Task 3: Networking Basics for Cyber Security

1. Learn basic networking concepts (IP, MAC, DNS, TCP/UDP):

IP Address (Internet Protocol)

What it is?

An IP address is a unique numerical identifier for a device on a network.

Just like a home address identifies where you live.

Types:

- IPv4 → 192.168.1.10
- IPv6 → 2001:0db8:85a3::8a2e:0370:7334

Public vs Private:

- **Private IP: Used inside local networks (home, office)**
  - **192.168.x.x**
  - **10.x.x.x**
- **Public IP: Used on the internet (assigned by ISP)**

Security relevance:

- **Attackers scan IPs to find open ports**
- **Firewalls filter traffic based on Ips**

MAC Address (Media Access Control)

What it is?

A MAC address is a hardware address permanently assigned to a network interface.

Example:

00:1A:2B:3C:4D:5E

Key points

- Works at Layer 2 (Data Link) of the OSI model
- Used inside local networks (LAN)

Difference between IP & MAC

IP Address	MAC Address
Logical	Physical
Can change	Usually fixed
Layer 3	Layer 2

Security relevance

- MAC spoofing can bypass weak network controls
- Used in ARP attacks

DNS (Domain Name System)

What it is

DNS translates **domain names into IP addresses**.

Example:

google.com → 142.250.192.14

Why it's needed

Humans remember names, computers use IPs.

DNS resolution flow

1. You type example.com
2. DNS server looks it up
3. IP address is returned

4. Browser connects to the server

Security relevance

- DNS spoofing / poisoning attacks
- Malicious domains used in phishing

TCP (Transmission Control Protocol)

What it is

TCP is a **reliable, connection-oriented** protocol.

Characteristics

- Guarantees delivery
- Error checking
- Packet ordering
- Uses **3-way handshake**

TCP Handshake

SYN → SYN-ACK → ACK

Common TCP services

Service	Port
HTTP	80
HTTPS	443
FTP	21
SSH	22

Security relevance

- TCP SYN flood attacks
- Session hijacking risks

UDP (User Datagram Protocol)

What it is

UDP is a **fast, connectionless** protocol.

Characteristics

- No guarantee of delivery
- No handshake
- Faster than TCP

Common UDP services

Service	Port
DNS	53
DHCP	67/68
VoIP	Various

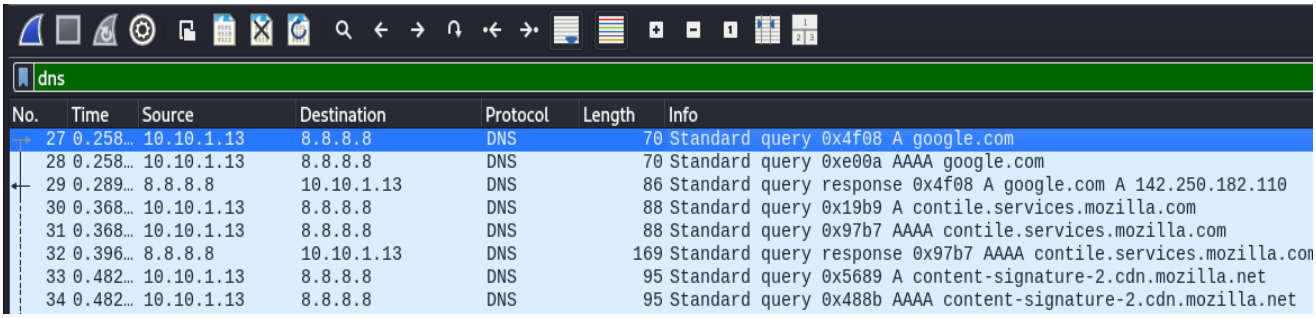
Security relevance

- UDP amplification attacks
- Used in DDoS attacks

2. Filter packets by protocol (DNS, TCP, HTTP) using Wirershark:

DNS (Domain Name System)

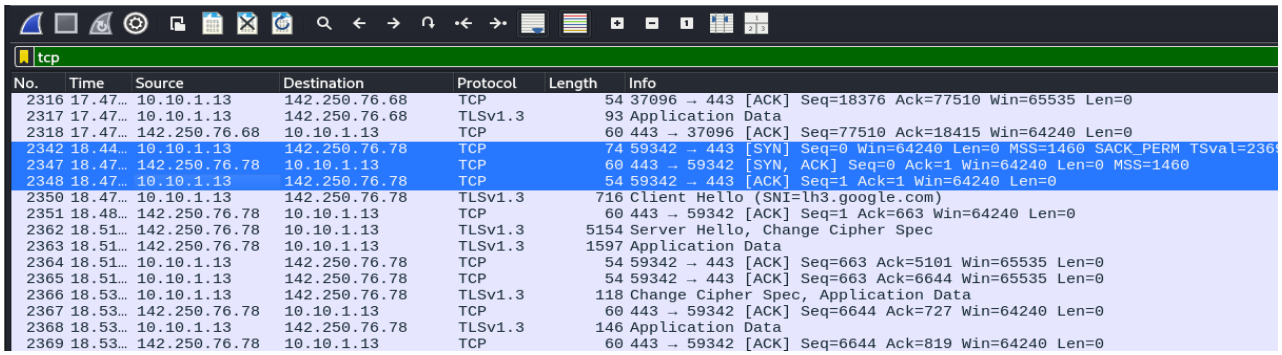
Used for resolving domain names (e.g., www.google.com) into IP addresses.
Example:
Source: 10.10.1.13 → Destination: 8.8.8.8
Query: A www.google.com
Response: 142.250.182.110



TCP (Transmission Control Protocol)

Used to establish reliable connections between client and server.

Example:



Source: 10.10.1.13 → Destination: 142.250.76.78

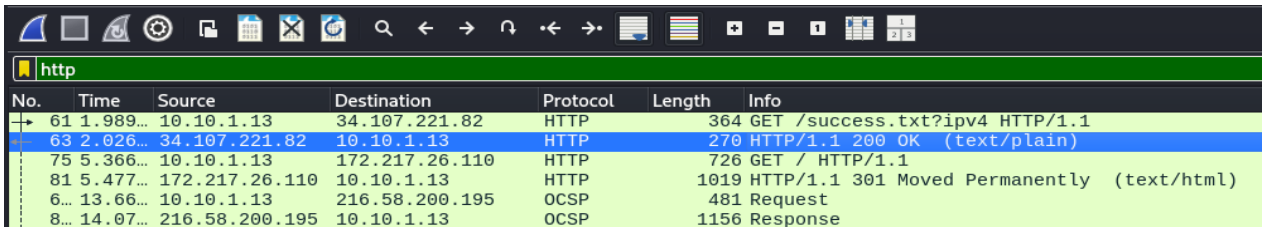
Flags: SYN → SYN/ACK → ACK (3-way handshake)

HTTP (Hypertext Transfer Protocol)

Application layer protocol used for web requests.

Example:

GET / HTTP/1.1



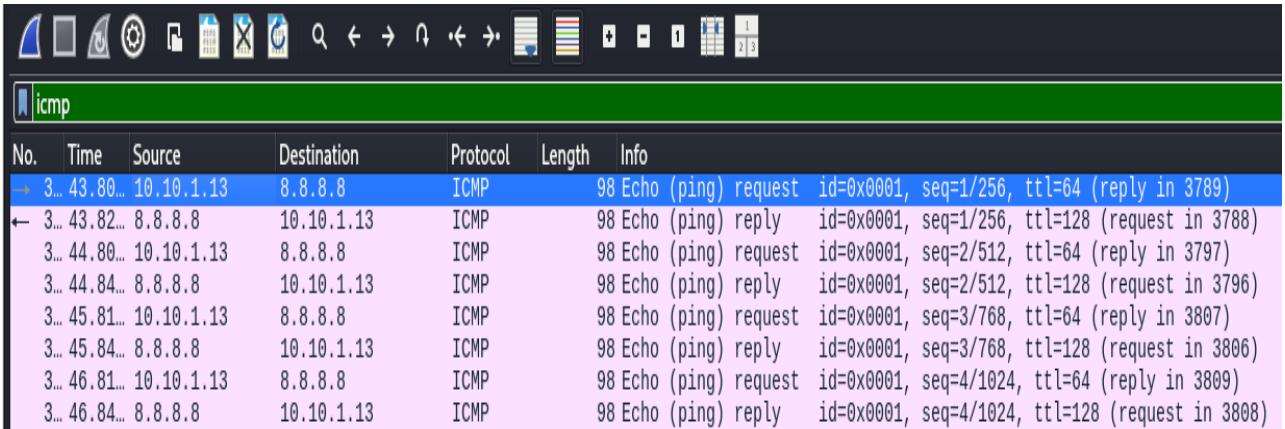
Host: www.google.com

Response: 200 OK

4. ICMP (Internet Control Message Protocol)

Used for ping and diagnostic messages.

Example:



Echo (ping) request → Echo reply from 8.8.8.8

3. Identify plain-text traffic vs encrypted traffic:

How to Identify Plain-Text in Wireshark

1. Use Display Filters

http, ftp, telnet.

2. Look at Packet Details

- Expand Application Layer
- You can read:
  - URLs
  - Usernames
  - Passwords
  - Form data

3. Follow Stream:

Right-click a packet → Follow → TCP Stream

If you can read the conversation clearly, it's plain-text.

Example (HTTP):

- GET /login.php HTTP/1.1
- Host: example.com
- username=admin&password=12345

Security risk:

Anyone sniffing the network can see this.

How to Identify Encrypted Traffic in Wireshark

Use Filters:

- Tls
- Ssl
- tcp.port == 443

Packet Appearance:

- Data appears as random bytes
- You cannot see usernames or content

TLS Handshake Indicators:

Look for--

- Client Hello
- Server Hello

- Certificate exchange

Example (Encrypted Payload):

- Data: 8f 3a b9 e2 91 c4 7a ...
- This is unreadable without decryption keys.

Observations:

- Wireshark was used to capture live network traffic.
- DNS packets showed domain names being translated into IP addresses.
- TCP packets displayed a three-way handshake using SYN, SYN-ACK, and ACK flags.
- HTTP traffic was readable in plain text, while HTTPS traffic was encrypted and unreadable.
- This shows how secure communication protects user data.