DNS Traffic Analysis

Name: Redjaimia Imad Eddine

Course: Network Security

Date: September 19, 2025

Objective : The goal of this project was to analyze a packet capture (PCAP) file to identify suspicious DNS activities, detect signs of a potential infected client, and understand how malicious domains might be queried in the network

Tools Used:

Wireshark : for packet capture inspection and filtering.

Malware-Traffic-Analysis.net dataset : as the source of real-world network traffic.

DNS filters in Wireshark ( dns, dns.flags.rcode = 3,dns.flags.opcode==5) to investigate domain queries and responses.

Steps Taken:

1.Loaded the PCAP file into Wireshark.

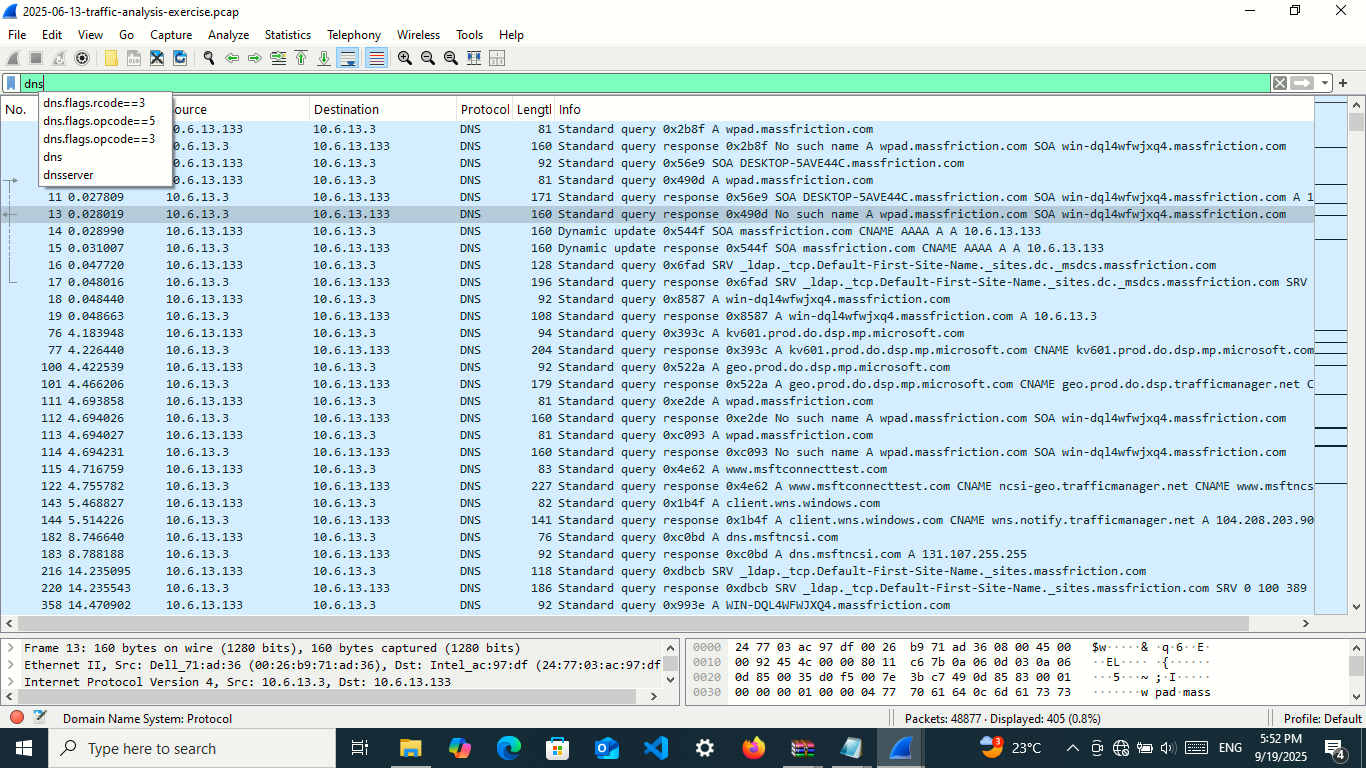
2. Applied filters to focus on DNS traffic (dns, dns.flags.rcode = 3,dns.flags.opcode==5).

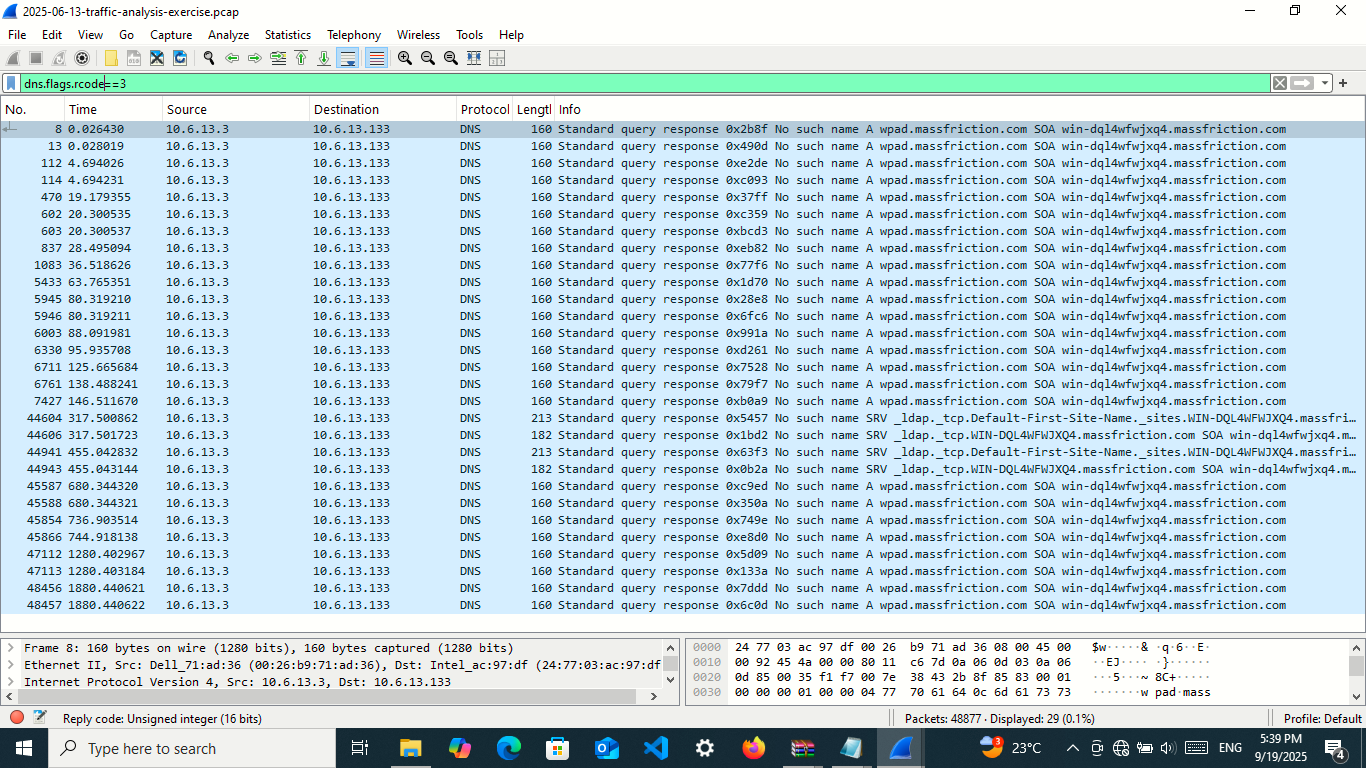
3. Identified suspicious queries to uncommon or strange domains ( wpad.massfriction.com,random string).

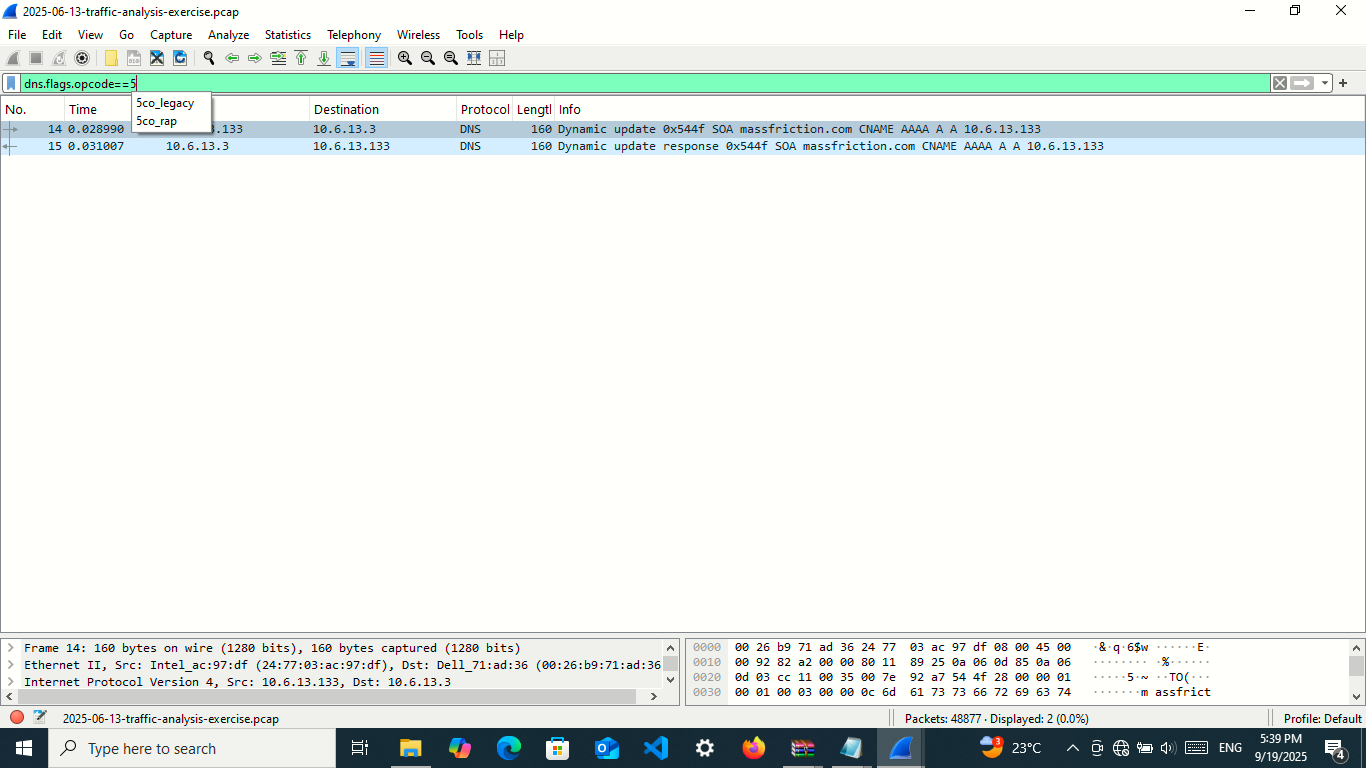
4. Observed failed responses (No such name) and repeated attempts to resolve the same domain a common sign of automated malware behavior.

5. Checked for Dynamic DNS updates that could indicate suspicious host-IP bindings.

6. Correlated source IPs with repeated suspicious queries to determine the potentially infected client.







Results:

Multiple DNS queries were directed towards unusual domains such as massfriction.com, which are not commonly used in normal environments. Several responses returned "No such name", showing failed attempts to reach these domains. The repeated and automated nature of the queries suggests that at least one client in the network may be infected with malware attempting to communicate with its command-and-control server (C2). The suspicious client IP was identified as [10.6.13.133](https://l.facebook.com/l.php?u=http%3A%2F%2F10.6.13.133%2F%3Ffbclid%3DIwZXh0bgNhZW0CMTAAYnJpZBExcGdnOUJlN2lwOFdUU0xYMAEeRn6vGz1xOctb7MtB2IVu62tHfaNj5SQRSf8C2U7fU072nu7MABcz5pFlMjU_aem_tFXtg_4lsF7hQ6_4VoetmA&h=AT2RfIaMvhwtdExmj3-OJbFlB594XH2WGtPNNzU9puJSgZWgQi9u6H5RCvl3xqSFYoM1laCKeS4tPIRslpGVZQ3jLo0H3IFSUNtMZInL3cPE10_bdUtZ7qYpNGpaM1-FSdH6SQ), based on abnormal query patterns.

Recommendations:

Isolate the infected host (10.6.13.133) from the network to prevent further malicious activity.

Perform malware scanning on the suspected client to confirm infection and remove malicious software. Block suspicious domains ( massfriction.com) at the DNS/firewall level.

Enable DNS logging & monitoring to detect repeated failed queries to uncommon domains in real time. Apply security patches and ensure endpoint protection (EDR/antivirus) is up to date.

Train users to avoid suspicious websites and downloads that could lead to infection.