Report: Week 2: Exploitation, Web Application Testing, and Advanced Networking

Lab 7: Practical Use Cases for Wireshark in Real-World Scenarios.

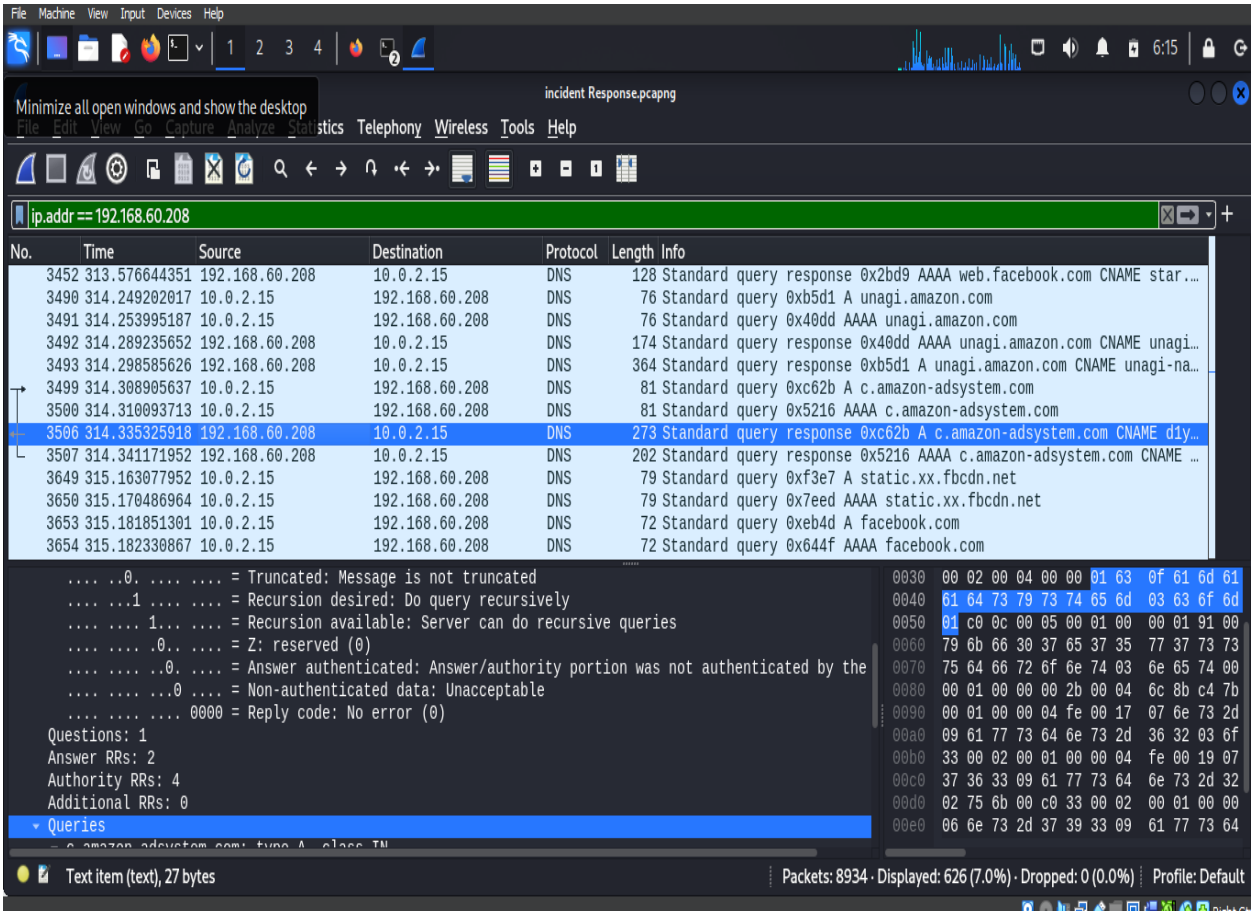
Report Summary of the incident.

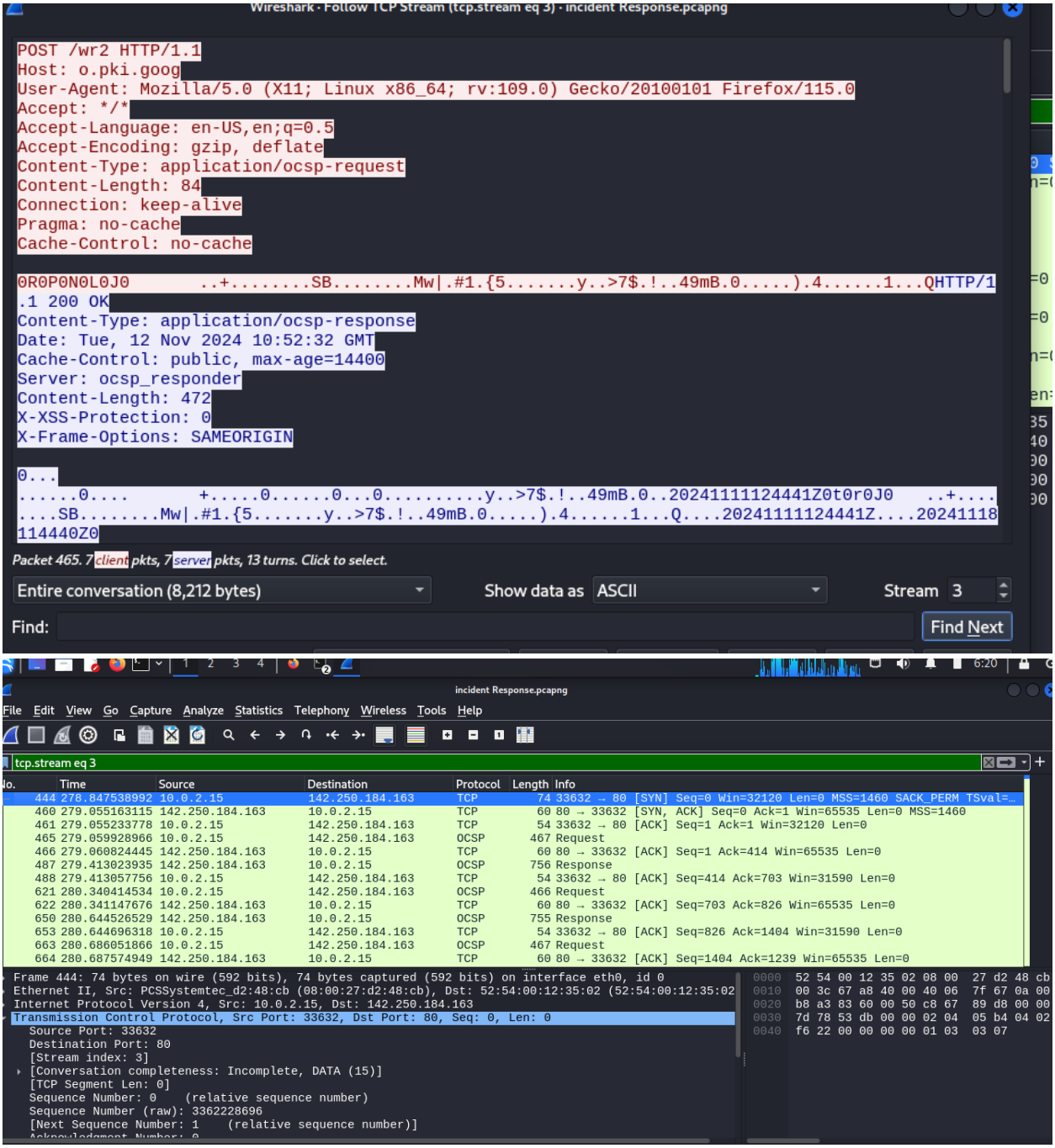
Timeline of events: 12 November 2024

Exercise 1:

• Describe the overall network traffic during the incident. Are there any noticeable spikes or anomalies? What potential indicators of compromise did you identify?

As the incident response team, a network traffics were analysis on both suspect IP address 192.168.60.208, source port 33632 and destination port 80. No suspicious activities were found, and no potential compromise was identified while analyzing the packet.

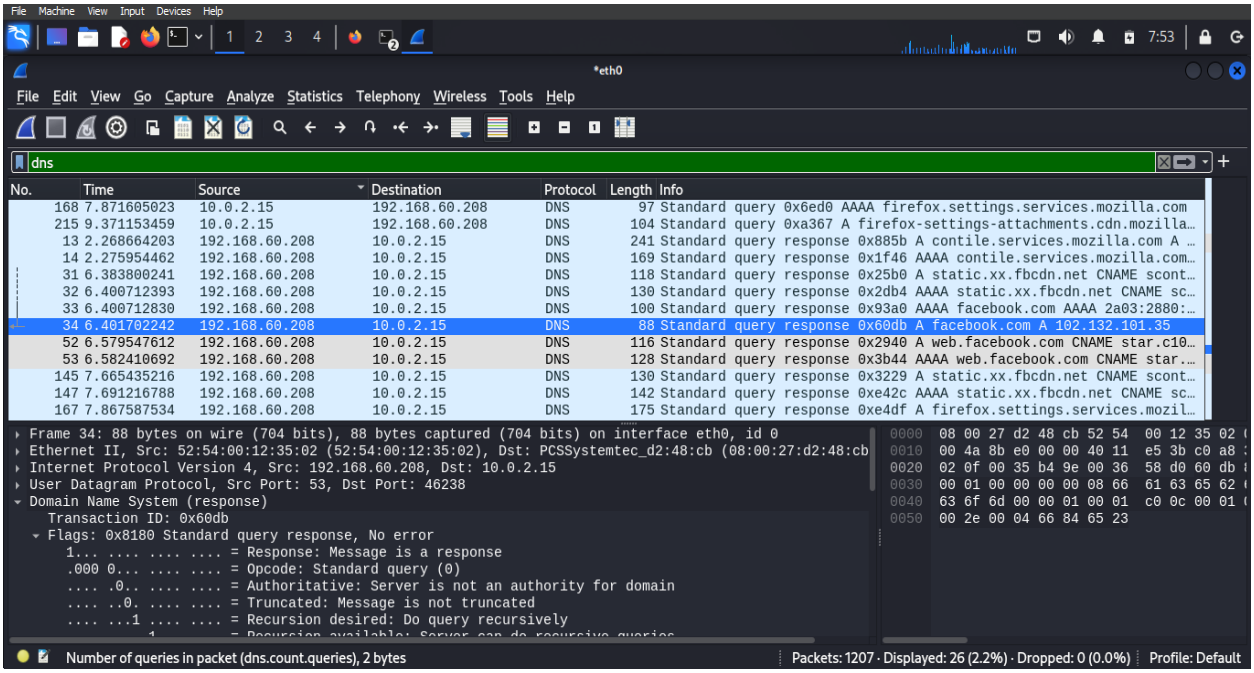




Exercise 2:

• Identify a specific packet that raises suspicion. Provide details about the packet, including source and destination IPs, ports, and protocol. What makes this packet suspicious?

A failed login attempts on Facebook.com source IP 192.168.60.208, and destination IP is 10.0.2.15, the source and destination ports are 53 and 50339, the protocol is DNS. The reason for suspicion is because of the login failure

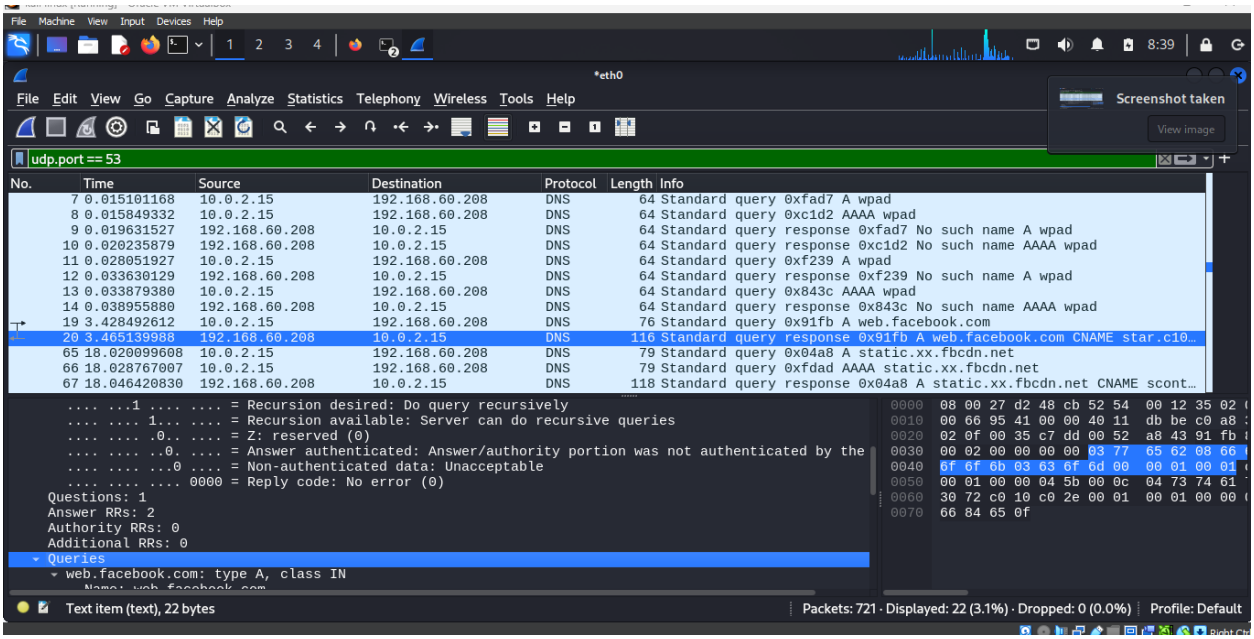


On the flag, answer authentication: answer/authority portion was not authenticate by server.

Exercise 3:

• Implement a capture filter to monitor DNS traffic. Analyze the captured packets and summarize any findings related to unusual queries or connections.

The packet captured was filter using udp.port == 53 and there is no unusual queries or connections.



Exercise 4:

• Identify any DNS packets that may indicate a connection to a suspicious or malicious domain. Provide details about the domain queried and any associated IP addresses

The domain was examine carefully and no malicious domain. The queries are, web . facebook.com: type A, class IN, Name: web.Facebook.com, Name Length: 16, Label Count: 3, Type: A (1) (Host Address).

Exercise 5:

• Document any anomalous traffic patterns you discovered. What does this suggest about potential malicious activity?

No abnormality is discovered, and this suggests that the system is secure from potential malicious activities.