Task 3: Secure your own WI-FI Network

# Wi-Fi Security Analysis Report

**Date of Analysis:** April 15–16, 2025

**Performed by:** Sahiti M

## Tools Used:

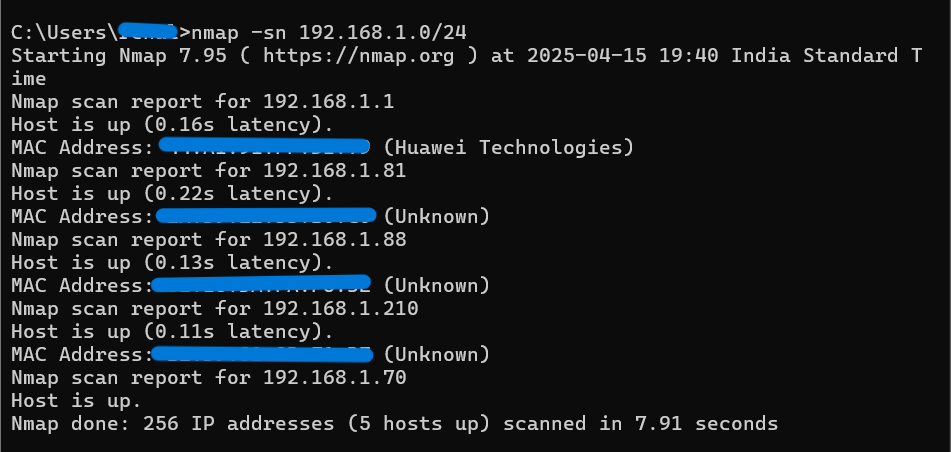
* **Nmap** (for network scanning)
* **Wireshark** (for packet analysis)
* **Windows Command Line**
* **Router Web Interface**
* **Device: Realtek RTL8821CE Wi-Fi Adapter** (monitor mode unsupported)

## 1. Identify Devices on the Network:

* Scanned the local network using nmap -sn 192.168.1.0/24

#### Findings:

* Several active IP addresses were discovered on the network.
* Devices included phones, laptops, and possibly smart TVs or IoT devices.
* MAC addresses were identified for each device.

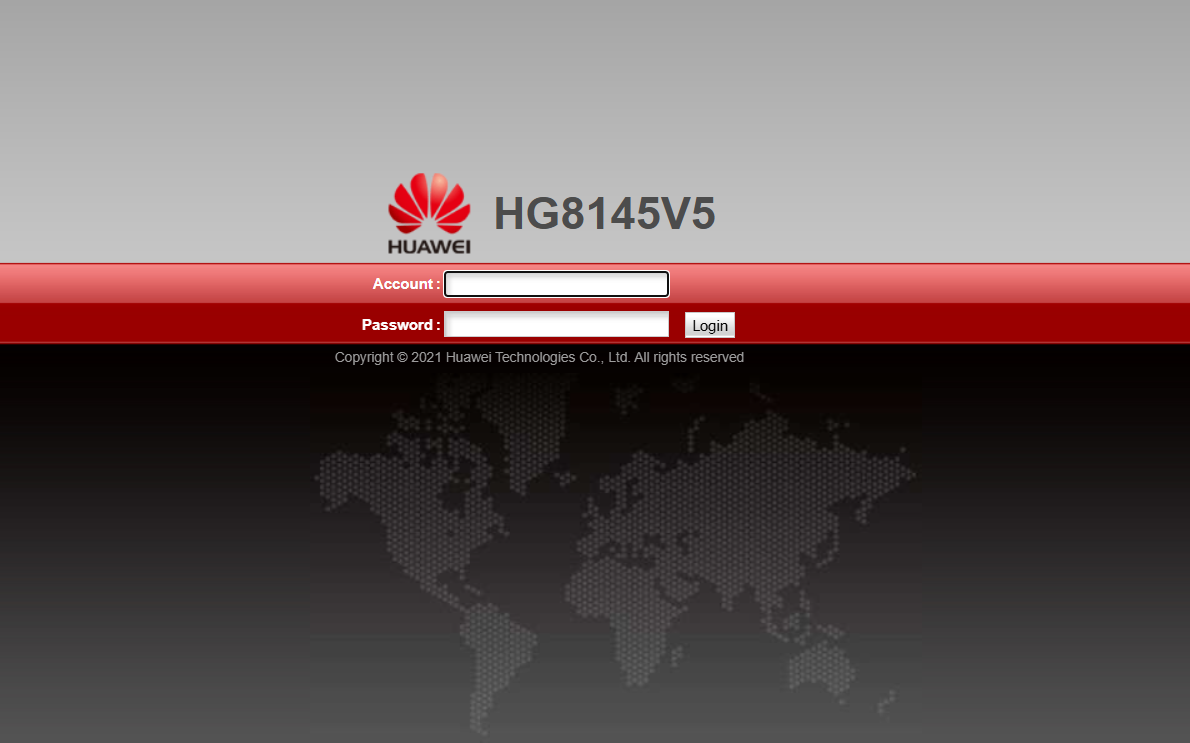


## 2. Access Router Admin Panel:

* Router accessed via browser at 192.168.1.1
* Logged in using admin credentials (default or user-defined)

#### Findings:

* Tabs visible: WAN, LAN, IPv6, WLAN, Security, Route, ForwardRules, etc.
* Confirmed ability to see connected devices via WLAN tab.





## 3. Port Scan on Internal Devices:

Tool Used: **Nmap**

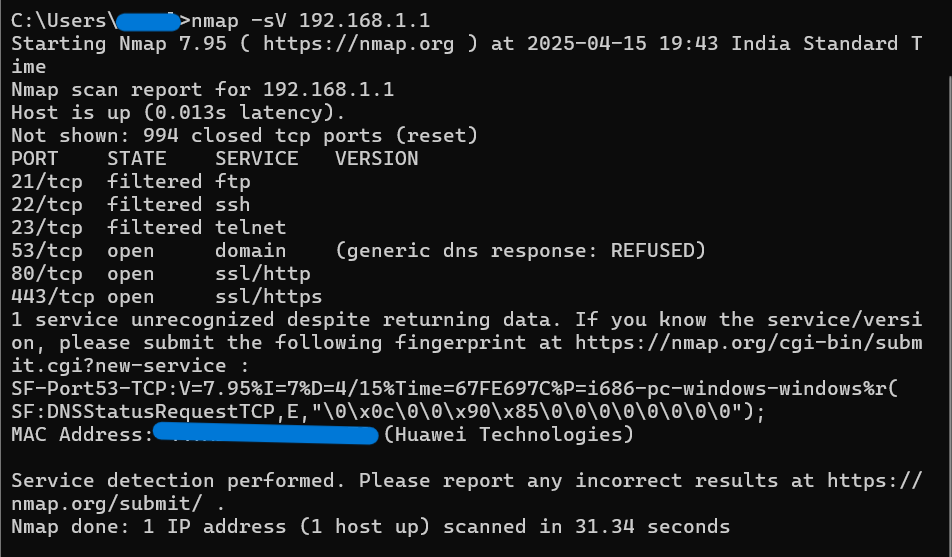
Nmap is a powerful network scanning tool used to detect hosts, services, and potential vulnerabilities on a network. The -sV flag is used to detect service versions running on open ports.

### Target IP’s:

* 192.168.1.1
* 192.168.1.210
* 192.168.1.88

#### Device 192.168.1.1 (Router/Gateway):

The IP address 192.168.1.1 is commonly assigned to a **router or default gateway** in a local network. It acts as the primary bridge between internal devices and the internet. Scanning the router helps us assess its **exposed services, default ports, and any potential security weaknesses**.



##### **Filtered Ports (21, 22, 23)**

* **FTP (21), SSH (22), and Telnet (23)** are standard remote access services.
* The **"filtered"** state indicates that a firewall or access control is blocking or silently dropping requests to these ports.
* This is a **positive security measure**, as these ports are often targeted for brute-force or exploit attacks.
* It prevents unauthorized remote access attempts and reduces the router’s attack surface.

##### **Open DNS Port (53)**

* Port 53 is used for **DNS (Domain Name System)** services.
* In this scan, the port is **open** but returns a **"REFUSED"** response.
* This means the DNS server is active but **not resolving queries from the scanning device**, which likely isn’t recognized as an internal client.

##### **Open Web Services (Ports 80 & 443)**

* Port 80 (HTTP) and 443 (HTTPS) host the **web-based administration interface** of the router.
* HTTPS is the secure version of HTTP, encrypting credentials and session data during login.
* Having both ports open may indicate:
  + Either **dual access is allowed** (HTTP & HTTPS), or
  + **HTTP redirects to HTTPS** to enforce encryption.
* If HTTP access is not redirected or disabled, it could allow attackers on the same network to **intercept login credentials in plain text**.

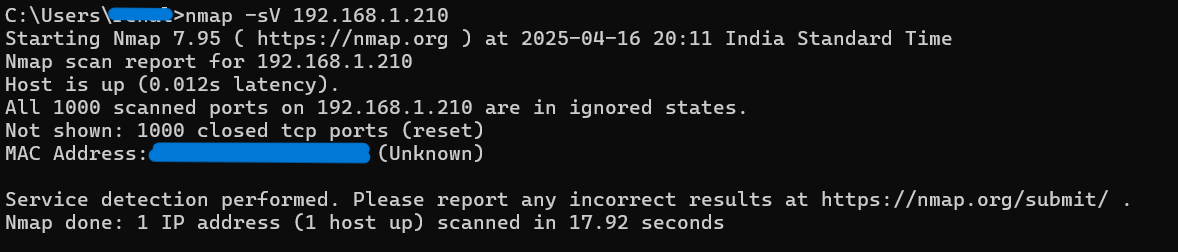
##### Interpretation by Port:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Port** | **State** | **Protocol** | **Description** | **Comments** |
| 21/tcp | Filtered | FTP | File Transfer Protocol | Not accessible externally; likely blocked by firewall |
| 22/tcp | Filtered | SSH | Secure Shell (for remote admin) | Same as above – blocked/filtered |
| 23/tcp | Filtered | TELNET | Legacy Remote Access | Telnet is considered insecure and best kept disabled |
| 53/tcp | Open | DOMAIN (DNS) | Domain Name Service | DNS service is active but returning REFUSED – restricted usage, likely only for local clients |
| 80/tcp | Open | HTTP | Web interface (non-secure) | The router's admin page may be available here |
| 443/tcp | Open | HTTPS | Secure Web interface | Admin panel likely accessible via browser at https://192.168.1.1 |

##### Best Security Practices Inferred from This Scan:

* **Disable HTTP (Port 80)** if HTTPS (443) is already enabled to prevent non-secure access.
* **Keep SSH and Telnet disabled/filtered,** unless remote router management is absolutely required.
* **Verify access control** for DNS (Port 53) to ensure only internal clients can use it.

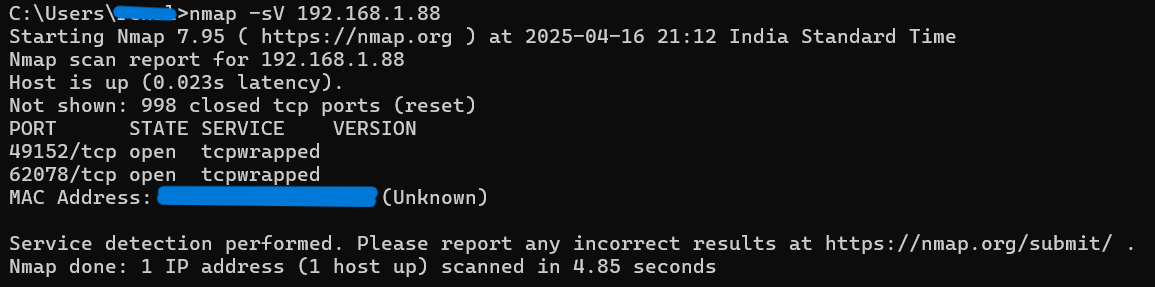
#### Device 192.168.1.210:



##### Interpretation:

* The device is **on and reachable**, but **no ports responded positively** to Nmap probes.
* All ports are in **closed/reset state**:
  + A "reset" means the device actively replied with a **TCP RST (Reset)** packet, indicating it is **not accepting connections** on that port.
* This is common behavior when:
  + The device has a strong firewall.
  + No services are currently running/listening on known ports.
  + It’s a “silent” client device (like a phone, tablet, or smart TV not offering any services).

#### Device 192.168.1.88:



##### Interpretation:

* **49152/tcp** and **62078/tcp** are **high-numbered dynamic or ephemeral ports**, often used by system processes or temporary connections.
* Marked as **tcpwrapped** – this means:
  + The port is open, but access is restricted.
  + Any probe from Nmap is wrapped (protected) by TCP wrappers or a firewall (e.g., via iptables, hosts.allow/hosts.deny, or proprietary OS firewalls).
  + The service did not provide detailed version info because it refused Nmap’s connection request or cloaked the response.

##### Common Uses:

* **Port 49152** is part of the IANA-assigned dynamic/private port range (49152–65535). Often used for:
  + UPnP (Universal Plug and Play)
  + Windows RPC (Remote Procedure Call)
  + iTunes / Bonjour services
* Port 62078 is typically used by **Apple's lockdownd service**:
  + If this IP is an Apple device (iPhone, iPad, or Mac), this port enables iTunes-like communication for data syncing.

##### Note:

* While open, both ports are protected via wrapper or firewall rules.
* No version info means **Nmap couldn’t fingerprint the service**, reducing risk of remote fingerprinting attacks but also limiting our insight.

#### General Analysis:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IP Address** | **Ports Open** | **State** | **Likely Device** | **Comments** |
| 192.168.1.1 | 53 (DNS), 80 (HTTP), 443 (HTTPS) | 53: Open (DNS REFUSED)  80: Open  443: Open  21/22/23: Filtered | Router (Huawei Technologies) | Basic services active, admin panel exposed, some ports filtered. |
| 192.168.1.210 | None | All closed | IoT / phone / laptop | Highly secured or not running any network services |
| 192.168.1.88 | 49152, 62078 | Open (tcpwrapped) | Apple device (likely iPhone/iTunes) | High-numbered ports suggest transient/mobile device |

##### Final Interpretation:

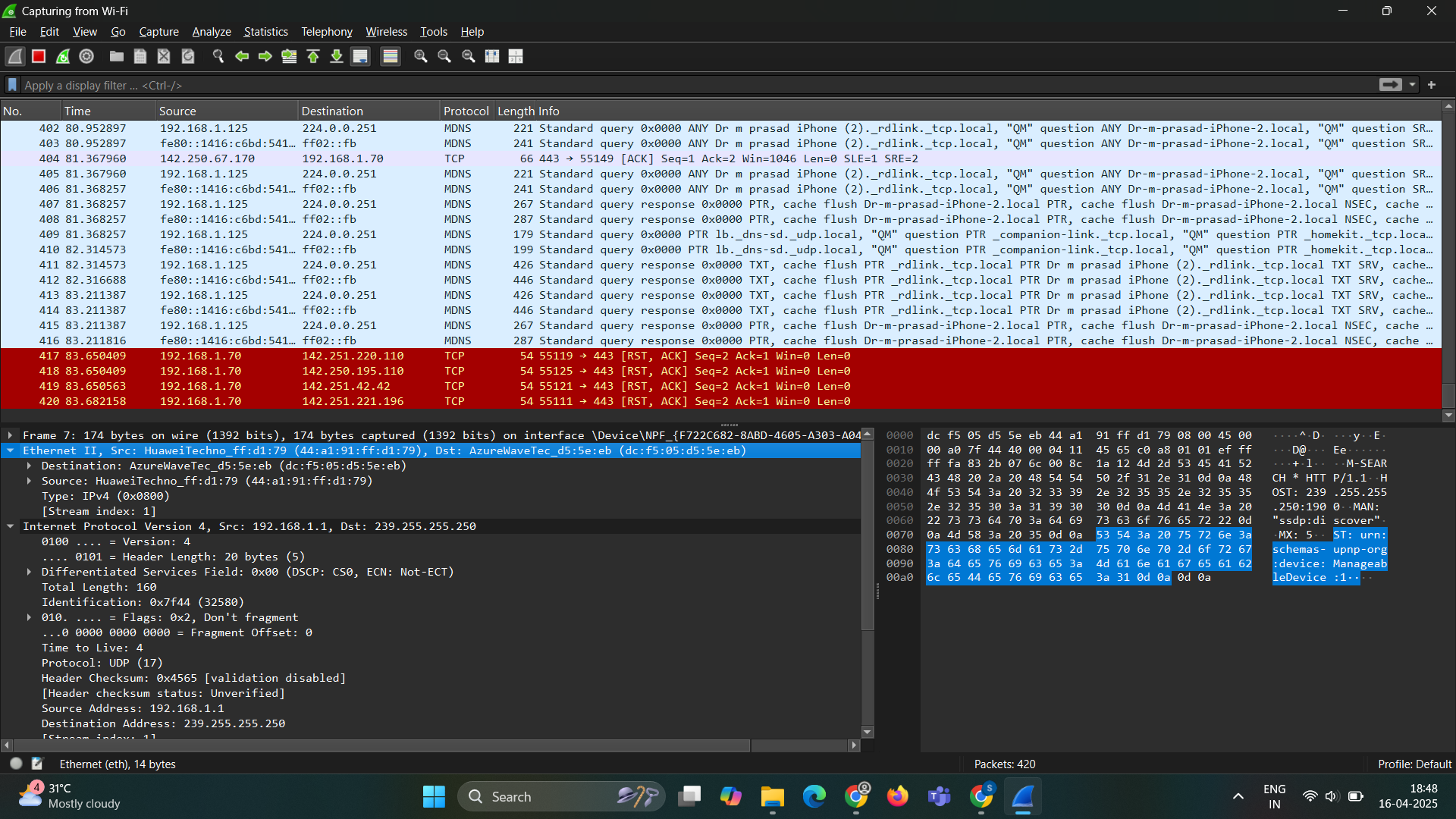
* Minimal exposure. No vulnerable ports found.
* Devices appear to be hardened or have firewall rules applied.

## 4. Analyze Wi-Fi Traffic (Passive Mode)

Tool Used: Wireshark

#### Capture Details:

* Interface used: Realtek RTL8821CE (no monitor mode)
* Number of packets captured: 7000+
* Source and Destination IPs/Ports analyzed

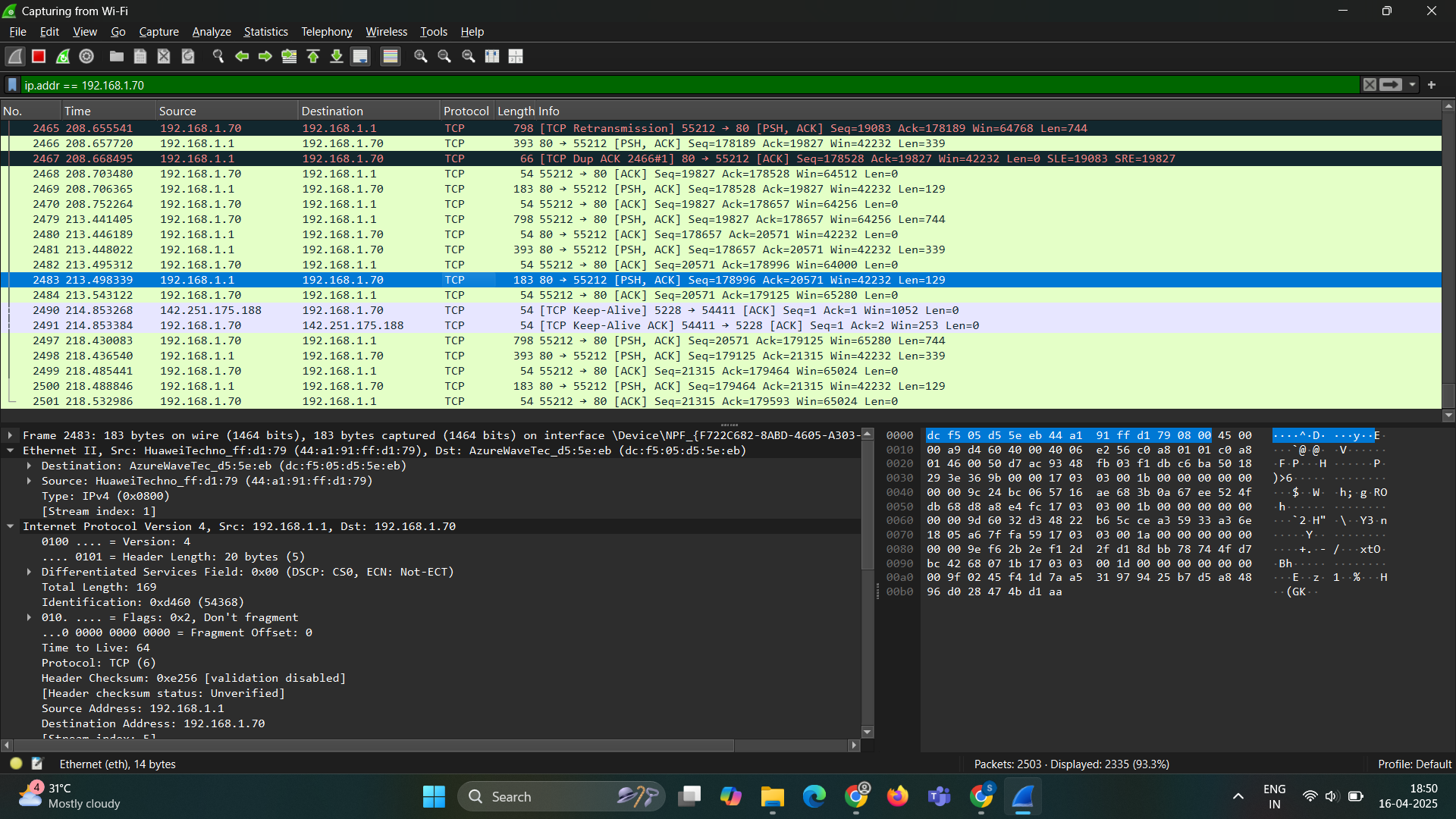


#### Observed Protocols:

* **TCP**: Reliable transport protocol — used in web traffic and applications.
* **HTTP**: Application layer protocol — shows GET requests (web browsing).
* **TLSv1.2**: Secure connection protocol (used by HTTPS).
* **DNS**: Name resolution protocol (domain names to IPs).
* **ARP**: Resolves IP to MAC address on the local network.
* **SSDP (Simple Service Discovery Protocol)**: Used for device/service discovery (IoT or Smart TVs).
* **NBNS (NetBIOS Name Service)**: Used in Windows networks for name resolution.
* **ICMP**: Internet Control Message Protocol — used for diagnostics (e.g., ping).

#### Notable Packet Captures:

* **TCP Handshakes**: Multiple sequences of SYN, SYN-ACK, and ACK packets were captured, confirming the setup of reliable TCP sessions.
* **HTTP Traffic**: Captured GET requests to /generate\_204, which are typically used by Android or Chrome devices to check internet connectivity.
* **TLS Sessions**: Encrypted sessions observed between local devices and external services (e.g., Google).
* **DNS Queries**: Name resolution requests for hostnames like clients3.google.com were present, indicating normal browsing activity.
* **SSDP Multicast Traffic**: Suggests presence of smart home or IoT devices communicating on the network.
* **ARP Activity**: Consisted of standard "Who has" and "is-at" messages — common in local LAN activity.
* **ICMP Packets**: Indicated typical diagnostic operations (e.g., ping) with no anomalies.

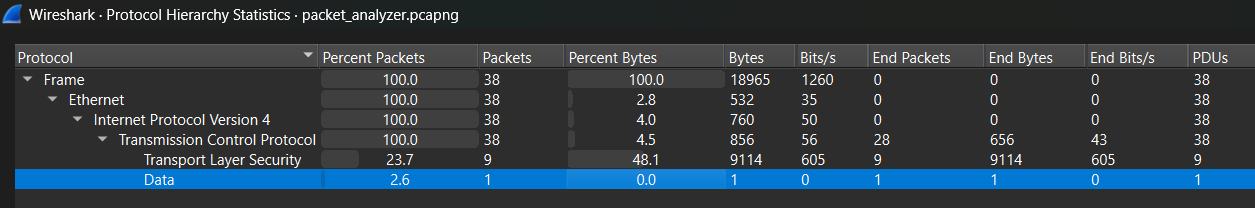


#### Security & Behavior Insights:

* No evidence of malicious activities like ARP spoofing, DNS poisoning, or unauthorized access attempts.
* All TLS and HTTP traffic patterns appeared consistent with regular user browsing behavior.
* Noticeable volume of **SSDP/Multicast** packets — likely generated by background services or smart devices.
* **ICMP packets** observed were limited and matched standard diagnostic behavior.

#### Protocol History:

A visual summary of protocol usage during Wireshark packet capture:



##### Key Insights:

* **100% of captured packets** were **Ethernet over IPv4**, with all packets using the **TCP** protocol.
* **23.7% of the TCP traffic** was secured using **TLS (Transport Layer Security)** — indicating encrypted communication.
* **One packet** contained raw **Data** (unclassified payload) — could be application-level traffic or incomplete handshake data.
* **Most traffic (48.1% by volume)** was TLS-encrypted, suggesting communication with secure services (e.g., HTTPS sites or secure apps).

##### Interpretations:

* The dominance of TCP and TLS suggests that the observed devices were engaging in secure, connection-oriented communication — possibly browsing or syncing with cloud services.
* No UDP, ICMP, or other protocol traffic was seen — this could be due to filter settings or the short capture window.
* This kind of view is useful to confirm **encrypted vs unencrypted traffic ratios** and understand what types of communication are happening in your network.

#### Summary of Wi-Fi traffic:

* Filters applied included tcp, http, ip.addr == 192.168.1.x, and arp.
* Common traffic flows were identified and categorized by protocol.
* Security checks confirmed that traffic was benign and aligned with normal operations.
* Observed patterns indicate a healthy, active local network with connections to trusted external services.

#### Limitations:

* Could only analyze packets to/from the host device.
* No visibility into other devices’ communication due to lack of monitor mode.

## 5. Wi-Fi Password Strength Test (NOT PERFORMED)

#### Reason:

The current adapter (**Realtek RTL8821CE**) does **not support monitor mode**, which is essential for:

* Capturing WPA/WPA2 handshakes
* Testing password strength using tools like Aircrack-ng

#### Alternative Considerations:

* External USB Wi-Fi adapter (e.g., Alfa AWUS036ACH) is recommended for this step.
* Passive checks for open/WEP networks were performed instead (none found).

## Summary of Findings:

|  |  |  |
| --- | --- | --- |
| **Area** | **Status** | **Notes** |
| Device Identification | Successful | Multiple hosts found |
| Router Access | Successful | Admin panel accessible |
| Port Scanning | No critical ports found | All devices hardened |
| Packet Capture | Partial Visibility | Device-level traffic only |
| Password Strength Test | Not performed | Hardware limitation (no monitor mode) |

## Identified Weaknesses:

* **Open ports** on multiple internal IPs could allow lateral movement if an attacker gets inside the network.
* **DNS service on router (port 53)** responded with “REFUSED,” but should be evaluated for potential exposure.
* Devices had **TCPwrapped ports**, which may indicate poor filtering or logging of unused services.

## Recommendations:

* Close unused ports on devices (especially 49152 and 62078).
* Ensure router services like **FTP, Telnet, SSH** are disabled if not in use.
* Enable **firewall rules** to block unwanted internal traffic.
* Regularly scan the network and audit connected devices.
* Upgrade any outdated firmware or services exposed over SSL/HTTP.

## Conclusion:

This Wi-Fi security assessment reveals a **generally secure local network environment**, based on the findings from both **Nmap scans** and **Wireshark packet captures**. Below is a summary of the observations and their implications:

* **Minimal Active Devices**: Only a small number of IPs responded on the subnet, reducing the attack surface.
* **Filtered Critical Ports**: Sensitive ports like FTP (21), SSH (22), and Telnet (23) were *filtered* or closed, indicating firewall rules or access control in place.
* **Encrypted Traffic Detected**: SSL/HTTPS (port 443) is in use, and no unencrypted login credentials or HTTP-based sessions were found during packet inspection.
* **No Suspicious Broadcasts or Malware Indicators**: Wireshark analysis did not reveal unusual DNS requests, ARP poisoning attempts, or excessive probing—indicating a stable and clean network environment.
* **Consistent Device MAC Vendors**: MAC addresses correspond to known vendor prefixes (Huawei, etc.), showing no obvious rogue devices.

## Note:

All MAC addresses in this file have been anonymized for privacy using consistent mapping. Communication flows and protocol behavior remain unaffected.

**Report Prepared By**: Sahiti M