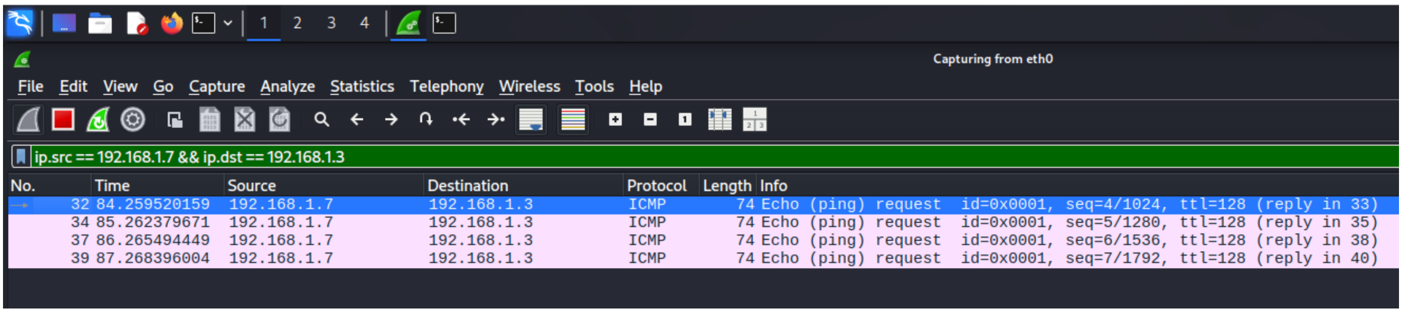
Task 5 : Capture and Analyze Network Traffic Using Wireshark.

Objective: Capture live network packets and identify basic protocols and traffic types.

Tools: Wireshark (free).

Deliverables: A packet capture **(.pcap)** file and a short report of protocols identified.



```
ip.src == 192.168.1.7 && ip.dst == 192.168.1.3
```

```
No.   Time           Source        Destination   Protocol Length Info
   32 84.259520159  192.168.1.7   192.168.1.3   ICMP       74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 33)
   34 85.262379671  192.168.1.7   192.168.1.3   ICMP       74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (reply in 35)
   37 86.265494449  192.168.1.7   192.168.1.3   ICMP       74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (reply in 38)
   39 87.268396004  192.168.1.7   192.168.1.3   ICMP       74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128 (reply in 40)
```

The captured traffic shown in the screenshot is :

1. ICMP (Internet Control Message Protocol) traffic between two IP addresses:

- **Source: 192.168.1.7**
- **Destination: 192.168.1.3**

Protocol Details: ICMP

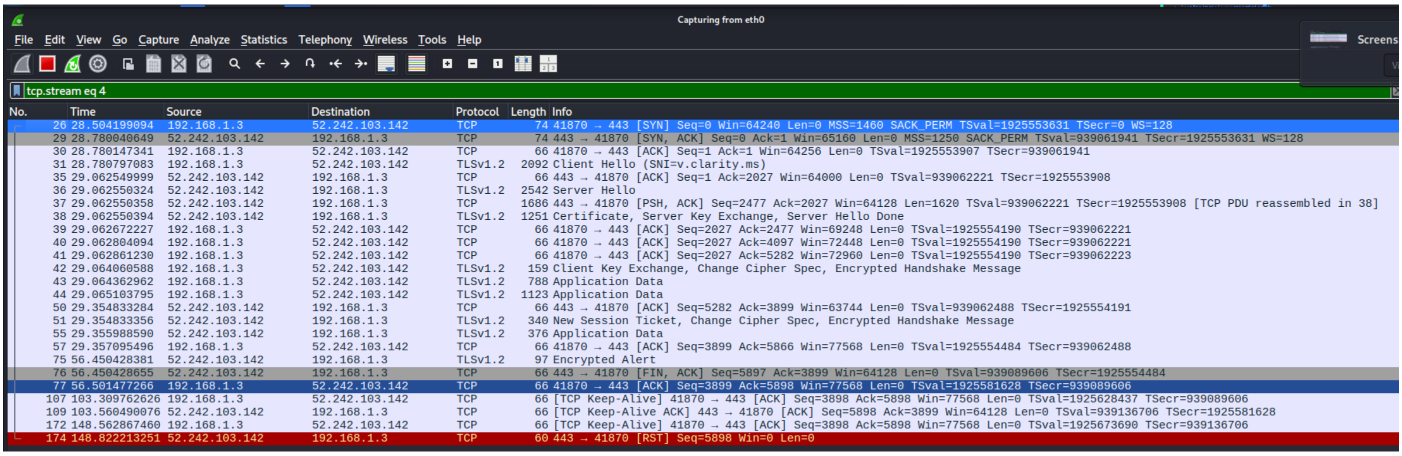
- ICMP is a network-layer protocol used primarily for **diagnostic** or **control purposes.**
- It is commonly used by tools like ping and traceroute **to test connectivity and measure round-trip time between hosts**.
- ICMP messages include types such as Echo Request and Echo Reply, Destination Unreachable, Time Exceeded, etc**.**

Traffic Characteristics in the Capture

- **Echo Request**: Sent by the source (192.168.1.7) to the destination (192.168.1.3) as a "ping" to check if the destination is reachable.
- **Echo Reply**: Sent by the destination (192.168.1.3) back to the source as a response confirming connectivity.

Purpose of This Traffic

- This traffic is typical of **connectivity testing** between two devices on a network.
- It helps determine if the destination host is reachable and measures the response time.


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Screens

tcp.stream eq 4

```
No.  Time           Source          Destination     Protocol Length Info
  26 28.504199094   192.168.1.3     52.242.103.142  TCP        74 41870 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1925553631 TSecr=0 WS=128
  29 28.780040649   52.242.103.142  192.168.1.3     TCP        74 443 → 41870 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1250 SACK_PERM TSval=939061941 TSecr=1925553631 WS=128
  30 28.780147341   192.168.1.3     52.242.103.142  TCP        66 41870 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1925553907 TSecr=939061941
  31 28.780797083   192.168.1.3     52.242.103.142  TLSv1.2  2092 Client Hello (SNI=v.clarity.ms)
  35 29.062549999   52.242.103.142  192.168.1.3     TCP        66 443 → 41870 [ACK] Seq=1 Ack=2027 Win=64000 Len=0 TSval=939062221 TSecr=1925553908
  36 29.062550324   52.242.103.142  192.168.1.3     TLSv1.2  2542 Server Hello
  37 29.062550358   52.242.103.142  192.168.1.3     TCP      1686 443 → 41870 [PSH, ACK] Seq=2477 Ack=2027 Win=64128 Len=1620 TSval=939062221 TSecr=1925553908 [TCP PDU reassembled in 38]
  38 29.062550394   52.242.103.142  192.168.1.3     TLSv1.2  1251 Certificate, Server Key Exchange, Server Hello Done
  39 29.062672227   192.168.1.3     52.242.103.142  TCP        66 41870 → 443 [ACK] Seq=2027 Ack=2477 Win=69248 Len=0 TSval=1925554190 TSecr=939062221
  40 29.062804094   192.168.1.3     52.242.103.142  TCP        66 41870 → 443 [ACK] Seq=2027 Ack=4097 Win=72448 Len=0 TSval=1925554190 TSecr=939062221
  41 29.062861230   192.168.1.3     52.242.103.142  TCP        66 41870 → 443 [ACK] Seq=2027 Ack=5282 Win=72960 Len=0 TSval=1925554190 TSecr=939062223
  42 29.064060588   192.168.1.3     52.242.103.142  TLSv1.2   159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  43 29.064362962   192.168.1.3     52.242.103.142  TLSv1.2   788 Application Data
  44 29.065103795   192.168.1.3     52.242.103.142  TLSv1.2  1123 Application Data
  50 29.354833284   52.242.103.142  192.168.1.3     TCP        66 443 → 41870 [ACK] Seq=5282 Ack=3899 Win=63744 Len=0 TSval=939062488 TSecr=1925554191
  51 29.354833356   52.242.103.142  192.168.1.3     TLSv1.2   340 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
  55 29.355988590   52.242.103.142  192.168.1.3     TLSv1.2   376 Application Data
  57 29.357095496   192.168.1.3     52.242.103.142  TCP        66 41870 → 443 [ACK] Seq=3899 Ack=5866 Win=77568 Len=0 TSval=1925554484 TSecr=939062488
  75 56.450428381   52.242.103.142  192.168.1.3     TLSv1.2    97 Encrypted Alert
  76 56.450428655   52.242.103.142  192.168.1.3     TCP        66 443 → 41870 [FIN, ACK] Seq=5897 Ack=3899 Win=64128 Len=0 TSval=939089606 TSecr=1925554484
  77 56.501477266   192.168.1.3     52.242.103.142  TCP        66 41870 → 443 [ACK] Seq=3899 Ack=5898 Win=77568 Len=0 TSval=1925581628 TSecr=939089606
 107 103.309762626  192.168.1.3     52.242.103.142  TCP        66 [TCP Keep-Alive] 41870 → 443 [ACK] Seq=3898 Ack=5898 Win=77568 Len=0 TSval=1925628437 TSecr=939089606
 109 103.560490076  52.242.103.142  192.168.1.3     TCP        66 [TCP Keep-Alive ACK] 443 → 41870 [ACK] Seq=5898 Ack=3899 Win=64128 Len=0 TSval=939136706 TSecr=1925581628
 172 148.562867460  192.168.1.3     52.242.103.142  TCP        66 [TCP Keep-Alive] 41870 → 443 [ACK] Seq=3898 Ack=5898 Win=77568 Len=0 TSval=1925673690 TSecr=939136706
 174 148.822213251  52.242.103.142  192.168.1.3     TCP        60 443 → 41870 [RST] Seq=5898 Win=0 Len=0
```

The captured traffic in the screenshot is :

Protocols Observed

- **TCP (Transmission Control Protocol):**
  - Provides reliable, ordered, and error-checked delivery of data.
  - Used here for establishing and maintaining a connection between the two hosts.
- **TLSv1.2 (Transport Layer Security):**
  - Cryptographic protocol for secure communications over a computer network.
  - Used here to encrypt the session after the TCP connection is established.

Step-by-Step Process

1. TCP Three-Way Handshake

- **Packet 26:** 192.168.1.3 → 52.242.103.142 [SYN]
  - Initiates a TCP connection (SYN flag set).
- **Packet 27:** 52.242.103.142 → 192.168.1.3 [SYN, ACK]
  - Server acknowledges the SYN and responds with SYN, ACK.
- **Packet 28:** 192.168.1.3 → 52.242.103.142 [ACK]
  - Client acknowledges the SYN, ACK, completing the handshake.

2. TLS Handshake

- **Packet 29 onwards:** TLS negotiation begins.
  - **Client Hello:** Client proposes security parameters.
  - **Server Hello, Certificate, Key Exchange:** Server responds, sends its certificate, and establishes encryption keys.
  - **Encrypted Handshake Message:** Both sides exchange encrypted handshake messages to confirm keys and parameters.

3. Secure Data Exchange

- **Packets 41–45, 75:** Application data is exchanged securely using TLS encryption.
    - This includes encrypted HTTP (HTTPS) traffic, file transfers, or other secure communications.

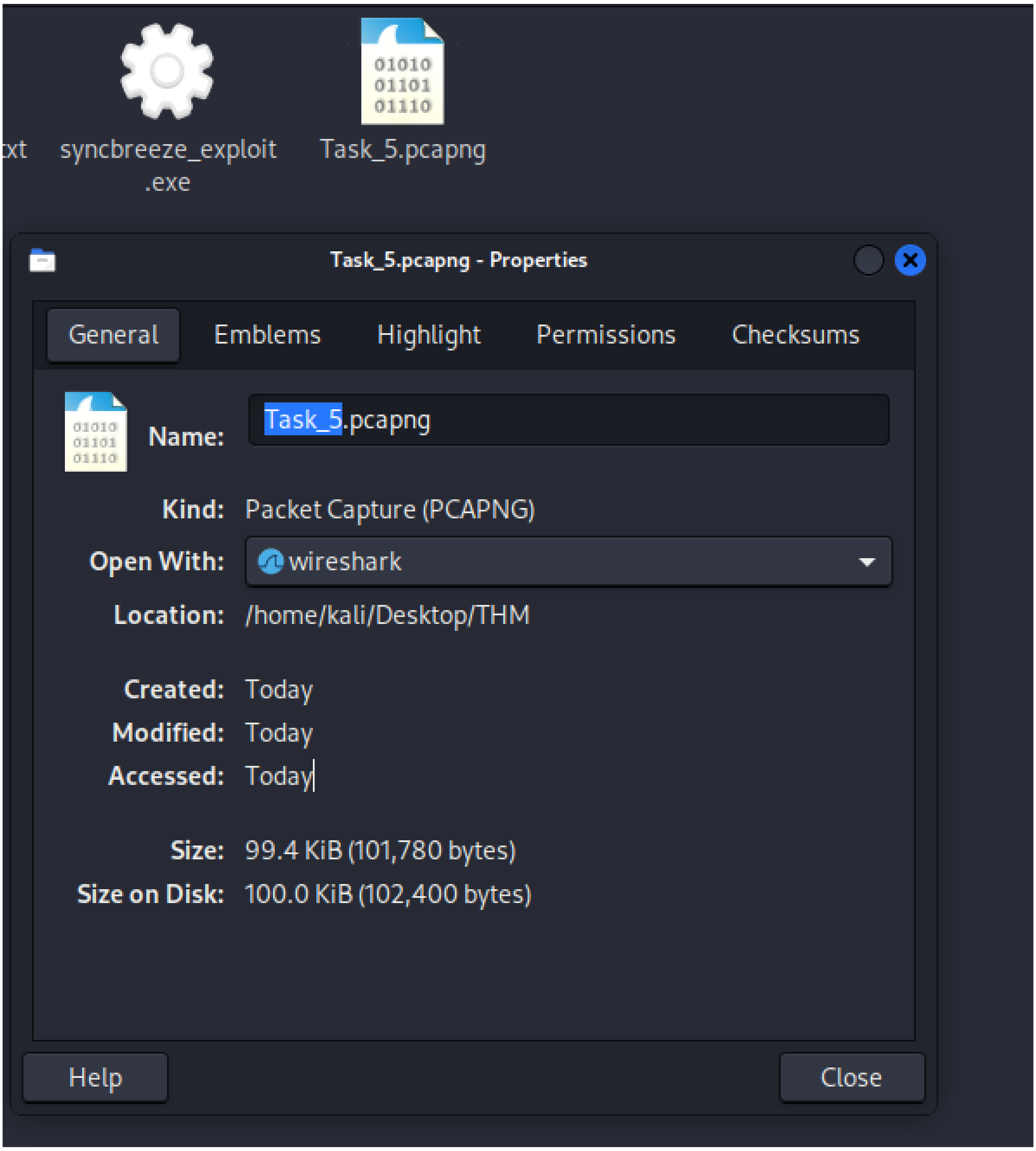
4. Connection Maintenance

- **Packets 109–112:** TCP Keep-Alive packets are exchanged to maintain the session if there is a period of inactivity.

5. Connection Termination

- **Packet 174:** 52.242.103.142 → 192.168.1.3 [RST]
    - The server resets the connection, ending the session.

Captured Pcap file of the traffic



Name: Task_5.pcapng

Kind: Packet Capture (PCAPNG)

Open With: wireshark

Location: /home/kali/Desktop/THM

Created: Today

Modified: Today

Accessed: Today

Size: 99.4 KiB (101,780 bytes)

Size on Disk: 100.0 KiB (102,400 bytes)