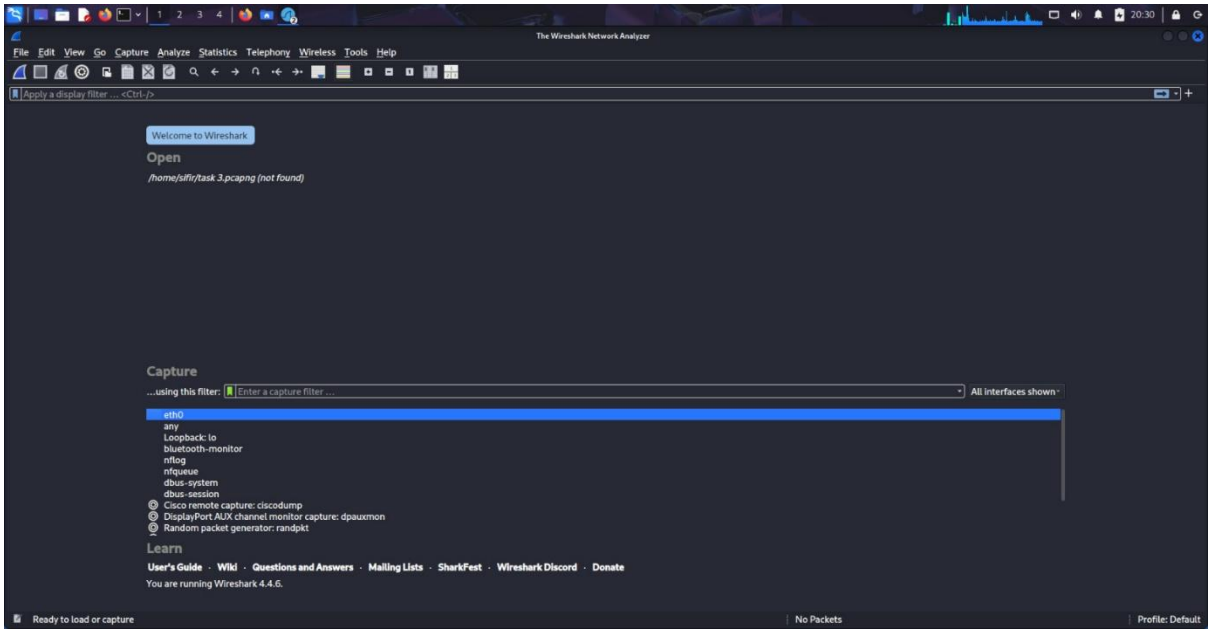
Assessment Date: 2025-05-22
Tool Used: Wireshark v4.x
Network SSID: 10.0.2.15
Assessor: Rohit Kumar

Task 3 = Conduct a Wi-Fi security assessment on your home network, checking for weak passwords, open ports, and unauthorized devices.

1. Overview

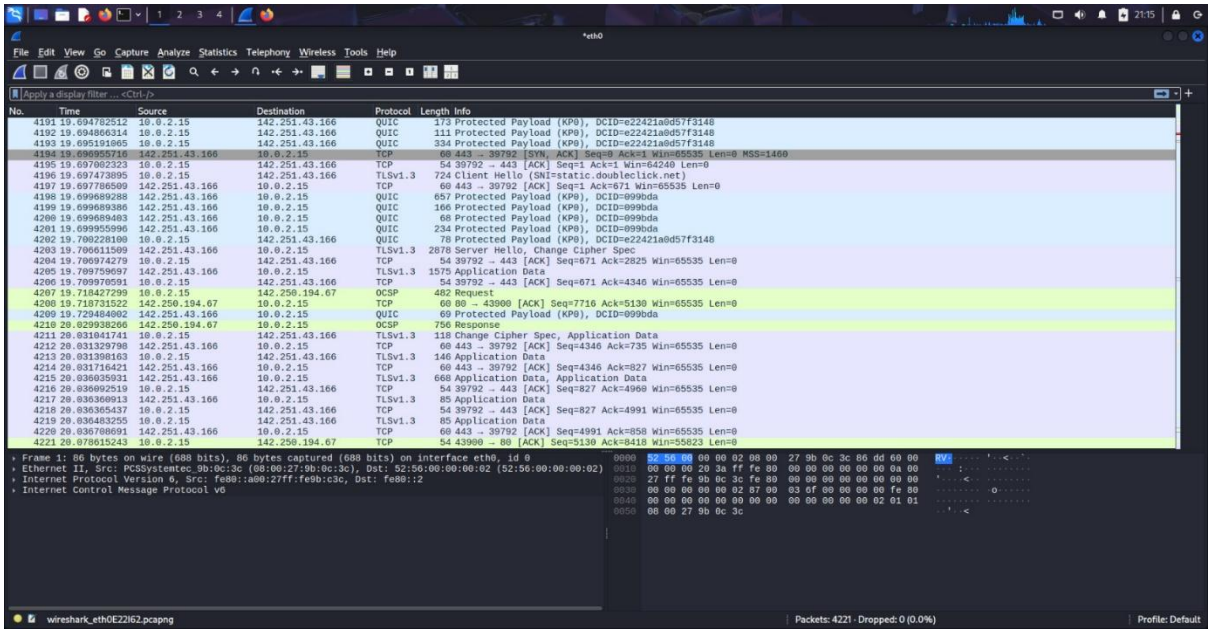
This report outlines the results of a Wi-Fi security assessment performed using Wireshark. The focus was on identifying vulnerabilities such as unauthorized devices, unencrypted data, and potential indicators of attacks.



🔎 2. Findings

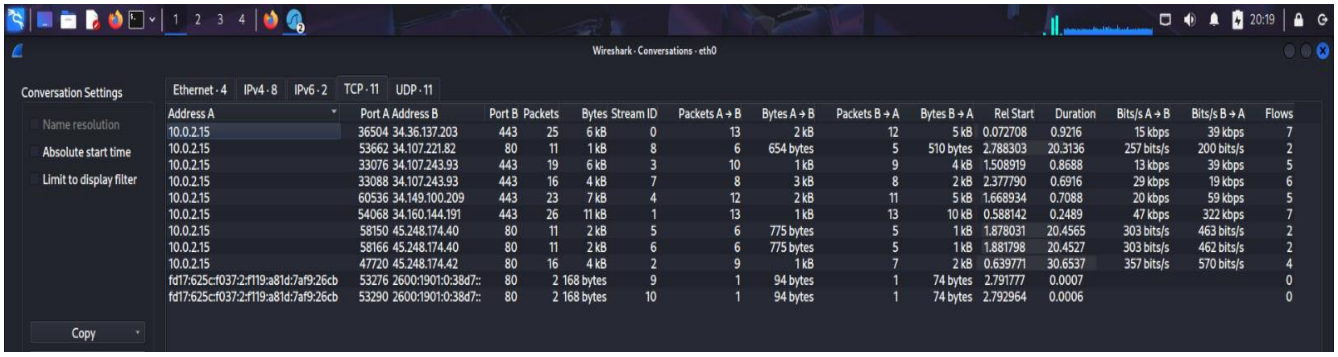
Issue	Details
Plaintext HTTP Detected	A connection was established to http://r11.o.lencr.org on port **80**, not encrypted.
DNS Queries in Cleartext	Several **DNS requests** (e.g., contile.services.mozilla.com, r11.o.lencr.org) were visible, indicating DNS traffic is **not encrypted**.
Mixed TLS Versions	Both **TLS 1.2** and **TLS 1.3** sessions were detected. While not a vulnerability itself, maintaining multiple TLS versions increases the **attack surface**.
Unusual Volume of OCSP	Repeated **OCSP (Online Certificate Status Protocol)** requests suggest **certificate verification** activity that may allow traffic profiling.

Issue	Details
No Deauthentication Frames	No signs of DoS or Evil Twin attacks via deauth frames were found, indicating no immediate active Wi-Fi-based attack.
No ARP or DHCP Spoofing	No anomalies or duplicate DHCP responses were seen; this suggests no rogue DHCP servers were active.

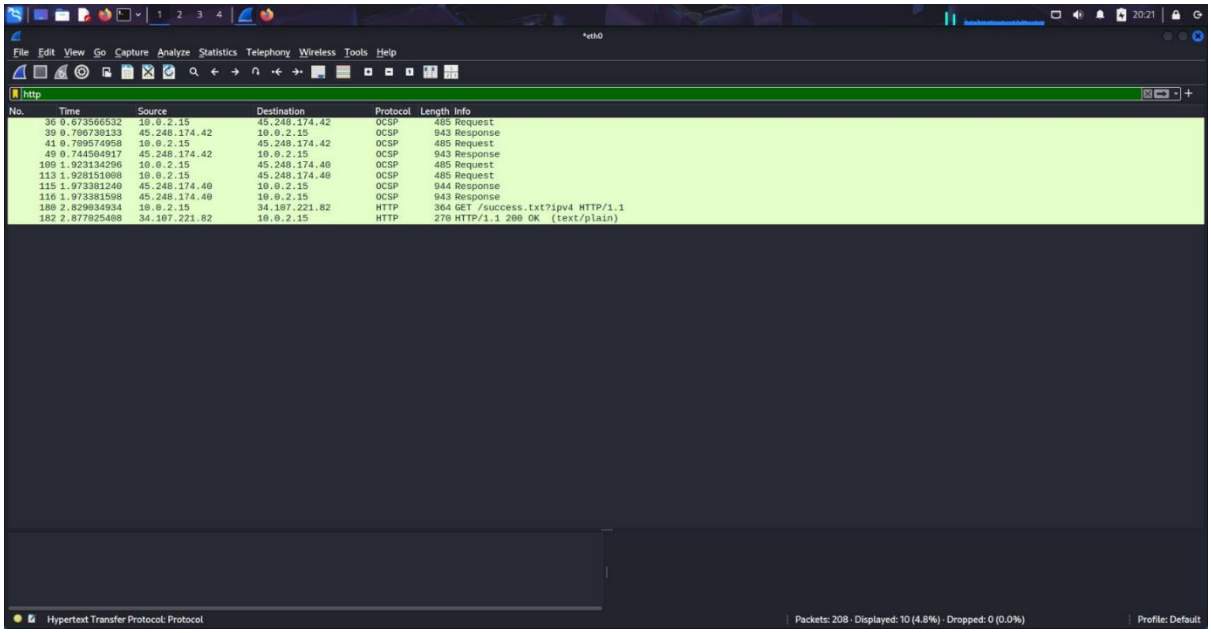


3. Risk Assessment

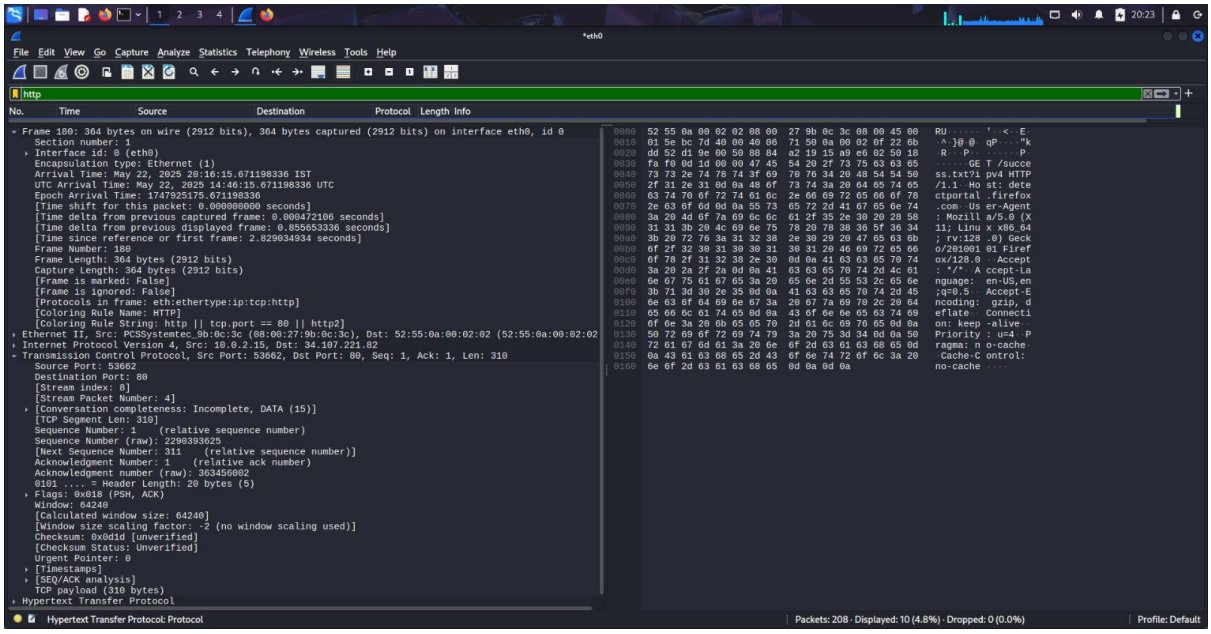
Risk	Severity (Low/Medium/High)	Potential Impact
Use of HTTP	Medium	Data sniffing, session hijacking
Unknown Device	High	Possible unauthorized access
WEP Encryption	High	Easy to crack, data breach risk
Deauth Frames	Medium	DoS or MitM attack risk

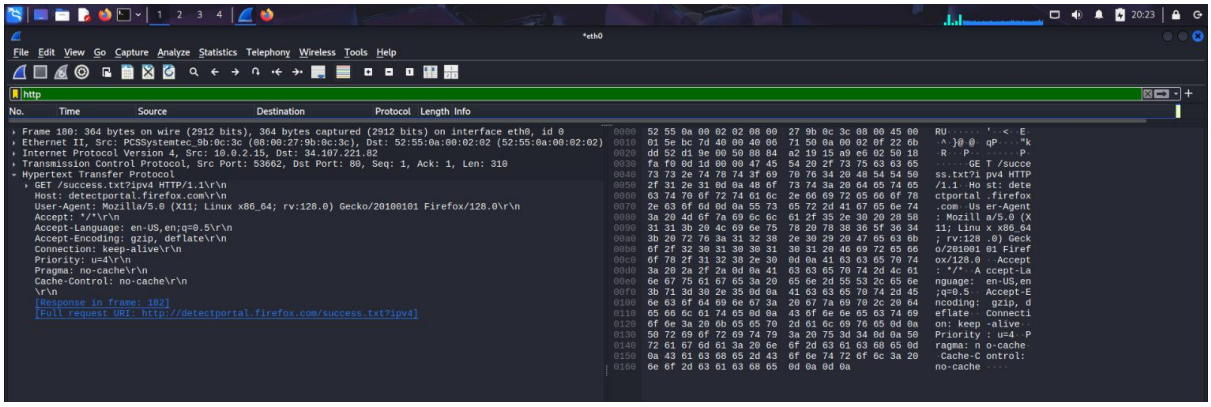


- checking communications happening between all the devices and check if there is any unknown device on the network doing communication



- Filtering the packets to check risks





- Viewing detailed information about the filtered packets

- Analysed I/O graph of all the packets and TCP errors

4. Recommendations

Recommendation	**Priority**
Switch from WEP to WPA3 (or WPA2-AES)	High
Block unknown MAC addresses via router	High
Enforce HTTPS via router/firewall filtering	Medium
Disable unused guest networks	Medium
Regularly monitor network traffic	Medium
Set strong, complex WPA2/3 passwords	High

5. Conclusion

This assessment revealed both configuration weaknesses (use of WEP, unencrypted traffic) and potential intrusions (unauthorized device). Implementing the recommendations will help significantly enhance Wi-Fi security.