

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.

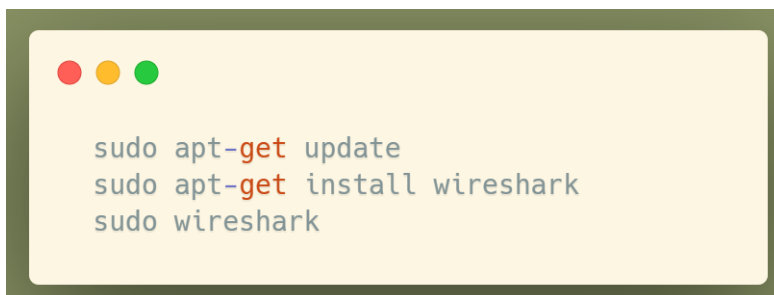
#### Key features of Wireshark

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>

#### Download Wireshark

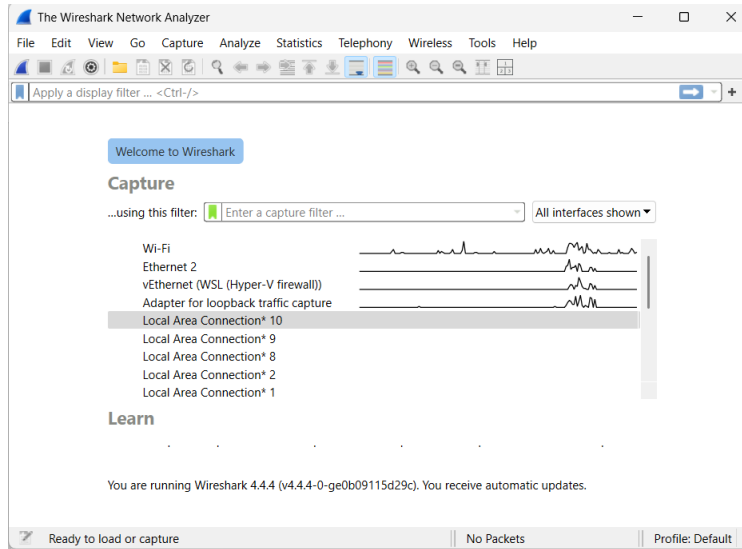
The current stable release of Wireshark is 4.4.4. It supersedes all previous releases.

##### ▼ Stable Release: 4.4.4

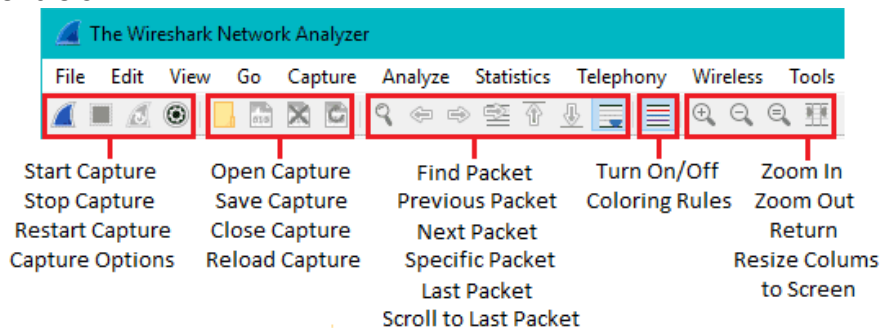
-  [Windows x64 Installer](#)
-  [Windows Arm64 Installer](#)
-  [Windows x64 PortableApps®](#)
-  [macOS Arm Disk Image](#)
-  [macOS Intel Disk Image](#)
-  [Source Code](#)

Date: 24/02/2025

### Home Screen:

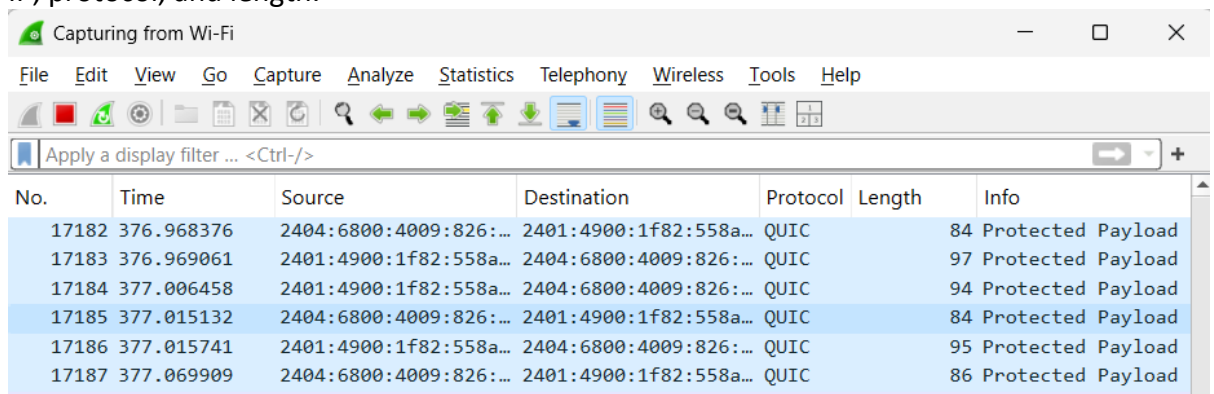


### Basic Controls:



### Examine the Packet List:

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

The image shows the Wireshark Network Analyzer interface with the 'Packet List' pane selected. It displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are QUIC packets with protected payloads.

No.	Time	Source	Destination	Protocol	Length	Info
17182	376.968376	2404:6800:4009:826:...	2401:4900:1f82:558a...	QUIC	84	Protected Payload
17183	376.969061	2401:4900:1f82:558a...	2404:6800:4009:826:...	QUIC	97	Protected Payload
17184	377.006458	2401:4900:1f82:558a...	2404:6800:4009:826:...	QUIC	94	Protected Payload
17185	377.015132	2404:6800:4009:826:...	2401:4900:1f82:558a...	QUIC	84	Protected Payload
17186	377.015741	2401:4900:1f82:558a...	2404:6800:4009:826:...	QUIC	95	Protected Payload
17187	377.069909	2404:6800:4009:826:...	2401:4900:1f82:558a...	QUIC	86	Protected Payload

Date: 24/02/2025

## 2. Filtering Packets: Use the filter bar to isolate specific protocols or traffic.

- Http traffic

No.	Time	Source	Destination	Protocol	Length	Info
41	34.422718723	2409:4080:deb3:fc81...	2600:1901:0:38d7::	HTTP	361	GET /success.txt?ip=6 HTTP/1.1
44	34.628812118	2600:1901:0:38d7::	2409:4080:deb3:fc81...	HTTP	302	HTTP/1.1 200 OK (text/plain)
48	34.641435176	2409:4080:deb3:fc81...	2405:200:1602::312c...	OCSP	502	Request
50	34.737870494	2405:200:1602::312c...	2409:4080:deb3:fc81...	OCSP	975	Response
57	35.620051594	192.168.20.136	34.107.221.82	HTTP	361	GET /success.txt?ip=4 HTTP/1.1
59	35.746786395	34.107.221.82	192.168.20.136	HTTP	282	HTTP/1.1 200 OK (text/plain)
134	40.584098024	2409:4080:deb3:fc81...	2404:6800:4002:812::	OCSP	498	Request
138	40.754890141	2404:6800:4002:812::	2409:4080:deb3:fc81...	OCSP	787	Response
179	42.279624760	2409:4080:deb3:fc81...	2405:200:1602::312c...	OCSP	502	Request
217	42.399655893	2405:200:1602::312c...	2409:4080:deb3:fc81...	OCSP	976	Response
225	42.425084922	2409:4080:deb3:fc81...	2404:6800:4002:812::	OCSP	498	Request
455	43.564379276	2404:6800:4002:812::	2409:4080:deb3:fc81...	OCSP	787	Response
554	51.234611157	2409:4080:deb3:fc81...	2404:6800:4002:812::	OCSP	499	Request
606	51.382723771	2409:4080:deb3:fc81...	2405:200:1602::312c...	OCSP	502	Request
615	51.426203875	2404:6800:4002:812::	2409:4080:deb3:fc81...	OCSP	788	Response
654	51.572878366	2405:200:1602::312c...	2409:4080:deb3:fc81...	OCSP	975	Response
698	58.731867388	2409:4080:deb3:fc81...	2405:200:1602::312c...	OCSP	502	Request
706	58.998840430	2405:200:1602::312c...	2409:4080:deb3:fc81...	OCSP	975	Response
848	62.726259824	2409:4080:deb3:fc81...	2404:6800:4002:812::	OCSP	498	Request

- TCP traffic

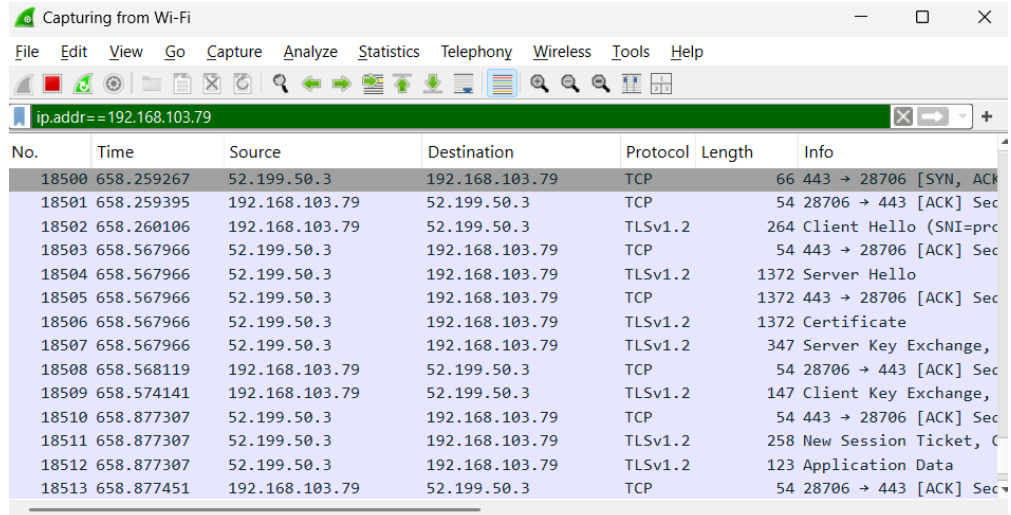
No.	Time	Source	Destination	Protocol	Length	Info
18213	608.291499	192.168.103.79	20.189.173.7	TLSv1.3	927	Application Data
18214	608.699381	20.189.173.7	192.168.103.79	TCP	54	443 → 28427 [ACK] Seq
18215	608.699381	20.189.173.7	192.168.103.79	TLSv1.3	93	Application Data
18216	608.699381	20.189.173.7	192.168.103.79	TLSv1.3	86	Application Data
18217	608.699381	20.189.173.7	192.168.103.79	TCP	54	443 → 28427 [ACK] Seq
18218	608.699573	192.168.103.79	20.189.173.7	TCP	54	28427 → 443 [ACK] Seq
18219	609.108762	20.189.173.7	192.168.103.79	TLSv1.3	153	Application Data
18220	609.110168	192.168.103.79	20.189.173.7	TLSv1.3	89	Application Data
18221	609.518024	20.189.173.7	192.168.103.79	TCP	54	443 → 28427 [ACK] Seq
18222	612.650233	2401:4900:1f82:558a...	2404:6800:4003:c00::	TCP	75	[TCP Keep-Alive] 2565
18223	612.794152	2404:6800:4003:c00::	2401:4900:1f82:558a...	TCP	86	[TCP Keep-Alive ACK]
18224	624.119746	192.168.103.79	20.212.88.117	TCP	55	[TCP Keep-Alive] 2565
18225	624.262825	20.212.88.117	192.168.103.79	TCP	66	[TCP Keep-Alive ACK]

- DNS traffic

No.	Time	Source	Destination	Protocol	Length	Info
18361	649.579912	192.168.103.79	192.168.103.84	DNS	77	Standard query 0x11fc
18362	649.595979	192.168.103.84	192.168.103.79	DNS	157	Standard query respon
18363	649.727875	2401:4900:1f82:558a...	2401:4900:1f82:558a...	DNS	97	Standard query 0x87dc
18364	649.737824	192.168.103.84	192.168.103.79	DNS	186	Standard query respon
18365	649.738634	2401:4900:1f82:558a...	2401:4900:1f82:558a...	DNS	209	Standard query respon
18403	650.863912	192.168.103.79	192.168.103.84	DNS	87	Standard query 0x5821
18406	650.864025	192.168.103.79	192.168.103.84	DNS	87	Standard query 0xc7d2
18409	650.864365	192.168.103.79	192.168.103.84	DNS	87	Standard query 0x52fc
18422	651.151993	192.168.103.84	192.168.103.79	DNS	145	Standard query respon
18423	651.151993	192.168.103.84	192.168.103.79	DNS	116	Standard query respon
18424	651.153245	192.168.103.84	192.168.103.79	DNS	104	Standard query respon
18458	651.517219	192.168.103.79	192.168.103.84	DNS	81	Standard query 0xd5b6
18459	651.522314	192.168.103.84	192.168.103.79	DNS	81	Standard query respon

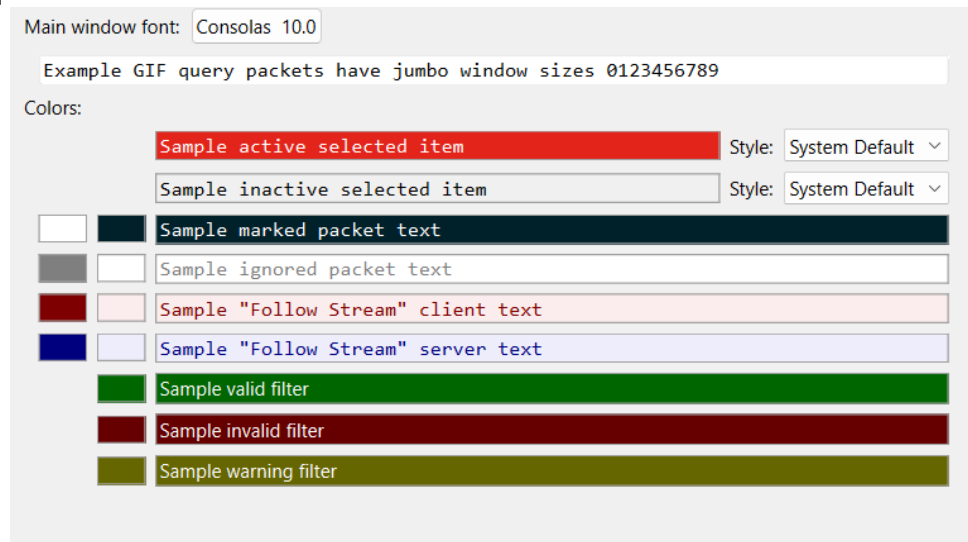
Date: 24/02/2025

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



No.	Time	Source	Destination	Protocol	Length	Info
18500	658.259267	52.199.50.3	192.168.103.79	TCP	66	443 → 28706 [SYN, ACK]
18501	658.259395	192.168.103.79	52.199.50.3	TCP	54	28706 → 443 [ACK] Seq
18502	658.260106	192.168.103.79	52.199.50.3	TLSv1.2	264	Client Hello (SNI=prc
18503	658.567966	52.199.50.3	192.168.103.79	TCP	54	443 → 28706 [ACK] Seq
18504	658.567966	52.199.50.3	192.168.103.79	TLSv1.2	1372	Server Hello
18505	658.567966	52.199.50.3	192.168.103.79	TCP	1372	443 → 28706 [ACK] Seq
18506	658.567966	52.199.50.3	192.168.103.79	TLSv1.2	1372	Certificate
18507	658.567966	52.199.50.3	192.168.103.79	TLSv1.2	347	Server Key Exchange,
18508	658.568119	192.168.103.79	52.199.50.3	TCP	54	28706 → 443 [ACK] Seq
18509	658.574141	192.168.103.79	52.199.50.3	TLSv1.2	147	Client Key Exchange,
18510	658.877307	52.199.50.3	192.168.103.79	TCP	54	443 → 28706 [ACK] Seq
18511	658.877307	52.199.50.3	192.168.103.79	TLSv1.2	258	New Session Ticket, C
18512	658.877307	52.199.50.3	192.168.103.79	TLSv1.2	123	Application Data
18513	658.877451	192.168.103.79	52.199.50.3	TCP	54	28706 → 443 [ACK] Seq

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



Main window font: Consolas 10.0

Example GIF query packets have jumbo window sizes 0123456789

Colors:

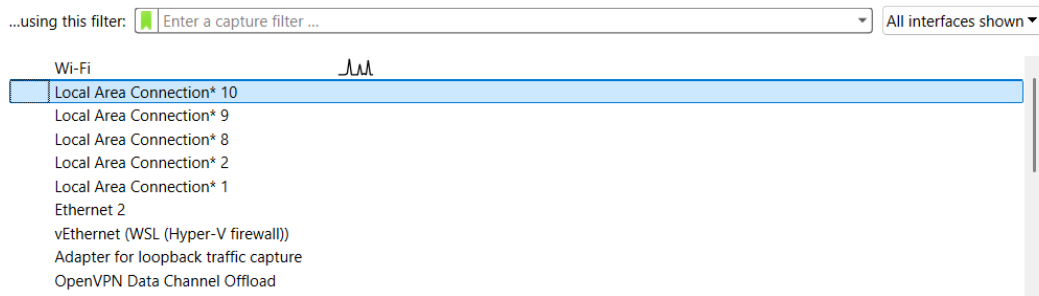
- Sample active selected item (Red) Style: System Default
- Sample inactive selected item (Grey) Style: System Default
- Sample marked packet text (Dark Blue)
- Sample ignored packet text (Light Grey)
- Sample "Follow Stream" client text (Red)
- Sample "Follow Stream" server text (Blue)
- Sample valid filter (Green)
- Sample invalid filter (Dark Red)
- Sample warning filter (Olive)

## 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.

#### Capture



## Analyzing Specific Network Traffic Types

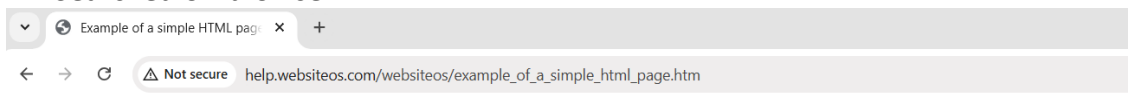
Use a browser to visit a website (e.g., <http://example.com>).

In Wireshark, apply the filter `http` to see the HTTP requests and responses.

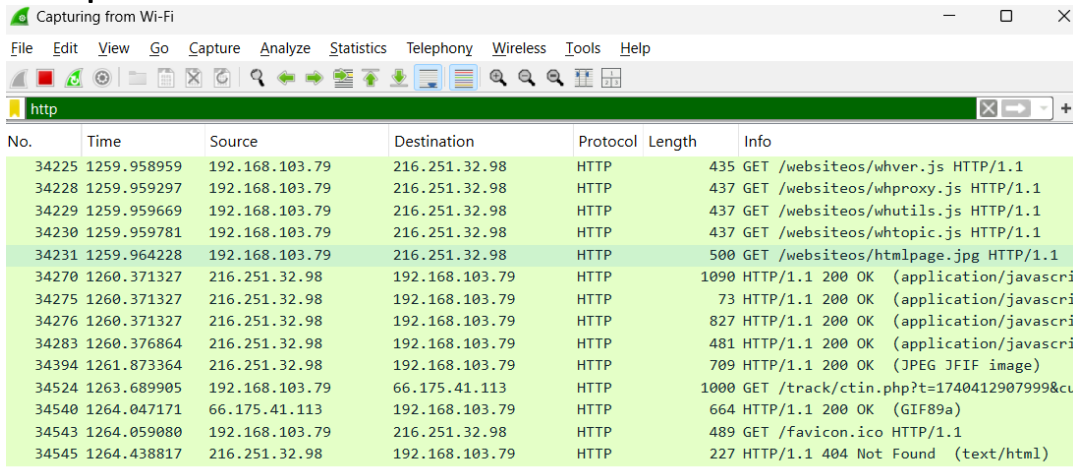
Look for HTTP GET or POST requests to examine the URLs, headers, and any transmitted data.

### Capture and Analyze HTTP Traffic

#### - Searched on browser:



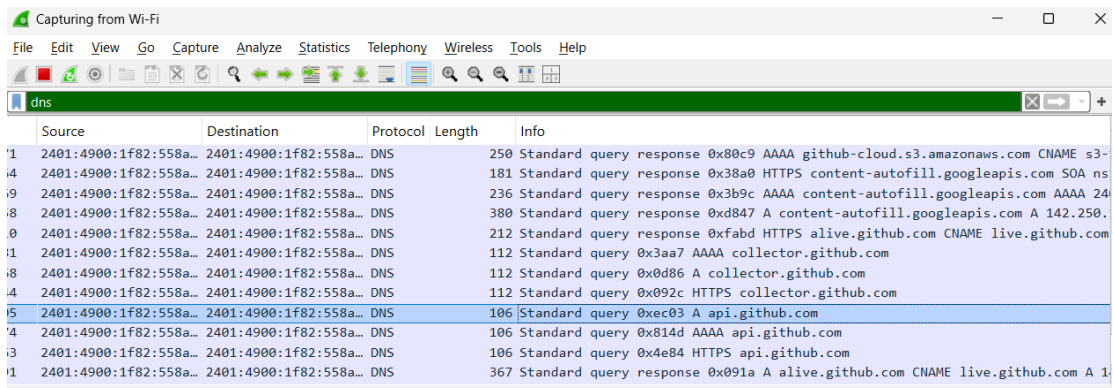
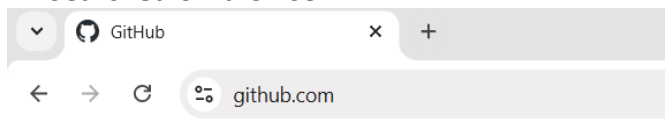
#### - Captured Packets:

The image shows the Wireshark packet capture window. The top bar indicates 'Capturing from Wi-Fi'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The packet list pane shows a list of captured packets, with the filter 'http' applied. The selected packet is a GET request for '/websites/whver.js'.

Date: 24/02/2025

### Capture and Analyze DNS Traffic

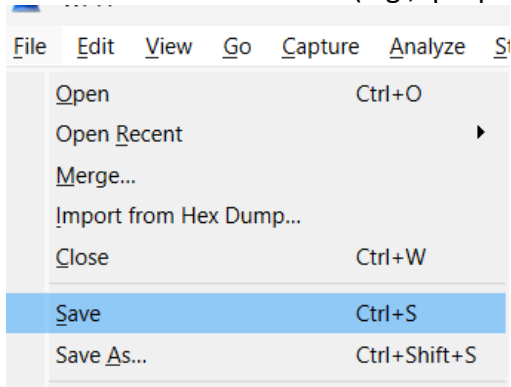
- Searched on browser:



### 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.

## 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
```

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-AFD4-4F0D-96EE-664C49C20F56}
  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

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).