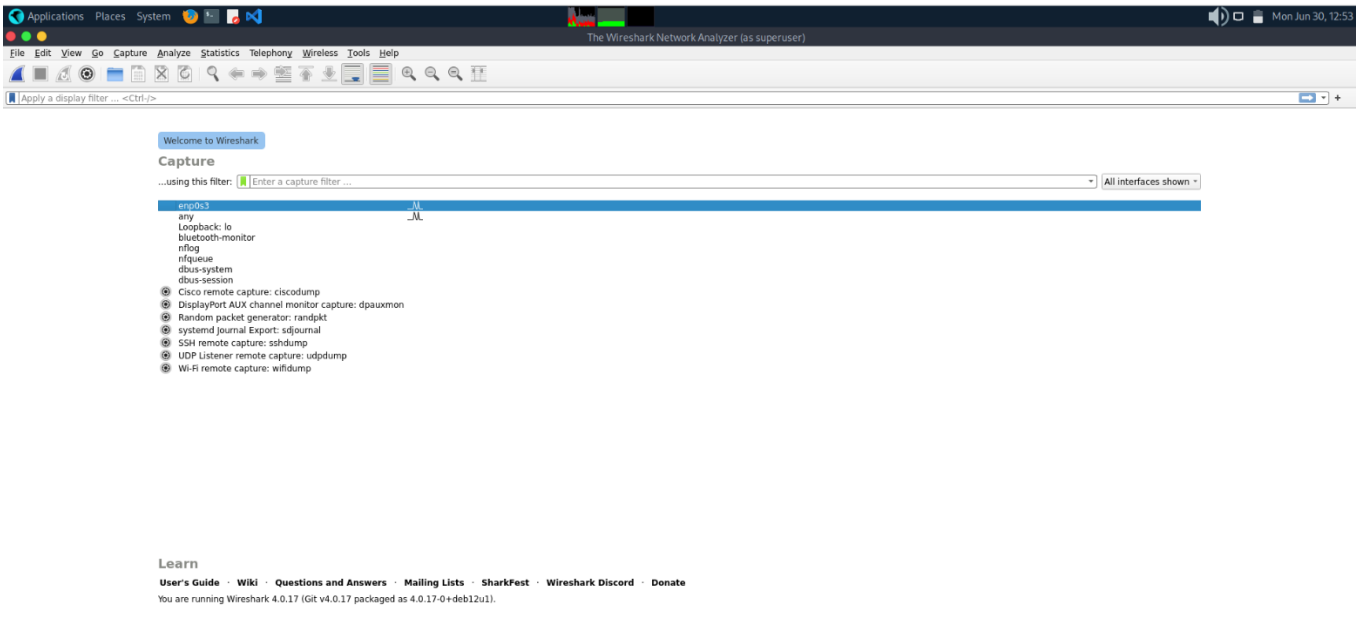
Capture and Analyze Network Traffic Using the Wireshark

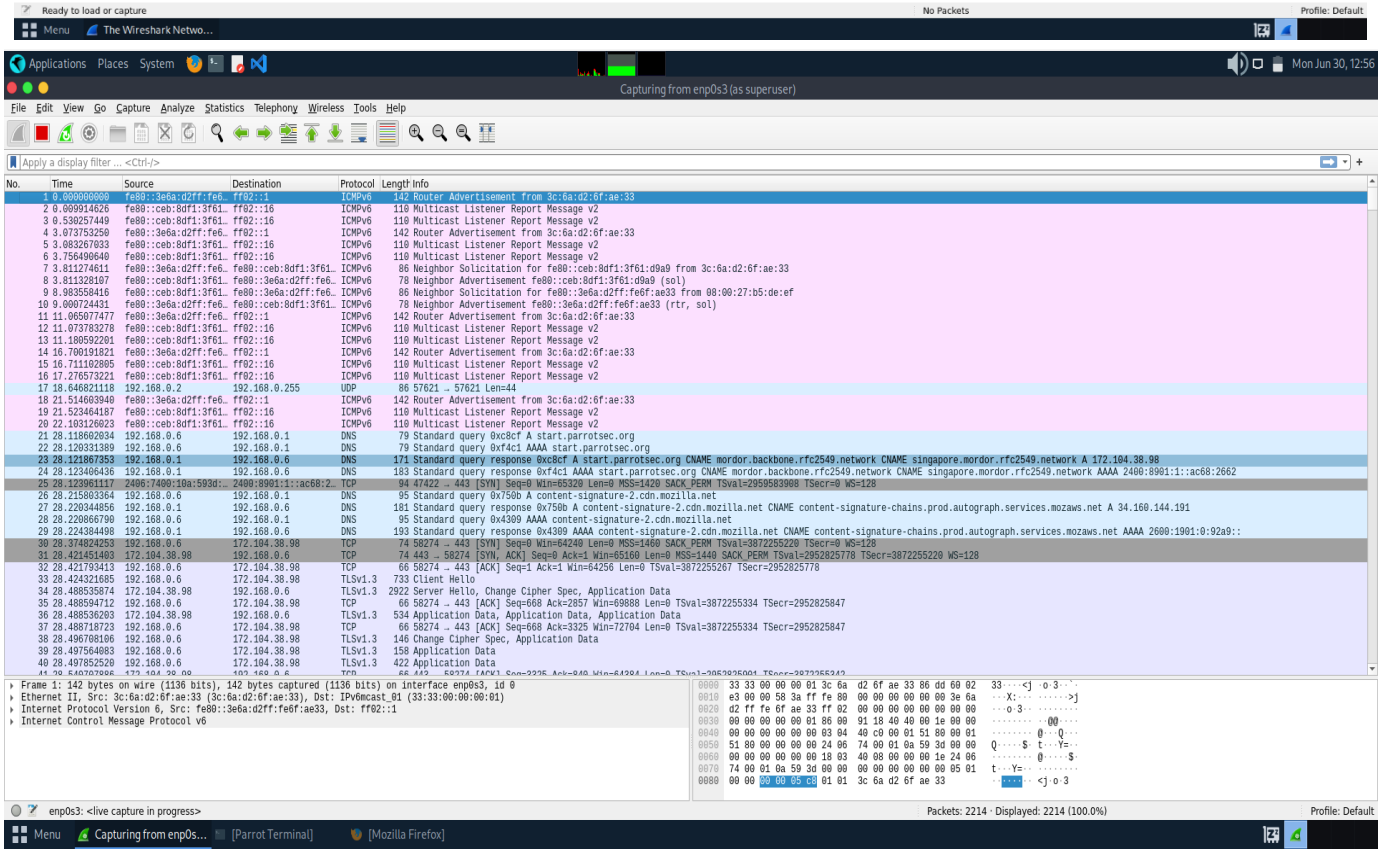
1. Install Wireshark

- Download from: https://www.wireshark.org/download.html

2. Start Capturing

- Open Wireshark.
- Choose your active network interface (usually Wi-Fi or Ethernet or enp0s3).
- Click on the Start Capturing Packets icon (top left).



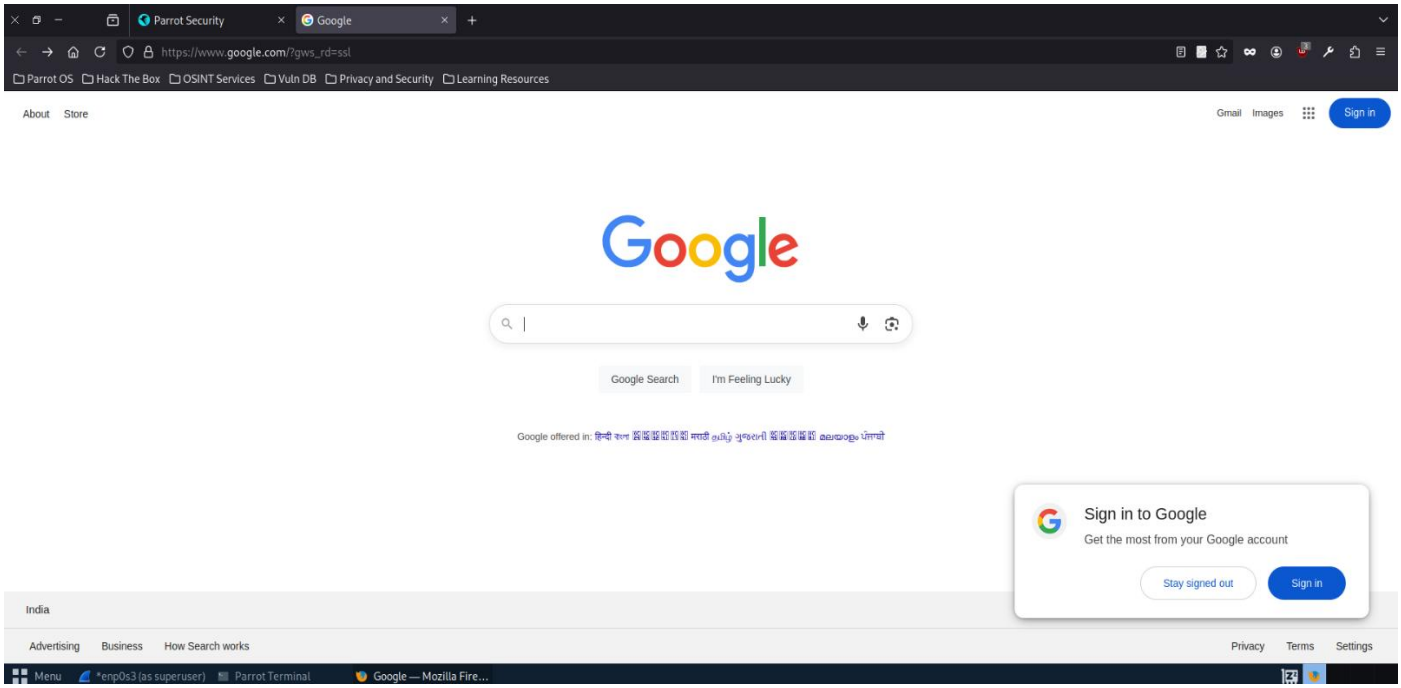


3. Generate Network Traffic

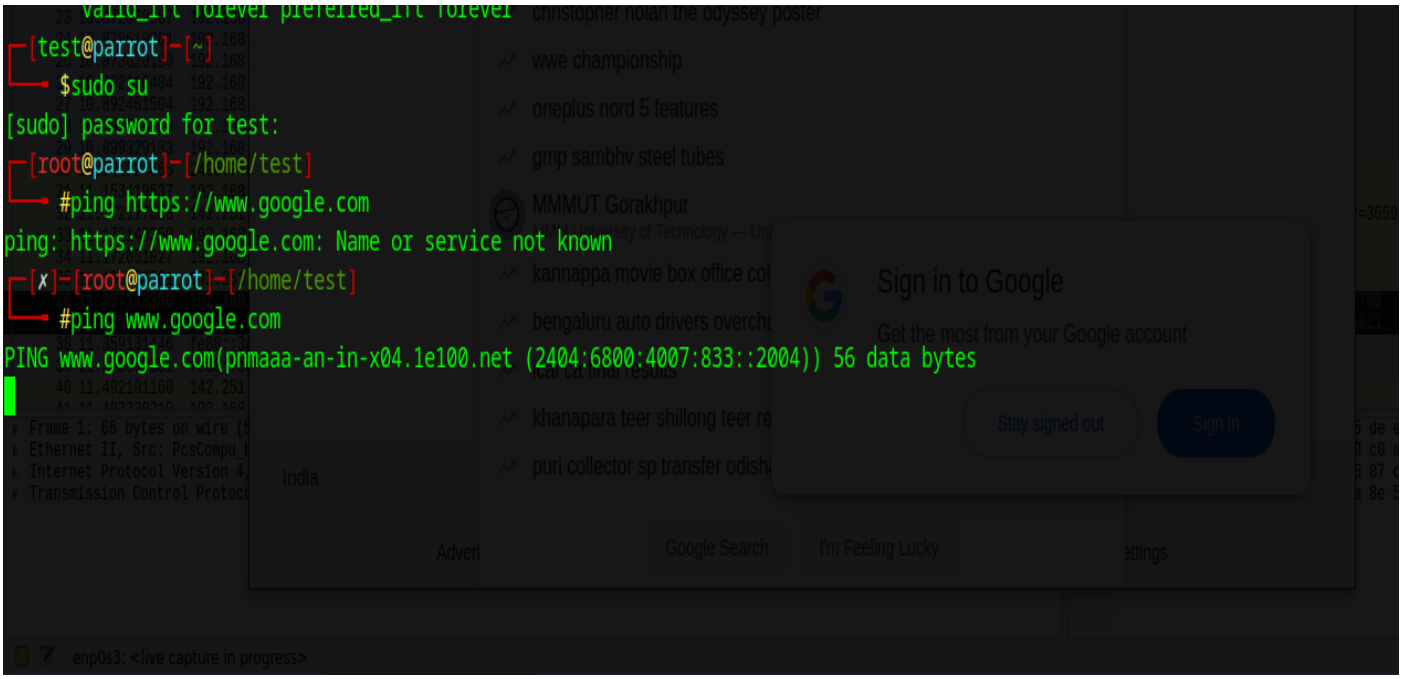
While capturing:

- Open a browser and visit 2–3 websites (e.g., example.com, google.com).
- open Command Prompt and run:

  ping google.com

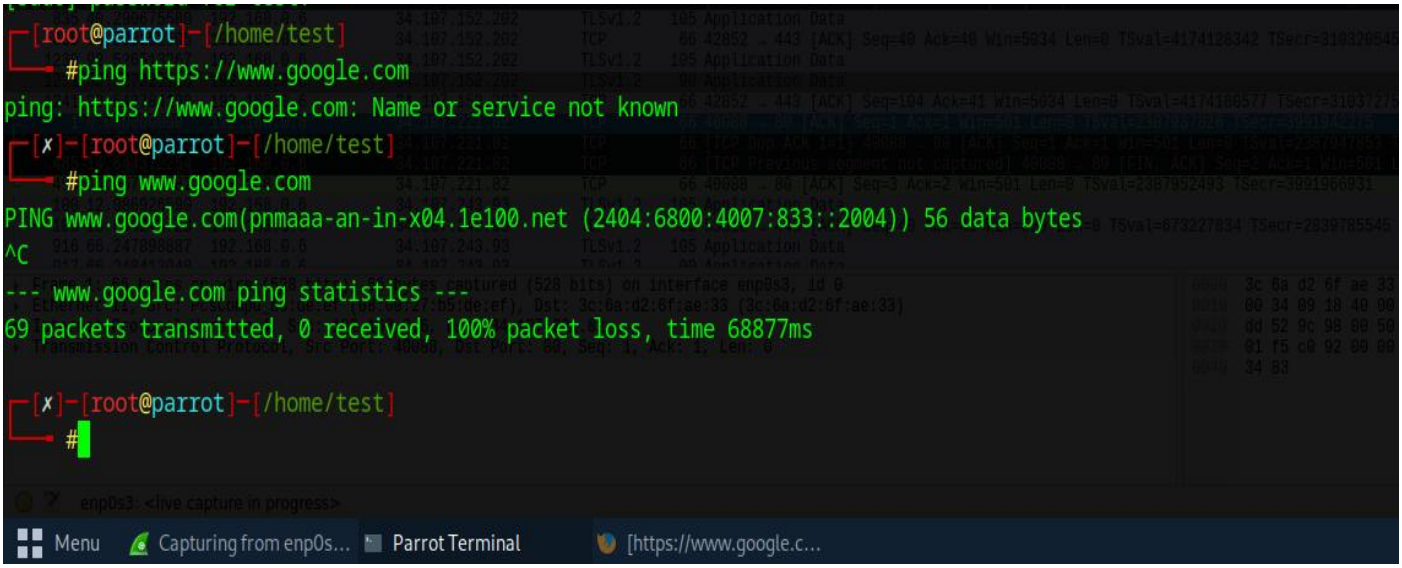


•Open a browser and visit 2–3 websites



• open Command Prompt and run:

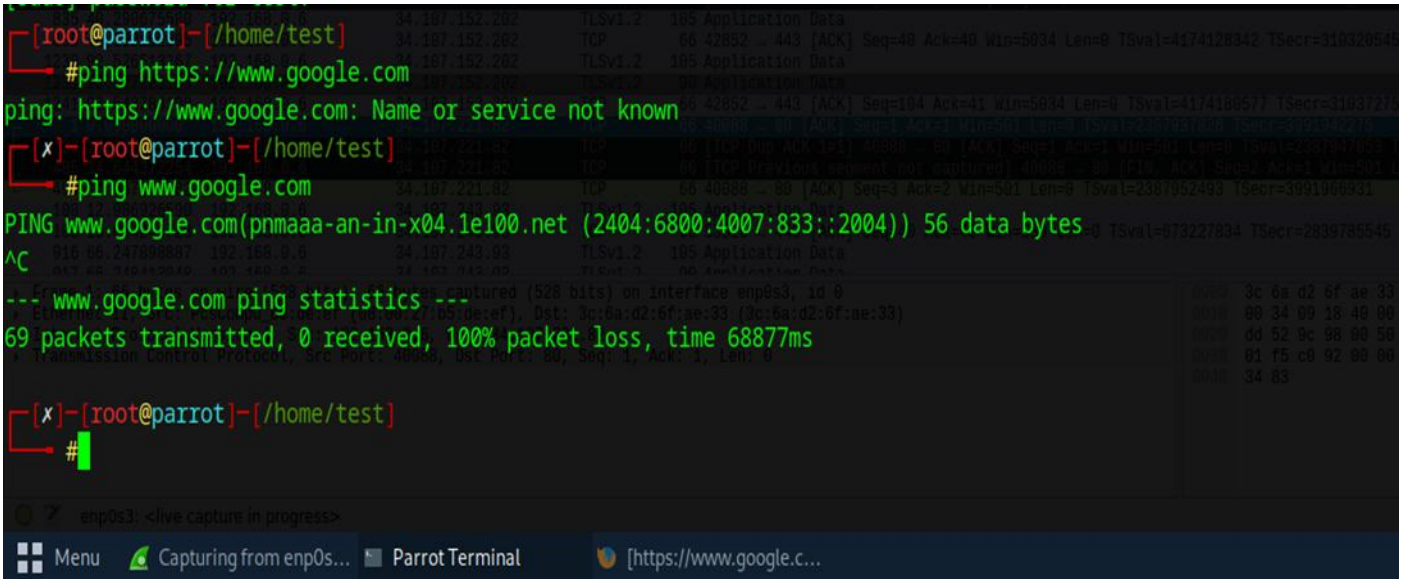
ping google.com



Stop the ping by ctrl+c or ctrl+z

4. <u>Stop Capturing</u>

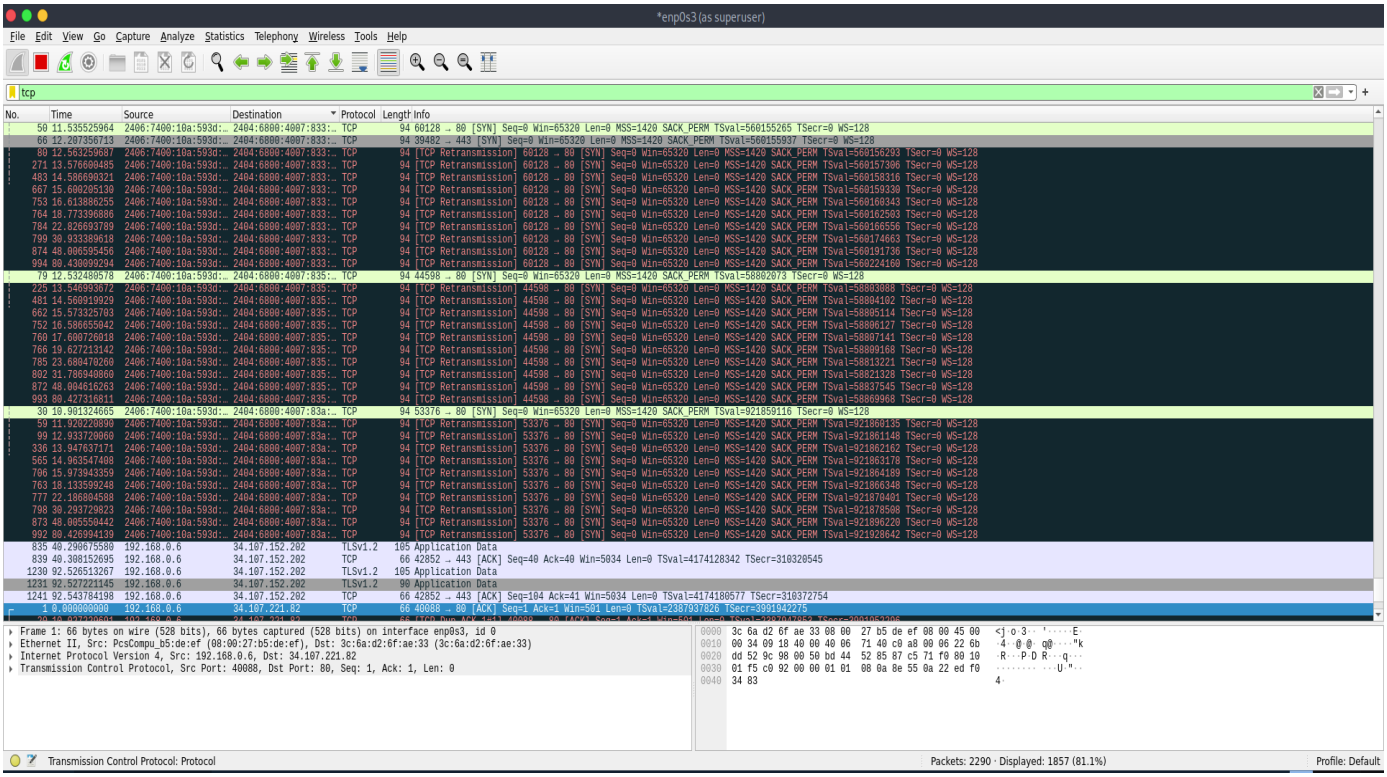
Wait about 1 minute, then click the red square stop button in Wireshark.



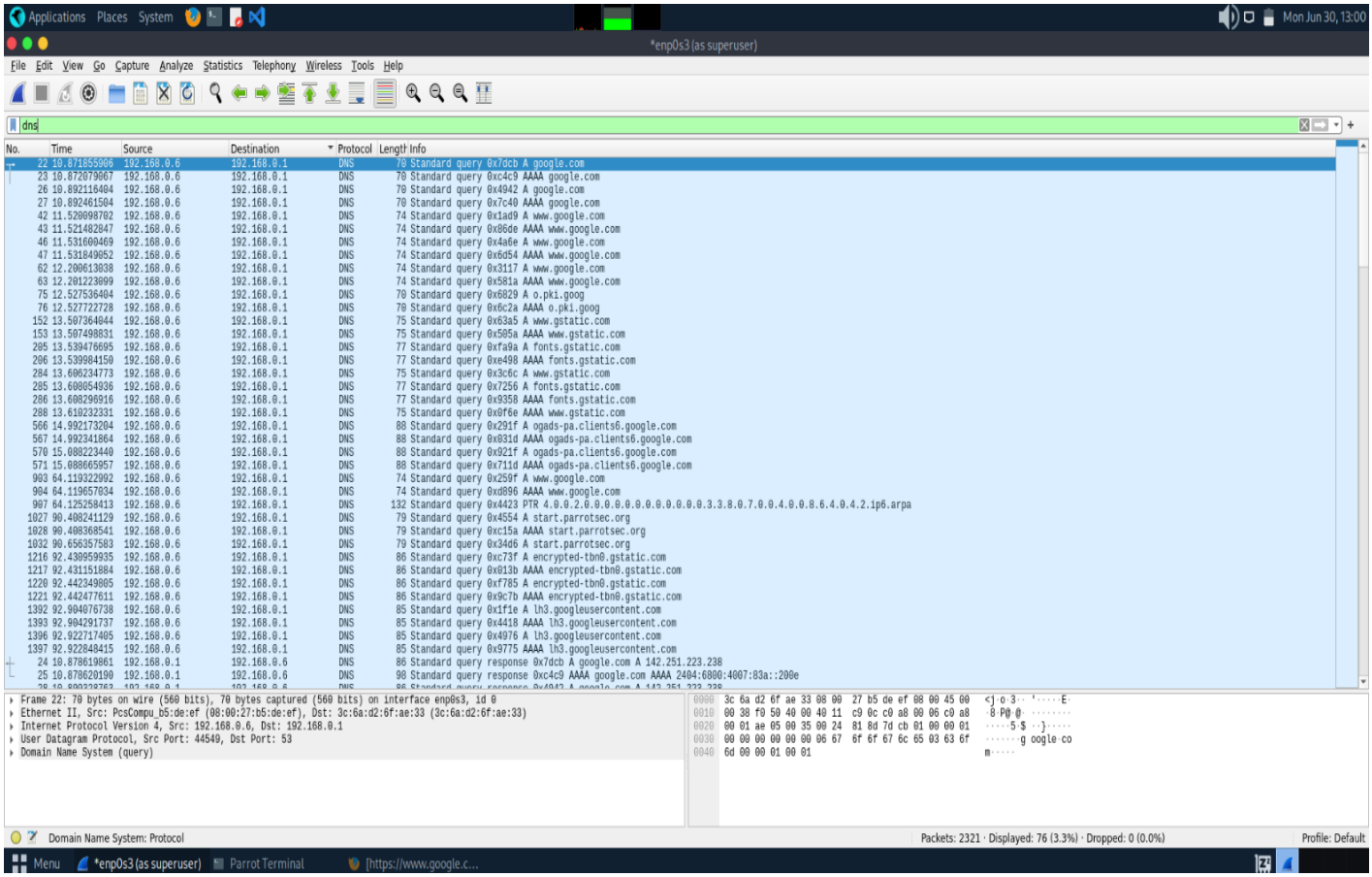
5. <u>Filter Captured Packets by Protocol</u>

Use filters in the top filter bar in Wireshark to isolate protocols:

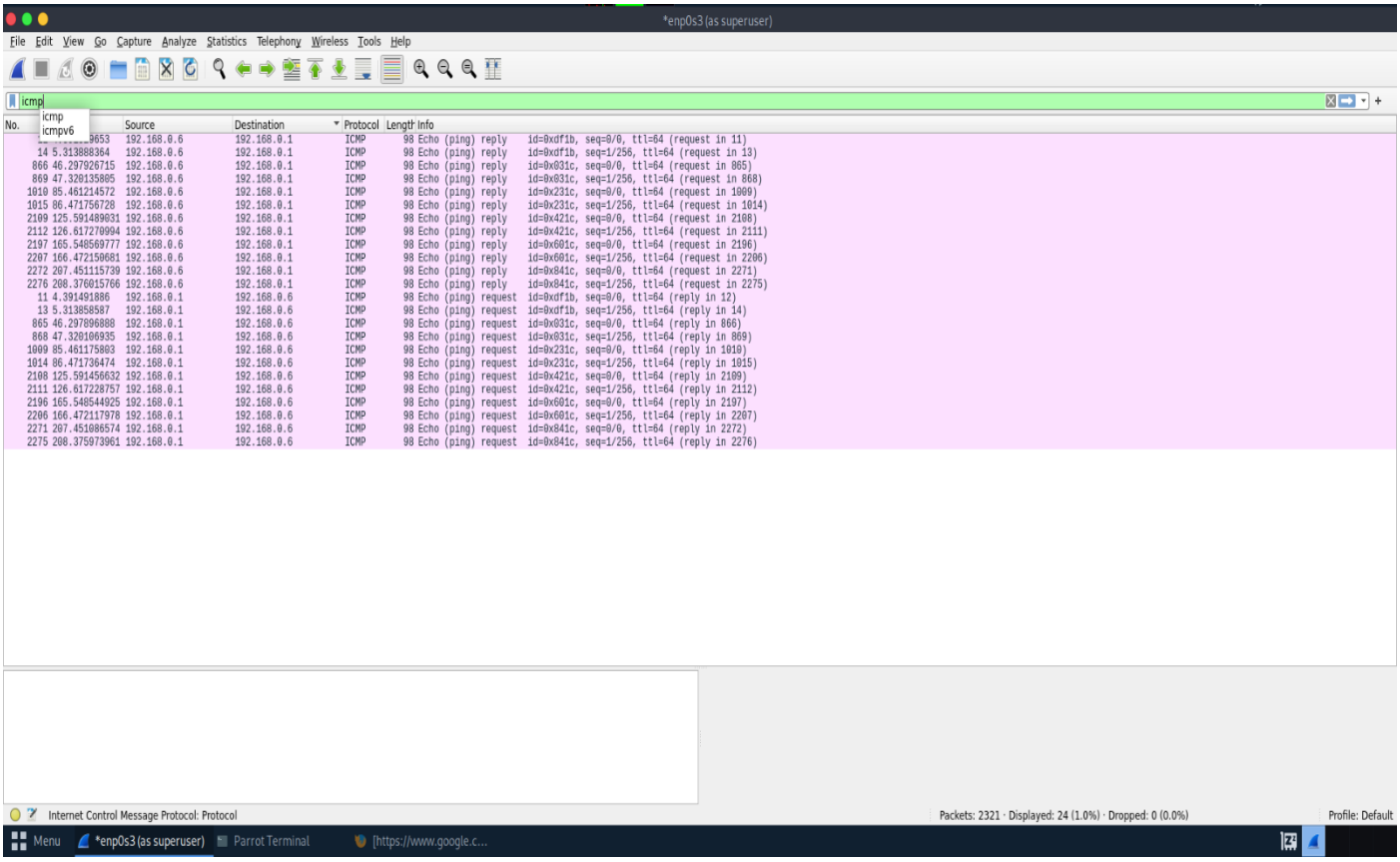
- DNS → dns
- HTTP → http
- TCP → tcp
- ICMP (for ping) → icmp



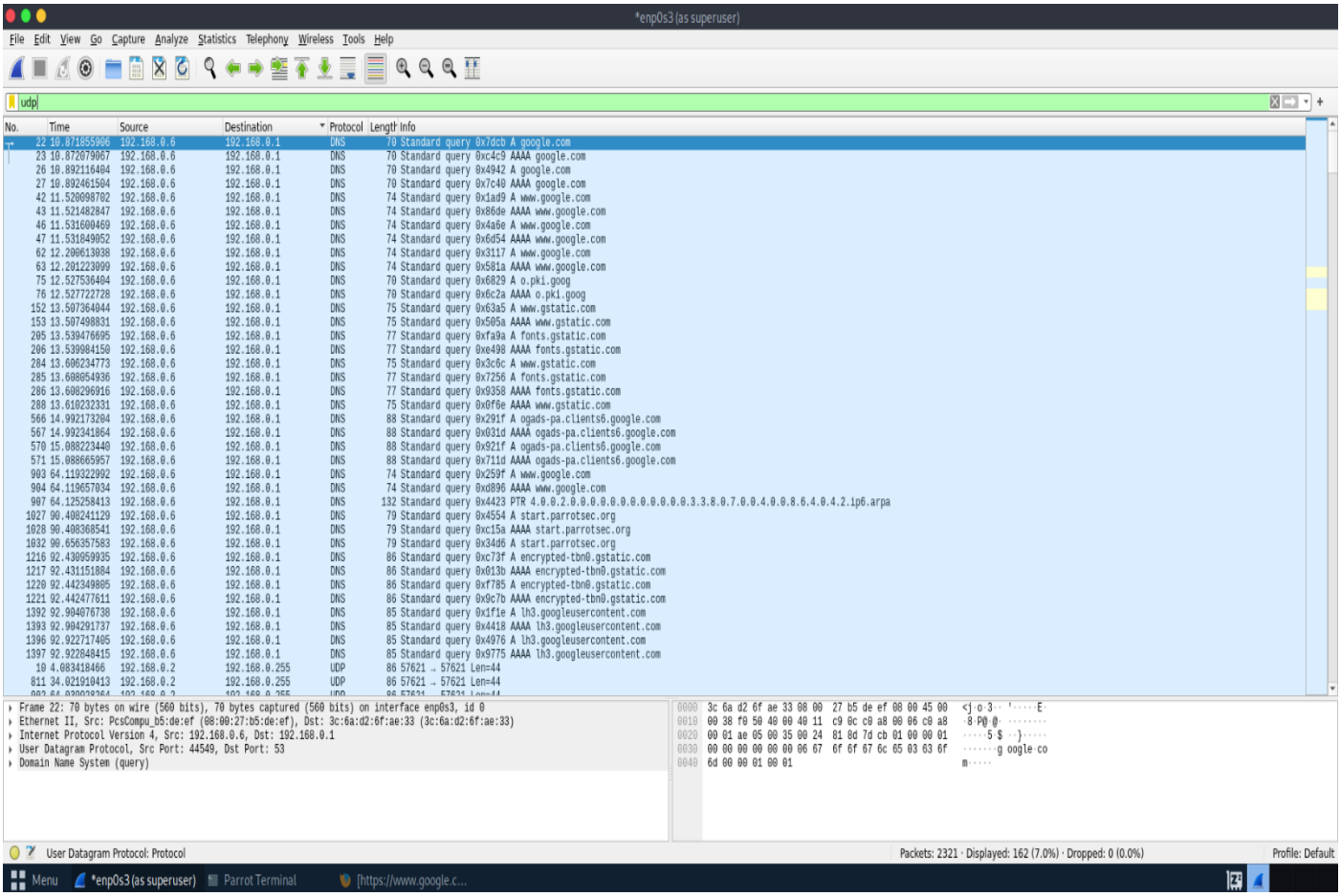
TCP filter



DNS filter



ICMP filter



UDP filter

6. Identify 3 Different Protocols

Look at the "Protocol" column.

Identify and note at least 3 distinct protocols, such as:

- TCP
- DNS
- HTTP

1. TCP (Transmission Control Protocol)

- Most traffic was between IPv6 addresses, showing many TCP **SYN** and **Retransmission** packets.
- Port `443` (HTTPS) and `593d` were involved in communication.
- These may indicate secure web browsing or SSL handshake attempts.

Notable Packet Detail:

Protocol: TCP
Info: [SYN] Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM TSval=…
Likely a client trying to initiate a TLS/HTTPS connection.

2. DNS (Domain Name System)

- Standard DNS queries from `192.168.0.6` to `192.168.0.1`
- Many domain lookups for:
  - `google.com`
  - `gstatic.com`
  - `start.parrotsec.org`
  - `clients6.google.com`

Notable Packet Detail:

Query: AAAA google.com
Protocol: DNS
Length: 70–85 bytes

3. UDP (User Datagram Protocol)

- Mostly used for DNS traffic (as DNS uses UDP/53)
- DNS queries (like `A`, `AAAA`, and `PTR`) were sent over UDP
- One packet clearly shows `Protocol: UDP`, `Length: 44`

4. ICMP (Internet Control Message Protocol)

- Classic **ping** packets using `Echo (ping) request` and `reply`
- These are ICMP type 8 (request) and type 0 (reply)
- All between `192.168.0.6` and `192.168.0.1`

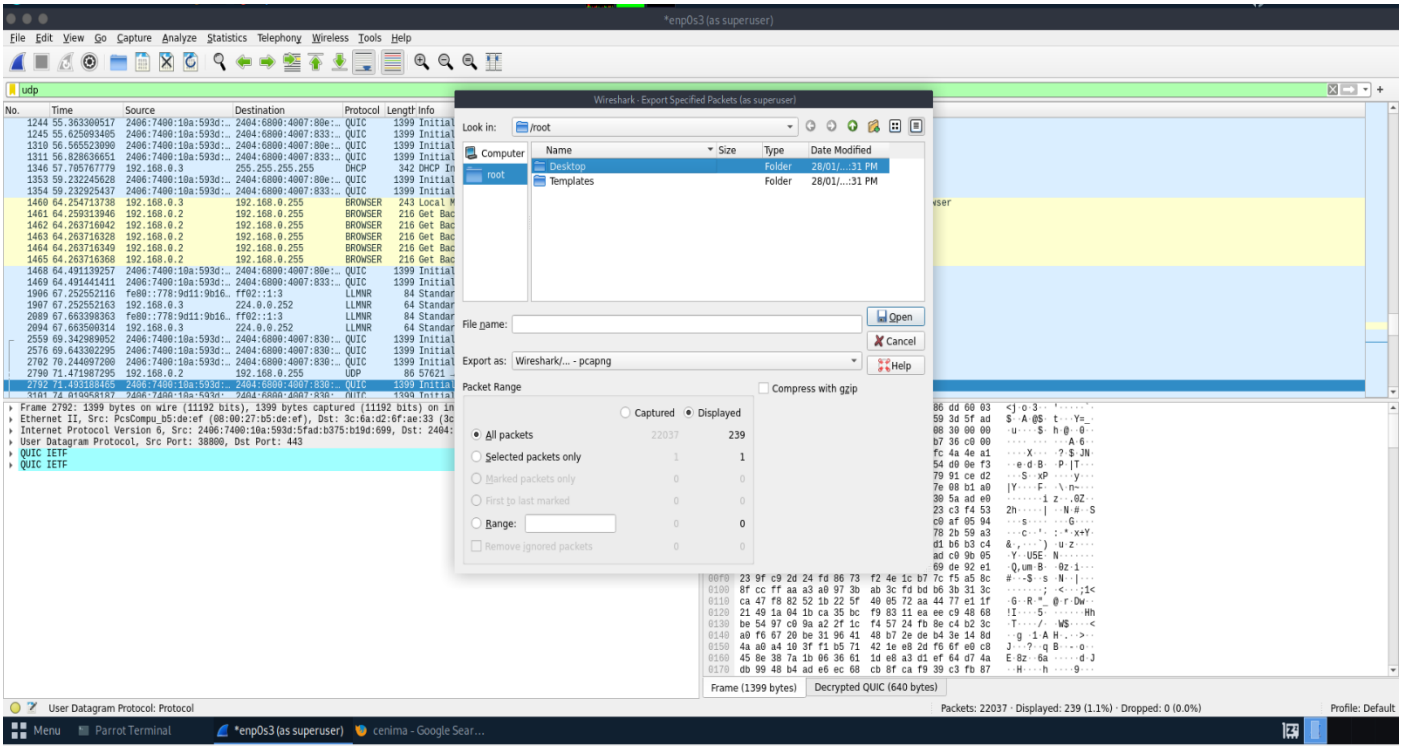
Notable Packet Detail:

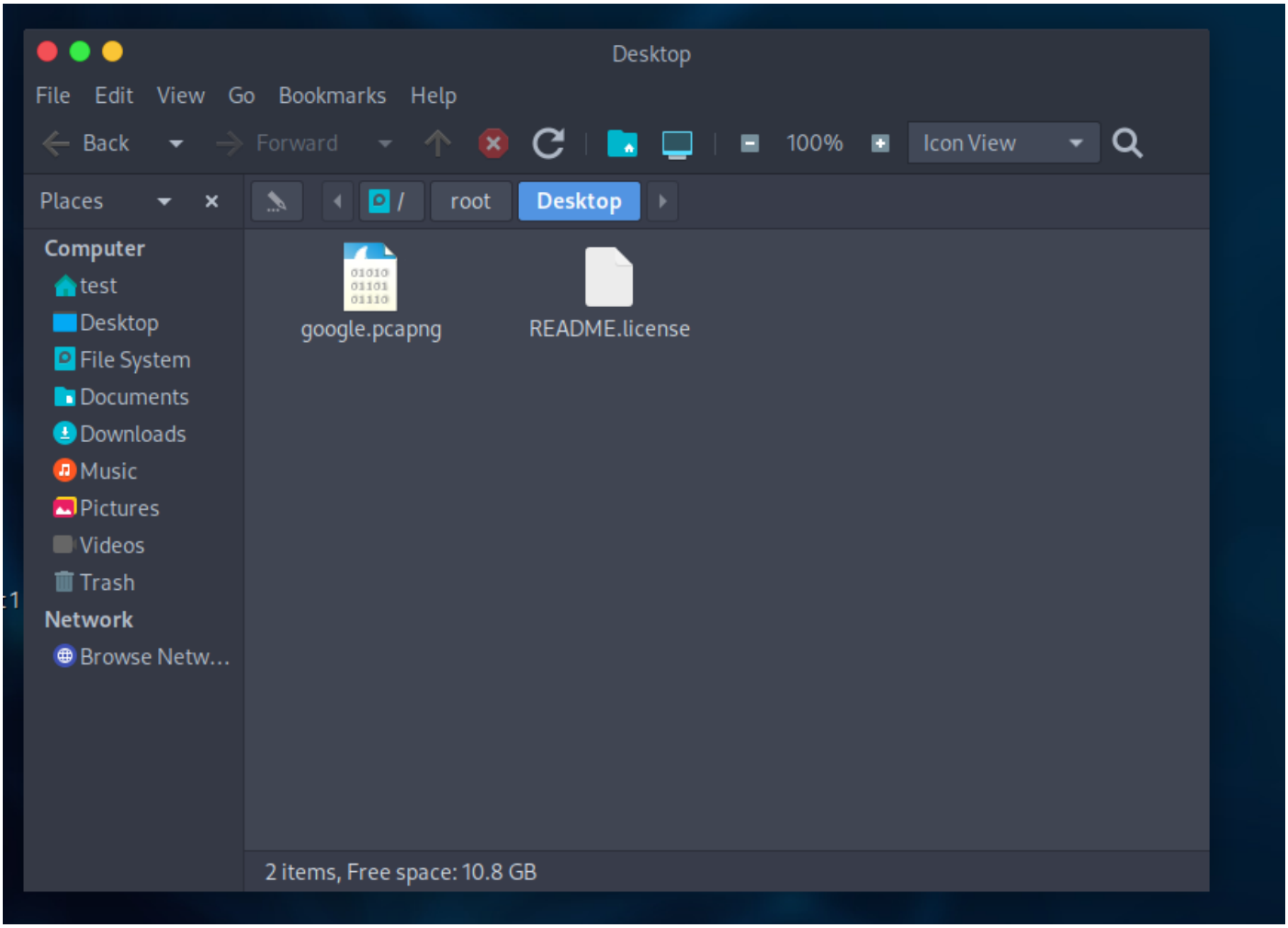
```
Protocol: ICMP
Type: Echo (ping) request
Reply received successfully from gateway
```

7. Export Capture as .pcap File

Go to File > Export Specified Packets.

Save the file with .pcap extension (e.g., mycapture.pcap).





8. Summary of Findings

Protocol	Purpose	Observation
TCP	Reliable transport (HTTPS, TLS)	Seen with SYN, retransmissions on IPv6
DNS	Domain name resolution	Lookups for Google, ParrotSec, etc.
UDP	Lightweight transport	Used by DNS queries
ICMP	Network diagnostics (ping)	Echo requests & replies between local IPs