

# 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).

The screenshot displays the Wireshark Network Analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for applying display filters, starting and stopping capture, and other functions. The main window is divided into three panes: the top pane shows the 'Capture' settings with 'enp0s3' selected as the interface; the middle pane shows the 'Learn' section with links to the User's Guide, Wiki, Questions and Answers, Mailing Lists, SharkFest, Wireshark Discord, and Donate; the bottom pane shows the packet list, packet details, and packet bytes. The packet list shows a series of ICMPv6 Router Advertisement and Multicast Listener Report messages. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 6, and ICMPv6. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Ready to load or capture

No Packets

Profile: Default

Menu The Wireshark Network...

Capturing from enp0s3 (as superuser)

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::3e6a:d2ff:fe6::ff02::1	ff02::1	ICMPv6	142	Router Advertisement from 3c:6a:d2:6f:ae:33
2	0.009914626	fe80::ceb:8df1:3f61::ff02::16	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
3	0.536257449	fe80::ceb:8df1:3f61::ff02::16	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
4	0.973753250	fe80::3e6a:d2ff:fe6::ff02::1	ff02::1	ICMPv6	142	Router Advertisement from 3c:6a:d2:6f:ae:33
5	0.883267833	fe80::ceb:8df1:3f61::ff02::16	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
6	3.756490640	fe80::ceb:8df1:3f61::ff02::16	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
7	8.11274611	fe80::3e6a:d2ff:fe6::ff02::1	ff02::1	ICMPv6	86	Neighbor Solicitation for fe80::ceb:8df1:3f61:d9a0 from 3c:6a:d2:6f:ae:33
8	9.811328107	fe80::ceb:8df1:3f61::ff02::16	ff02::16	ICMPv6	78	Neighbor Advertisement fe80::ceb:8df1:3f61:d9a0 (sol)
9	9.88358416	fe80::ceb:8df1:3f61::ff02::16	ff02::16	ICMPv6	86	Neighbor Solicitation for fe80::3e6a:d2ff:fe6::ae33 from 08:00:27:b5:de:ef
10	0.000724431	fe80::3e6a:d2ff:fe6::ff02::1	ff02::1	ICMPv6	78	Neighbor Advertisement fe80::3e6a:d2ff:fe6::ae33 (rtr, sol)
11	11.065077477	fe80::3e6a:d2ff:fe6::ff02::1	ff02::1	ICMPv6	142	Router Advertisement from 3c:6a:d2:6f:ae:33
12	11.07378278	fe80::ceb:8df1:3f61::ff02::16	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
13	11.180592201	fe80::ceb:8df1:3f61::ff02::16	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
14	16.700191821	fe80::3e6a:d2ff:fe6::ff02::1	ff02::1	ICMPv6	142	Router Advertisement from 3c:6a:d2:6f:ae:33
15	16.711102805	fe80::ceb:8df1:3f61::ff02::16	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
16	17.76573221	fe80::ceb:8df1:3f61::ff02::16	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
17	18.46821118	192.168.0.2	192.168.0.255	UDP	86	57621 -> 57621 Len=44
18	21.514603940	fe80::3e6a:d2ff:fe6::ff02::1	ff02::1	ICMPv6	142	Router Advertisement from 3c:6a:d2:6f:ae:33
19	21.52364187	fe80::ceb:8df1:3f61::ff02::16	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
20	22.103126023	fe80::ceb:8df1:3f61::ff02::16	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
21	28.118692934	192.168.0.6	192.168.0.1	DNS	79	Standard query 0xc8cf A start.parrotsec.org
22	28.12031389	192.168.0.6	192.168.0.1	DNS	79	Standard query 0xf4c1 AAAA start.parrotsec.org
23	28.121867353	192.168.0.1	192.168.0.6	DNS	173	Standard query response 0xc8cf A start.parrotsec.org CNAME morder.backbone.rfc2549.network CNAME singapore.morder.rfc2549.network A 172.104.38.98
24	28.12340436	192.168.0.1	192.168.0.6	DNS	183	Standard query response 0xf4c1 AAAA start.parrotsec.org CNAME morder.backbone.rfc2549.network CNAME singapore.morder.rfc2549.network AAAA 2668:5961:1::ac68:2662
25	28.123961117	2408:1400:100:593d::2408:8902:1::ac68:2	2408:8902:1::ac68:2	TCP	94	47422 -> 443 [SYN] Seq=0 Win=65536 Len=0 MSS=1460 SACK_PERM TSval=2959583908 TSecr=0 WS=128
26	28.215603364	192.168.0.6	192.168.0.1	DNS	95	Standard query 0x750b A content-signature-2.cdn.mozilla.net
27	28.220344856	192.168.0.1	192.168.0.6	DNS	181	Standard query response 0x750b A content-signature-2.cdn.mozilla.net CNAME content-signature-chains.prod.autograph.services.mozilla.net A 34.108.144.191
28	28.220866790	192.168.0.6	192.168.0.1	DNS	95	Standard query 0x4309 AAAA content-signature-2.cdn.mozilla.net
29	28.224344498	192.168.0.1	192.168.0.6	DNS	193	Standard query response 0x4309 AAAA content-signature-2.cdn.mozilla.net CNAME content-signature-chains.prod.autograph.services.mozilla.net A 34.108.144.191
30	28.374824253	192.168.0.6	172.104.38.98	TCP	74	58274 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3872255220 TSecr=0 WS=128
31	28.424541408	172.104.38.98	192.168.0.6	TCP	74	443 -> 58274 [SYN, ACK] Seq=669 Ack=1 Win=65536 Len=0 MSS=1440 SACK_PERM TSval=2952825778 TSecr=3872255220 WS=128
32	28.421334115	192.168.0.6	172.104.38.98	TCP	66	58274 -> 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3872255278 TSecr=2952825778
33	28.42421695	192.168.0.6	172.104.38.98	TLSv1.3	733	Client Hello
34	28.488535874	172.104.38.98	192.168.0.6	TLSv1.3	2922	Server Hello, Change Cipher Spec, Application Data
35	28.48854712	192.168.0.6	172.104.38.98	TCP	66	58274 -> 443 [ACK] Seq=669 Ack=2057 Win=69888 Len=0 TSval=3872255334 TSecr=2952825847
36	28.488536293	172.104.38.98	192.168.0.6	TLSv1.3	534	Application Data, Application Data, Application Data
37	28.488718723	192.168.0.6	172.104.38.98	TCP	66	58274 -> 443 [ACK] Seq=668 Ack=3325 Win=72704 Len=0 TSval=3872255334 TSecr=2952825847
38	28.496708106	192.168.0.6	172.104.38.98	TLSv1.3	146	Change Cipher Spec, Application Data
39	28.497564863	192.168.0.6	172.104.38.98	TLSv1.3	158	Application Data
40	28.497625220	192.168.0.6	172.104.38.98	TLSv1.3	422	Application Data
41	28.497625220	172.104.38.98	192.168.0.6	TCP	66	443 -> 58274 [ACK] Seq=668 Ack=3325 Win=72704 Len=0 TSval=3872255334 TSecr=2952825847

Frame 1: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface enp0s3, id 0

Ethernet II, Src: 3c:6a:d2:6f:ae:33 (3c:6a:d2:6f:ae:33), Dst: IPv6multicast\_01 (33:33:00:00:00:01)

Internet Protocol Version 6, Src: fe80::3e6a:d2ff:fe6::ae33, Dst: ff02::1

Internet Control Message Protocol v6

enp0s3: <live capture in progress>

Packets: 2214 - Displayed: 2214 (100.0%)

Profile: Default

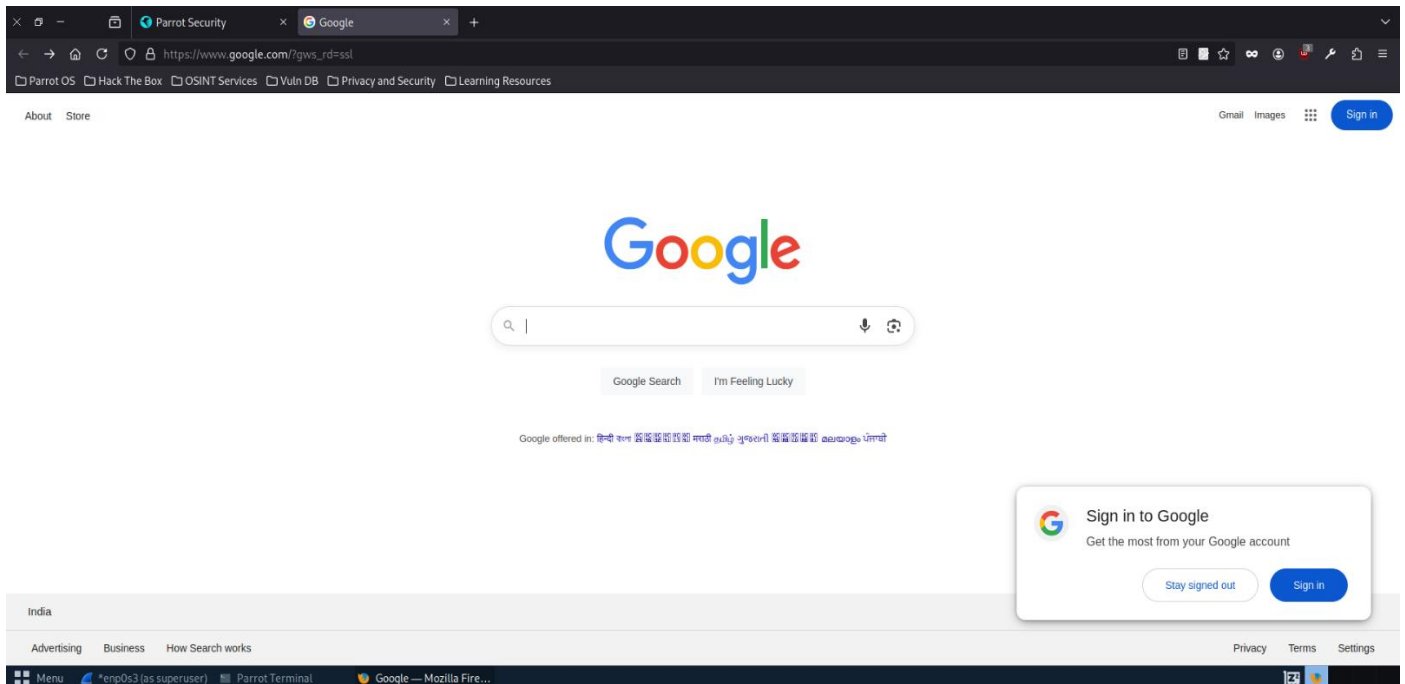
Menu Capturing from enp0s3... [Parrot Terminal] [Mozilla Firefox]

### 3. Generate Network Traffic

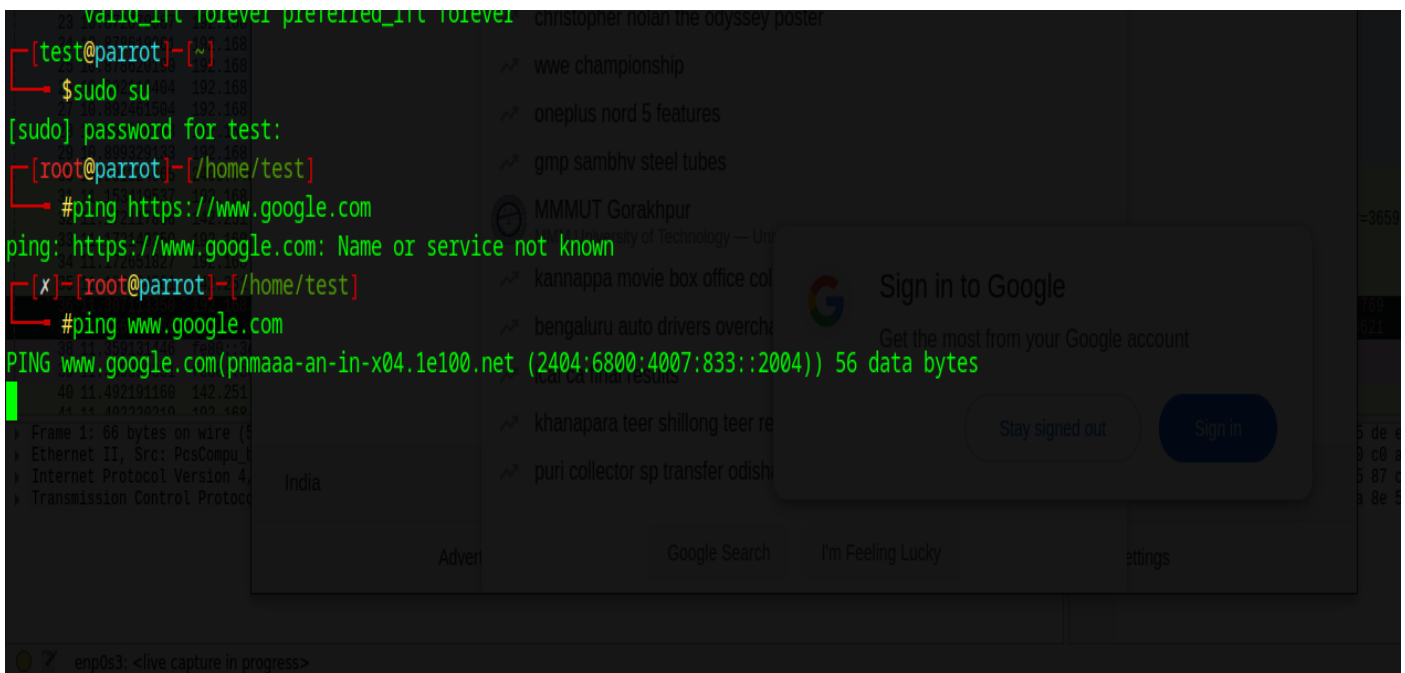
While capturing:

- 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

```
[root@parrot]~[/home/test] 34.187.152.282 TLSv1.2 185 Application Data
#ping https://www.google.com 34.187.152.282 TCP 66 42852 - 443 [ACK] Seq=48 Ack=48 Win=5834 Len=0 TSval=4174128342 TSecr=319326543
ping: https://www.google.com: Name or service not known 34.187.152.282 TLSv1.2 185 Application Data
[x]-[root@parrot]~[/home/test] 34.187.152.282 TCP 66 42852 - 443 [ACK] Seq=104 Ack=41 Win=5834 Len=0 TSval=4174188577 TSecr=31937221
#ping www.google.com 34.187.152.282 TCP 66 40088 - 80 [ACK] Seq=3 Ack=2 Win=581 Len=0 TSval=2387952493 TSecr=3991966931
PING www.google.com(pnmaaa-an-in-x04.1e100.net (2404:6800:4007:833::2004)) 56 data bytes-8 TSval=673227834 TSecr=2839785545
^C 916 66 247898867 192.168.0.0 34.187.243.93 TLSv1.2 185 Application Data
--- www.google.com ping statistics --- 34.187.243.93 TLSv1.2 60 Application Data
69 packets transmitted, 0 received, 100% packet loss, time 68877ms
Transmission Control Protocol, Src Port: 40088, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

[x]-[root@parrot]~[/home/test]
#
```

Stop the ping by ctrl+c or ctrl+z

#### 4. Stop Capturing

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

```
[root@parrot]~[/home/test] 34.187.152.282 TLSv1.2 185 Application Data
#ping https://www.google.com 34.187.152.282 TCP 66 42852 - 443 [ACK] Seq=48 Ack=48 Win=5834 Len=0 TSval=4174128342 TSecr=319326543
ping: https://www.google.com: Name or service not known 34.187.152.282 TLSv1.2 185 Application Data
[x]-[root@parrot]~[/home/test] 34.187.152.282 TCP 66 42852 - 443 [ACK] Seq=104 Ack=41 Win=5834 Len=0 TSval=4174188577 TSecr=31937221
#ping www.google.com 34.187.152.282 TCP 66 40088 - 80 [ACK] Seq=3 Ack=2 Win=581 Len=0 TSval=2387952493 TSecr=3991966931
PING www.google.com(pnmaaa-an-in-x04.1e100.net (2404:6800:4007:833::2004)) 56 data bytes-8 TSval=673227834 TSecr=2839785545
^C 916 66 247898867 192.168.0.0 34.187.243.93 TLSv1.2 185 Application Data
--- www.google.com ping statistics --- 34.187.243.93 TLSv1.2 60 Application Data
69 packets transmitted, 0 received, 100% packet loss, time 68877ms
Transmission Control Protocol, Src Port: 40088, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

[x]-[root@parrot]~[/home/test]
#
```

#### 5. Filter Captured Packets by Protocol

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





## 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

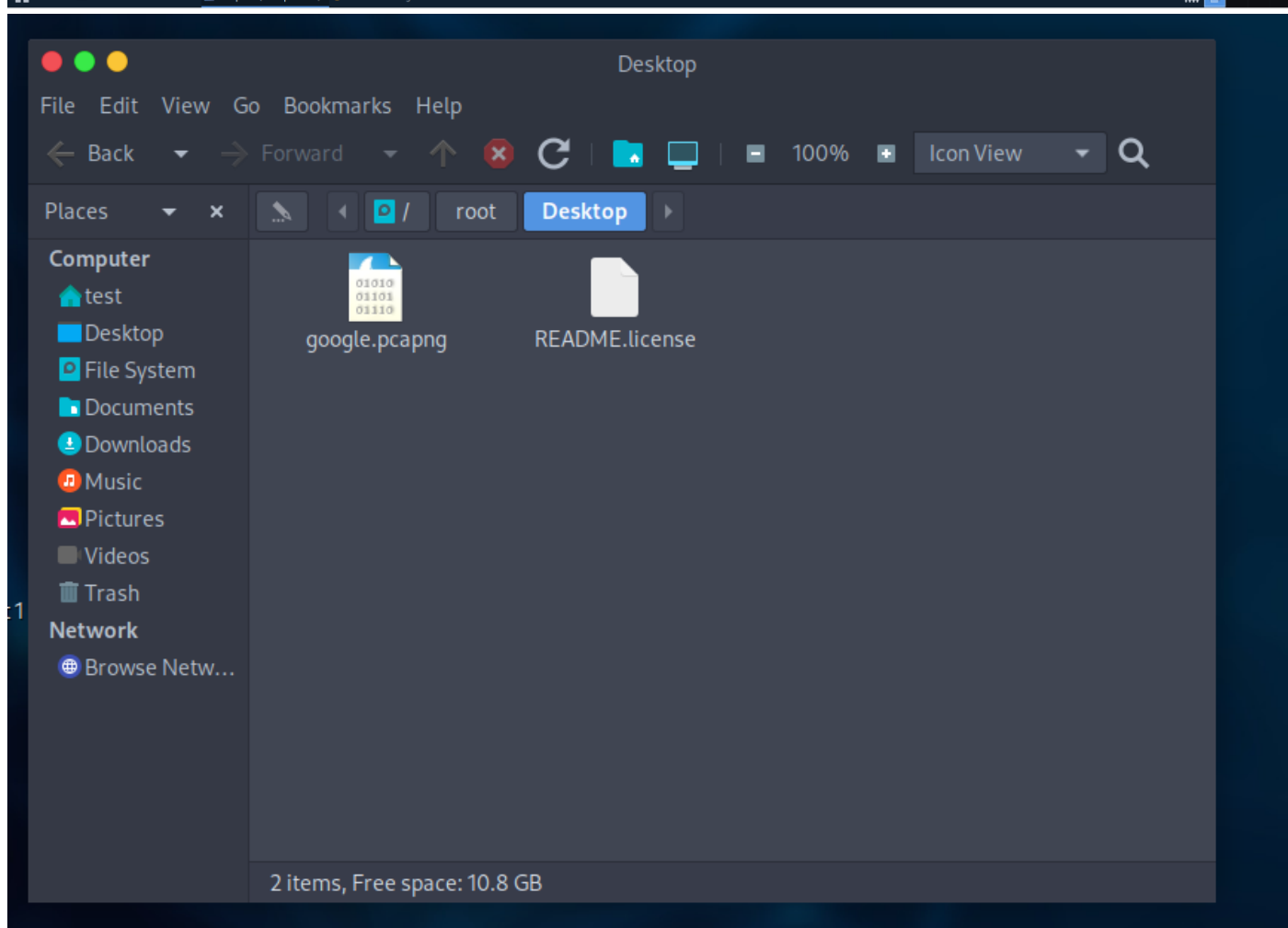
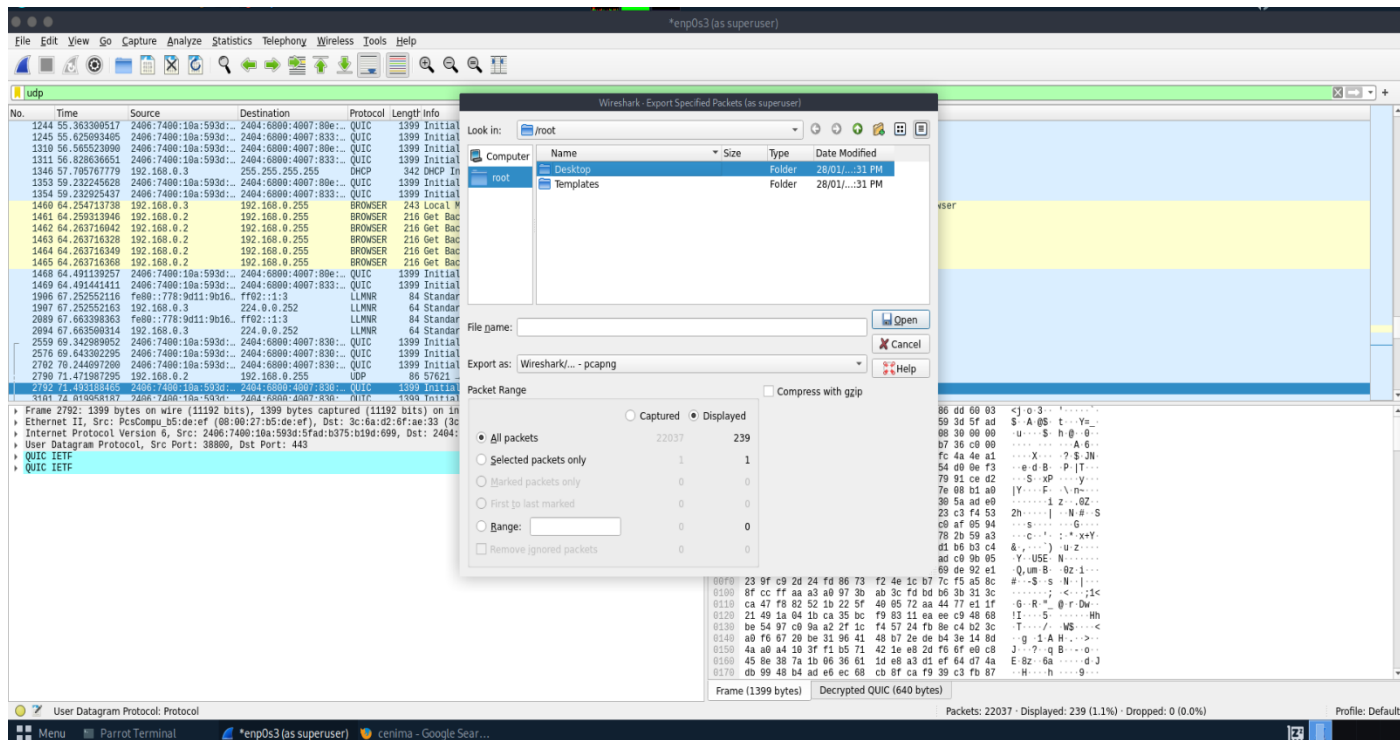
Type: Echo (ping) request

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