Cyber Security Internships

1. Installed Zenmap in windows
2. Founded the My local IP address using ipconfig command and found my WIFI IP address and using subnet mask 255.255.255.0
3. So, my local ip address 192.168.31.1/24
4. So, using this local address => nmap -sS -T4 192.168.31.1/24
5. There are Few Host, like we group of friends living in room , so there are few many hosts like laptops and mobiles

A screenshot of a computer

AI-generated content may be incorrect.

1. When I scanned my target … there are few open ports and lot of information has popped up in my output terminal…. Like MAC address, open ports,

A screenshot of a computer

AI-generated content may be incorrect.

Open ports :

1. 192.168.31.1 - a web gate way for Jio Fiber

**PORT STATE SERVICE**

53/tcp open domain

80/tcp open http

443/tcp open https

7443/tcp open oracleas-https

8080/tcp open http-proxy

8443/tcp open https-alt

1. 192.168.31.128

PORT STATE SERVICE

3306/tcp open mysql

1. 192.168.31.144 – iphone.lan

PORT STATE SERVICE

49152/tcp open unknown

62078/tcp open iphone-sync

1. 192.168.31.187 –

PORT STATE SERVICE

3306/tcp open mysql

3580/tcp open nati-svrloc

1. 192.168.31.205

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

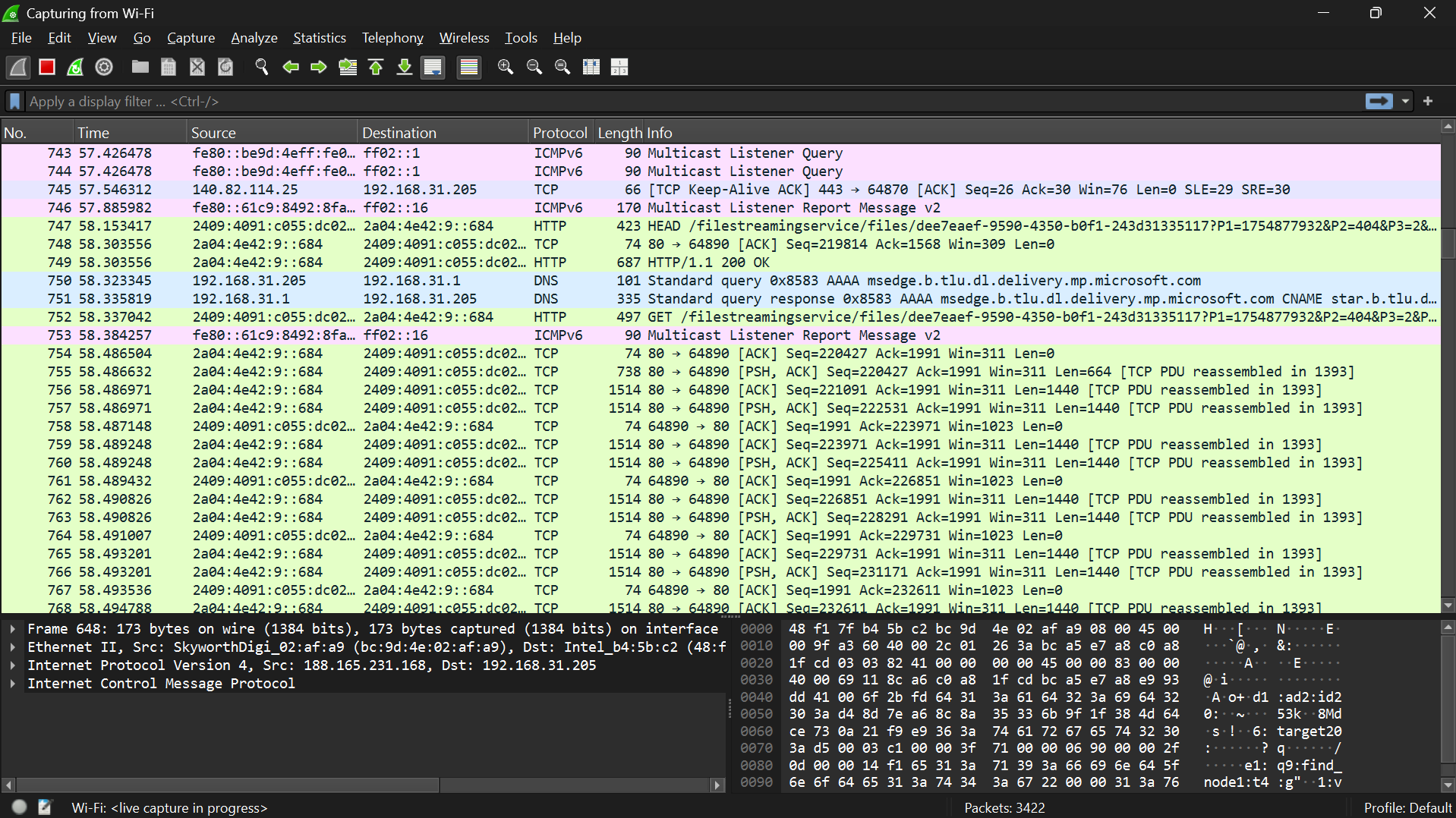
902/tcp open iss-realsecure

912/tcp open apex-mesh

5060/tcp open sip

5061/tcp open sip-tls

And analyze the my flow of network through wireshark tool



Nmap scan report for iPhone.lan (192.168.31.144)

Host is up (0.012s latency).

Not shown: 998 closed tcp ports (reset)

PORT STATE SERVICE

49152/tcp open unknown

62078/tcp open iphone-sync

MAC Address: 26:0E:B3:03:45:F5 (Unknown)

Identified Few Potential Vulnerebilities :

There is an open port in iphone.lan port number 49152

Found an exploit in google .