Capture and Analyze Network Traffic Using Wireshark

Packet Capture and Analysis is the process of intercepting, recording, and examining data packets that travel across a network. It helps in understanding network behavior, diagnosing issues, and detecting security threats.

Packet Capture

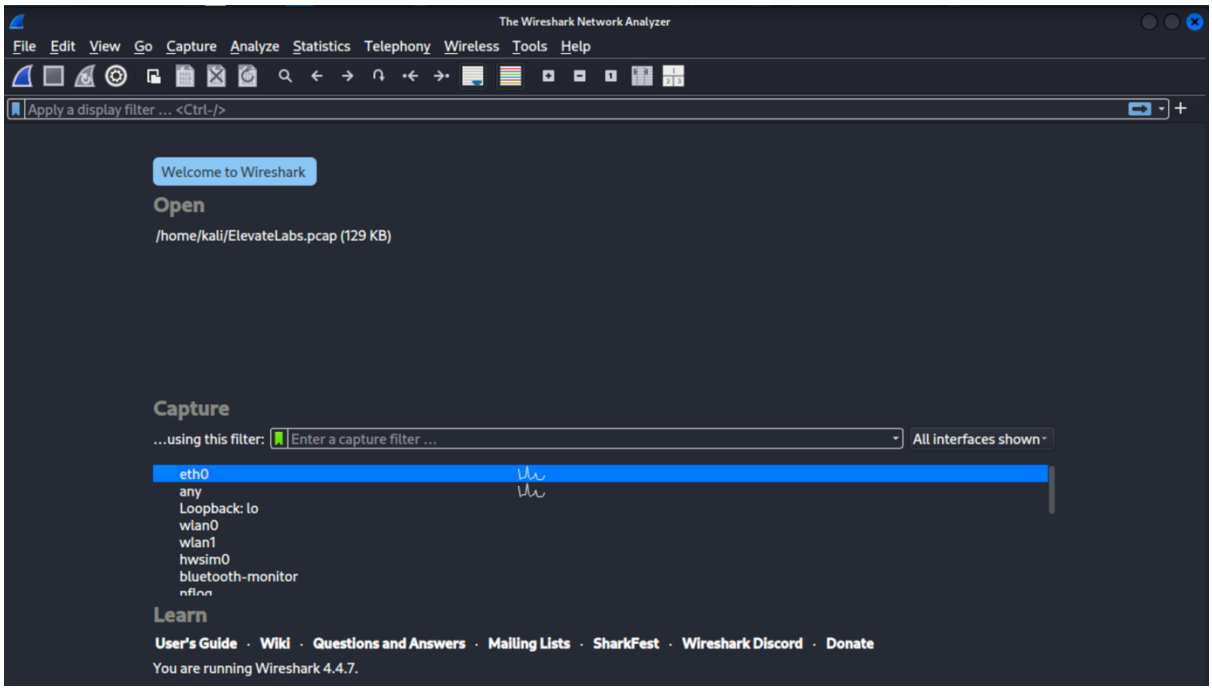
- Involves using tools (e.g., **Wireshark**, **tcpdump**) to **record network traffic**. For this time , I will be using wireshark.
- Captures individual data packets including their **source, destination, protocol, size, and payload**.
- Stored in files like .pcap (Packet Capture) format for later analysis.

Steps to Capture Packets using Wireshark:

1. To install the Wireshark Tool we will open Kali Linux and use Command :

   sudo apt install wireshark

2. Open Wireshark
3. Click **Start Capture**

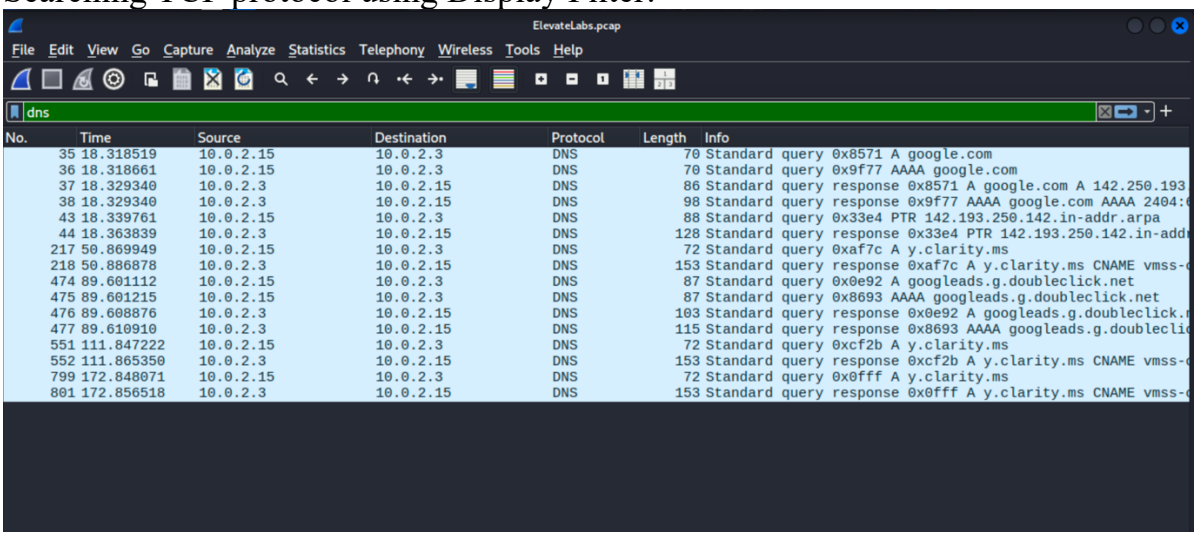


4. **Generate Traffic:**

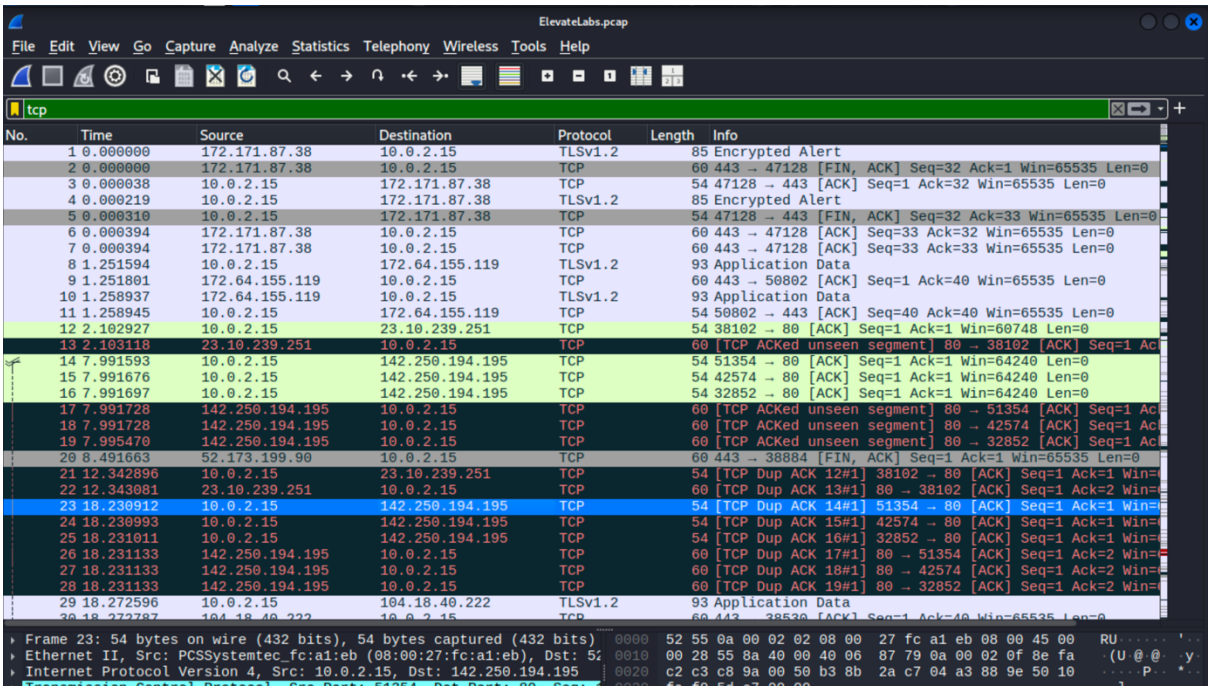
```
┌──(kali㉿vbox)-[~]
└─$ ping google.com
PING google.com (142.250.193.142) 56(84) bytes of data.
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=1 ttl=255 time=7.02 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=2 ttl=255 time=8.55 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=3 ttl=255 time=8.17 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=4 ttl=255 time=16.0 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=5 ttl=255 time=16.1 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=6 ttl=255 time=17.1 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=7 ttl=255 time=17.2 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=8 ttl=255 time=8.02 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=9 ttl=255 time=14.3 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=10 ttl=255 time=6.93 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=11 ttl=255 time=7.43 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=12 ttl=255 time=12.3 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=13 ttl=255 time=16.3 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=14 ttl=255 time=7.99 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=15 ttl=255 time=13.9 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=16 ttl=255 time=6.60 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=17 ttl=255 time=18.1 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=18 ttl=255 time=13.8 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=19 ttl=255 time=15.2 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=20 ttl=255 time=14.4 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=21 ttl=255 time=18.0 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=22 ttl=255 time=13.4 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=23 ttl=255 time=15.9 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=24 ttl=255 time=6.27 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=25 ttl=255 time=14.9 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=26 ttl=255 time=6.54 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=27 ttl=255 time=6.90 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=28 ttl=255 time=8.78 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=29 ttl=255 time=14.4 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=30 ttl=255 time=6.72 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=31 ttl=255 time=15.3 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=32 ttl=255 time=8.38 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=33 ttl=255 time=16.8 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=202 ttl=255 time=17.1 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=203 ttl=255 time=16.5 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=204 ttl=255 time=7.56 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=205 ttl=255 time=8.63 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=206 ttl=255 time=8.33 ms
64 bytes from tzdelb-at-in-f14.1e100.net (142.250.193.142): icmp_seq=207 ttl=255 time=7.63 ms
^C
── google.com ping statistics ──
207 packets transmitted, 206 received, +1 duplicates, 0.483092% packet loss, time 206345ms
rtt min/avg/max/mdev = 6.159/12.322/18.624/4.040 ms
```

5. Filter Captured Packets by Protocol

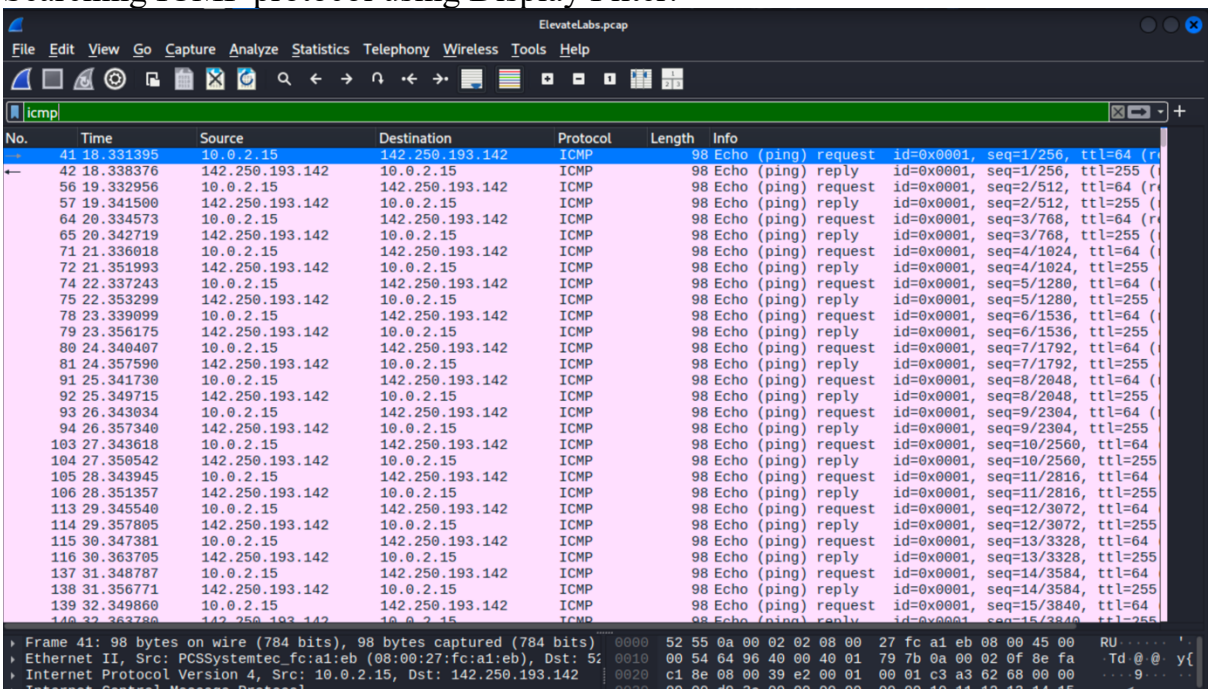
Searching TCP protocol using Display Filter:



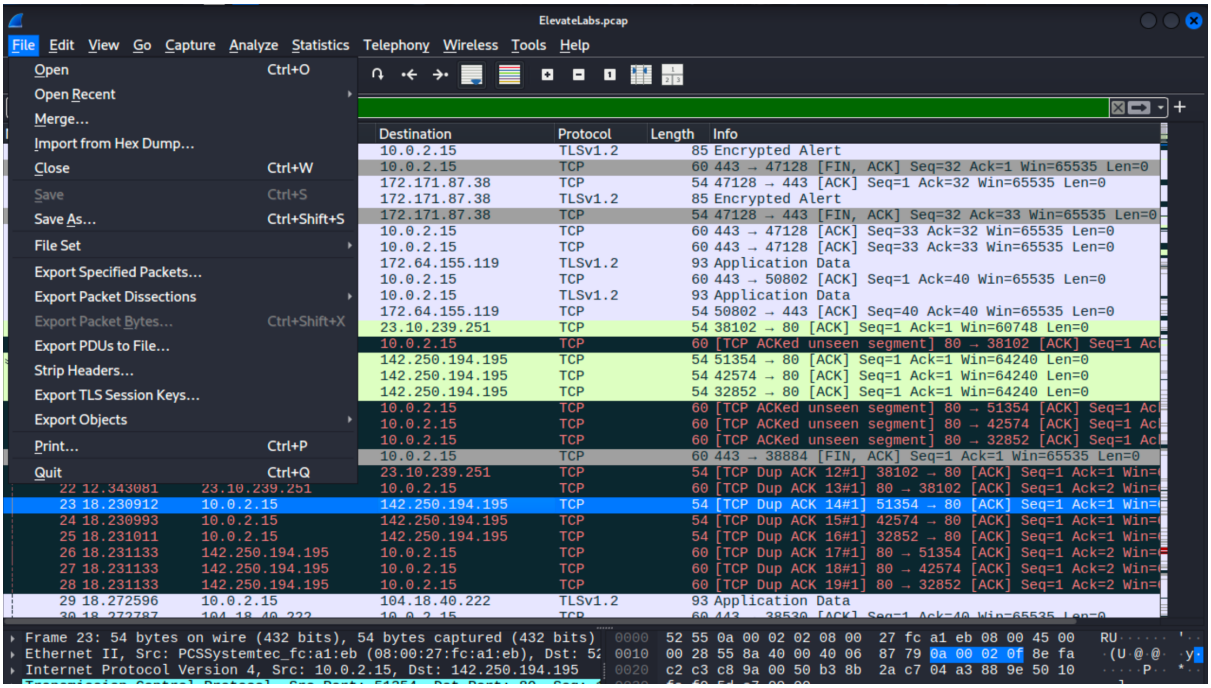
Searching DNS protocol using Display Filter:



Searching ICMP protocol using Display Filter:



6. **Save the file as ElevateLAbs.pcap by clicking save as on “File”:**



Traffic Capture Summary Report

🔧 Interface Used

- **Interface:** eth0
  Tool: Wireshark

📩 Traffic Generated

- Pinged: google.com

Protocols Captured

Protocol	Description	Example Packet Details
DNS	Resolves domain names to IPs	Standard query A google.com
TCP	Handles connection setup	SYN, ACK flags in TCP handshake
ICMP	Web traffic	diagnostic and error-reporting