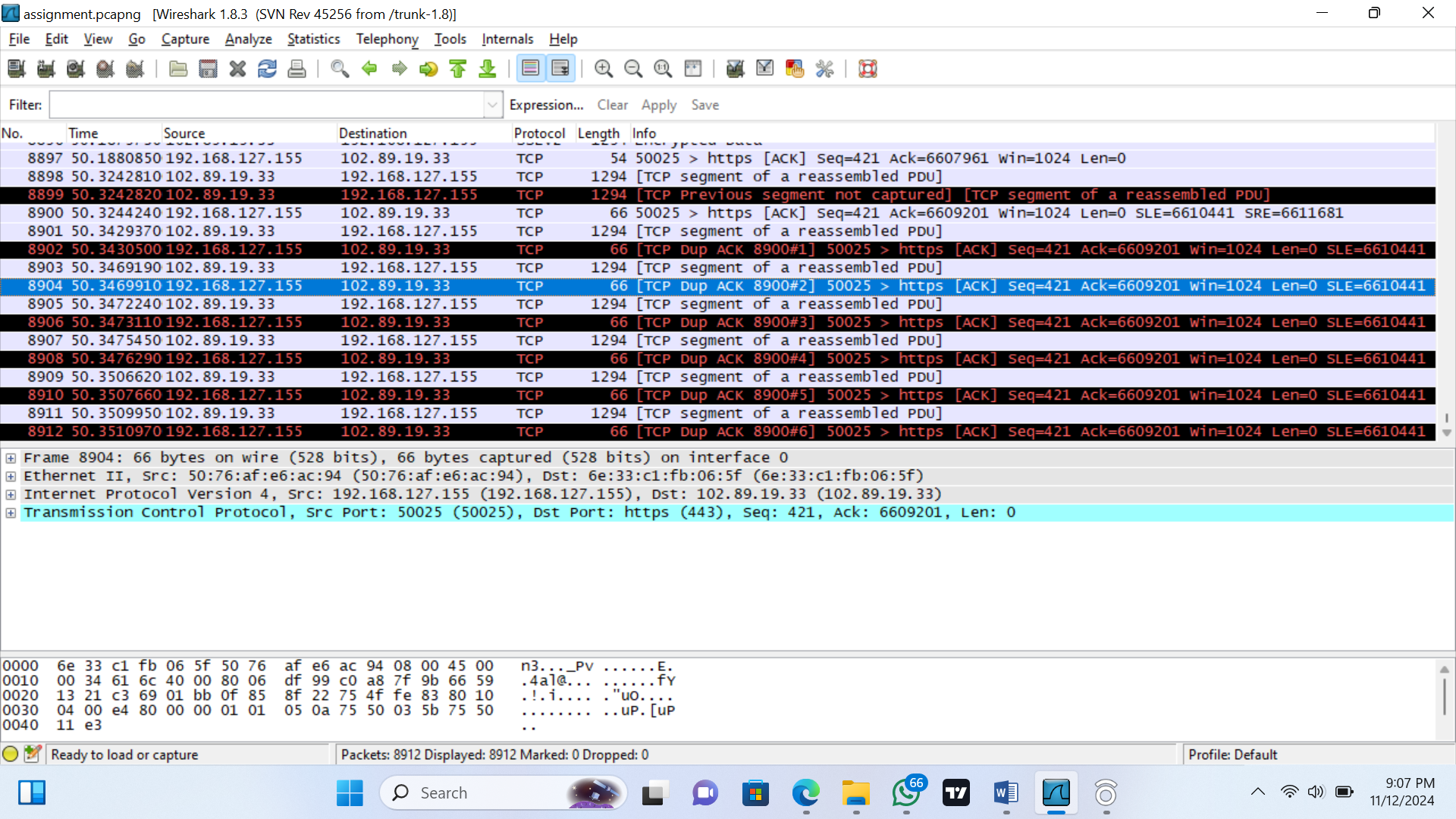
Week 2: Exploitation, Web Application Testing, and Advanced Networking

INT302: Kali Linux Tools and System Security – Lab 7: Practical Use Cases for Wireshark in Real-World Scenarios.

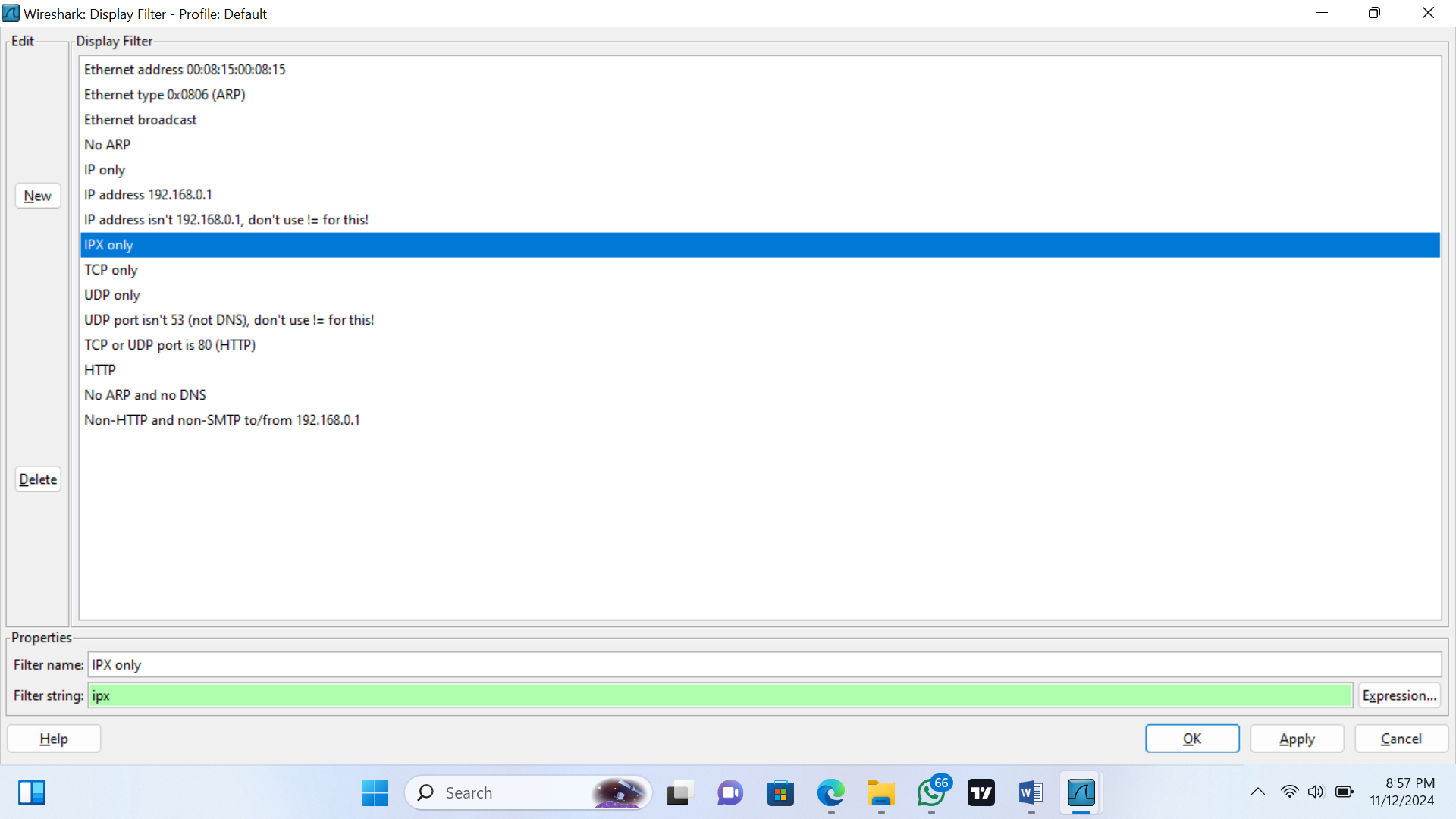
Step 1: Incident Response Analysis

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? \_\_\_\_\_\_\_\_\_\_



The ip address 102.89.19.33 is using a tcp port that isn’t secured ( it’s not port 53).

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? \_\_\_\_\_\_\_\_\_\_

Exercise 3: • Implement a capture filter to monitor DNS traffic. Analyze the captured packets and summarize any findings related to unusual queries or connections. \_\_\_\_\_\_\_\_\_

