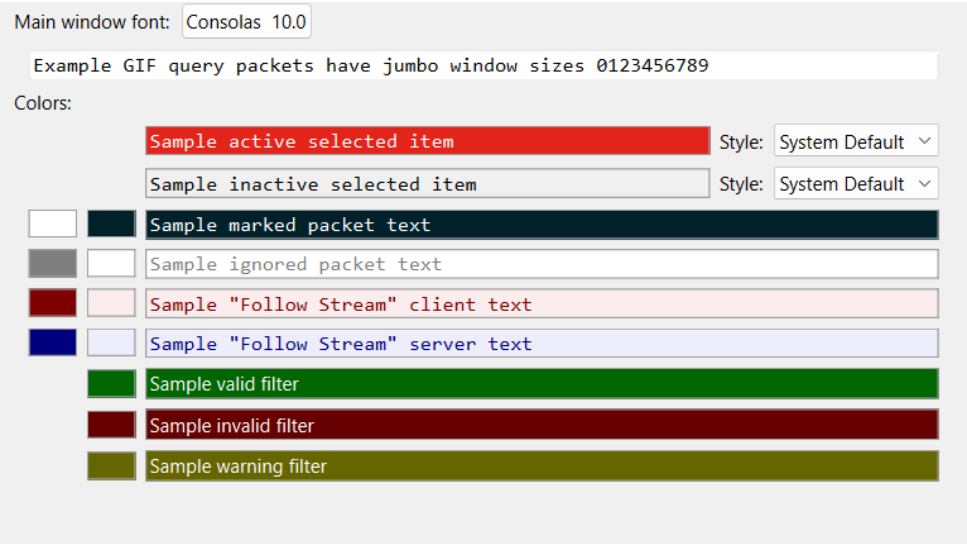


Date: 24/02/2025

- Traffic from a specific IP: ip.addr == 192.168.103.79



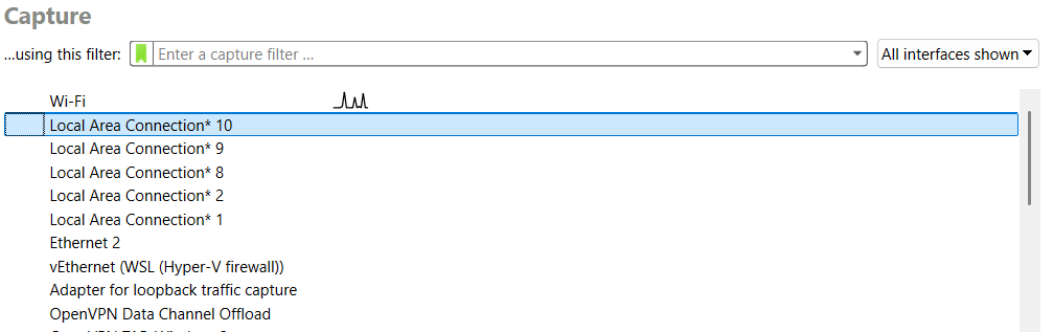
3. **Color Coding:** Wireshark uses color coding to visually differentiate between different types of packets.



Date: 24/02/2025

Applying Filters and Inspecting Packets

- **Inspect Packet Details**
  1. In Wireshark, you will see a list of network interfaces (e.g., eth0, wlan0). Choose the interface you want to monitor (typically eth0 for Ethernet or wlan0 for Wi-Fi).
  2. Click on the interface name to begin packet capturing.

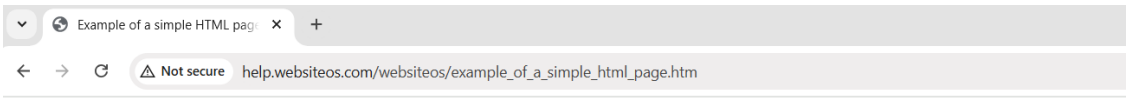


Analyzing Specific Network Traffic Types

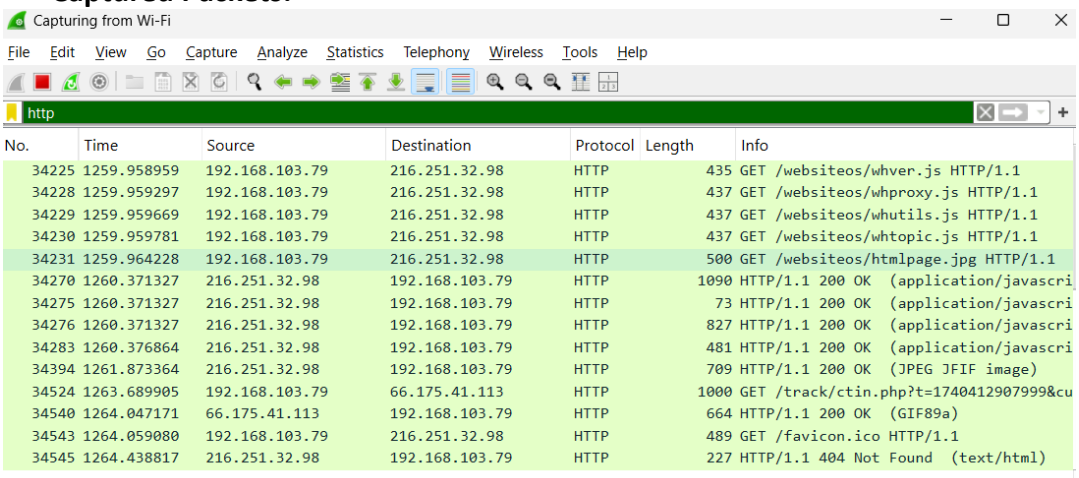
Use a browser to visit a website (e.g., http://example.com).
In Wireshark, apply the filter http to see the HTTP requests and responses.
Look for HTTP GET or POST requests to examine the URLs, headers, and any transmitted data.

Capture and Analyze HTTP Traffic

- **Searched on browser:**



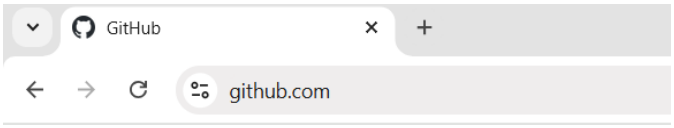
- **Captured Packets:**

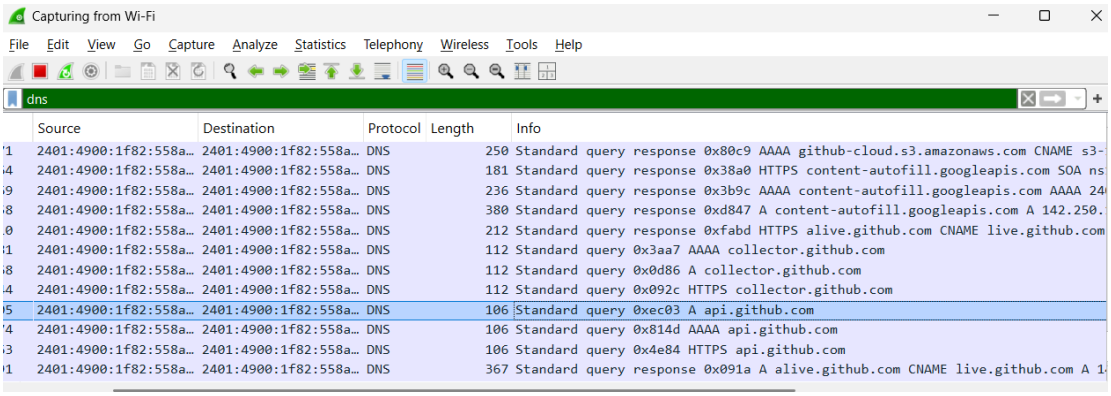


Date: 24/02/2025

Capture and Analyze DNS Traffic

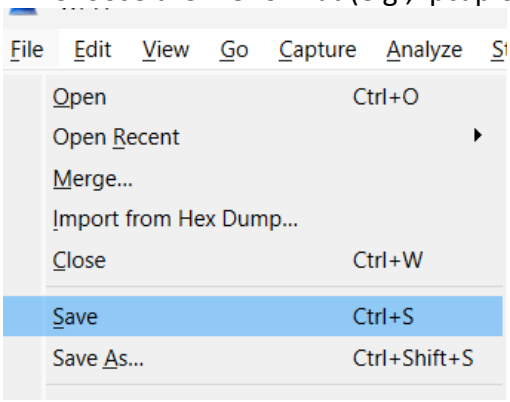
- **Searched on browser:**





Saving and Exporting Capture Data

1. **Save the Capture File**
   - To save the captured packets for later analysis, click File > Save As.
   - Choose the file format (e.g., .pcap or .pcapng) and save the file.



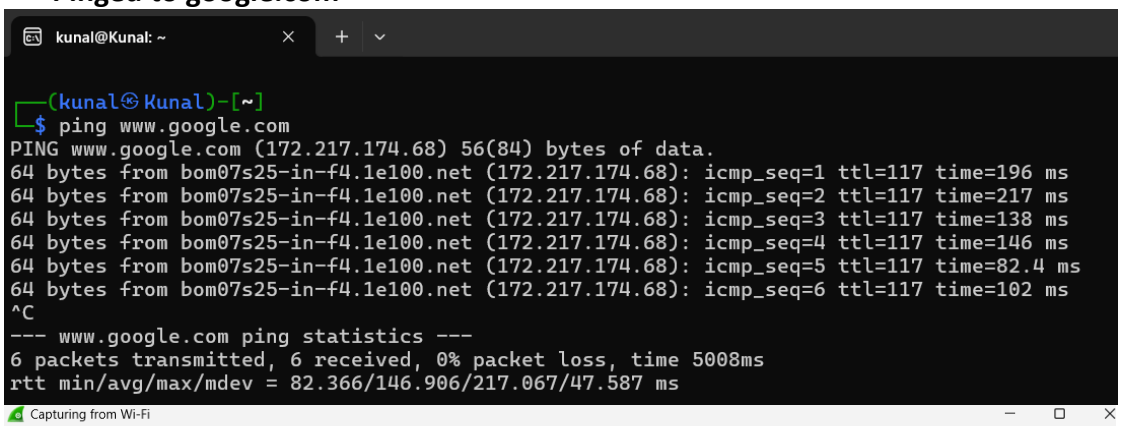
2. **Export Specific Packet Data**
   - Apply a filter (e.g., http).
   - Click File > Export Packet Dissections > As Plain Text to save the filtered data in a readable format.

Date: 24/02/2025

Basic Network Troubleshooting

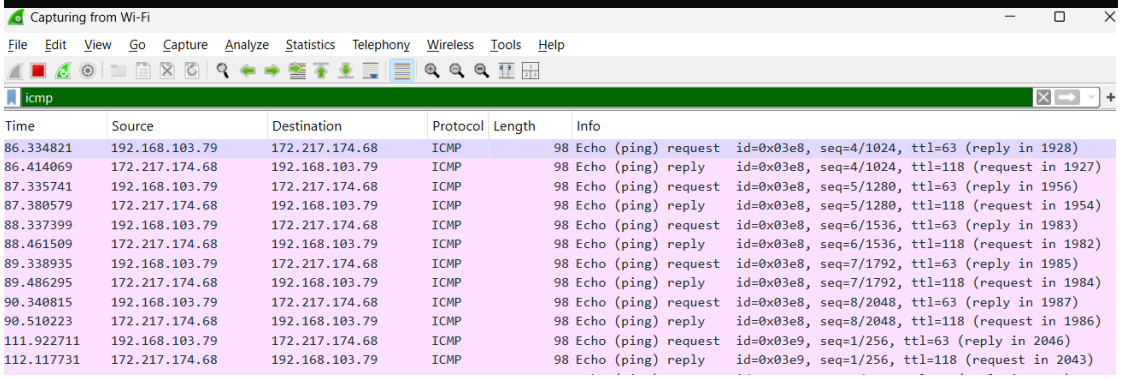
1. Analyze Network Latency and Packet Loss

- **Pinged to google.com**



```
kunal@Kunal: ~

┌──(kunal㉿Kunal)-[~]
└─$ ping www.google.com
PING www.google.com (172.217.174.68) 56(84) bytes of data.
64 bytes from bom07s25-in-f4.1e100.net (172.217.174.68): icmp_seq=1 ttl=117 time=196 ms
64 bytes from bom07s25-in-f4.1e100.net (172.217.174.68): icmp_seq=2 ttl=117 time=217 ms
64 bytes from bom07s25-in-f4.1e100.net (172.217.174.68): icmp_seq=3 ttl=117 time=138 ms
64 bytes from bom07s25-in-f4.1e100.net (172.217.174.68): icmp_seq=4 ttl=117 time=146 ms
64 bytes from bom07s25-in-f4.1e100.net (172.217.174.68): icmp_seq=5 ttl=117 time=82.4 ms
64 bytes from bom07s25-in-f4.1e100.net (172.217.174.68): icmp_seq=6 ttl=117 time=102 ms
^C
--- www.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 82.366/146.906/217.067/47.587 ms
```



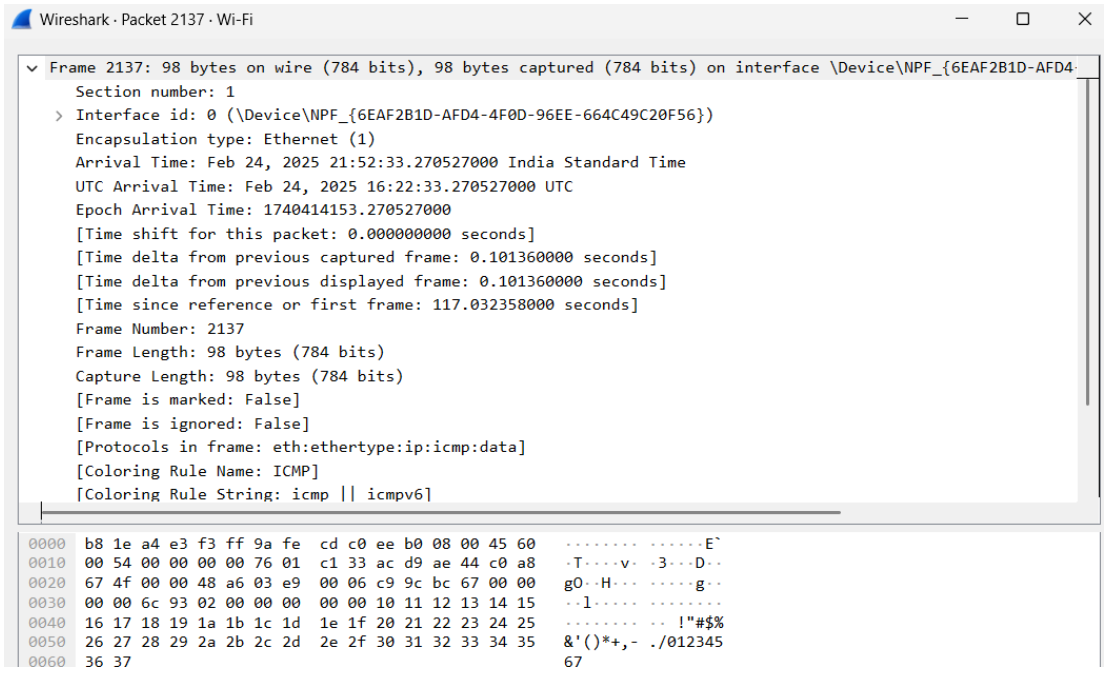
Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

Time	Source	Destination	Protocol	Length	Info
86.334821	192.168.103.79	172.217.174.68	ICMP	98	Echo (ping) request id=0x03e8, seq=4/1024, ttl=63 (reply in 1928)
86.414069	172.217.174.68	192.168.103.79	ICMP	98	Echo (ping) reply id=0x03e8, seq=4/1024, ttl=118 (request in 1927)
87.335741	192.168.103.79	172.217.174.68	ICMP	98	Echo (ping) request id=0x03e8, seq=5/1280, ttl=63 (reply in 1956)
87.380579	172.217.174.68	192.168.103.79	ICMP	98	Echo (ping) reply id=0x03e8, seq=5/1280, ttl=118 (request in 1954)
88.337399	192.168.103.79	172.217.174.68	ICMP	98	Echo (ping) request id=0x03e8, seq=6/1536, ttl=63 (reply in 1983)
88.461509	172.217.174.68	192.168.103.79	ICMP	98	Echo (ping) reply id=0x03e8, seq=6/1536, ttl=118 (request in 1982)
89.338935	192.168.103.79	172.217.174.68	ICMP	98	Echo (ping) request id=0x03e8, seq=7/1792, ttl=63 (reply in 1985)
89.486295	172.217.174.68	192.168.103.79	ICMP	98	Echo (ping) reply id=0x03e8, seq=7/1792, ttl=118 (request in 1984)
90.340815	192.168.103.79	172.217.174.68	ICMP	98	Echo (ping) request id=0x03e8, seq=8/2048, ttl=63 (reply in 1987)
90.510223	172.217.174.68	192.168.103.79	ICMP	98	Echo (ping) reply id=0x03e8, seq=8/2048, ttl=118 (request in 1986)
111.922711	192.168.103.79	172.217.174.68	ICMP	98	Echo (ping) request id=0x03e9, seq=1/256, ttl=63 (reply in 2046)
112.117731	172.217.174.68	192.168.103.79	ICMP	98	Echo (ping) reply id=0x03e9, seq=1/256, ttl=118 (request in 2043)

Packet Insite's:



Wireshark · Packet 2137 · Wi-Fi

```
Frame 2137: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{6EAF2B1D-AFD4-
    Section number: 1
  > Interface id: 0 (\Device\NPF_{6EAF2B1D-AFD4-4F0D-96EE-664C49C20F56})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 24, 2025 21:52:33.270527000 India Standard Time
    UTC Arrival Time: Feb 24, 2025 16:22:33.270527000 UTC
    Epoch Arrival Time: 1740414153.270527000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.101360000 seconds]
    [Time delta from previous displayed frame: 0.101360000 seconds]
    [Time since reference or first frame: 117.032358000 seconds]
    Frame Number: 2137
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
```

```
0000  b8 1e a4 e3 f3 ff 9a fe  cd c0 ee b0 08 00 45 60   ........ ......E`
0010  00 54 00 00 00 00 76 01  c1 33 ac d9 ae 44 c0 a8   ·T····v· ·3···D··
0020  67 4f 00 00 48 a6 03 e9  00 06 c9 9c bc 67 00 00   gO··H··· ·····g··
0030  00 00 6c 93 02 00 00 00  00 00 10 11 12 13 14 15   ··l····· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

Date: 24/02/2025

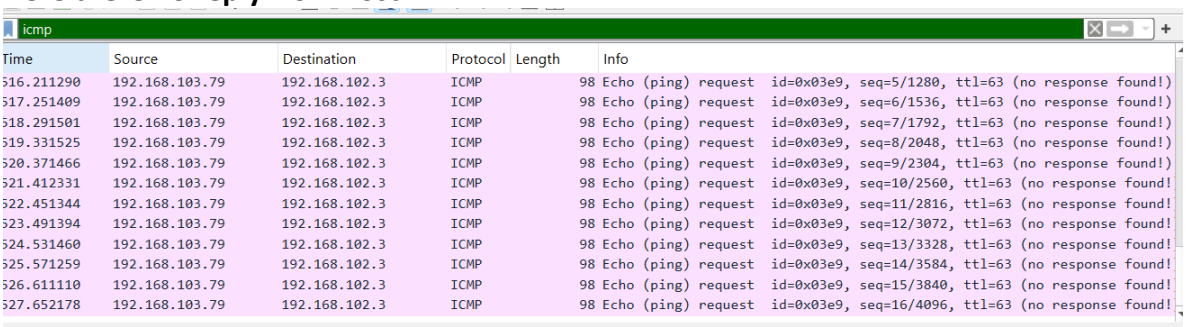
2. Investigate Packet Loss

Look for duplicate packets or timeouts in the capture. Packet loss can be detected if there are many retransmitted TCP packets or if ICMP Echo replies are missing.

- Here pinged non existing ip:

```
┌──(kunal㉿Kunal)-[~]
└─$ ping 192.168.102.3
PING 192.168.102.3 (192.168.102.3) 56(84) bytes of data.
^C
--- 192.168.102.3 ping statistics ---
16 packets transmitted, 0 received, 100% packet loss, time 15637ms
```

- **Here there no reply from host**



icmp

Time	Source	Destination	Protocol	Length	Info
516.211290	192.168.103.79	192.168.102.3	ICMP	98	Echo (ping) request id=0x03e9, seq=5/1280, ttl=63 (no response found!)
517.251409	192.168.103.79	192.168.102.3	ICMP	98	Echo (ping) request id=0x03e9, seq=6/1536, ttl=63 (no response found!)
518.291501	192.168.103.79	192.168.102.3	ICMP	98	Echo (ping) request id=0x03e9, seq=7/1792, ttl=63 (no response found!)
519.331525	192.168.103.79	192.168.102.3	ICMP	98	Echo (ping) request id=0x03e9, seq=8/2048, ttl=63 (no response found!)
520.371466	192.168.103.79	192.168.102.3	ICMP	98	Echo (ping) request id=0x03e9, seq=9/2304, ttl=63 (no response found!)
521.412331	192.168.103.79	192.168.102.3	ICMP	98	Echo (ping) request id=0x03e9, seq=10/2560, ttl=63 (no response found!
522.451344	192.168.103.79	192.168.102.3	ICMP	98	Echo (ping) request id=0x03e9, seq=11/2816, ttl=63 (no response found!
523.491394	192.168.103.79	192.168.102.3	ICMP	98	Echo (ping) request id=0x03e9, seq=12/3072, ttl=63 (no response found!
524.531460	192.168.103.79	192.168.102.3	ICMP	98	Echo (ping) request id=0x03e9, seq=13/3328, ttl=63 (no response found!
525.571259	192.168.103.79	192.168.102.3	ICMP	98	Echo (ping) request id=0x03e9, seq=14/3584, ttl=63 (no response found!
526.611110	192.168.103.79	192.168.102.3	ICMP	98	Echo (ping) request id=0x03e9, seq=15/3840, ttl=63 (no response found!
527.652178	192.168.103.79	192.168.102.3	ICMP	98	Echo (ping) request id=0x03e9, seq=16/4096, ttl=63 (no response found!

Common Wireshark Features and Usage Tips

Step 1: Use the "Follow

- TCP Streams: Right-click on any TCP packet and select Follow > TCP Stream. This allows you to view the entire conversation (e.g., an HTTP request and response).
- HTTP Streams: Similarly, follow HTTP traffic by selecting Follow > HTTP Stream.

Step 2: Packet Statistics

- Go to Statistics > Summary to view basic network traffic statistics, such as the number of packets captured, protocol distribution, and data rates.
- Statistics > Conversations: View detailed information about network conversations (IP pairs, protocols used, and packet counts).