

# 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

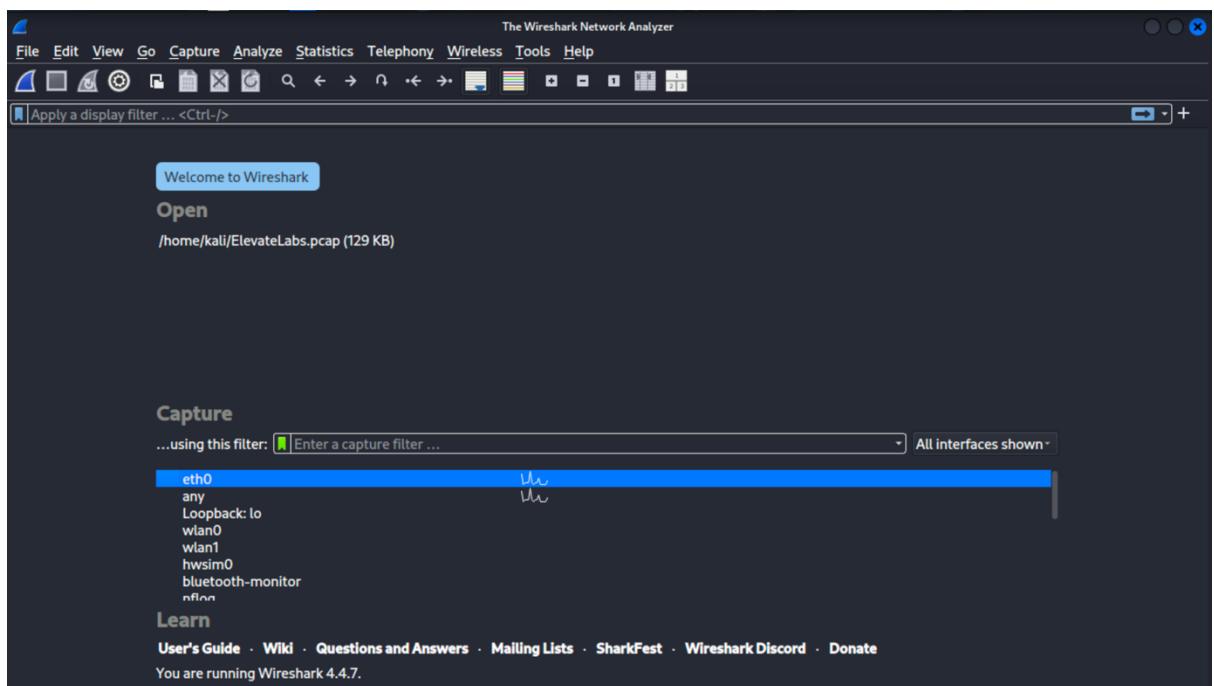
- Involves using tools (e.g., **Wireshark**, **tcpdump**) to **record network traffic**. For this time , I will be using wireshark.
- Captures individual data packets including their **source, destination, protocol, size, and payload**.
- Stored in files like .pcap (Packet Capture) format for later analysis.

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:

No.	Time	Source	Destination	Protocol	Length	Info
35	18.318519	10.0.2.15	10.0.2.3	DNS	70	Standard query 0x8571 A google.com
36	18.318661	10.0.2.15	10.0.2.3	DNS	70	Standard query 0x9f77 AAAA google.com
37	18.329340	10.0.2.3	10.0.2.15	DNS	86	Standard query response 0x8571 A google.com A 142.250.193.142
38	18.329340	10.0.2.3	10.0.2.15	DNS	98	Standard query response 0x9f77 AAAA google.com AAAA 2404:204:204:204:1000:1000:1000:1000
43	18.339761	10.0.2.15	10.0.2.3	DNS	88	Standard query 0x33e4 PTR 142.193.250.142.in-addr.arpa
44	18.363839	10.0.2.3	10.0.2.15	DNS	128	Standard query response 0x33e4 PTR 142.193.250.142.in-addr.arpa
217	59.869949	10.0.2.15	10.0.2.3	DNS	72	Standard query 0xaf7c A y.clarity.ms
218	59.886878	10.0.2.3	10.0.2.15	DNS	153	Standard query response 0xaf7c A y.clarity.ms CNAME vmsse-00000000000000000000000000000000
474	89.601112	10.0.2.15	10.0.2.3	DNS	87	Standard query 0x0e92 A googleads.g.doubleclick.net
475	89.601215	10.0.2.15	10.0.2.3	DNS	87	Standard query 0x8693 AAAA googleads.g.doubleclick.net
476	89.608876	10.0.2.3	10.0.2.15	DNS	103	Standard query response 0x0e92 A googleads.g.doubleclick.net
477	89.610910	10.0.2.3	10.0.2.15	DNS	115	Standard query response 0x8693 AAAA googleads.g.doubleclick.net
551	111.847222	10.0.2.15	10.0.2.3	DNS	72	Standard query 0xcfc2b A y.clarity.ms
552	111.865350	10.0.2.3	10.0.2.15	DNS	153	Standard query response 0xfcfc2b A y.clarity.ms CNAME vmsse-00000000000000000000000000000000
799	172.848671	10.0.2.15	10.0.2.3	DNS	72	Standard query 0x0fff A y.clarity.ms
801	172.856518	10.0.2.3	10.0.2.15	DNS	153	Standard query response 0x0fff A y.clarity.ms CNAME vmsse-00000000000000000000000000000000

Searching DNS protocol using Display Filter:

ElevateLabs.pcap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.171.87.38	10.0.2.15	TLSv1.2	85	Encrypted Alert
2	0.000000	172.171.87.38	10.0.2.15	TCP	60	443 -> 47128 [FIN, ACK] Seq=32 Ack=1 Win=65535 Len=0
3	0.000038	10.0.2.15	172.171.87.38	TCP	54	47128 -> 443 [ACK] Seq=1 Ack=32 Win=65535 Len=0
4	0.000219	10.0.2.15	172.171.87.38	TLSv1.2	85	Encrypted Alert
5	0.000310	10.0.2.15	172.171.87.38	TCP	54	47128 -> 443 [FIN, ACK] Seq=32 Ack=33 Win=65535 Len=0
6	0.000394	172.171.87.38	10.0.2.15	TCP	60	443 -> 47128 [ACK] Seq=33 Ack=32 Win=65535 Len=0
7	0.000394	172.171.87.38	10.0.2.15	TCP	60	443 -> 47128 [ACK] Seq=33 Ack=33 Win=65535 Len=0
8	1.251594	10.0.2.15	172.64.155.119	TLSv1.2	93	Application Data
9	1.251801	172.64.155.119	10.0.2.15	TCP	60	443 -> 50802 [ACK] Seq=1 Ack=40 Win=65535 Len=0
10	1.258937	172.64.155.119	10.0.2.15	TLSv1.2	93	Application Data
11	1.258945	10.0.2.15	172.64.155.119	TCP	54	50802 -> 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
12	2.102927	10.0.2.15	23.10.239.251	TCP	54	38102 -> 80 [ACK] Seq=1 Ack=1 Win=60748 Len=0
13	2.103118	23.10.239.251	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 80 -> 38102 [ACK] Seq=1 Ack=1 Win=60748 Len=0
14	7.991593	10.0.2.15	142.250.194.195	TCP	54	51354 -> 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
15	7.991676	10.0.2.15	142.250.194.195	TCP	54	42574 -> 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16	7.991697	10.0.2.15	142.250.194.195	TCP	54	32852 -> 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
17	7.991728	142.250.194.195	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 80 -> 51354 [ACK] Seq=1 Ack=1 Win=64240 Len=0
18	7.991728	142.250.194.195	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 80 -> 42574 [ACK] Seq=1 Ack=1 Win=64240 Len=0
19	7.991750	142.250.194.195	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 80 -> 32852 [ACK] Seq=1 Ack=1 Win=64240 Len=0
20	8.491663	52.173.199.90	10.0.2.15	TCP	60	443 -> 38884 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
21	12.342896	10.0.2.15	23.10.239.251	TCP	54	[TCP Dup ACK 12#1] 38102 -> 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
22	12.343081	23.10.239.251	10.0.2.15	TCP	60	[TCP Dup ACK 13#1] 80 -> 38102 [ACK] Seq=1 Ack=2 Win=65535 Len=0
23	18.236912	10.0.2.15	142.250.194.195	TCP	54	[TCP Dup ACK 14#1] 51354 -> 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
24	18.236993	10.0.2.15	142.250.194.195	TCP	54	[TCP Dup ACK 15#1] 42574 -> 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
25	18.231011	10.0.2.15	142.250.194.195	TCP	54	[TCP Dup ACK 16#1] 32852 -> 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
26	18.231133	142.250.194.195	10.0.2.15	TCP	60	[TCP Dup ACK 17#1] 80 -> 51354 [ACK] Seq=1 Ack=2 Win=64240 Len=0
27	18.231133	142.250.194.195	10.0.2.15	TCP	60	[TCP Dup ACK 18#1] 80 -> 42574 [ACK] Seq=1 Ack=2 Win=64240 Len=0
28	18.231133	142.250.194.195	10.0.2.15	TCP	60	[TCP Dup ACK 19#1] 80 -> 32852 [ACK] Seq=1 Ack=2 Win=64240 Len=0
29	18.272596	10.0.2.15	104.18.40.222	TLSv1.2	93	Application Data
30	18.272787	104.18.40.222	10.0.2.15	TCP	60	443 -> 38830 [ACK] Seq=1 Ack=40 Win=65525 Len=0

Frame 23: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) 0000 52 55 0a 00 02 02 08 00 27 fc a1 eb 08 00 45 00 RU ...  
 Ethernet II, Src: PCSSystemtec\_fc:a1:eb (08:00:27:fc:a1:eb), Dst: 52.173.199.90 (08:00:27:fc:1a:12) 0010 00 28 55 8a 40 00 40 06 87 79 0a 00 02 0f 8e fa Td 0:0 y  
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.194.195 0020 c2 c3 c8 9a 00 50 b3 8d 2a c7 04 a3 88 9e 50 10 P ...

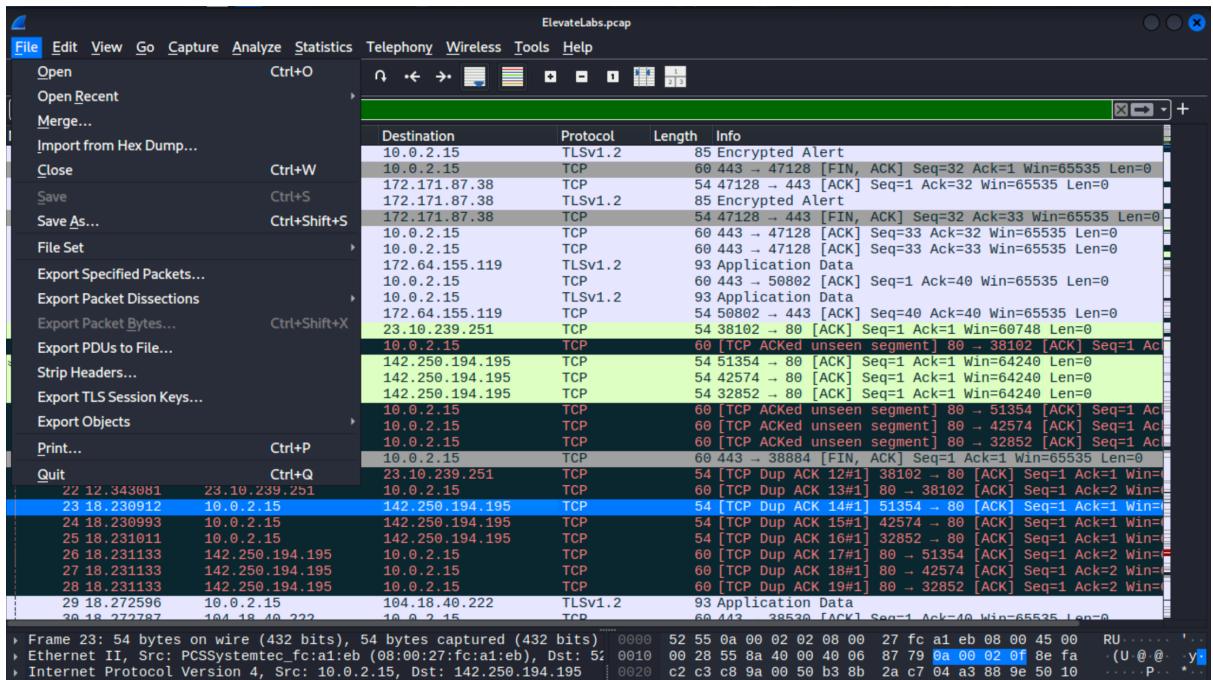
Searching ICMP protocol using Display Filter:

ElevateLabs.pcap

No.	Time	Source	Destination	Protocol	Length	Info
41	18.331395	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (r)
42	18.338376	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=1/256, ttl=255 (r)
56	19.332956	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (r)
57	19.341500	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=2/512, ttl=255 (r)
64	20.334573	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (r)
65	20.342719	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=3/768, ttl=255 (r)
71	21.336018	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (r)
72	21.351993	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=4/1024, ttl=255 (r)
74	22.337243	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (r)
75	22.353299	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=5/1280, ttl=255 (r)
78	23.339099	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=6/1536, ttl=64 (r)
79	23.356175	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=6/1536, ttl=255 (r)
80	24.340467	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=7/1792, ttl=64 (r)
81	24.357590	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=7/1792, ttl=255 (r)
91	25.341730	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=8/2048, ttl=64 (r)
92	25.349715	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=8/2048, ttl=255 (r)
93	26.343034	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=9/2304, ttl=64 (r)
94	26.357340	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=9/2304, ttl=255 (r)
103	27.343618	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=10/2560, ttl=64 (r)
104	27.356542	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=10/2560, ttl=255 (r)
105	28.343945	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=11/2816, ttl=64 (r)
106	28.351357	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=11/2816, ttl=255 (r)
113	29.345540	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=12/3072, ttl=64 (r)
114	29.357805	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=12/3072, ttl=255 (r)
115	30.347381	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=13/3328, ttl=64 (r)
116	30.363705	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=13/3328, ttl=255 (r)
137	31.348787	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=14/3584, ttl=64 (r)
138	31.356771	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=14/3584, ttl=255 (r)
139	32.349860	10.0.2.15	142.250.193.142	ICMP	98	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (r)
140	32.363780	142.250.193.142	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0001, seq=15/3840, ttl=255 (r)

Frame 41: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) 0000 52 55 0a 00 02 02 08 00 27 fc a1 eb 08 00 45 00 RU ...  
 Ethernet II, Src: PCSSystemtec\_fc:a1:eb (08:00:27:fc:a1:eb), Dst: 52.173.199.90 (08:00:27:fc:1a:12) 0010 00 54 64 96 40 00 40 01 79 7b 0a 00 02 0f 8e fa Td 0:0 y  
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.193.142 0020 c1 8e 08 00 39 e2 00 01 00 01 c3 a3 62 68 00 00 ... 9 ...

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