Assignment 2:

Connect two IoT devices (e.g., Raspberry Pi or ESP32) to a Wi-Fi network. Use Wireshark to capture network traffic and identify any unsecured communications between the devices.

I choose Android Phone and Laptop. Network Traffic Capture and Analysis Between Android Phone and Laptop Using Wireshark

Equipment and Tools Used

- Android smartphone connected to Wi-Fi
- Laptop connected to the same Wi-Fi network
- Wireshark installed on the laptop

Step 1: Setup HTTP Server on Laptop

1. Open a terminal on the laptop.

2. Start a simple HTTP server using Python 2 on port 80:

```
sudo python2 -m http Server 80
```

3. Confirm that the server is running and listening on port 80.

Step 2: Connect Devices and Generate Traffic

1. Both devices connected to the same Wi-Fi network (note their IP addresses).

2. From the Android device, open a browser and navigate to the laptop's IP: http://. This generates HTTP traffic captured by Wireshark.

3. Additionally, from the laptop, ping the Android device IP:

```
Ping 192.168.0.113
```

This generates ICMP packets seen in Wireshark.

Step 3: Capture Traffic in Wireshark

1. Open Wireshark and start capturing on the laptop's network interface connected to the Wi-Fi.

2. Apply a capture filter to limit traffic to the two devices: text host or host

3. Perform the browsing and ping steps.

4. Stop capture after enough packets are collected.

Step 4: Analyze Captured Traffic

1. Apply a display filter to focus on interactions between devices: text ip.addr == && ip.addr ==

2. Filter HTTP traffic:

Text

http

3. Filter ICMP (ping) traffic:

text

icmp

4. Analyze HTTP packets to see that the server response is unencrypted (HTTP on port 80).

5. Examine ping request and reply packets under ICMP protocol.

6. Note absence of encryption on HTTP traffic, highlighting security risk if sensitive data is sent.

Findings

- HTTP communication between the Android phone and laptop is unencrypted, visible in plaintext to any network sniffer.
- ICMP ping packets are seen as expected, confirming connectivity.
- Potential security risk: Any login or sensitive data sent over HTTP can be intercepted.

Conclusion

This practical exercise illustrates the exposure of unencrypted HTTP traffic and the nature of ICMP packets during device communication over Wi-Fi. Securing IoT device interactions with encrypted protocols like HTTPS or VPN