

# **TASK 3**

## **SECURE YOUR OWN WI-FI NETWORK**

### **Objective**

To evaluate the home Wi-Fi network security using Wireshark, identifying unencrypted traffic, unauthorized devices, and potential vulnerabilities.

### **Tools Used**

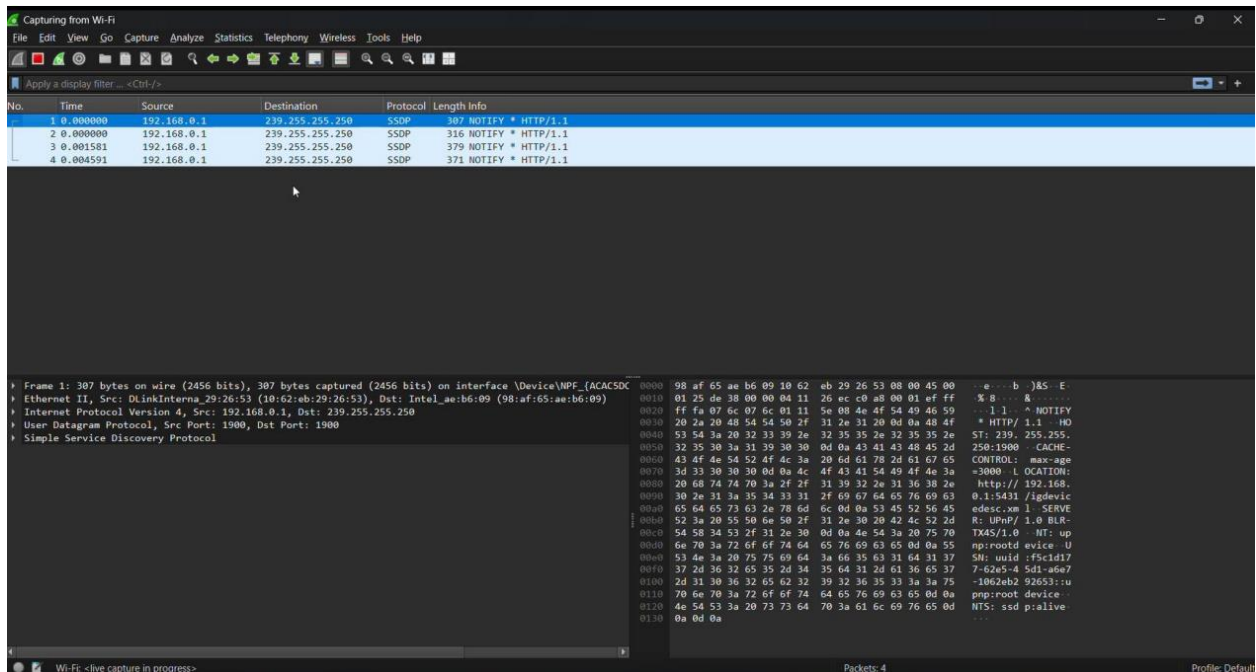
- Wireshark: Packet capture and analysis tool

### **Sequence of Events**

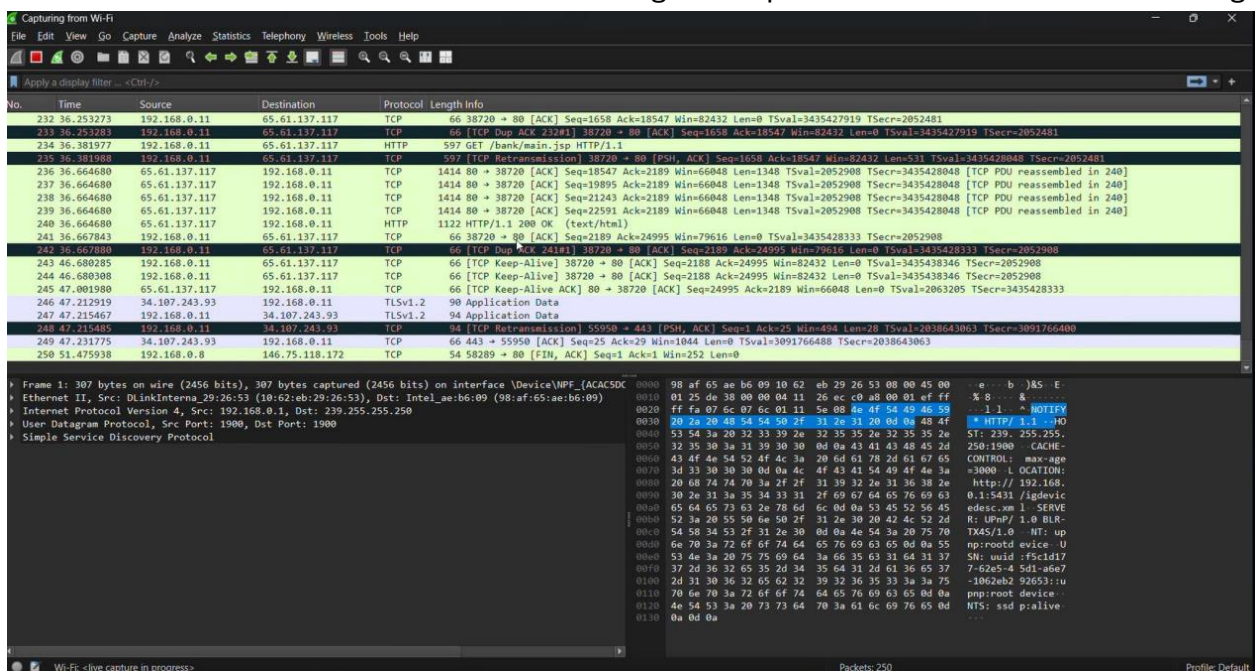
1. Launch Wireshark and select the correct Wi-Fi interface.
2. Enable monitor/promiscuous mode (e.g., wlan0mon on Linux).
3. Start capturing packets by clicking the 'Start' button.
4. Use filters to analyze traffic (e.g., http, ip.addr, tcp).
5. Identify unencrypted traffic (e.g., HTTP, FTP) and follow TCP streams to inspect data.
6. Use 'Statistics > Endpoints' to list all connected devices and check for unauthorized ones.
7. Watch for suspicious activities like excessive ARP requests or unusual port usage.
8. Stop capture and save the .pcap file for detailed analysis.

### **Findings and Alterations**

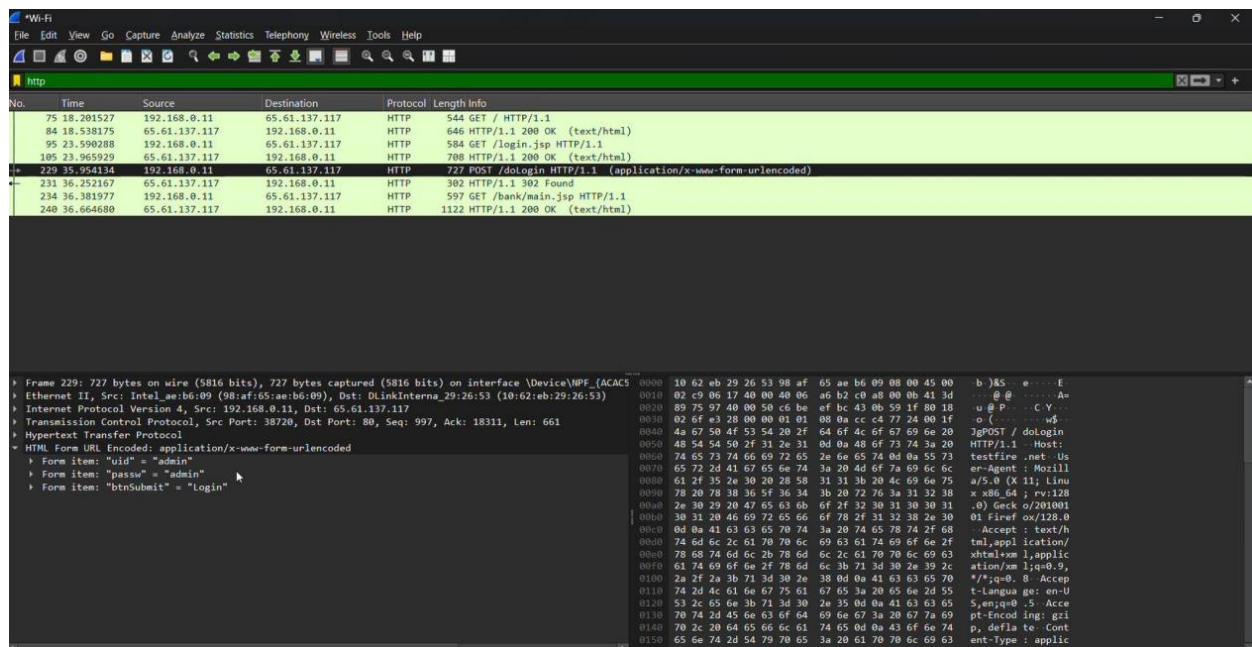
- Unencrypted HTTP traffic can expose sensitive data. Use HTTPS.



- Unknown devices detected on network. Change Wi-Fi password and enable MAC filtering.



- No major suspicious behavior found during packet analysis.



- Overall recommendation:

Upgrade to WPA3 encryption, regularly audit devices, disable WPS.

## Conclusion

Wireshark is a highly effective and widely used tool for analyzing and diagnosing vulnerabilities within Wi-Fi networks. Through this assessment, it becomes evident how critical it is to implement proper security measures to protect wireless communication. Wireshark allows network administrators to capture and inspect real-time data packets, helping them identify potential threats such as unauthorized access points, unencrypted data transmissions, packet sniffing, and man-in-the-middle attacks.

The analysis emphasizes the importance of using strong encryption protocols like WPA3 to safeguard data in transit. It also underscores the need for continuous monitoring of connected devices to detect unusual activity or rogue devices attempting to join the network. Additionally, properly securing network configurations—such as disabling WPS, changing default credentials, and segmenting networks for different user groups—plays a vital role in reducing attack surfaces.

Overall, Wireshark serves as a valuable tool in maintaining the integrity, confidentiality, and availability of wireless networks, reinforcing the need for a proactive approach to Wi-Fi security.