LAB 5

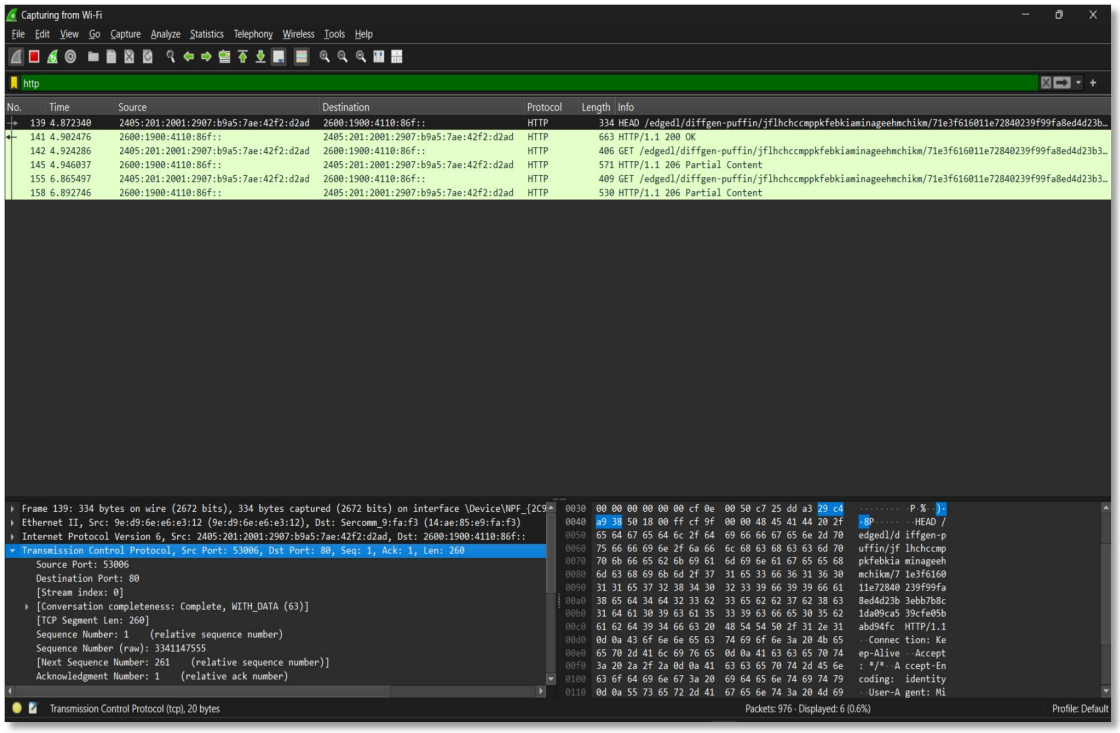
AIM: Using tools like Wireshark and tcpdump to capture and analyze mobile and IoT network traffic.

Introduction:

Wireshark and tcpdump are two of the most widely used tools for network traffic analysis. Wireshark, known for its powerful graphical interface and comprehensive packet analysis capabilities, is often favored for detailed, in-depth inspections of network data. Tcpdump, a command-line tool, is lightweight and highly effective for quick, real-time packet captures, making it ideal for mobile and IoT network environments where resources may be limited or where rapid diagnostics are needed.

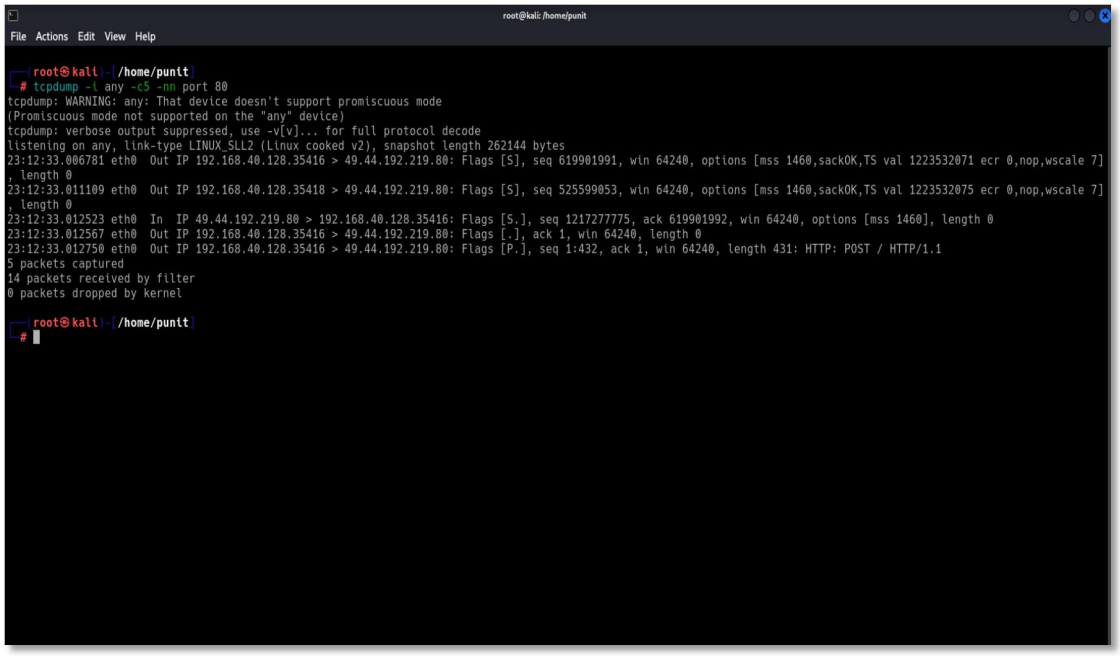
By capturing and analyzing network traffic from mobile and IoT devices, these tools provide valuable insights into the data flow, protocols, and potential vulnerabilities in the communication between devices and servers. They are indispensable in ensuring that these networks run smoothly, efficiently, and securely. This analysis is especially crucial as the volume of connected devices continues to rise, and the complexity of mobile and IoT networks grows.

WireShark Capturing:

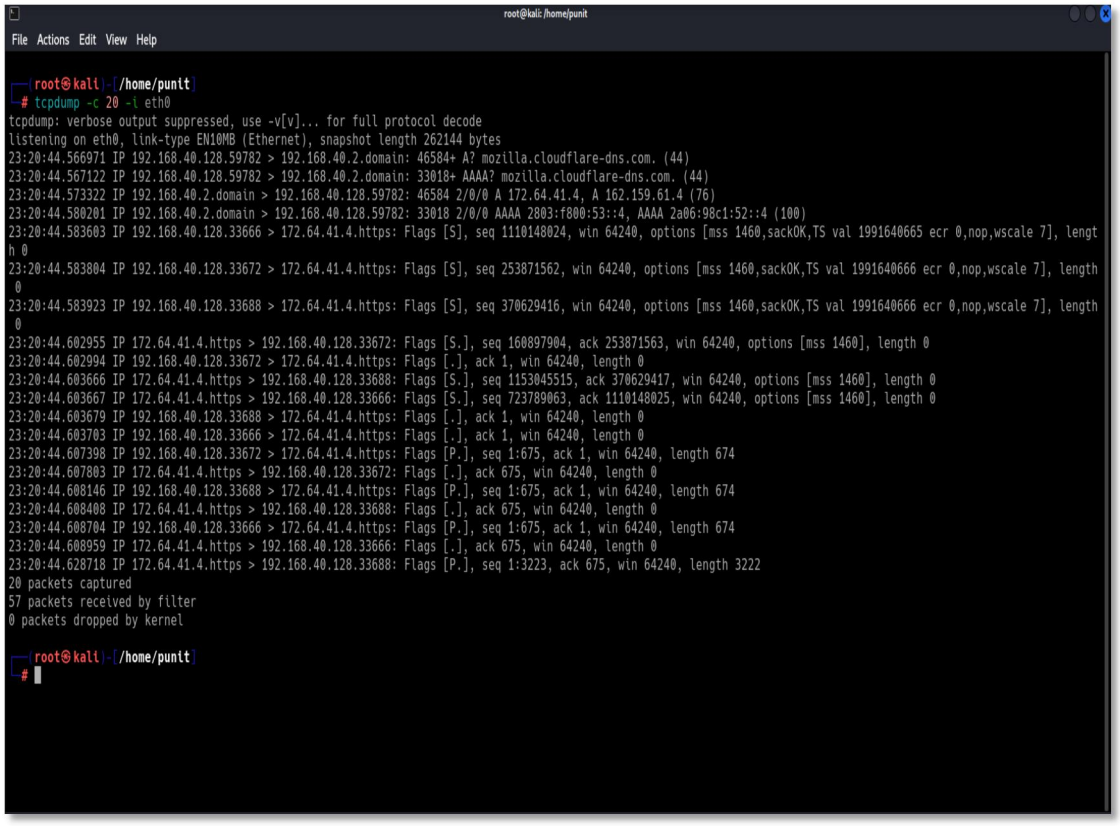


Tcpdump Capturing:

tcpdump -i any -c5 -nn port 80:



tcp -c 20 -I eth0:



Conclusion:

Using tools like Wireshark and tcpdump to capture and analyze mobile and IoT network traffic offers significant advantages for network administrators, security professionals, and developers. These tools allow for the detailed examination of the data exchanged between devices and servers, helping to diagnose issues, monitor performance, and ensure network security.