

Task 3: Networking Basics for Cyber Security

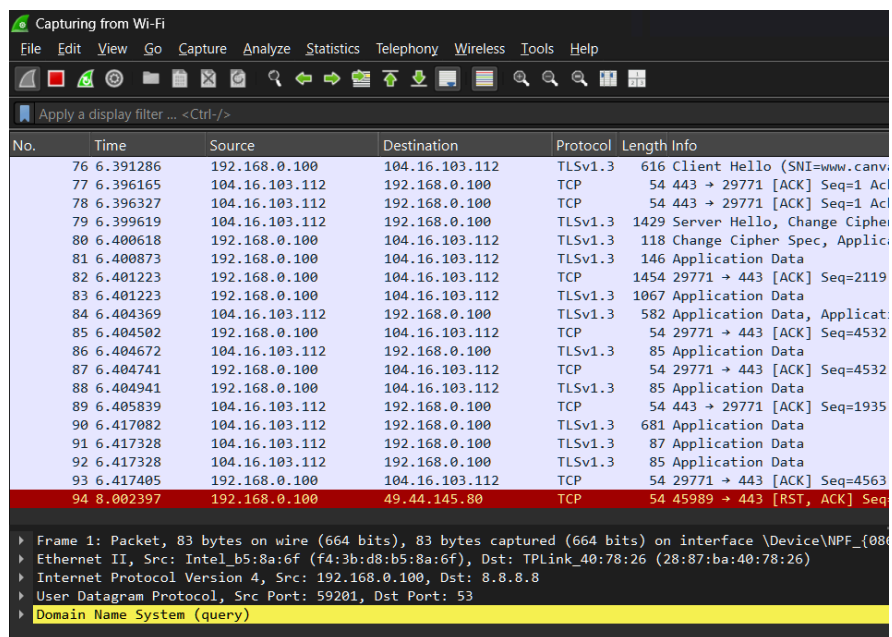
Task Execution

1. Learn Basic Networking Concepts

- IP Address: Identifies a device on a network.
- MAC Address: Physical address of a network interface.
- DNS: Resolves domain names into IP addresses.
- TCP: Reliable, connection-oriented protocol.
- UDP: Fast, connectionless protocol.

2. Capture Live Network Traffic

- Install Wireshark.
- Run Wireshark as administrator.
- Select an active network interface (Wi-Fi or Ethernet).
- Start capturing live packets.



The image shows the Wireshark network traffic capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. A display filter bar shows 'Apply a display filter ... <Ctrl-/>'. The main packet list table has columns for No., Time, Source, Destination, Protocol, and Length Info. The table contains 94 packets, with the last packet (No. 94) highlighted in red. The detailed view pane at the bottom shows the structure of the selected packet (No. 94), which is a DNS query. The structure is as follows:

No.	Time	Source	Destination	Protocol	Length Info
76	6.391286	192.168.0.100	104.16.103.112	TLSv1.3	616 Client Hello (SNI=www.canv...
77	6.396165	104.16.103.112	192.168.0.100	TCP	54 443 → 29771 [ACK] Seq=1 Acl
78	6.396327	104.16.103.112	192.168.0.100	TCP	54 443 → 29771 [ACK] Seq=1 Acl
79	6.399619	104.16.103.112	192.168.0.100	TLSv1.3	1429 Server Hello, Change Ciph...
80	6.400618	192.168.0.100	104.16.103.112	TLSv1.3	118 Change Cipher Spec, Applic...
81	6.400873	192.168.0.100	104.16.103.112	TLSv1.3	146 Application Data
82	6.401223	192.168.0.100	104.16.103.112	TCP	1454 29771 → 443 [ACK] Seq=2119
83	6.401223	192.168.0.100	104.16.103.112	TLSv1.3	1067 Application Data
84	6.404369	104.16.103.112	192.168.0.100	TLSv1.3	582 Application Data, Applicat...
85	6.404502	192.168.0.100	104.16.103.112	TCP	54 29771 → 443 [ACK] Seq=4532
86	6.404672	104.16.103.112	192.168.0.100	TLSv1.3	85 Application Data
87	6.404741	192.168.0.100	104.16.103.112	TCP	54 29771 → 443 [ACK] Seq=4532
88	6.404941	192.168.0.100	104.16.103.112	TLSv1.3	85 Application Data
89	6.405839	104.16.103.112	192.168.0.100	TCP	54 443 → 29771 [ACK] Seq=1935
90	6.417082	104.16.103.112	192.168.0.100	TLSv1.3	681 Application Data
91	6.417328	104.16.103.112	192.168.0.100	TLSv1.3	87 Application Data
92	6.417328	104.16.103.112	192.168.0.100	TLSv1.3	85 Application Data
93	6.417405	192.168.0.100	104.16.103.112	TCP	54 29771 → 443 [ACK] Seq=4563
94	8.002397	192.168.0.100	49.44.145.80	TCP	54 45989 → 443 [RST, ACK] Seq...

The detailed view pane shows the following information for the selected packet (No. 94):

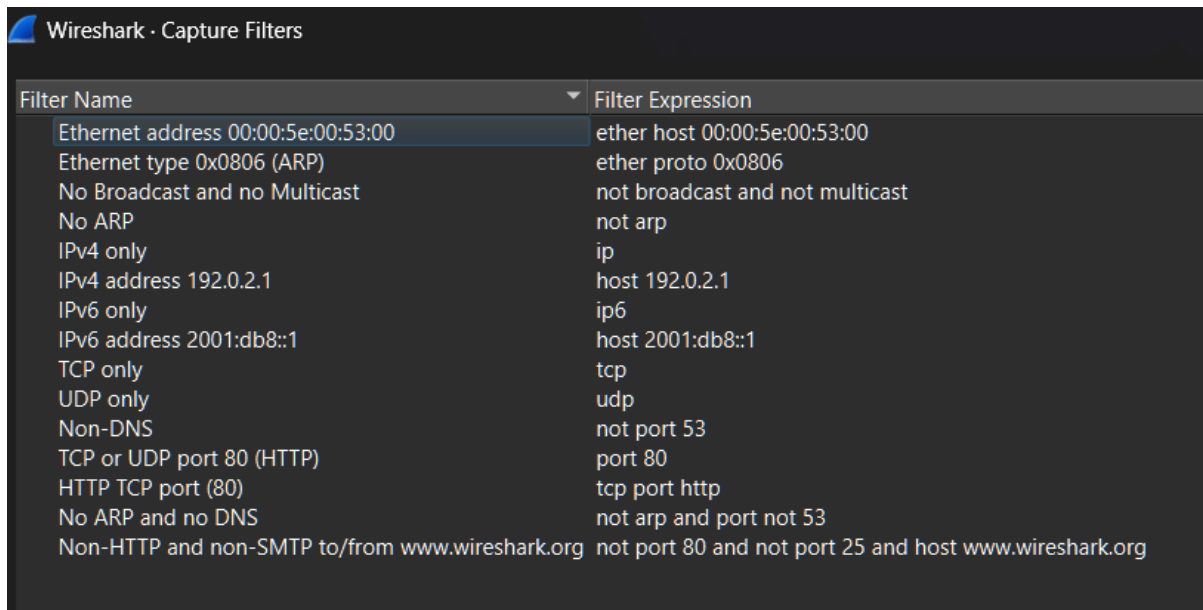
- Frame 1: Packet, 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{08...}
- Ethernet II, Src: Intel_b5:8a:6f (f4:3b:d8:b5:8a:6f), Dst: TPLink_40:78:26 (28:87:ba:40:78:26)
- Internet Protocol Version 4, Src: 192.168.0.100, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 59201, Dst Port: 53
- Domain Name System (query)

3. Filter Packets by Protocol

Use display filters in Wireshark:

- http
- dns
- tcp

This helps analyze specific types of traffic.

A screenshot of the Wireshark 'Capture Filters' window. It shows a list of filter names and their corresponding filter expressions. The first filter, 'Ethernet address 00:00:5e:00:53:00', is highlighted. The table lists various filters for capturing specific network traffic based on MAC addresses, protocols, ports, and hostnames.

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	not port 53
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org

4. Observe TCP Three-Way Handshake

Identify the following TCP flags:

1. SYN
2. SYN-ACK
3. ACK

This handshake establishes a TCP connection between client and server.

TCP packets showing SYN, SYN-ACK, and ACK flags.

5. Identify Plain-Text vs Encrypted Traffic

- HTTP: Data is visible in plain text.
- HTTPS: Data is encrypted and not readable.
- HTTP traffic showing readable data.
- HTTPS/TLS traffic showing encrypted data.

6. Capture and Analyze DNS Queries

- Apply the dns filter.
- Open a website in a browser.
- Observe DNS queries and responses with IP addresses.

DNS query and response visible in Wireshark.

This file is mandatory for submission.

7. Write Observations in Simple Language

Write short observations based on what you captured.

```
Checksum: 0x262f [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
▼ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ► TCP Option - No-Operation (NOP)
  ► TCP Option - No-Operation (NOP)
  ► TCP Option - Timestamps: TSval 824635422, TSecr 3249934137
▼ [SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 15]
  [The RTT to ACK the segment was: 0.002592000 seconds]
▼ [TCP Analysis Flags]
  ▼ [Expert Info (Warning/Sequence): Previous segment not captured (common at capture start)]
    [Previous segment not captured (common at capture start)]
    [Severity level: Warning]
    [Group: Sequence]
```

Tools Used

- Primary Tool: Wireshark
- Alternative Tools: tcpdump, Microsoft Network Monitor

Task Execution (According to Given Steps)

1. Learn Basic Networking Concepts

- IP Address: Identifies a device on a network.
- MAC Address: Physical address of a network interface.
- DNS: Resolves domain names into IP addresses.
- TCP: Reliable, connection-oriented protocol.
- UDP: Fast, connectionless protocol.

2. Capture Live Network Traffic

- Install Wireshark.
- Run Wireshark as administrator.
- Select an active network interface (Wi-Fi or Ethernet).
- Start capturing live packets.

Live packet capture running in Wireshark.

3. Filter Packets by Protocol

Use display filters in Wireshark:

- http
- dns
- tcp

This helps analyze specific types of traffic.

Protocol filter applied (HTTP, DNS, or TCP).

4. Observe TCP Three-Way Handshake

Identify the following TCP flags:

1. SYN
2. SYN-ACK
3. ACK

This handshake establishes a TCP connection between client and server.

TCP packets showing SYN, SYN-ACK, and ACK flags.

5. Identify Plain-Text vs Encrypted Traffic

- HTTP: Data is visible in plain text.
- HTTPS: Data is encrypted and not readable.
- HTTP traffic showing readable data.
- HTTPS/TLS traffic showing encrypted data.

6. Capture and Analyze DNS Queries

- Apply the dns filter.
- Open a website in a browser.
- Observe DNS queries and responses with IP addresses.
DNS query and response visible in Wireshark.