"Network Traffic Analysis using Wireshark: Identifying Legitimate vs Malicious Packets."

Editor – Arya Mokashi

Project Overview – Packet Analysis with Wireshark

1. Objective

To explore and understand how network traffic works, how packets can be analyzed in Wireshark, and how different types of records (A vs HTTPS) behave in DNS queries.

---

2. Key Learning Activities

1. **Packet Analysis Basics**
    - Captured live traffic using Wireshark.
    - Learned how to filter by protocol (DNS, ICMP, HTTP/HTTPS).
    - Observed packet headers (source/destination IP, port, protocol).
2. **Reachability Testing with Ping (ICMP)**
    - Sent ICMP Echo Requests (ping) to websites.
    - Understood that:
        - **Reply (Echo Reply)** → host is reachable.
        - **No reply/timeout** → ICMP may be blocked (by firewall/security policy), not always that the host is down.
3. **DNS Query Analysis**
    - Discovered why two DNS packets appear:
        - **A Record** → resolves domain to IPv4 address.
        - **HTTPS Record** → newer DNS type, used by modern browsers to check if a site supports HTTPS and extra security features (like QUIC, HTTP/3).
    - Example:
        - Query for A netacad.com → gives IPv4.

        - Query for HTTPS netacad.com → asks if HTTPS endpoints exist and what parameters they support.

7325	374.931226	192.168.0.106	192.168.0.1	DNS	83 Standard query 0x4dfe A idbroker-b-us.webex.com
7326	374.932543	192.168.0.106	192.168.0.1	DNS	83 Standard query 0x8233 HTTPS idbroker-b-us.webex.com

---

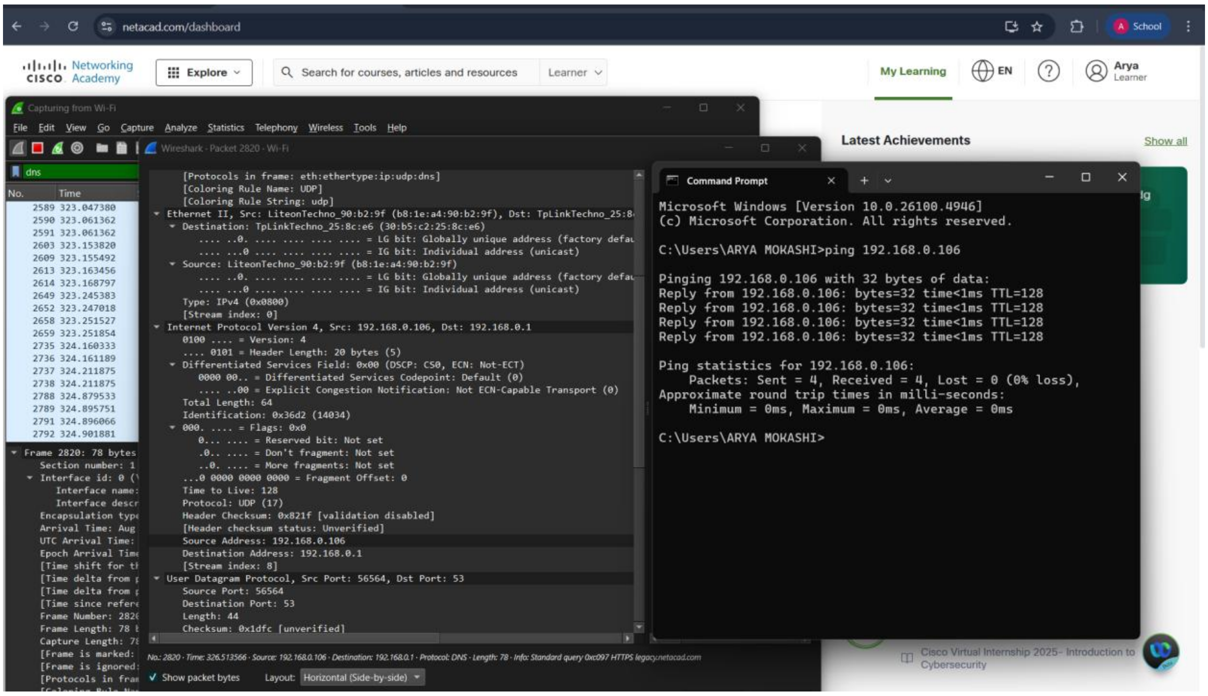
3. Observations

1. **Ping / ICMP Analysis**
    - **When pinging a website, Wireshark captured ICMP Echo Request and Echo Reply packets.**
    - **If the reply was received → server is reachable.**
    - **Some servers still responded to DNS/HTTP requests even when ICMP replies were blocked.**
2. **DNS Record Analysis**
    - **For a single domain query, Wireshark showed two DNS queries:**
        - **One for A Record → returned the IPv4 address of the domain.**
        - **One for HTTPS Record → checked HTTPS support and extra security info.**
    - **This explained why we saw two packets with similar information but at slightly different times.**
3. **Packet Details in Wireshark**
    - **We could view the source and destination IP addresses, port numbers, and protocol information.**
    - **For DNS responses, the exact IP address assigned to the domain was visible.**
    - **For ICMP, we saw the request–reply sequence clearly in Wireshark.**

---

4. Skills Gained

- Capturing and filtering packets using Wireshark.
- Identifying reachability using ICMP.
- Understanding DNS record types and why multiple queries appear.
- Beginning awareness of normal vs. abnormal traffic.



- [**Traffic analysis exercise: It's a trap!**](#)

Analysed a PCAP(Packet Capture) from https://www.malware-traffic-analysis.net/training-exercises.html

Conclusions n

1. Legitimate vs Malicious Data in Payload

- **Legitimate Packets**
  - DNS responses contain domain names (e.g., netacad.com).
  - HTTP/HTTPS traffic contains request headers (Host:, User-Agent:) and sometimes readable text (if not encrypted).
  - Application protocols (FTP, SMTP, etc.) have structured, human-readable commands (USER, PASS, MAIL FROM).
- **Malicious Packets**
  - Often have **empty payloads** or **garbled data** in the "Raw Bytes" section.
  - Data may appear as **random characters, encoded strings (Base64, hex dumps)**, or **no clear protocol structure**.
  - For example:
    - Instead of GET /index.html HTTP/1.1, you might see sdf9sd89f8sd... or hex-only values.

- This suggests obfuscation, exploitation, or command-and-control traffic.

---

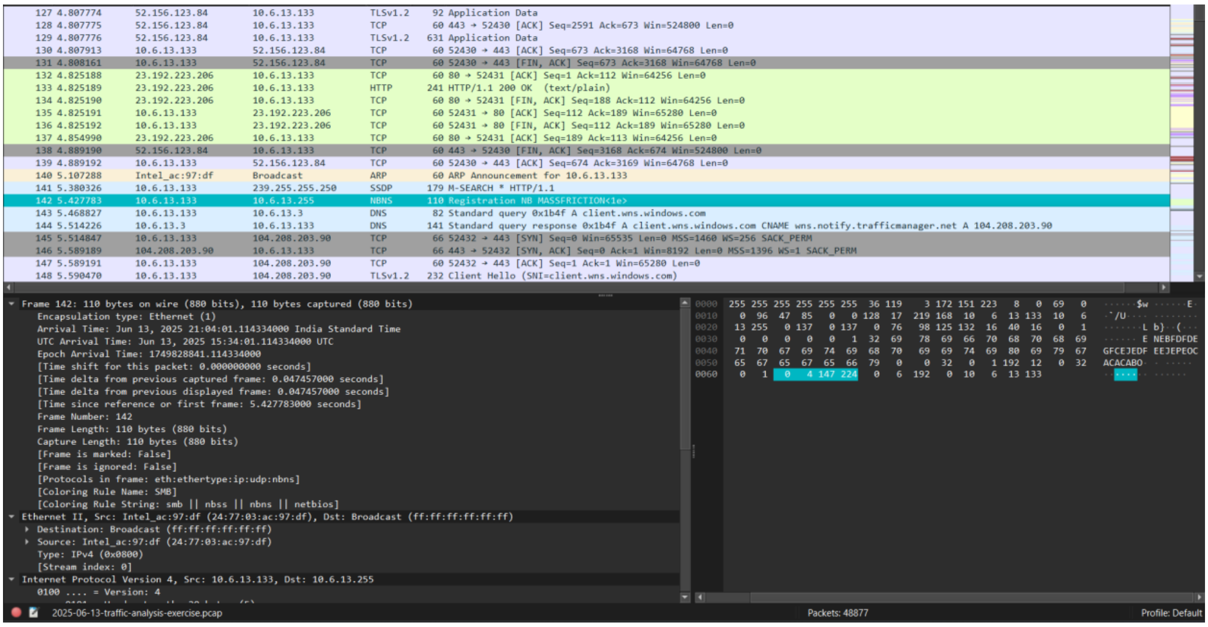
2. Color Coding in Wireshark

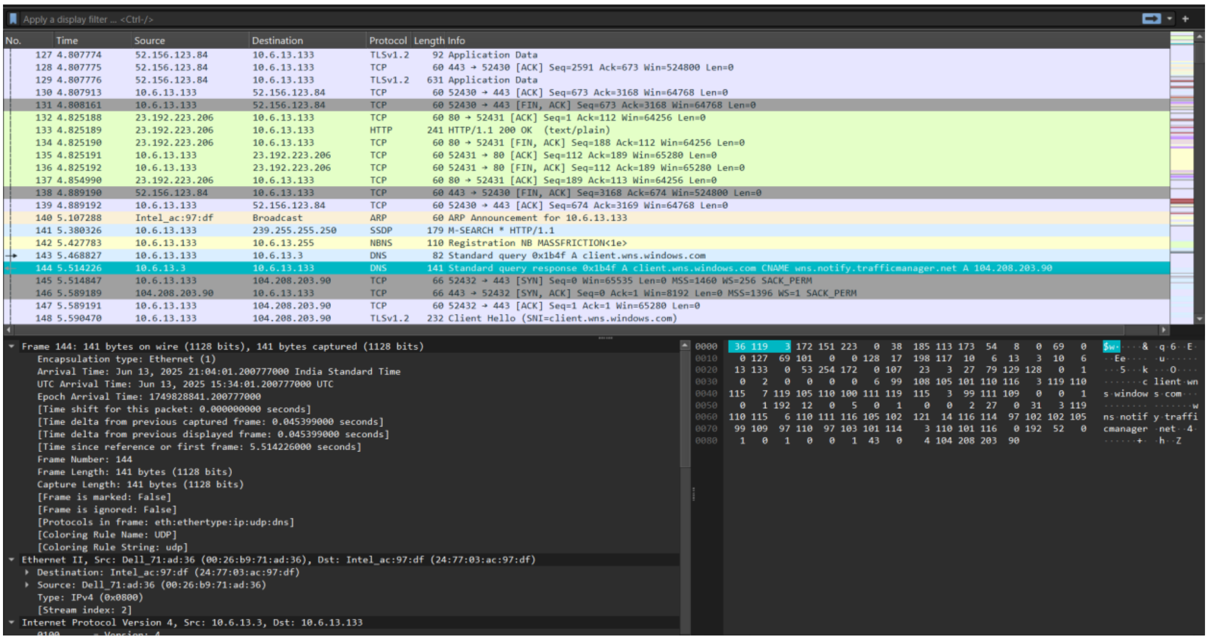
- Red highlighting usually marks **TCP problems** (retransmissions, resets, malformed packets).
- Not automatically “malicious,” but suspicious traffic often shows up in red due to broken protocol behavior.

---

3. Behavioral Indicators

- **Normal traffic:**
  - Predictable sequence of requests/responses (DNS → TCP Handshake → HTTP Request → Response).
  - Payload matches expected protocol format.
- **Malicious traffic:**
  - Irregular packet sizes (very small or very large compared to protocol norms).
  - Packets without a clear request/response pattern.
  - Use of uncommon ports or protocols (e.g., DNS queries carrying large encoded payloads).
  - Repeated failed attempts (could indicate scanning or brute force).





- **Conclusion**

In this traffic analysis exercise, we learned how to capture and inspect packets using Wireshark and differentiate between legitimate and suspicious network traffic. Legitimate packets followed proper protocol structures (e.g., DNS queries showing domain names, HTTP headers with readable information), while malicious or suspicious packets often lacked meaningful data in the raw field or displayed irregular/unexpected patterns. Color coding in Wireshark (e.g., red highlights for TCP problems) further helped in identifying abnormal packets that require closer inspection.

- **What Was Learned**

- How to use **Wireshark** to capture and analyze packets.
- The difference between **legitimate traffic** (structured, protocol-compliant, human-readable) and **malicious traffic** (unstructured, encoded, or abnormal behavior).
- Understanding of **DNS record types** (A vs HTTPS record) and how websites may respond differently.
- Use of **packet payload inspection** (raw data view) to infer intent behind traffic.