

Wireshark-Based Wi-Fi Security Assessment Report

Objective

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

Tools Used

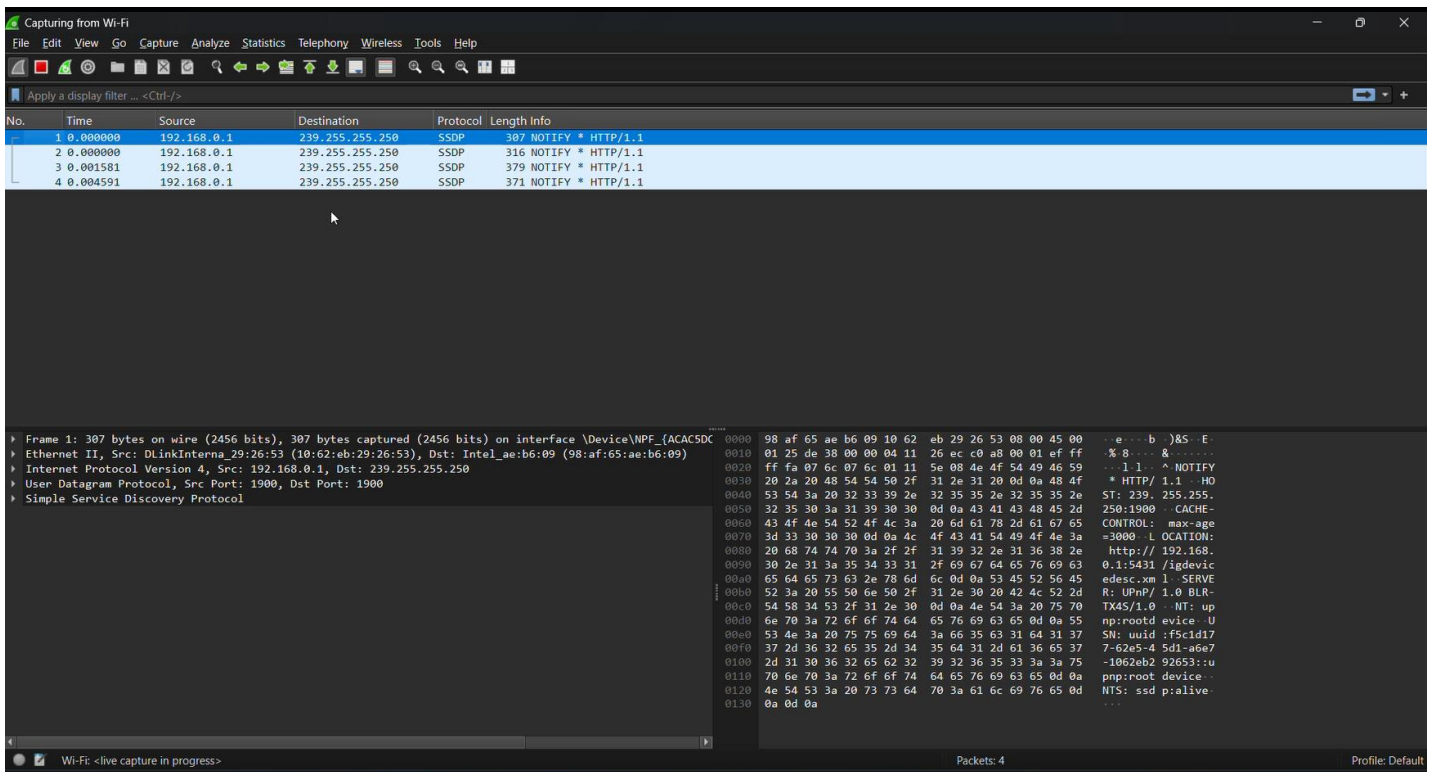
- Wireshark: Packet capture and analysis tool

Step-by-Step Process

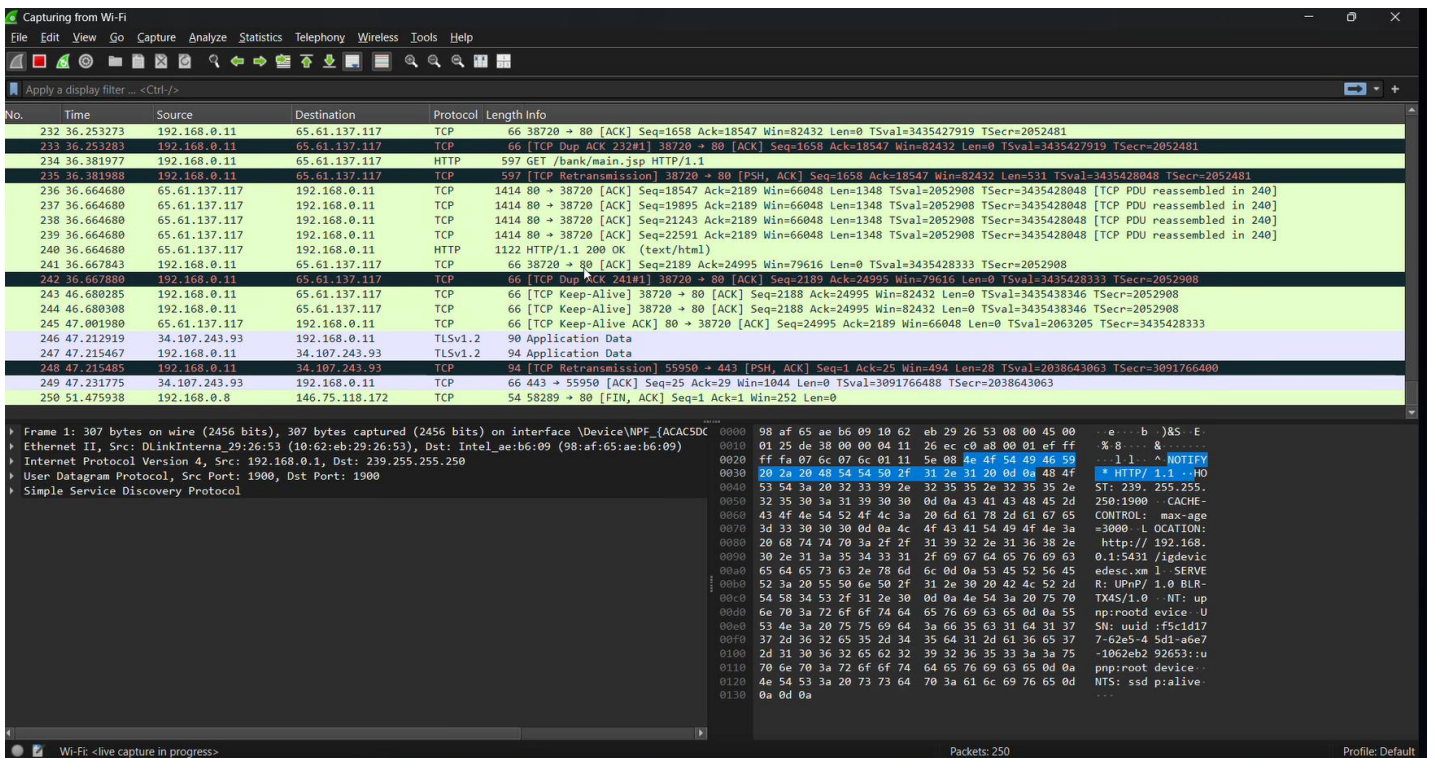
1. Launch Wireshark and select the correct Wi-Fi interface.
2. Enable monitor/promiscuous mode (e.g., wlan0mon on Linux).
3. Start capturing packets by clicking the 'Start' button.
4. Use filters to analyze traffic (e.g., http, ip.addr, tcp).
5. Identify unencrypted traffic (e.g., HTTP, FTP) and follow 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 Recommendations

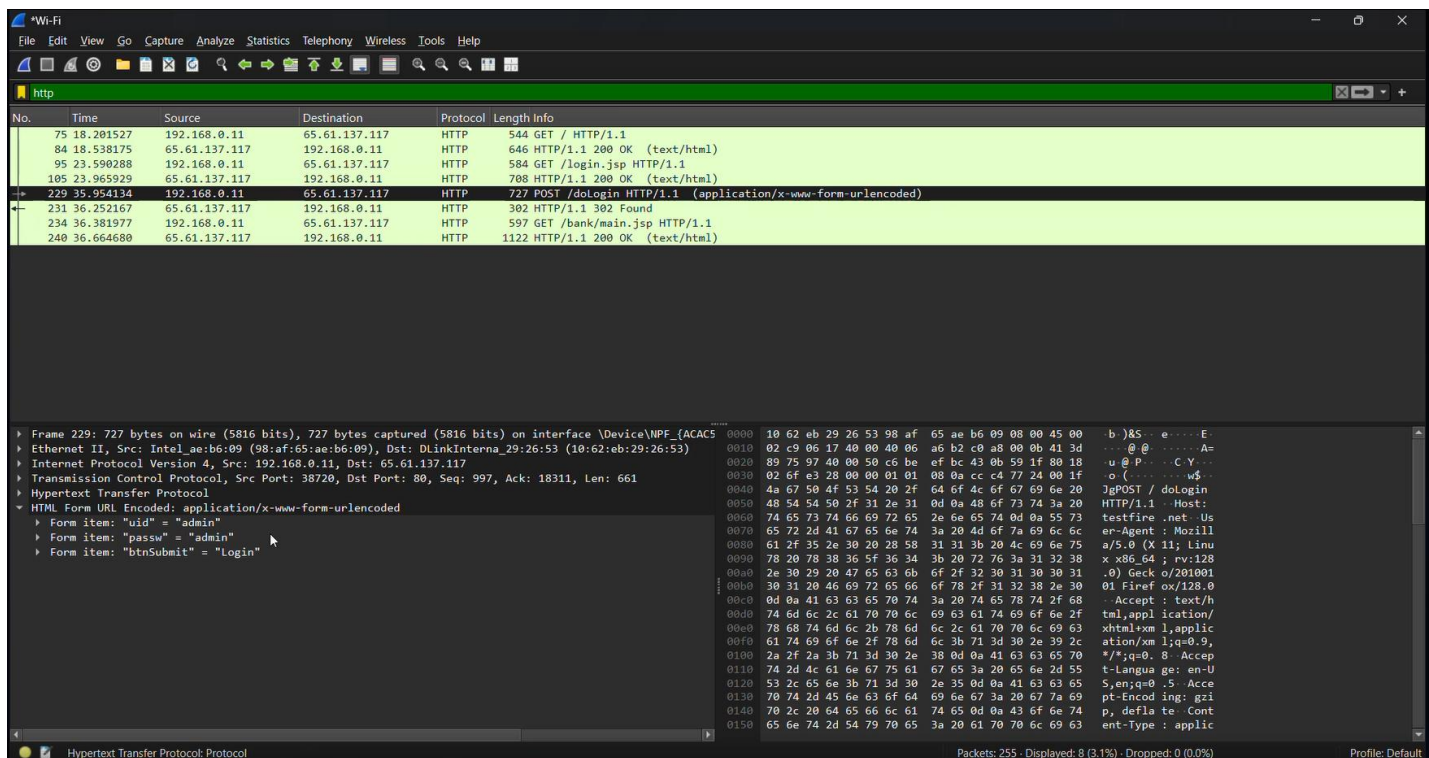
- Unencrypted HTTP traffic can expose sensitive data. Use HTTPS.



- 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 powerful tool to detect and diagnose Wi-Fi network vulnerabilities. This assessment highlights the importance of using encryption, monitoring devices, and securing network configurations.