Velocity Solutions Internship Tasks

Task 1: Cybersecurity Research

What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and data from digital attacks. These attacks often aim to access, modify, or destroy sensitive information, interrupt business processes, or extort money. It involves technologies, processes, and practices to defend against unauthorized access or damage.

Common Cyber Attacks

- **Phishing**:

  A deceptive attempt to steal sensitive data (e.g., passwords, credit card numbers) by pretending to be a trustworthy entity via email or websites.

- **Malware**:

  Malicious software such as viruses, worms, ransomware, and spyware that can disrupt or damage a system.

- **DDoS (Distributed Denial of Service)**:

  Overwhelming a server or network with traffic to render it unusable.

CIA Triad

- **Confidentiality**:

  Ensuring information is accessible only to those authorized to access it.

- **Integrity**:

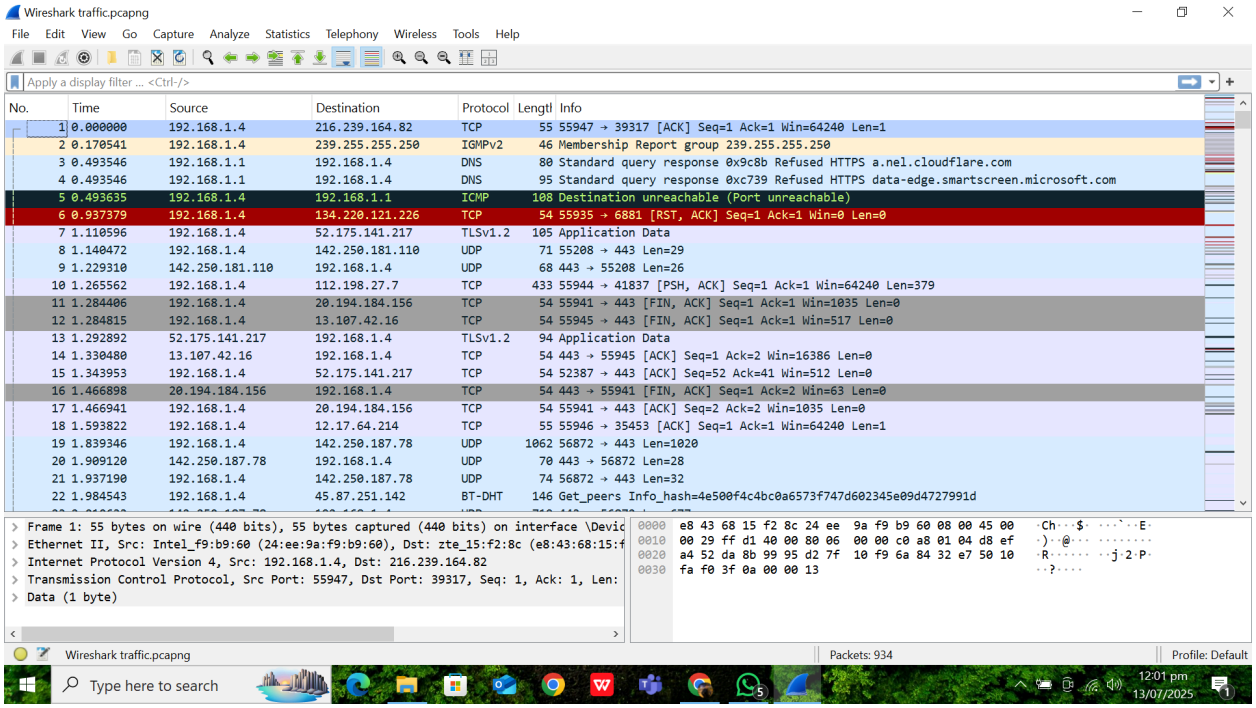
  Guaranteeing the data is accurate and unaltered.

- **Availability**:

  Making sure information and resources are available when needed.

Wireshark:

I observed the following protocols in the pcap file; the file is also listed on my github.



1. HTTP – Talking to Websites

HTTP stands for *Hypertext Transfer Protocol*. It's what your browser uses when you visit a website.

- When you go to a site like `facebook.com`, your browser says:
  "Hey server, can I have the homepage?"

- The server replies:
  "Sure, here it is!" (or *"Sorry, not found."*)

In **Wireshark**, you'll see messages like `GET` (asking for something) and responses like `200 OK` (everything worked).

---

2. DNS – Finding Website Addresses

DNS stands for *Domain Name System*. It helps your computer find out where a website is.

- It's like asking, *"What's the IP address of google.com?"*
- DNS replies: *"It's 142.250.190.14."*

This happens quickly and behind the scenes every time you open a site.

In **Wireshark**, you'll see DNS requests asking for website names and responses giving IP addresses.

---

3. TCP – Sending Data Safely

TCP stands for *Transmission Control Protocol*. It's used to send data reliably over the internet.

- First, two computers shake hands (not literally, but digitally).
  One says: *"Can we talk?"*, the other says: *"Yes, ready!"*, and they agree to start.
- Then they send and receive data in small pieces.

TCP makes sure nothing is missing or mixed up.

in **Wireshark**, you'll see this handshake and the back-and-forth sending of information.