Elevate_Labs_Task_5

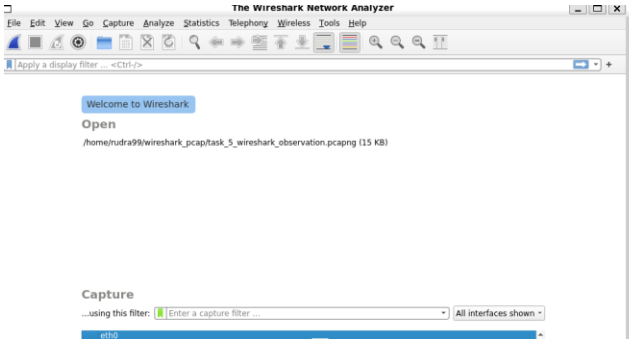
Rudra Srilakshmi

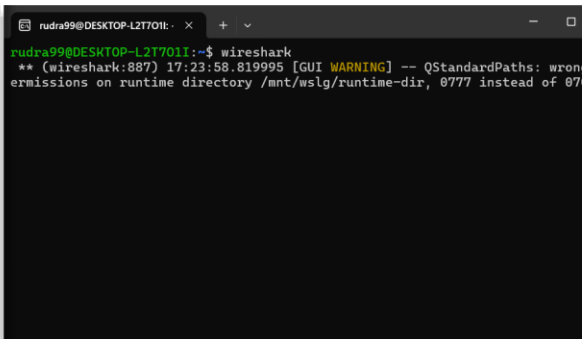
Task 5: Capture and Analyze Network Traffic Using Wireshark

To do this, Using Ubuntu installed and setup Wireshark already

1.Install Wireshark.

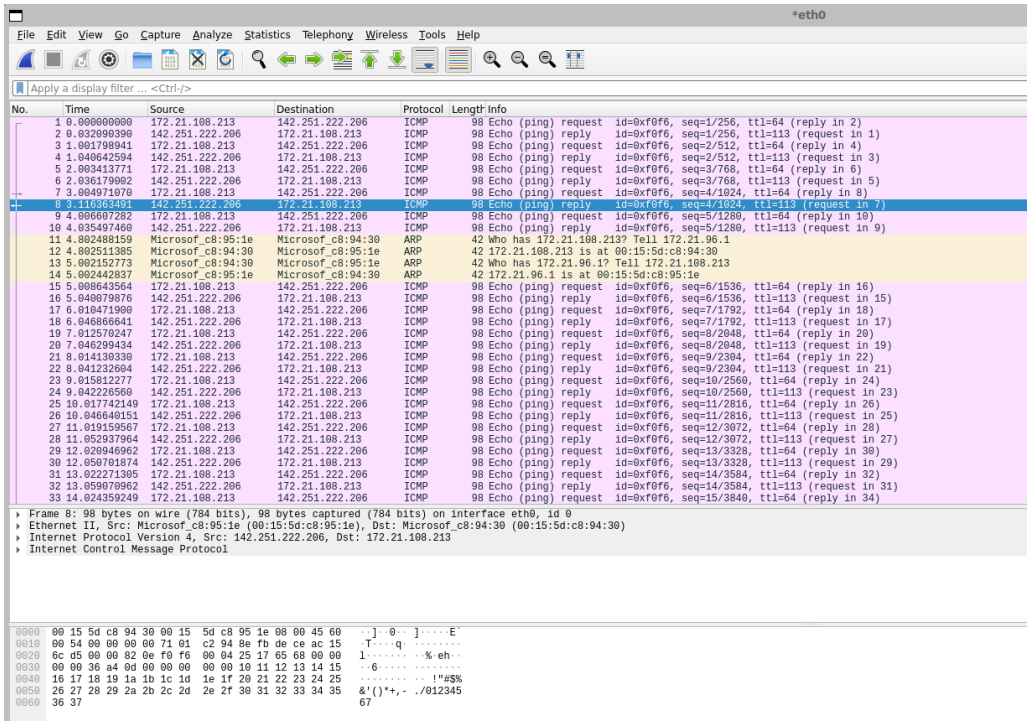
To launch Wireshark, used the command *"wireshark"*





2.Start capturing on your active network interface.

From the list of interfaces, the active interface eth0 was selected.
Live packet capturing began immediately on eth0.



3.Browse a website or ping a server to generate traffic.

To generate traffic, the following commands were executed in the terminal:

“ping google.com” - to generate ICMP traffic

```
rudra99@DESKTOP-L2T7O1I:~$ ping google.com
PING google.com (142.251.222.206) 56(84) bytes of data.
64 bytes from pnmaaa-as-in-f14.1e100.net (142.251.222.206): icmp_seq=1 ttl=113 time=32.1 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=2 ttl=113 time=38.9 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=3 ttl=113 time=32.8 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=4 ttl=113 time=111 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=5 ttl=113 time=28.9 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=6 ttl=113 time=31.5 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=7 ttl=113 time=36.4 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=8 ttl=113 time=33.8 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=9 ttl=113 time=27.1 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=10 ttl=113 time=26.4 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=11 ttl=113 time=28.9 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=12 ttl=113 time=33.8 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=13 ttl=113 time=29.8 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=14 ttl=113 time=36.8 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=15 ttl=113 time=31.8 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=16 ttl=113 time=33.8 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=17 ttl=113 time=24.6 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=18 ttl=113 time=30.1 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=19 ttl=113 time=26.7 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=20 ttl=113 time=26.8 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=21 ttl=113 time=26.8 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=22 ttl=113 time=30.6 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=23 ttl=113 time=28.2 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=24 ttl=113 time=58.4 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=25 ttl=113 time=30.6 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=26 ttl=113 time=25.5 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=27 ttl=113 time=26.9 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=28 ttl=113 time=26.7 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=29 ttl=113 time=27.8 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=30 ttl=113 time=23.9 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=31 ttl=113 time=31.6 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=32 ttl=113 time=28.8 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=33 ttl=113 time=210 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=34 ttl=113 time=31.1 ms
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp_seq=35 ttl=113 time=51.2 ms
^C
--- google.com ping statistics ---
35 packets transmitted, 35 received, 0% packet loss, time 34057ms
rtt min/avg/max/mdev = 23.861/38.862/209.739/32.883 ms
```

“curl http://example.com”- to generate HTTP and DNS traffic

```
rudra99@DESKTOP-L2T7O1I:~$ curl http://example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica,

    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
    </style>
</head>
```

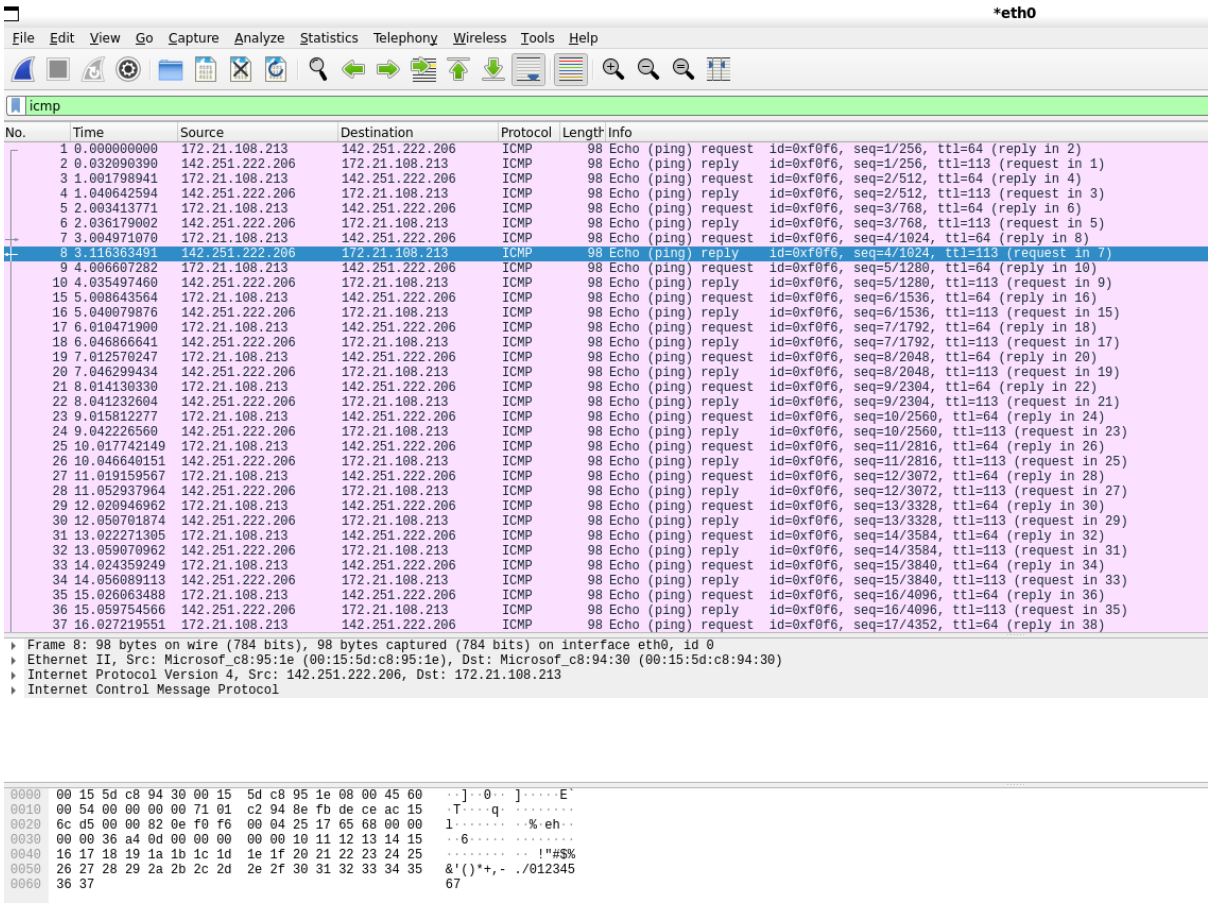
4.Stop capture after a minute.

The capture was left to run for about 60 seconds and then terminated by clicking the red square Stop button in Wireshark.

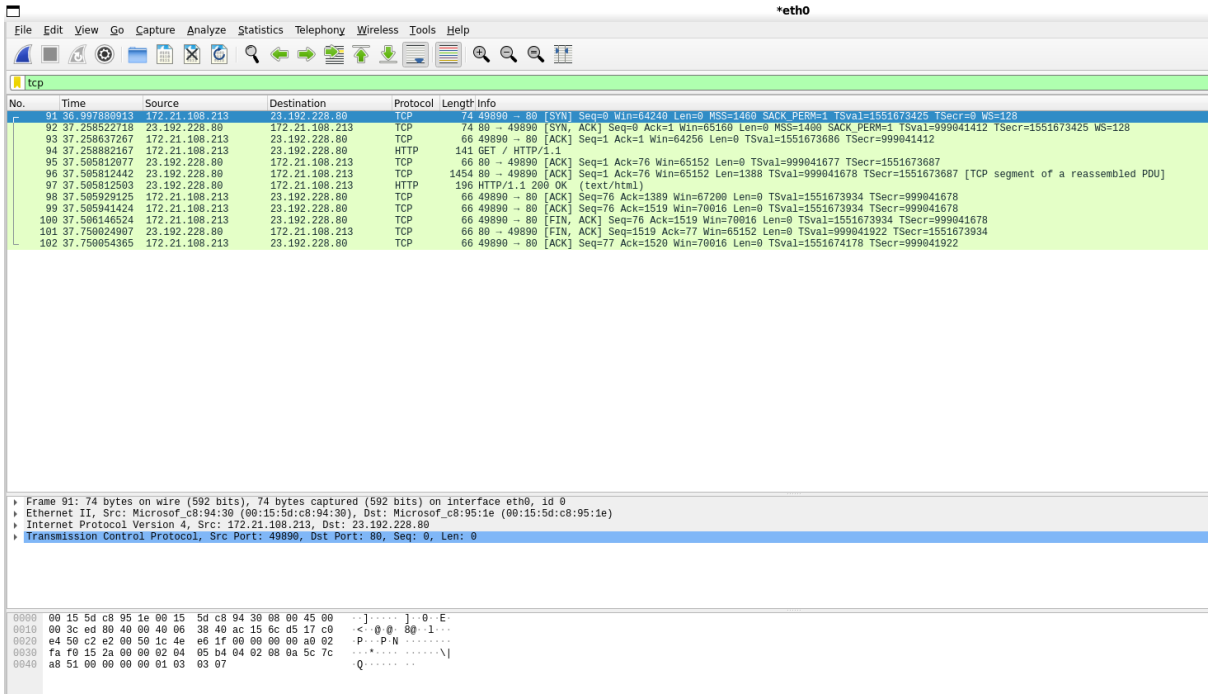
5.Filter captured packets by protocol.

The following filters are used:

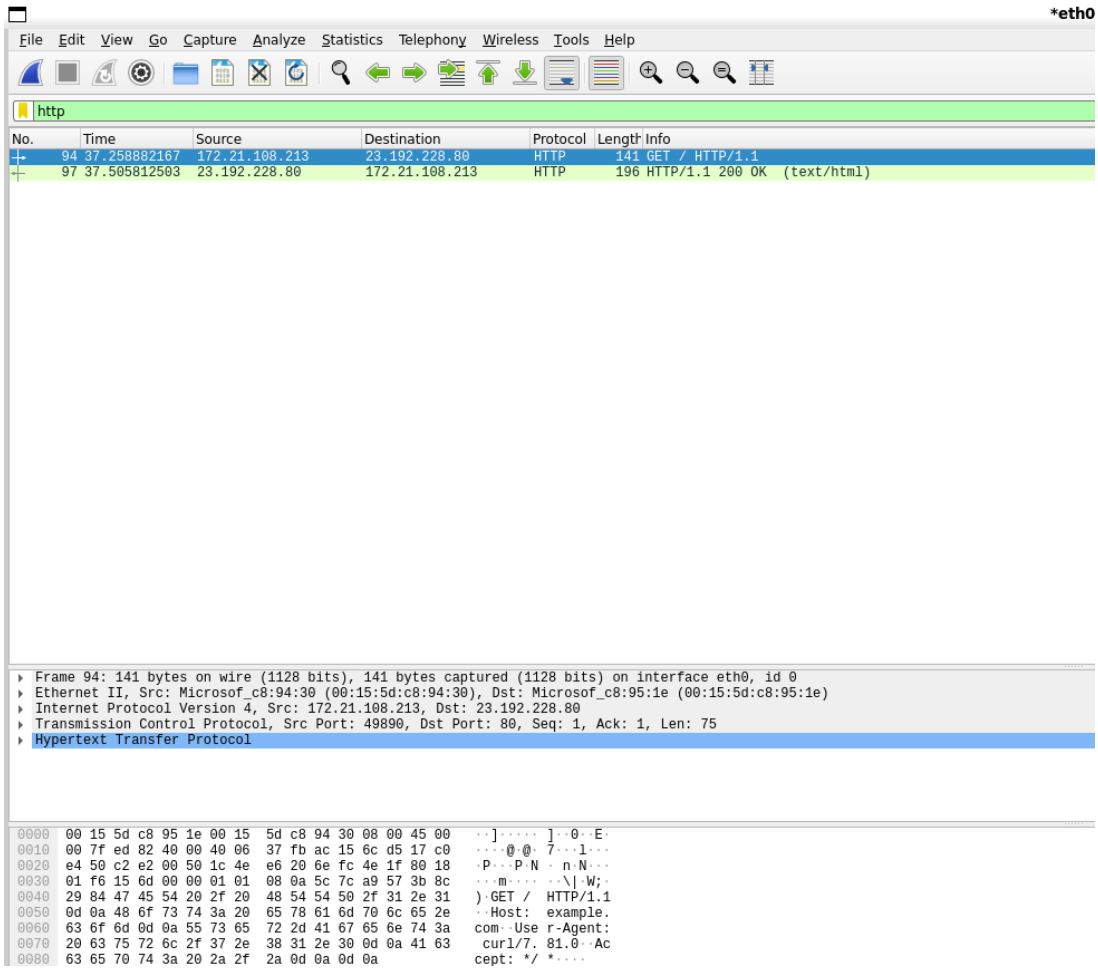
icmp


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
1 0.000000000 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=1/256, ttl=64 (reply in 2)
2 0.032090390 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=1/256, ttl=113 (request in 1)
3 1.001798941 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=2/512, ttl=64 (reply in 4)
4 1.040642594 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=2/512, ttl=113 (request in 3)
5 2.003413771 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=3/768, ttl=64 (reply in 6)
6 2.036179002 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=3/768, ttl=113 (request in 5)
7 3.004971070 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=4/1024, ttl=64 (reply in 8)
8 3.116363491 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=4/1024, ttl=113 (request in 7)
9 4.006607282 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=5/1280, ttl=64 (reply in 10)
10 4.035497460 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=5/1280, ttl=113 (request in 9)
15 5.008643564 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=6/1536, ttl=64 (reply in 16)
16 5.040079876 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=6/1536, ttl=113 (request in 15)
17 6.010471900 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=7/1792, ttl=64 (reply in 18)
18 6.046866641 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=7/1792, ttl=113 (request in 17)
19 7.012570247 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=8/2048, ttl=64 (reply in 20)
20 7.046299434 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=8/2048, ttl=113 (request in 19)
21 8.014130330 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=9/2304, ttl=64 (reply in 22)
22 8.041232604 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=9/2304, ttl=113 (request in 21)
23 9.015812277 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=10/2560, ttl=64 (reply in 24)
24 9.042226560 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=10/2560, ttl=113 (request in 23)
25 10.017742149 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=11/2816, ttl=64 (reply in 26)
26 10.046640151 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=11/2816, ttl=113 (request in 25)
27 11.019159567 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=12/3072, ttl=64 (reply in 28)
28 11.052937964 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=12/3072, ttl=113 (request in 27)
29 12.020946962 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=13/3328, ttl=64 (reply in 30)
30 12.050701874 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=13/3328, ttl=113 (request in 29)
31 13.022271305 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=14/3584, ttl=64 (reply in 32)
32 13.059070962 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=14/3584, ttl=113 (request in 31)
33 14.024359249 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=15/3840, ttl=64 (reply in 34)
34 14.056089113 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=15/3840, ttl=113 (request in 33)
35 15.026063488 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=16/4096, ttl=64 (reply in 36)
36 15.059754566 142.251.222.206 172.21.108.213 ICMP 98 Echo (ping) reply id=0xf0f6, seq=16/4096, ttl=113 (request in 35)
37 16.027219551 172.21.108.213 142.251.222.206 ICMP 98 Echo (ping) request id=0xf0f6, seq=17/4352, ttl=64 (reply in 38)
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_c8:95:1e (00:15:5d:c8:95:1e), Dst: Microsof_c8:94:30 (00:15:5d:c8:94:30)
Internet Protocol Version 4, Src: 142.251.222.206, Dst: 172.21.108.213
Internet Control Message Protocol
0000 00 15 5d c8 94 30 00 15 5d c8 95 1e 08 00 45 60
0010 00 54 00 00 00 00 71 01 c2 94 8e fb de ce ac 15
0020 6c d5 00 00 82 0e f0 f6 00 04 25 17 65 68 00 00
0030 00 00 36 a4 0d 00 00 00 00 00 10 11 12 13 14 15
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
0060 36 37

tcp


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
91 36.997080913 172.21.108.213 23.192.228.80 TCP 74 49890 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1551673425 TSecr=0 WS=128
92 37.258522718 23.192.228.80 172.21.108.213 TCP 74 80 → 49890 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1400 SACK_PERM=1 TSval=999041412 TSecr=1551673425 WS=128
93 37.258637267 172.21.108.213 23.192.228.80 TCP 66 49890 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1551673686 TSecr=999041412
94 37.258882167 172.21.108.213 23.192.228.80 HTTP 141 GET / HTTP/1.1
95 37.505812077 23.192.228.80 172.21.108.213 TCP 66 80 → 49890 [ACK] Seq=1 Ack=76 Win=65152 Len=0 TSval=999041677 TSecr=1551673687
96 37.505812442 23.192.228.80 172.21.108.213 TCP 1454 80 → 49890 [ACK] Seq=1 Ack=76 Win=65152 Len=1388 TSval=999041678 TSecr=1551673687 [TCP segment of a reassembled PDU]
97 37.505812503 23.192.228.80 172.21.108.213 HTTP 196 HTTP/1.1 200 OK (text/html)
98 37.505929125 172.21.108.213 23.192.228.80 TCP 66 49890 → 80 [ACK] Seq=76 Ack=1389 Win=67200 Len=0 TSval=1551673934 TSecr=999041678
99 37.505941424 172.21.108.213 23.192.228.80 TCP 66 49890 → 80 [ACK] Seq=76 Ack=1519 Win=70016 Len=0 TSval=1551673934 TSecr=999041678
100 37.506146524 172.21.108.213 23.192.228.80 TCP 66 49890 → 80 [FIN, ACK] Seq=76 Ack=1519 Win=70016 Len=0 TSval=1551673934 TSecr=999041678
101 37.750024907 23.192.228.80 172.21.108.213 TCP 66 80 → 49890 [FIN, ACK] Seq=1519 Ack=77 Win=65152 Len=0 TSval=999041922 TSecr=1551673934
102 37.750054365 172.21.108.213 23.192.228.80 TCP 66 49890 → 80 [ACK] Seq=77 Ack=1520 Win=70016 Len=0 TSval=1551674178 TSecr=999041922
Frame 91: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_c8:94:30 (00:15:5d:c8:94:30), Dst: Microsof_c8:95:1e (00:15:5d:c8:95:1e)
Internet Protocol Version 4, Src: 172.21.108.213, Dst: 23.192.228.80
Transmission Control Protocol, Src Port: 49890, Dst Port: 80, Seq: 0, Len: 0
0000 00 15 5d c8 95 1e 00 15 5d c8 94 30 08 00 45 00
0010 00 3c ed 80 40 00 40 06 38 40 ac 15 6c d5 17 c0
0020 e4 50 c2 e2 00 50 1c 4e e6 1f 00 00 00 00 a0 02
0030 fa f0 15 2a 00 00 02 04 05 b4 04 02 08 0a 5c 7c
0040 a8 51 00 00 00 00 01 03 03 07

http



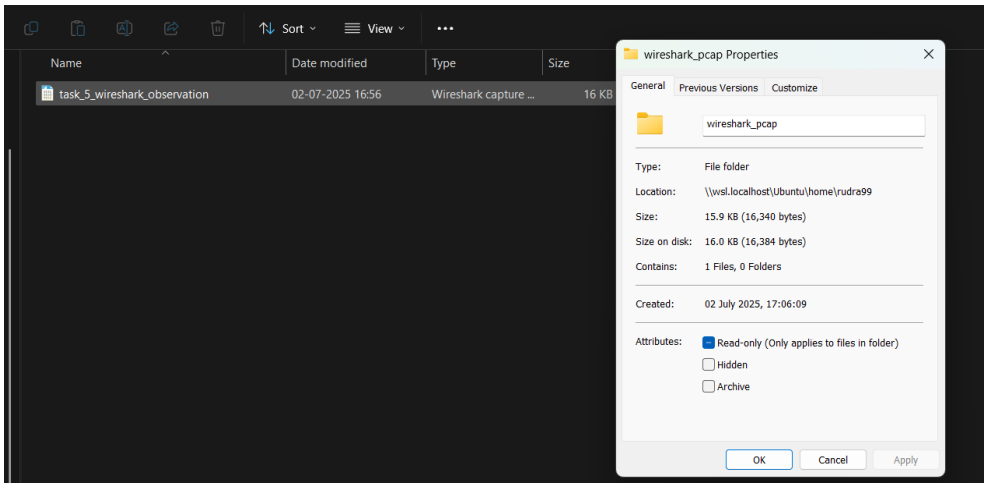
6.Identify at least 3 different protocols in the capture.

The following 4 protocols were identified and analyzed:

Protocol	Filter Used	Description
ICMP	icmp	Ping packets from ping google.com
ARP	arp	Address resolution requests/replies
HTTP	http	Web requests and responses
TCP	tcp	TCP handshake and segment packets

7.Export the capture as a .pcap file.

saved the file as task5_wireshark_observation.pcap



8.Summarize your findings and packet details.

Using Wireshark on Ubuntu on the eth0 interface, a packet capture session was successfully conducted. Generated traffic using ping and curl allowed observation of real-time ICMP, HTTP, TCP, and ARP packets. ICMP packets originated from the ping command, with request and reply messages displayed. ARP packets indicated how IP addresses were being matched with MAC addresses locally. HTTP traffic was intercepted from accessing a website via curl and transmitted over TCP, wherein connection establishment and data transfer were evident and the results were saved in .pcap format.