Cyber security internship

Elevate Labs

Task 2: Networking Basics for Cyber Security

Basic Networking Concepts Learned

4.1 IP Address

- IP address uniquely identifies a device on a network.
- Example: 192.168.1.5 (private/local IP)

4.2 MAC Address

- MAC address is the physical hardware address of a network adapter.
- Used mainly in LAN communication.

4.3 DNS (Domain Name System)

- Converts a website name like google.com into an IP address.
- DNS is very important in cybersecurity because attackers may redirect DNS traffic.

4.4 TCP and UDP

TCP (Transmission Control Protocol)

- Connection-oriented
- Reliable communication
- Uses handshake (SYN, SYN-ACK, ACK)

UDP (User Datagram Protocol)

- Connectionless
- Faster but not reliable
- Used in streaming, gaming, etc.

---

5. Procedure / Steps Followed

Step 1: Wireshark Installation

- Installed Wireshark on the system.
- Selected required drivers (Npcap) to capture packets.

Step 2: Capturing Live Traffic

1. Opened Wireshark
2. Selected active network interface (Wi-Fi / Ethernet)
3. Clicked **Start Capture**
4. Browsed websites and used internet services to generate traffic

Step 3: Applying Filters

To analyze specific traffic, protocol filters were used:

Protocol	Filter Used
DNS	dns
TCP	tcp
UDP	udp
HTTP	http
HTTPS	tls OR ssl

Step 4: TCP Three-Way Handshake Observation

To observe handshake packets:

- Applied filter: tcp
- Observed these packets:

1. **SYN**
2. **SYN-ACK**
3. **ACK**

This handshake confirms that a TCP connection is successfully established.

Step 5: Plain-Text vs Encrypted Traffic

- Plain-text traffic is readable in captured packets.
- Encrypted traffic cannot be read directly.

Examples:

- **HTTP** → Plain-text traffic
- **HTTPS (TLS)** → Encrypted traffic

---

6. Observations / Analysis

6.1 TCP Handshake Details

I observed TCP handshake when I opened a website or used any internet service.

Packet	**Meaning**
SYN	Client requests connection
SYN-ACK	Server accepts connection
ACK	Client confirms connection

This is important in cybersecurity because:

- Attackers may abuse SYN packets in **SYN flood attacks (DoS attack)**.

6.2 DNS Query Analysis

To view DNS queries:

- Used filter: dns

I noticed that whenever I typed a website name, DNS query packets were generated.

Example:

- Query: A record for google.com
- Response: IP address returned by DNS server

DNS analysis is useful because:

- Suspicious domains can indicate malware activity.
- DNS tunneling is used in data theft attacks.

6.3 Plain-Text Traffic vs Encrypted Traffic

Plain-text traffic example (HTTP):

- Website content like URL paths and some data can be visible.

Encrypted traffic example (HTTPS/TLS):

- Only handshake and certificate details visible.
- Actual content is hidden.

This shows why HTTPS is important to prevent:

- Password sniffing
- Session hijacking
- Sensitive data leakage

---

7. Packet Capture Saving

After capturing traffic:

1. Clicked **File → Save As**
2. Saved in format: **.pcapng**

Packet capture files are useful for:

- Forensic investigations
- Security monitoring
- Incident response evidence

---

8. Key Learnings

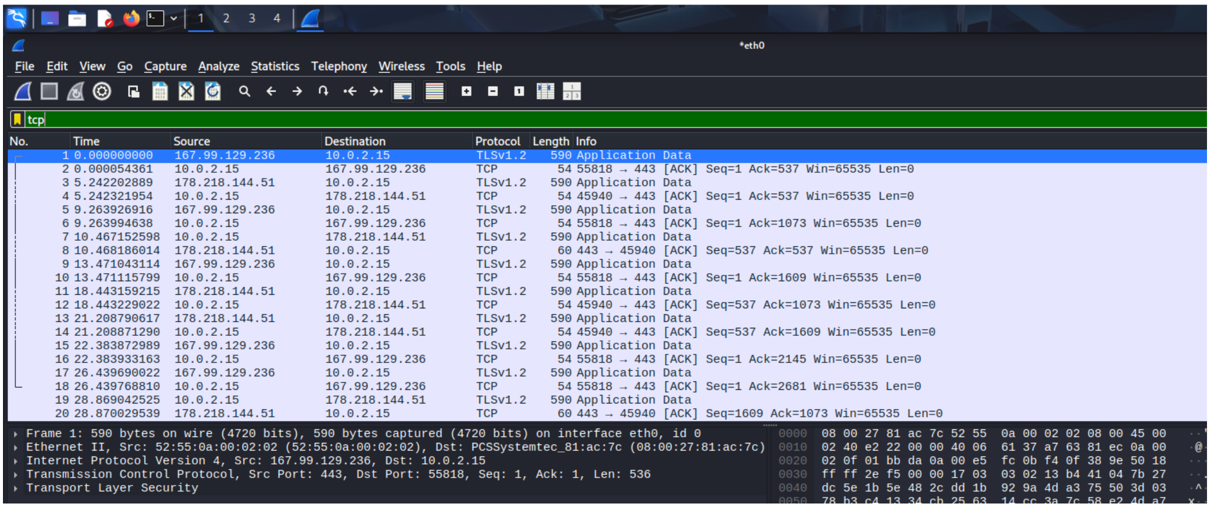
From this task, I learned:

- How to capture and analyze network packets

- How DNS works when visiting websites
- How TCP handshake occurs in real traffic
- Difference between HTTP and HTTPS traffic
- How packet analysis supports cybersecurity investigations

9. Conclusion

This task helped me understand basic networking and how it is related to cyber security. Using Wireshark, I captured live network traffic and learned how data travels between devices. I also learned how cyber security teams check insecure traffic, DNS queries, and TCP connections

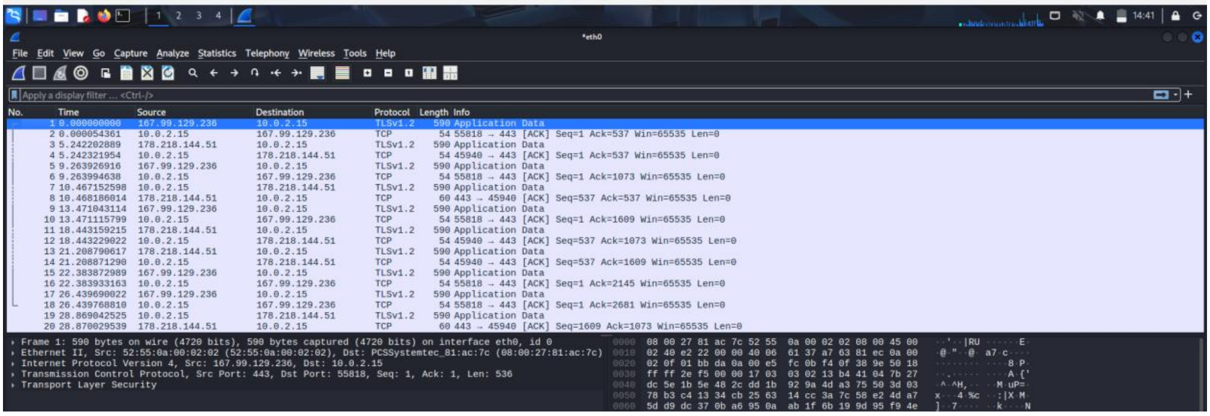


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.   Time          Source           Destination      Protocol Length Info
    1 0.000000000   167.99.129.236   10.0.2.15        TLSv1.2    590 Application Data
    2 0.000054361   10.0.2.15        167.99.129.236   TCP         54 55818 → 443 [ACK] Seq=1 Ack=537 Win=65535 Len=0
    3 5.242202889   178.218.144.51   10.0.2.15        TLSv1.2    590 Application Data
    4 5.242321954   10.0.2.15        178.218.144.51   TCP         54 45940 → 443 [ACK] Seq=1 Ack=537 Win=65535 Len=0
    5 9.263926916   167.99.129.236   10.0.2.15        TLSv1.2    590 Application Data
    6 9.263994638   10.0.2.15        167.99.129.236   TCP         54 55818 → 443 [ACK] Seq=1 Ack=1073 Win=65535 Len=0
    7 10.467152598  10.0.2.15        178.218.144.51   TLSv1.2    590 Application Data
    8 10.468186014  178.218.144.51   10.0.2.15        TCP         60 443 → 45940 [ACK] Seq=537 Ack=537 Win=65535 Len=0
    9 13.471043114  167.99.129.236   10.0.2.15        TLSv1.2    590 Application Data
   10 13.471115799  10.0.2.15        167.99.129.236   TCP         54 55818 → 443 [ACK] Seq=1 Ack=1609 Win=65535 Len=0
   11 18.443159215  178.218.144.51   10.0.2.15        TLSv1.2    590 Application Data
   12 18.443229022  10.0.2.15        178.218.144.51   TCP         54 45940 → 443 [ACK] Seq=537 Ack=1073 Win=65535 Len=0
   13 21.208790617  178.218.144.51   10.0.2.15        TLSv1.2    590 Application Data
   14 21.208871290  10.0.2.15        178.218.144.51   TCP         54 45940 → 443 [ACK] Seq=537 Ack=1609 Win=65535 Len=0
   15 22.383872989  167.99.129.236   10.0.2.15        TLSv1.2    590 Application Data
   16 22.383933163  10.0.2.15        167.99.129.236   TCP         54 55818 → 443 [ACK] Seq=1 Ack=2145 Win=65535 Len=0
   17 26.439690022  167.99.129.236   10.0.2.15        TLSv1.2    590 Application Data
   18 26.439768810  10.0.2.15        167.99.129.236   TCP         54 55818 → 443 [ACK] Seq=1 Ack=2681 Win=65535 Len=0
   19 28.869042525  10.0.2.15        178.218.144.51   TLSv1.2    590 Application Data
   20 28.870029539  178.218.144.51   10.0.2.15        TCP         60 443 → 45940 [ACK] Seq=1609 Ack=1073 Win=65535 Len=0
```

```
› Frame 1: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface eth0, id 0
› Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_81:ac:7c (08:00:27:81:ac:7c)
› Internet Protocol Version 4, Src: 167.99.129.236, Dst: 10.0.2.15
› Transmission Control Protocol, Src Port: 443, Dst Port: 55818, Seq: 1, Ack: 1, Len: 536
› Transport Layer Security
```

```
0000  08 00 27 81 ac 7c 52 55  0a 00 02 02 08 00 45 00
0010  02 40 e2 22 00 00 40 06  61 37 a7 63 81 ec 0a 00
0020  02 0f 01 bb da 0a 00 e5  fc 0b f4 0f 38 9e 50 18
0030  ff ff 2e f5 00 00 17 03  03 02 13 b4 41 04 7b 27
0040  dc 5e 1b 5e 48 2c dd 1b  92 9a 4d a3 75 50 3d 03
0050  78 b3 c4 13 34 cb 25 63  14 cc 3a 7c 58 e2 4d a7
```

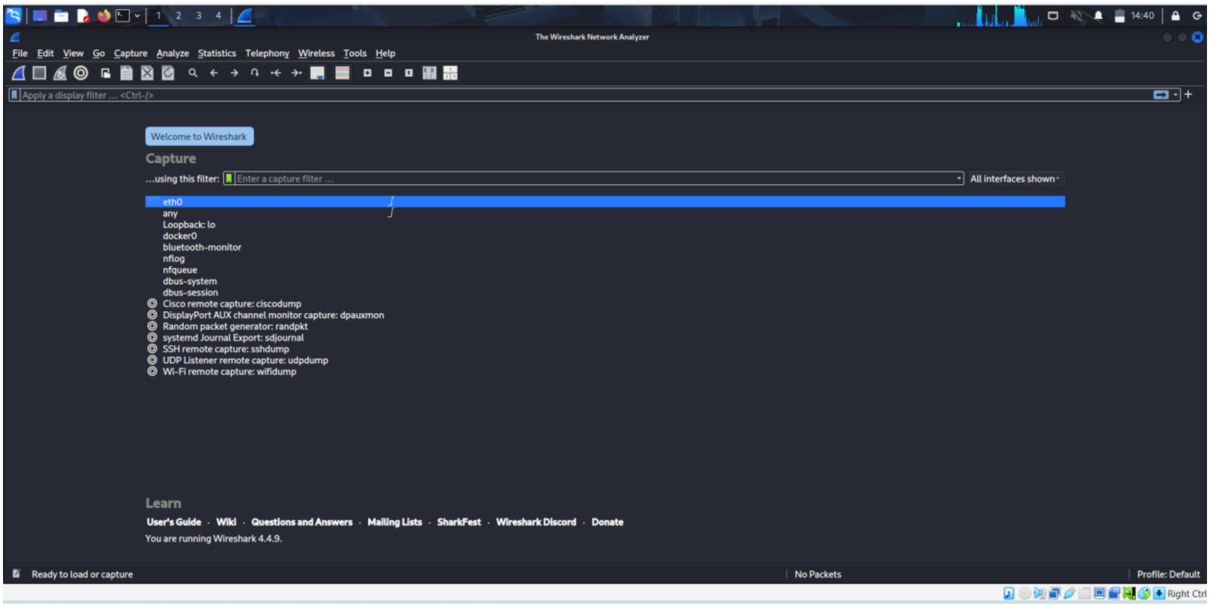


1 2 3 4
14:41
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source           Destination      Protocol Length Info
    1 0.000000000   167.99.129.236   10.0.2.15        TLSv1.2    590 Application Data
    2 0.000054361   10.0.2.15        167.99.129.236   TCP         54 55818 → 443 [ACK] Seq=1 Ack=537 Win=65535 Len=0
    3 5.242202889   178.218.144.51   10.0.2.15        TLSv1.2    590 Application Data
    4 5.242321954   10.0.2.15        178.218.144.51   TCP         54 45940 → 443 [ACK] Seq=1 Ack=537 Win=65535 Len=0
    5 9.263926916   167.99.129.236   10.0.2.15        TLSv1.2    590 Application Data
    6 9.263994638   10.0.2.15        167.99.129.236   TCP         54 55818 → 443 [ACK] Seq=1 Ack=1073 Win=65535 Len=0
    7 10.467152598  10.0.2.15        178.218.144.51   TLSv1.2    590 Application Data
    8 10.468186014  178.218.144.51   10.0.2.15        TCP         60 443 → 45940 [ACK] Seq=537 Ack=537 Win=65535 Len=0
    9 13.471043114  167.99.129.236   10.0.2.15        TLSv1.2    590 Application Data
   10 13.471115799  10.0.2.15        167.99.129.236   TCP         54 55818 → 443 [ACK] Seq=1 Ack=1609 Win=65535 Len=0
   11 18.443159215  178.218.144.51   10.0.2.15        TLSv1.2    590 Application Data
   12 18.443229022  10.0.2.15        178.218.144.51   TCP         54 45940 → 443 [ACK] Seq=537 Ack=1073 Win=65535 Len=0
   13 21.208790617  178.218.144.51   10.0.2.15        TLSv1.2    590 Application Data
   14 21.208871290  10.0.2.15        178.218.144.51   TCP         54 45940 → 443 [ACK] Seq=537 Ack=1609 Win=65535 Len=0
   15 22.383872989  167.99.129.236   10.0.2.15        TLSv1.2    590 Application Data
   16 22.383933163  10.0.2.15        167.99.129.236   TCP         54 55818 → 443 [ACK] Seq=1 Ack=2145 Win=65535 Len=0
   17 26.439690022  167.99.129.236   10.0.2.15        TLSv1.2    590 Application Data
   18 26.439768810  10.0.2.15        167.99.129.236   TCP         54 55818 → 443 [ACK] Seq=1 Ack=2681 Win=65535 Len=0
   19 28.869042525  10.0.2.15        178.218.144.51   TLSv1.2    590 Application Data
   20 28.870029539  178.218.144.51   10.0.2.15        TCP         60 443 → 45940 [ACK] Seq=1609 Ack=1073 Win=65535 Len=0
```

```
› Frame 1: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface eth0, id 0
› Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_81:ac:7c (08:00:27:81:ac:7c)
› Internet Protocol Version 4, Src: 167.99.129.236, Dst: 10.0.2.15
› Transmission Control Protocol, Src Port: 443, Dst Port: 55818, Seq: 1, Ack: 1, Len: 536
› Transport Layer Security
```

```
0000  08 00 27 81 ac 7c 52 55  0a 00 02 02 08 00 45 00   ··'··|RU ······E·
0010  02 40 e2 22 00 00 40 06  61 37 a7 63 81 ec 0a 00   ·@·"··@· a7·c····
0020  02 0f 01 bb da 0a 00 e5  fc 0b f4 0f 38 9e 50 18   ········ ····8·P·
0030  ff ff 2e f5 00 00 17 03  03 02 13 b4 41 04 7b 27   ··.····· ····A·{'
0040  dc 5e 1b 5e 48 2c dd 1b  92 9a 4d a3 75 50 3d 03   ·^·^H,·· ··M·uP=·
0050  78 b3 c4 13 34 cb 25 63  14 cc 3a 7c 58 e2 4d a7   x···4·%c ··:|X·M·
0060  5d d9 dc 37 0b a6 95 0a  ab 1f 6b 19 9d 95 f9 4e   ]··7···· ··k····N
```


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
14:40
Right Ctrl

Apply a display filter … <Ctrl-/>

Welcome to Wireshark

Capture

…using this filter: Enter a capture filter … All interfaces shown

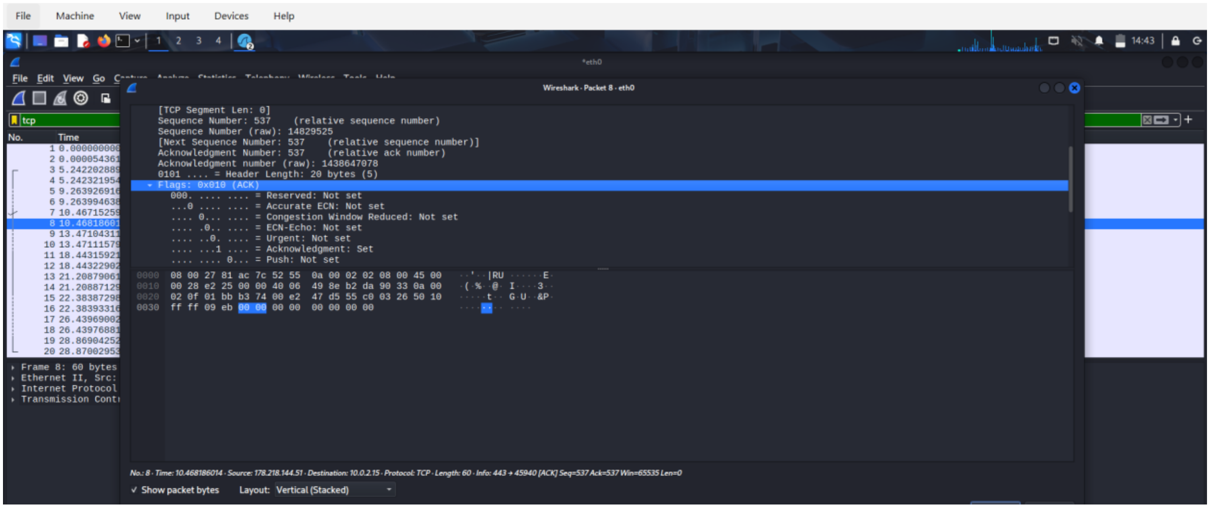
```
eth0
any
Loopback: lo
docker0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
```

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.4.9.

Ready to load or capture | No Packets | Profile: Default


File Machine View Input Devices Help
14:43
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 8 · eth0

tcp

```
No.  Time
  1 0.00000000
  2 0.00005436
  3 5.24220288
  4 5.24232195
  5 9.26392691
  6 9.26399463
  7 10.4671525
  8 10.4681860
  9 13.4710431
 10 13.4711157
 11 18.4431592
 12 18.4432290
 13 21.2087906
 14 21.2088712
 15 22.3838729
 16 22.3839331
 17 26.4396900
 18 26.4397688
 19 28.8690425
 20 28.8700295
```

```
› Frame 8: 60 bytes
› Ethernet II, Src:
› Internet Protocol
› Transmission Contr
```

```
    [TCP Segment Len: 0]
    Sequence Number: 537    (relative sequence number)
    Sequence Number (raw): 14829525
    [Next Sequence Number: 537    (relative sequence number)]
    Acknowledgment Number: 537    (relative ack number)
    Acknowledgment number (raw): 1438647078
    0101 .... = Header Length: 20 bytes (5)
  ▾ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
```

```
0000  08 00 27 81 ac 7c 52 55  0a 00 02 02 08 00 45 00   ··'··|RU ······E·
0010  00 28 e2 25 00 00 40 06  49 8e b2 da 90 33 0a 00   ·(·%··@· I····3··
0020  02 0f 01 bb b3 74 00 e2  47 d5 55 c0 03 26 50 10   ·····t·· G·U··&P·
0030  ff ff 09 eb 00 00 00 00  00 00 00 00               ········ ····
```

No.: 8 · Time: 10.468186014 · Source: 178.218.144.51 · Destination: 10.0.2.15 · Protocol: TCP · Length: 60 · Info: 443 → 45940 [ACK] Seq=537 Ack=537 Win=65535 Len=0

✓ Show packet bytes   Layout: Vertical (Stacked)