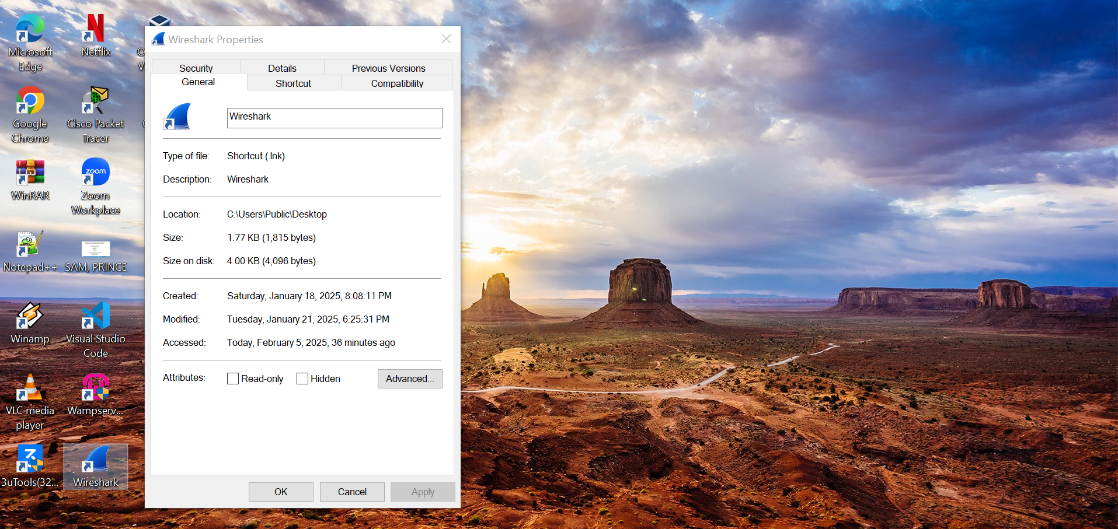
My recent cybersecurity project: A project on Packet Sniffer and Wi-Fi Security Analysis using Wire-shack

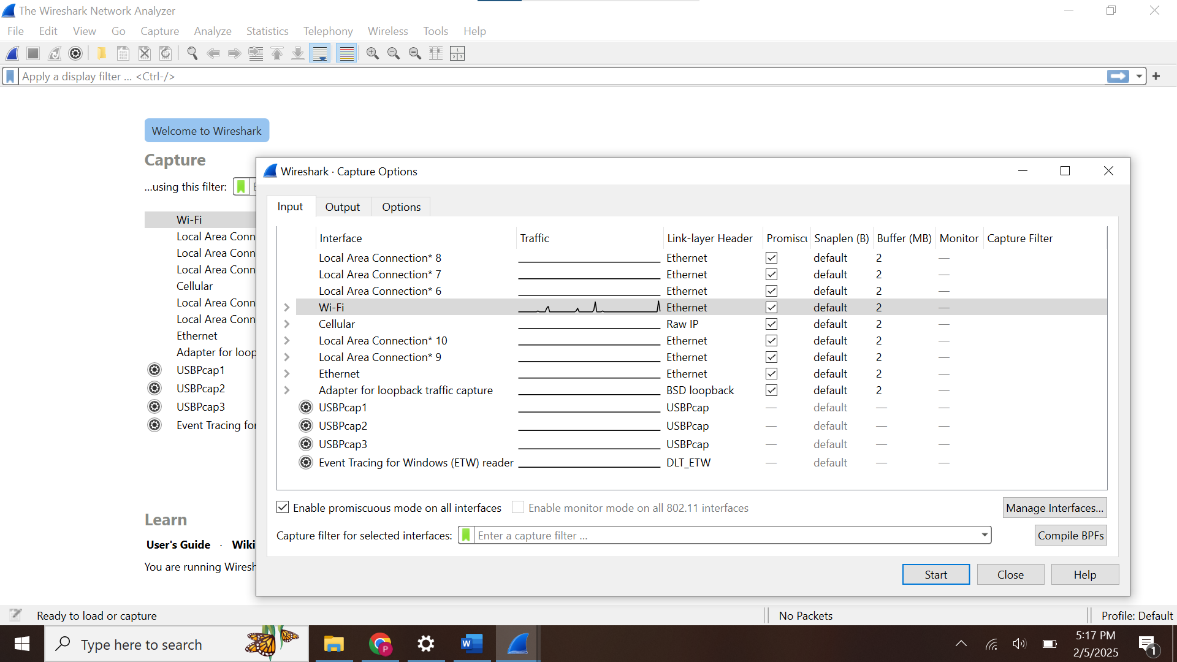
With the increasing reliance on wireless networks, ensuring their security has become critical. Packet sniffing is a technique used to analyze network traffic, detect vulnerabilities, and monitor security threats on a network.

Aim: Capturing, analyzing network packet and identify security weaknesses

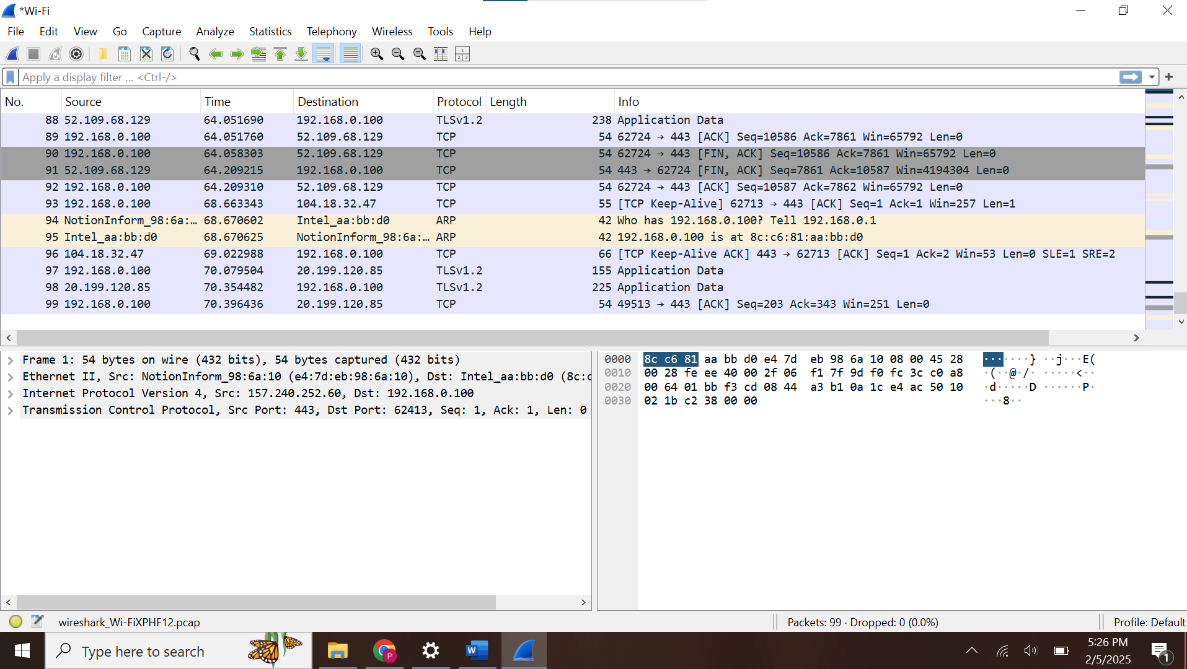
Process;  
Download and install wire shack



Open Wireshack, go to capture and turn on Promiscuous mode; this enables wireshack capture all packet even ones not intended for the network

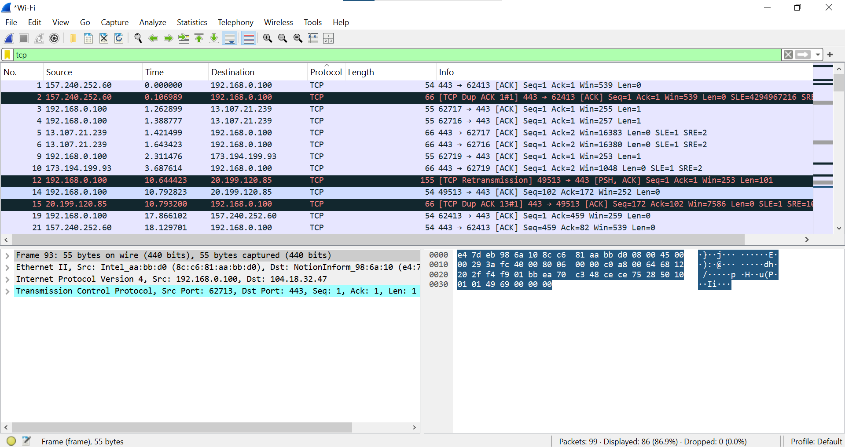
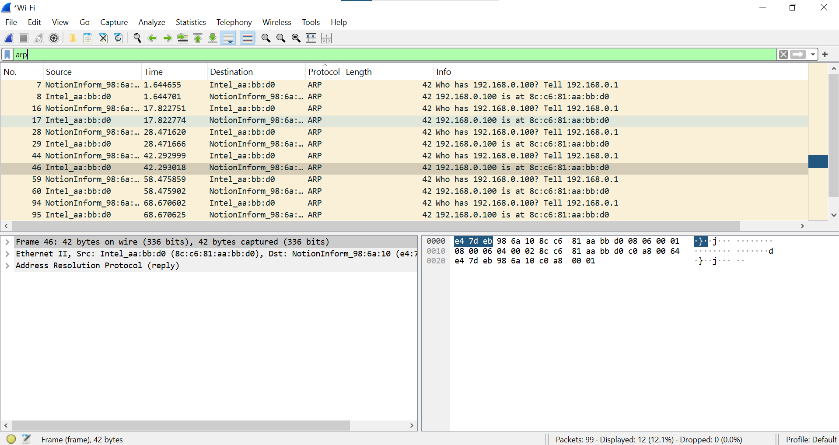


Here, we can start capturing on the WiFi interface by clicking the shark symbol

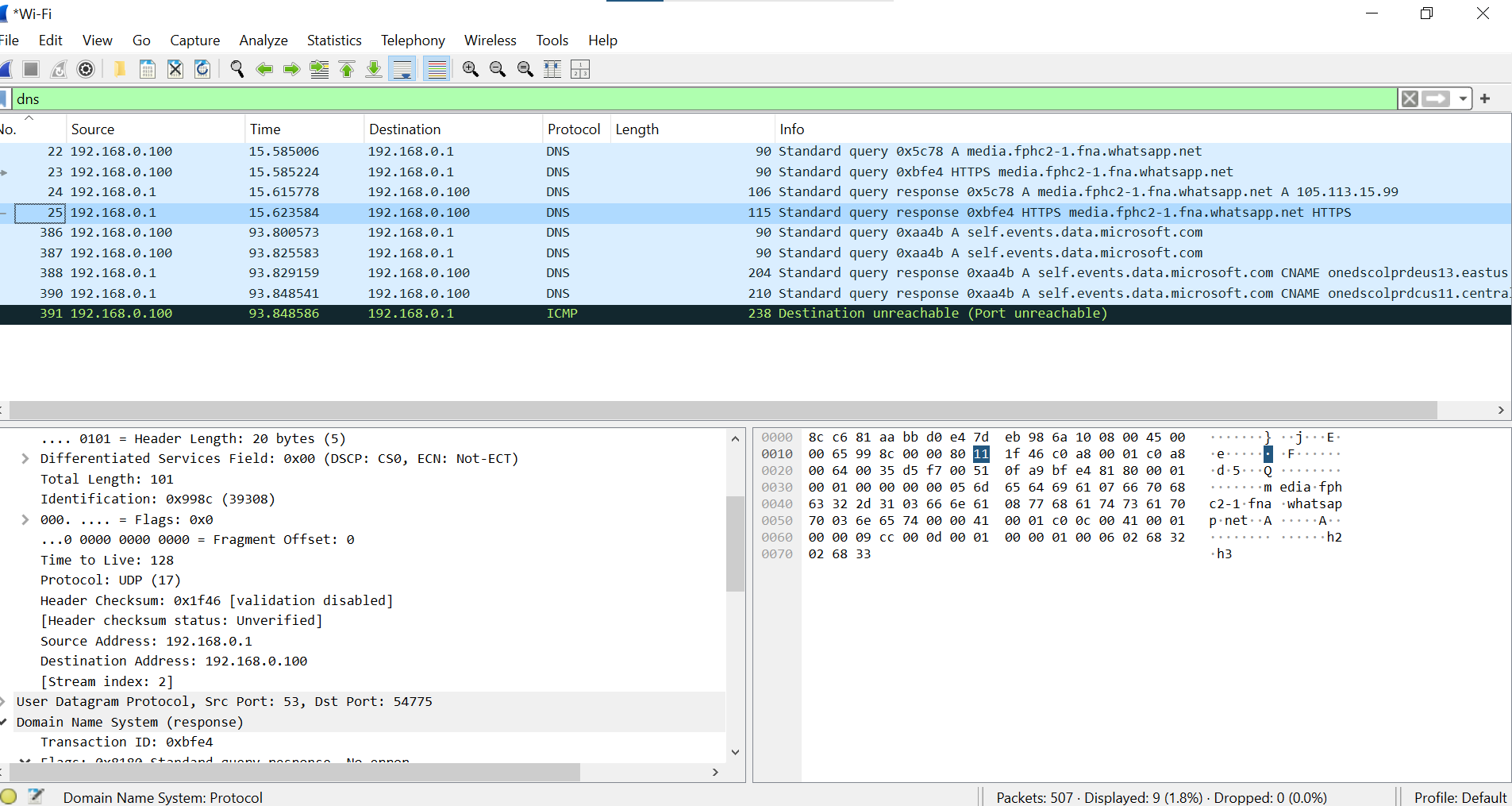


Analyzing Captured Packet;

* Use filter to differentiate TCP from ARP captured packet



* Filtering unencrypted network protocols such as HTTP, FTP, Telnet and DNS that expose sensitive information. In this case, DNS is the only unencrypted network protocol here with no suspicious activity or security weakness.



Result and Findings;  
\* Vulnerability: No vulnerability detected

\*Encrypted Protocol: SSH and TLS

\*Unencrypted protocol: Only DNS in this case

Conclusion: This project demonstrates the importance of packet sniffing and Wi-Fi security analysis in identifying vulnerabilities and strengthening network defenses. Wireshark when in promiscuous and monitor mode is a professional tool for troubleshooting and securing networks