# FUTURE INTERNS CS TASK 3

# TASK 3 SECURE YOUR OWN WI-FI NETWORK

# INTRODUCTION

This report presents the findings of a Wi-Fi security assessment conducted on the home network. The assessment included identifying devices on the network, scanning for open ports, and analyzing network traffic using tools like Nmap and Wireshark.

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

**Tools:** Wireshark, Nmap.

# IDENTIFY DEVICES ON THE NETWORK

To identify all connected devices within the internal network using Nmap, helping uncover potential rogue devices, unmonitored endpoints, or misconfigured hosts.

A port scan was conducted using Nmap to detect open ports and associated services.

**Commands Used:**

ip a

nmap -sn 192.xxx.x.x/24

nmap -sS -O 192.xxx.x.x/24

nmap -sS -Pn -p- 192.xxx.x.x/24

Visit <http://192.xxx.x.1> to manage the ports using GUI. Login using username and password.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Key Observation:**

* all connected devices were identified.
* Devices were verified by IP and MAC address.
* No unauthorized devices were detected.
* Findings indicate that some devices expose commonly open ports like 80 (HTTP), 443 (HTTPS), and 22 (SSH).
* Older versions of web servers, SSH, SMB, etc., may contain known CVEs (Common Vulnerabilities and Exposures).

**Recommendations to Improve Security:**

* Document all devices (IP, MAC, hostname, purpose, owner) and regularly reconcile them with discovery scans.
* Implement MAC address filtering or NAC solutions to allow only approved devices onto the network.
* Use Static IPs or DHCP Reservations for Known Devices.
* Use router-level firewall rules to block unused outbound ports and suspicious domains.

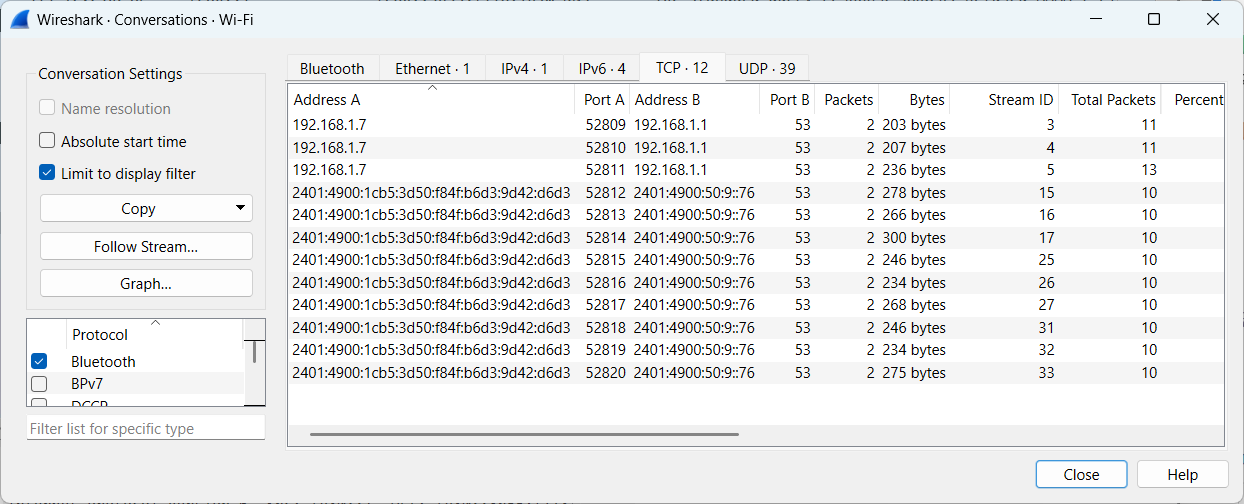
# ANALYZE NETWORK TRAFFIC FOR ANOMALIES

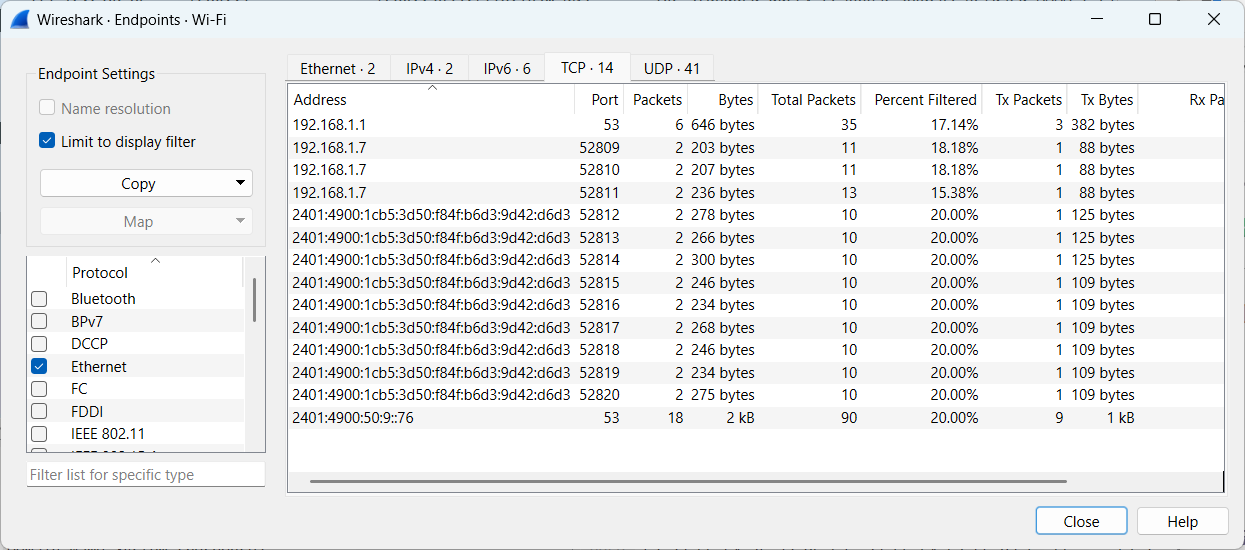
Traffic analysis was conducted using Wireshark. Observations revealed no long-lived or high-volume connections to external IPs, which indicates limited risk of external command and control activities. The protocol hierarchy showed standard usage of DNS, ARP, and minimal HTTPS, HTTP, or TLS traffic.

A screenshot of a computer

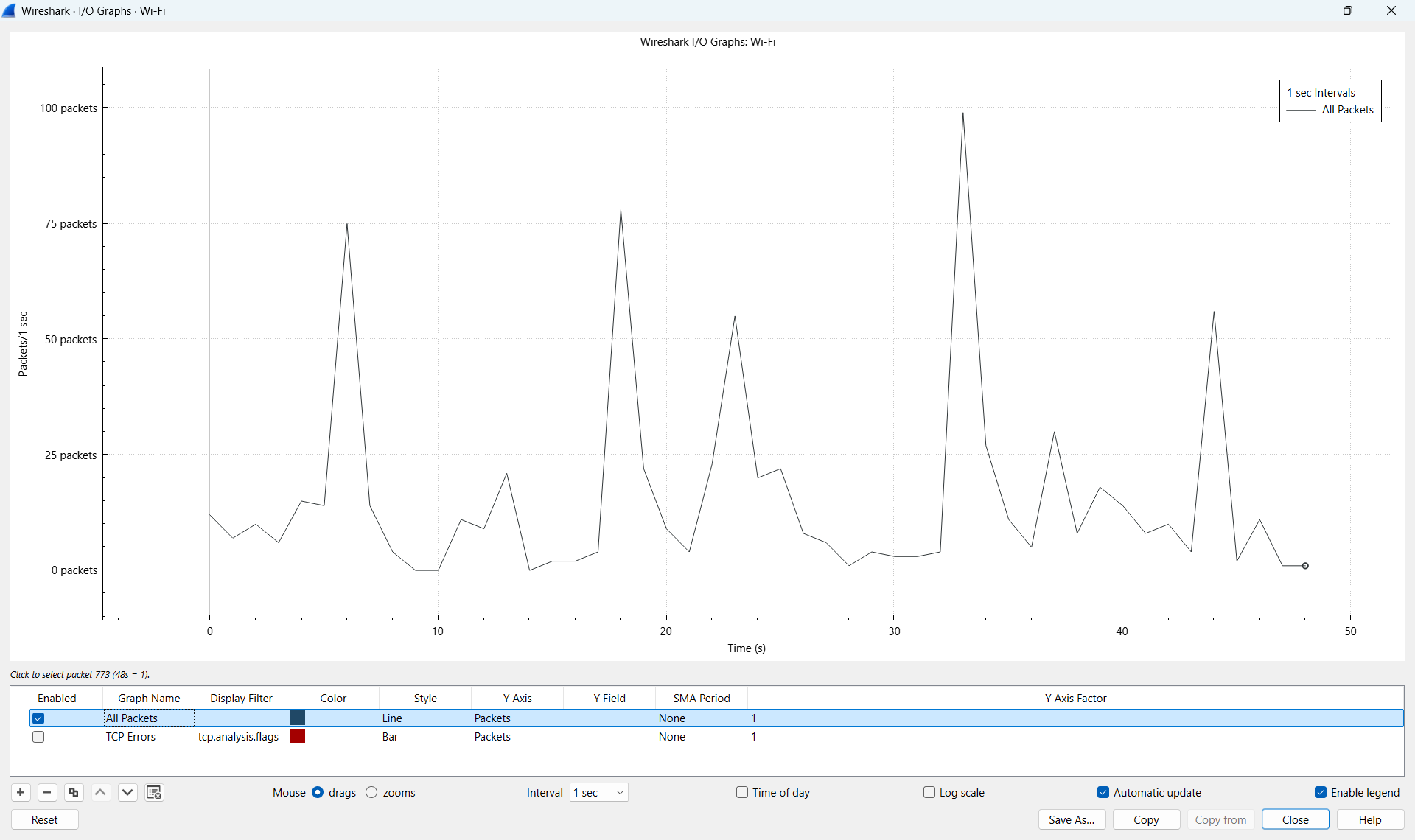
AI-generated content may be incorrect.

WIRESHARK UI

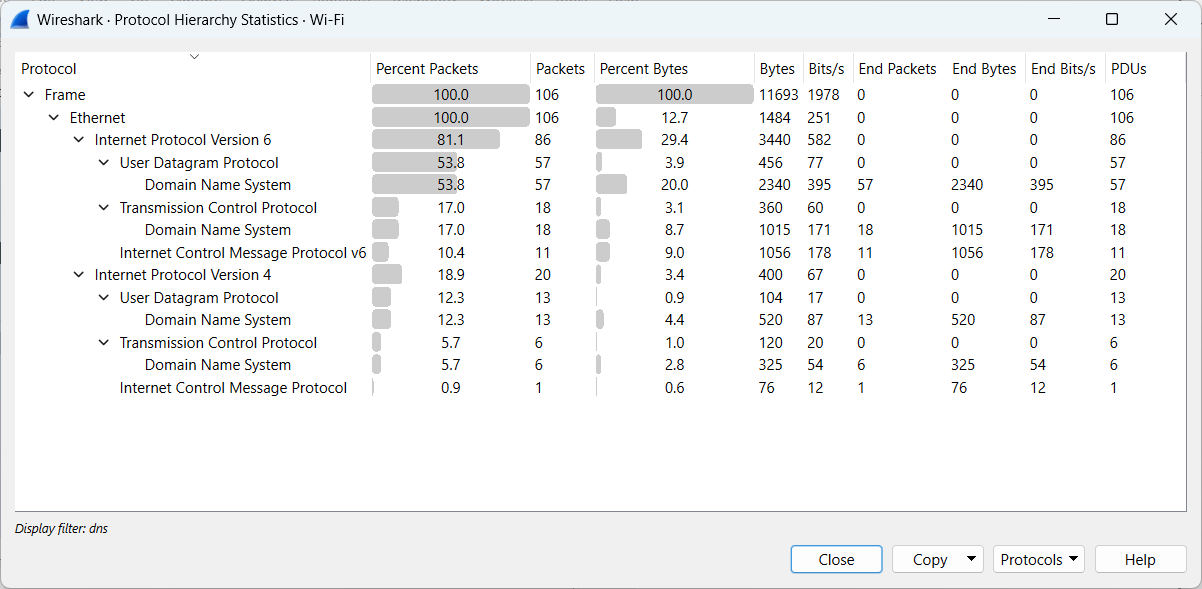
Wireshark Conversations



Wireshark Endpoints



Wireshark IO Graph



Wireshark Protocol Hierarchy

**Key Findings:**

Protocol Hierarchy - showed minimal use of HTTP, HTTPS, DNS, ARP, and TLS — all in normal proportions.

Conversations - No long-duration, high-volume connections and No significant external IP communication suggesting C2 activity.

Endpoints - No device overwhelmed with unusually high packet or byte counts.

IO Graph - No sudden spikes or sustained traffic bursts.

No suspicious packet patterns, such as ARP poisoning , DNS tunneling , Large file transfers to unknown Ips.

**Key Observations:**

* Some protocols observed (e.g., DNS or HTTP) may transmit data in plaintext, making them vulnerable to sniffing.
* While none were found here, traffic to unknown IPs or non-standard ports is a red flag for exfiltration or backdoor activity.

**Recommendations to Improve Security:**

* Transition all services to HTTPS, SFTP, SSH, and other encrypted alternatives.
* Devices generating large volumes (e.g., CCTV, NAS) should be on isolated VLANs to prevent network noise or lateral attacks.
* Use router-level firewall rules to block unused outbound ports and suspicious domains.

**SUBMITTED BY :** MODEKURTI SRIHARSHA

**ROLE:** Cybersecurity Intern

**COMPANY :** Future Interns