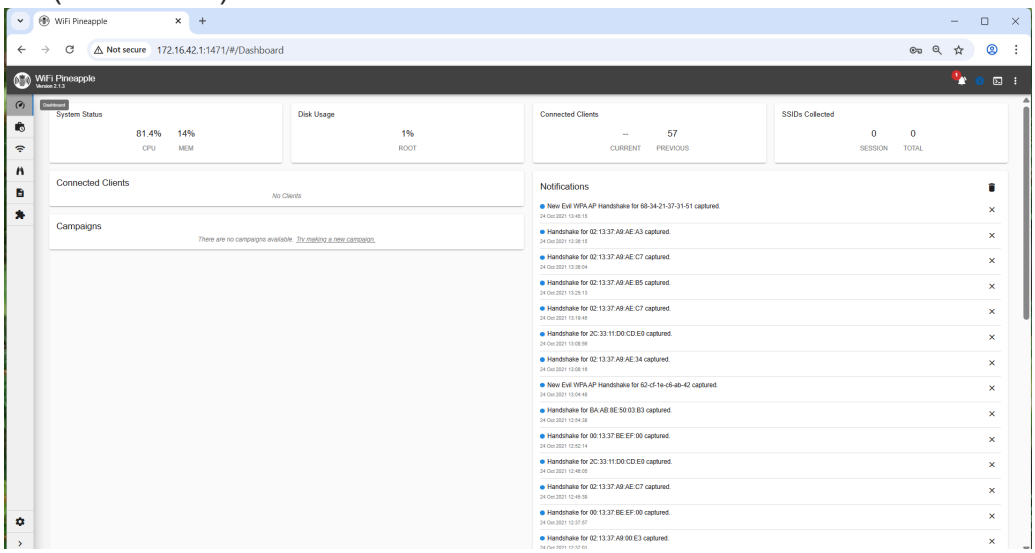
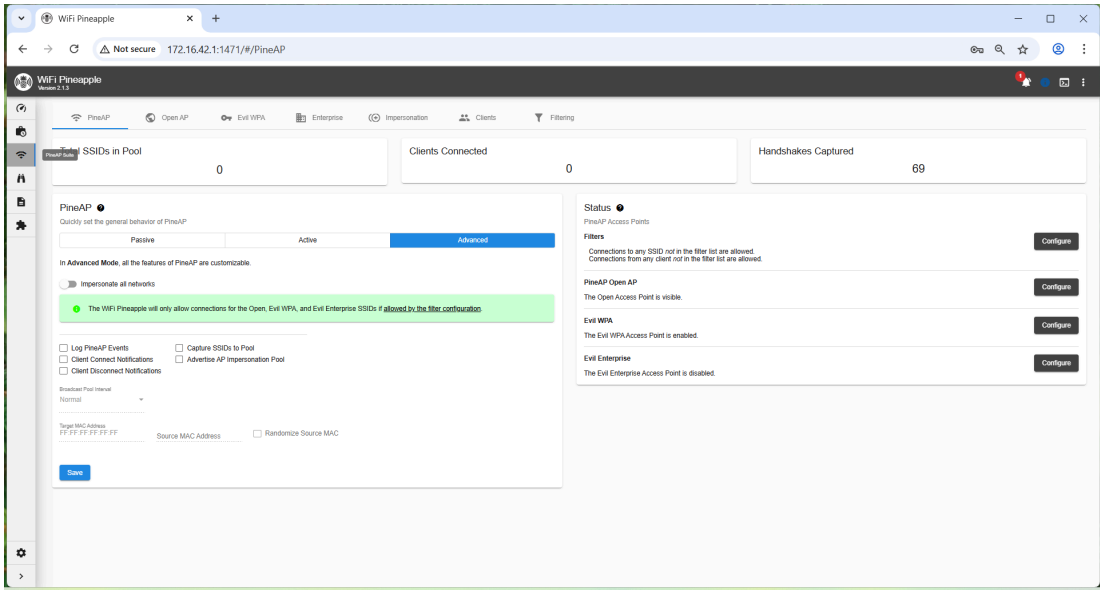
Lab 5 | CSE 3140 | Abdul Chowdhury (unable to communicate with partner asked TA said to work by myself) | amc20031 | ssh -L 127.0.0.1:8000:10.13.4.8:80 cse@10.13.6.41

Q1 (Dashboard):



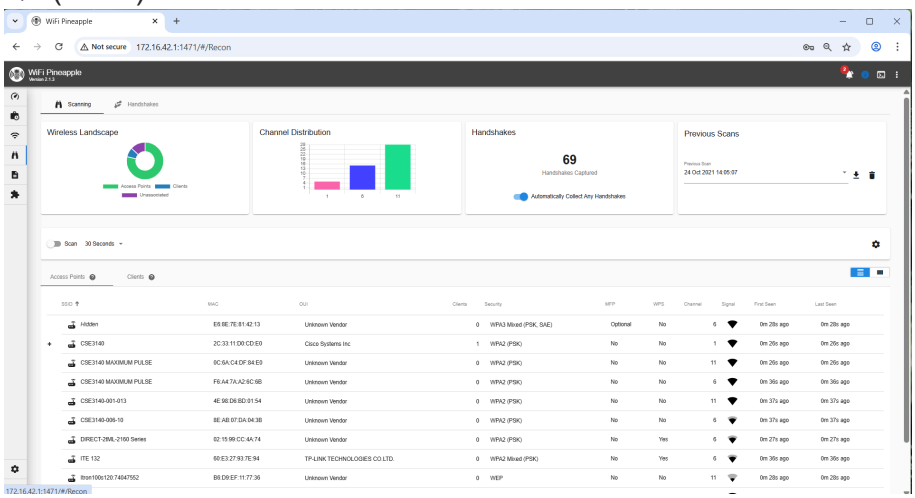

Above is the dashboard where we can view information about the system

- Top row shows **System Status**: which displays current CPU and RAM percentages
- **Disk Usage**: Displays current disk percentage
- **Connected Clients**: Displays every client (MAC address and IP address) that is currently and previously connected when the client is connected to the non-management server.
- **SSIDs collected**: Displays all SSIDs collected since the pineapple was booted
- **Campaigns**: Displays list of all current campaigns which includes status, types and names
- **Wireless landscape**: General overview of statistics on the recon scan that is done
- **Notification system**: Notifies user when there is a change or update in the system




Above is the Wifi Administration Console which is similar to the dashboard. The top 3 boxes are the number of SSIDS found from clients, number of handshakes captured, and number of clients connected. Handshakes can change and are captured when a client joins or refreshes the network. The PineAP section allows us various ways for how the system is able to scan, some ways are impersonating access points and controlling access with filters. My interface name was wlan2, and a WLAN is a network, for instance wifi is an example of WLAN.

Q2 (Scan).

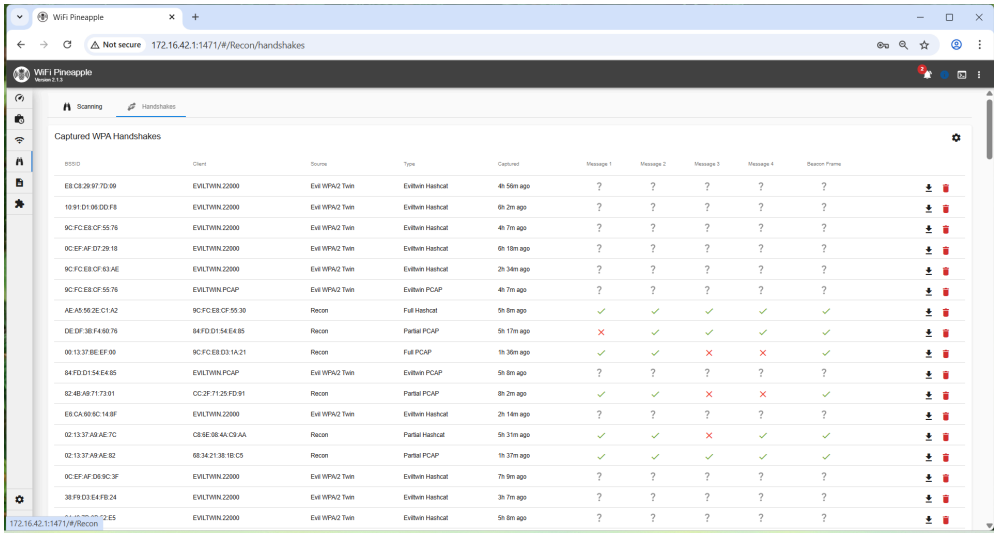



Above is the recon dashboard of the pineapple.

- **Scanning in the Wireless Landscape**: Displays pie chart containing APs, clients, and unassociated clients
- **Channel Distributions**: Displays channel frequencies picked up by Pineapple's antennas

- **Handshakes**: Number of handshakes capture via the scan (joining, refreshing - regular wifi traffic)
- Previous scans: Displays previous scans with date and time
- **Access points**: Displays information about detected APs (SSID, OUI, MAC, client security, MFP, WPS, Channel , signal, first and last seen times)
- **Clients**: Displays information about all detected clients in scan (IP, MAC, time of connection)
- **Handshakes in page information**: Information was displayed regarding captured WPA handshakes (client, BSSID, source, type, time since capture, message 1 + message 2)

Handshakes tab:

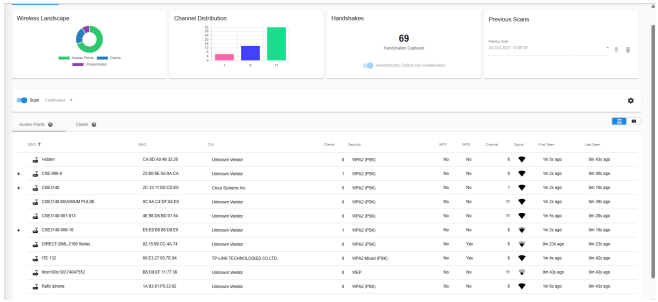



The handshakes tab shows details for every handshake the system has gotten, particularly the SSID, client, source, type, and time it took for handshake to be captured. It also shows various different statistics that show the strength and validity of connection created.

Q3:

This was the access point created by the personal hotspot on my iphone

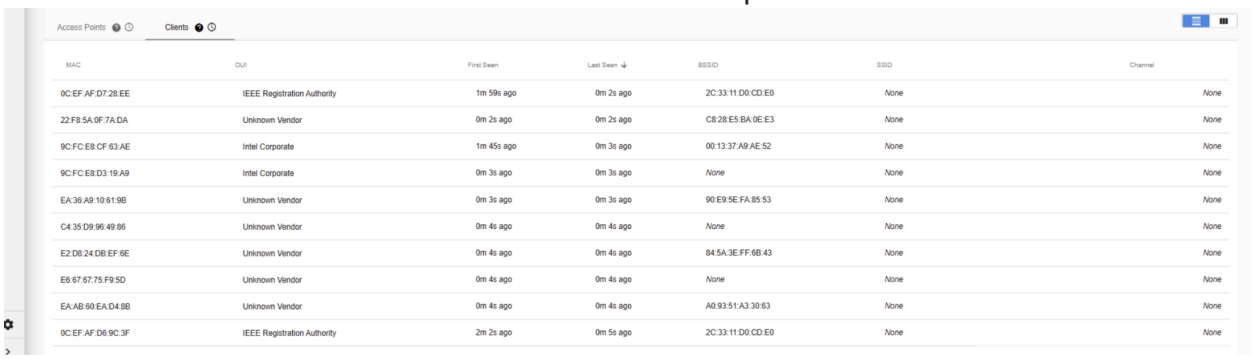


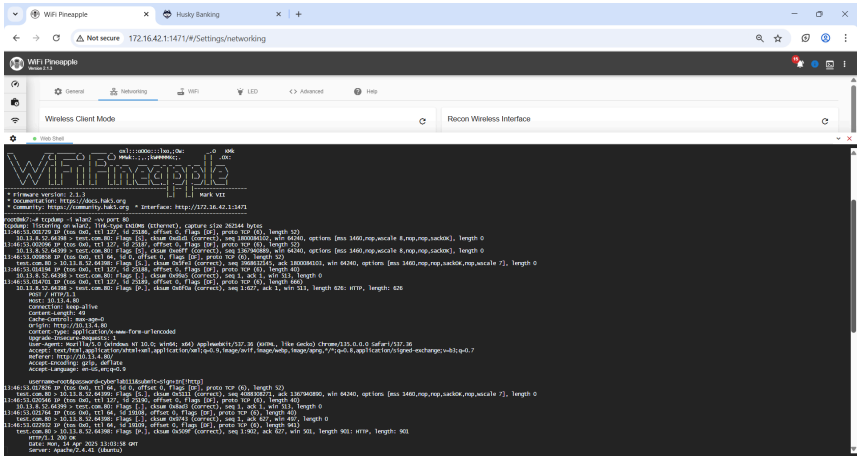
The SSID tab notifies user of the name of network, MAC tab shows the identifier assigned to Network interface controller, OUI shows vendor of network adapter (When that information is accessible), clients tab show the amount of clients that are connected to the network, Security shows type of security each network uses, and MFP is extra security system displays if the network has it

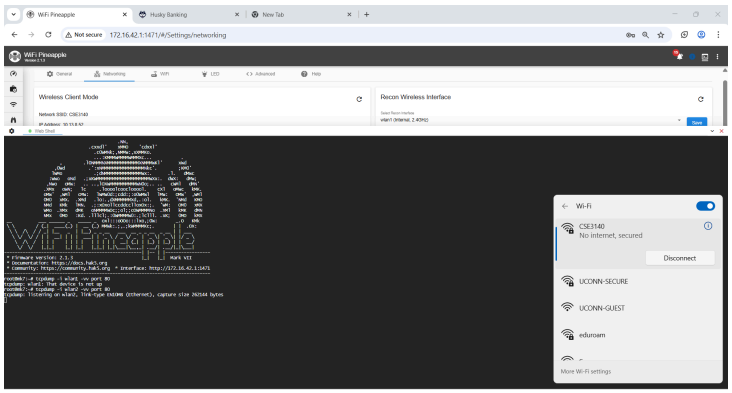
- I was able to find an access point through my hotspot, and I could see clients on the specific access point, especially when the left side of the access point was accessed. Information about client connection to the access point was also displayed and the network is using WPA2(PSK) security.

Below we can also see the handshakes that were captured in our vulnerable network



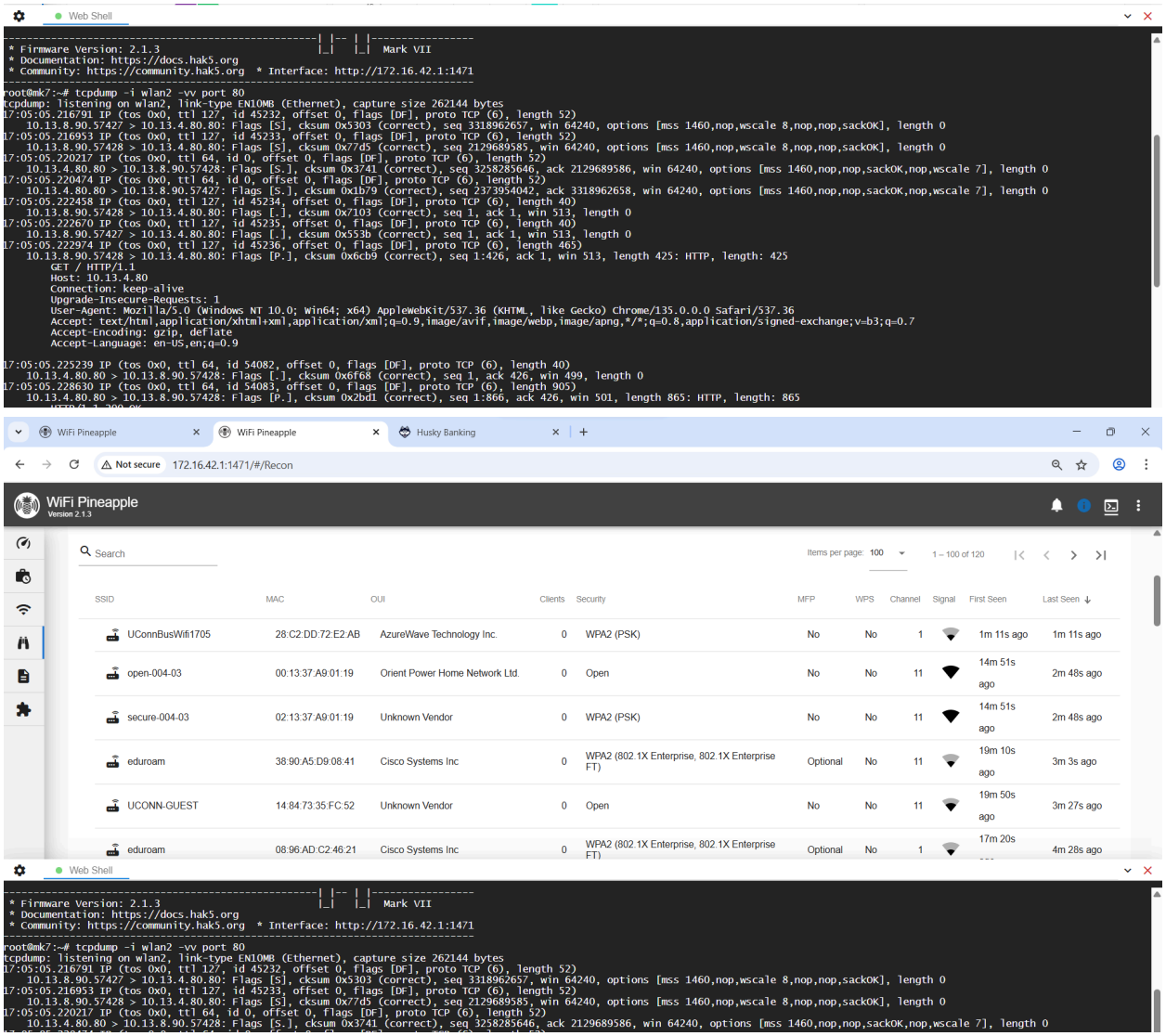

Q4.



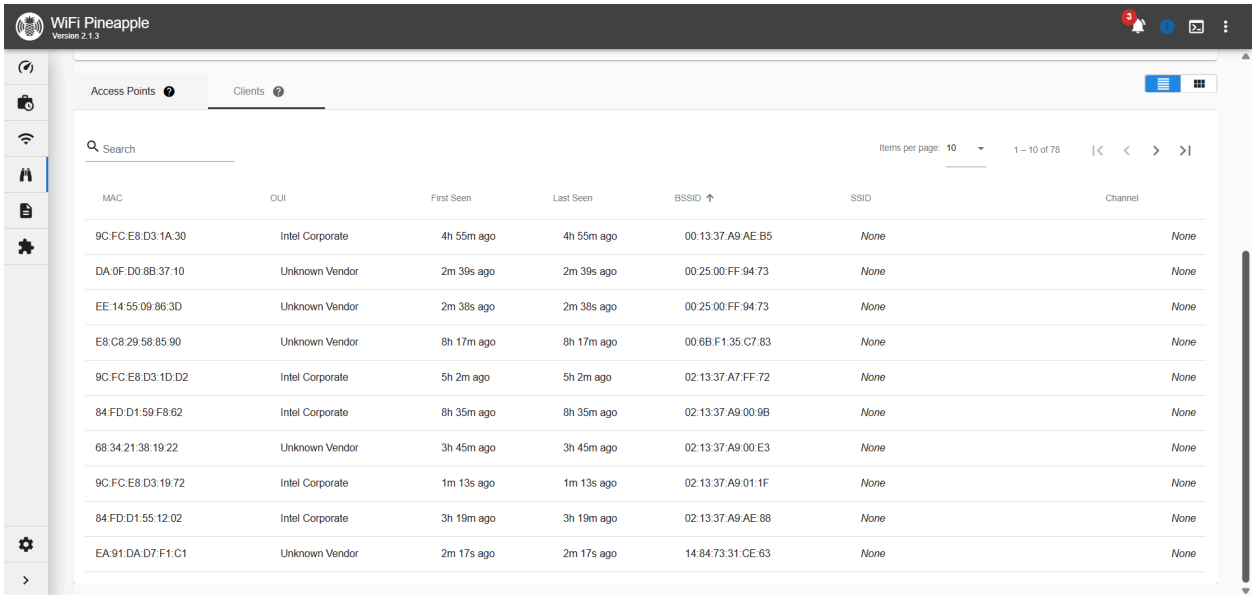
When connected to an unsecured network, traffic is able to be seen because it is unencrypted. Traffic that appeared came from a lab laptop, and when connected to a protected network however no traffic was able to be seen because of security and encryption. Information is more accessible on unsecured networks vs. secured networks.

Q5.

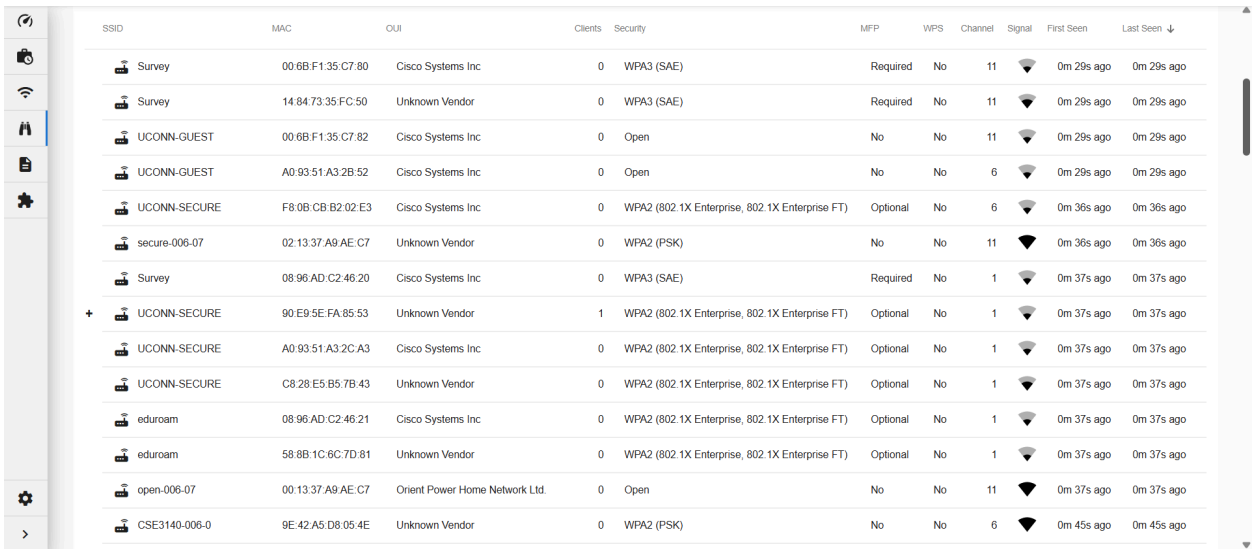



When TCPDUMP was ran off the secure networks no traffic was shown in the terminal due to the secure network preventing Pineapple from seeing data about IP addresses connected, connecting to protected networks is useful in order to protect privacy such as activity and information.

Q6.




| MAC | OUI | First Seen | Last Seen | BSSID | SSID | Channel |
|---|---|---|---|---|---|---|
| 9C:FC:E8:D3:1A:30 | Intel Corporate | 4h 55m ago | 4h 55m ago | 00:13:37:A9:AE:B5 | None | None |
| DA:0F:D0:8B:37:10 | Unknown Vendor | 2m 39s ago | 2m 39s ago | 00:25:00:FF:94:73 | None | None |
| EE:14:55:09:86:3D | Unknown Vendor | 2m 38s ago | 2m 38s ago | 00:25:00:FF:94:73 | None | None |
| E8:C8:29:58:85:90 | Unknown Vendor | 8h 17m ago | 8h 17m ago | 00:6B:F1:35:C7:83 | None | None |
| 9C:FC:E8:D3:1D:D2 | Intel Corporate | 5h 2m ago | 5h 2m ago | 02:13:37:A7:FF:72 | None | None |
| 84:FD:D1:59:F8:62 | Intel Corporate | 8h 35m ago | 8h 35m ago | 02:13:37:A9:00:9B | None | None |
| 68:34:21:38:19:22 | Unknown Vendor | 3h 45m ago | 3h 45m ago | 02:13:37:A9:00:E3 | None | None |
| 9C:FC:E8:D3:19:72 | Intel Corporate | 1m 13s ago | 1m 13s ago | 02:13:37:A9:01:1F | None | None |
| 84:FD:D1:55:12:02 | Intel Corporate | 3h 19m ago | 3h 19m ago | 02:13:37:A9:AE:88 | None | None |
| EA:91:DA:D7:F1:C1 | Unknown Vendor | 2m 17s ago | 2m 17s ago | 14:84:73:31:CE:63 | None | None |



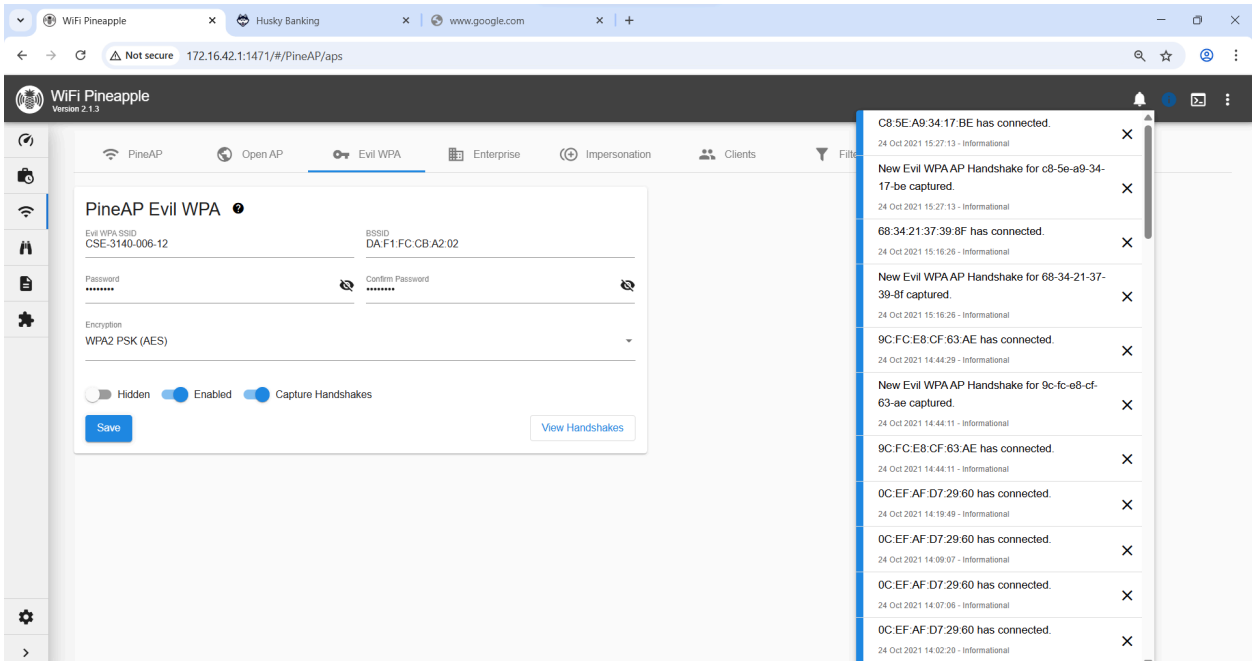
| SSID | MAC | OUI | Clients | Security | MFP | WPS | Channel | Signal | First Seen | Last Seen |
|---|---|---|---|---|---|---|---|---|---|---|
| Survey | 00:6B:F1:35:C7:80 | Cisco Systems Inc | 0 | WPA3 (SAE) | Required | No | 11 | | 0m 29s ago | 0m 29s ago |
| Survey | 14:84:73:35:FC:50 | Unknown Vendor | 0 | WPA3 (SAE) | Required | No | 11 | | 0m 29s ago | 0m 29s ago |
| UCONN-GUEST | 00:6B:F1:35:C7:82 | Cisco Systems Inc | 0 | Open | No | No | 11 | | 0m 29s ago | 0m 29s ago |
| UCONN-GUEST | A0:93:51:A3:2B:52 | Cisco Systems Inc | 0 | Open | No | No | 6 | | 0m 29s ago | 0m 29s ago |
| UCONN-SECURE | F8:0B:CB:B2:02:E3 | Cisco Systems Inc | 0 | WPA2 (802.1X Enterprise, 802.1X Enterprise FT) | Optional | No | 6 | | 0m 36s ago | 0m 36s ago |
| secure-006-07 | 02:13:37:A9:AE:C7 | Unknown Vendor | 0 | WPA2 (PSK) | No | No | 11 | | 0m 36s ago | 0m 36s ago |
| Survey | 08:96:AD:C2:46:20 | Cisco Systems Inc | 0 | WPA3 (SAE) | Required | No | 1 | | 0m 37s ago | 0m 37s ago |
| UCONN-SECURE | 90:E9:5E:FA:85:53 | Unknown Vendor | 1 | WPA2 (802.1X Enterprise, 802.1X Enterprise FT) | Optional | No | 1 | | 0m 37s ago | 0m 37s ago |
| UCONN-SECURE | A0:93:51:A3:2C:A3 | Cisco Systems Inc | 0 | WPA2 (802.1X Enterprise, 802.1X Enterprise FT) | Optional | No | 1 | | 0m 37s ago | 0m 37s ago |
| UCONN-SECURE | C8:28:E5:B5:7B:43 | Unknown Vendor | 0 | WPA2 (802.1X Enterprise, 802.1X Enterprise FT) | Optional | No | 1 | | 0m 37s ago | 0m 37s ago |
| eduroam | 08:96:AD:C2:46:21 | Cisco Systems Inc | 0 | WPA2 (802.1X Enterprise, 802.1X Enterprise FT) | Optional | No | 1 | | 0m 37s ago | 0m 37s ago |
| eduroam | 58:8B:1C:6C:7D:81 | Unknown Vendor | 0 | WPA2 (802.1X Enterprise, 802.1X Enterprise FT) | Optional | No | 1 | | 0m 37s ago | 0m 37s ago |
| open-006-07 | 00:13:37:A9:AE:C7 | Orient Power Home Network Ltd. | 0 | Open | No | No | 11 | | 0m 37s ago | 0m 37s ago |
| CSE3140-006-0 | 9E:42:A5:D8:05:4E | Unknown Vendor | 0 | WPA2 (PSK) | No | No | 6 | | 0m 45s ago | 0m 45s ago |

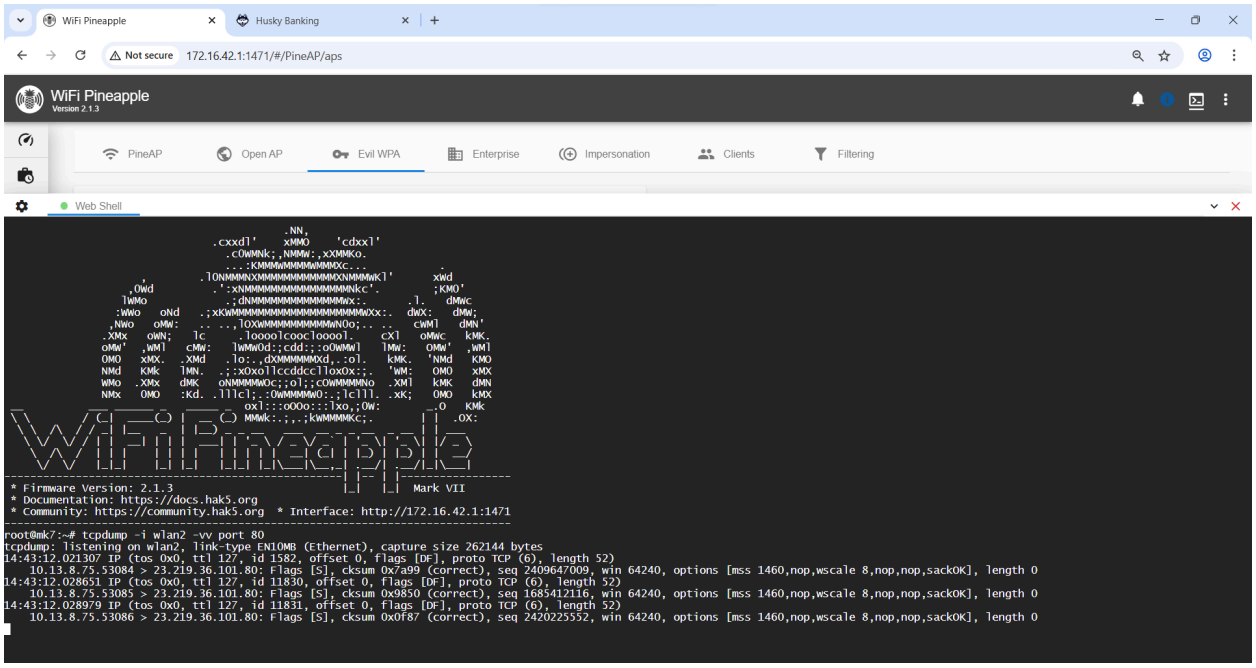
The wireless networks visible are UCONN-GUEST, UCONN-SECURE, eduroam, Survey and other networks created by other students in classroom.

UCONN SECURE and UCONN GUEST came up at various different times but each time UCONN SECURE was listed it had different values in MAC, while other columns were the same amongst secure and guest.

Open, WEP, WPA2(PSK) (CSE 3140 NETWORK) and WPA2(802 1x Enterprise, 802 1x Enterprise FT) were used for UCONN-secure networks were the different values listed.

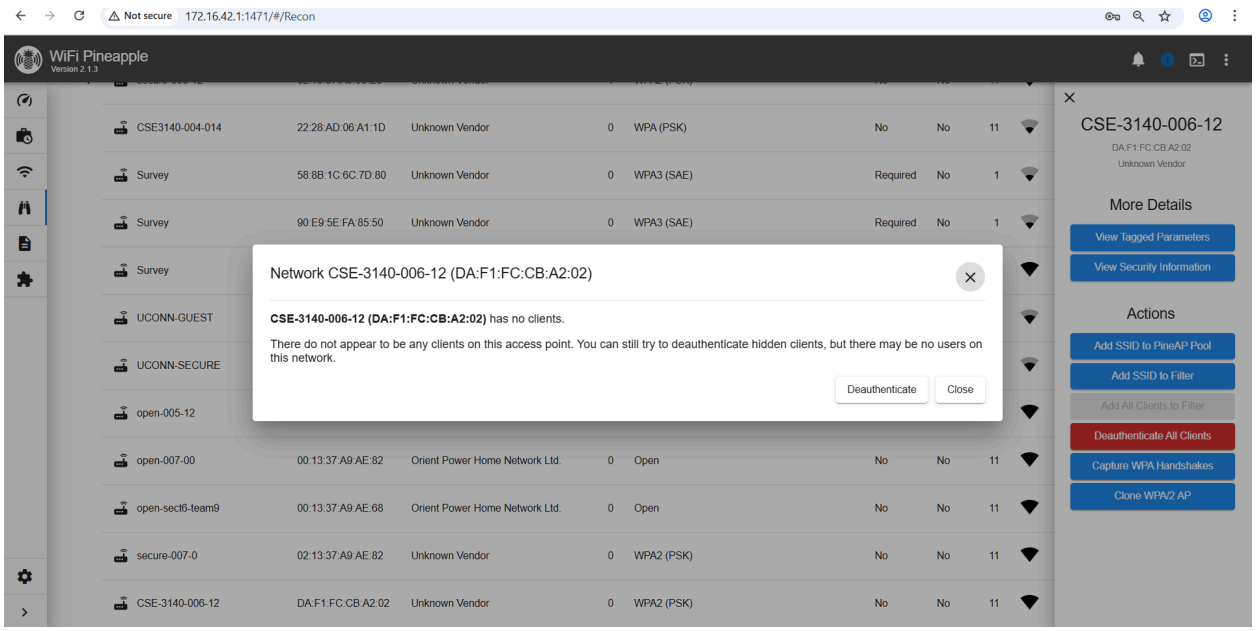
Q7.

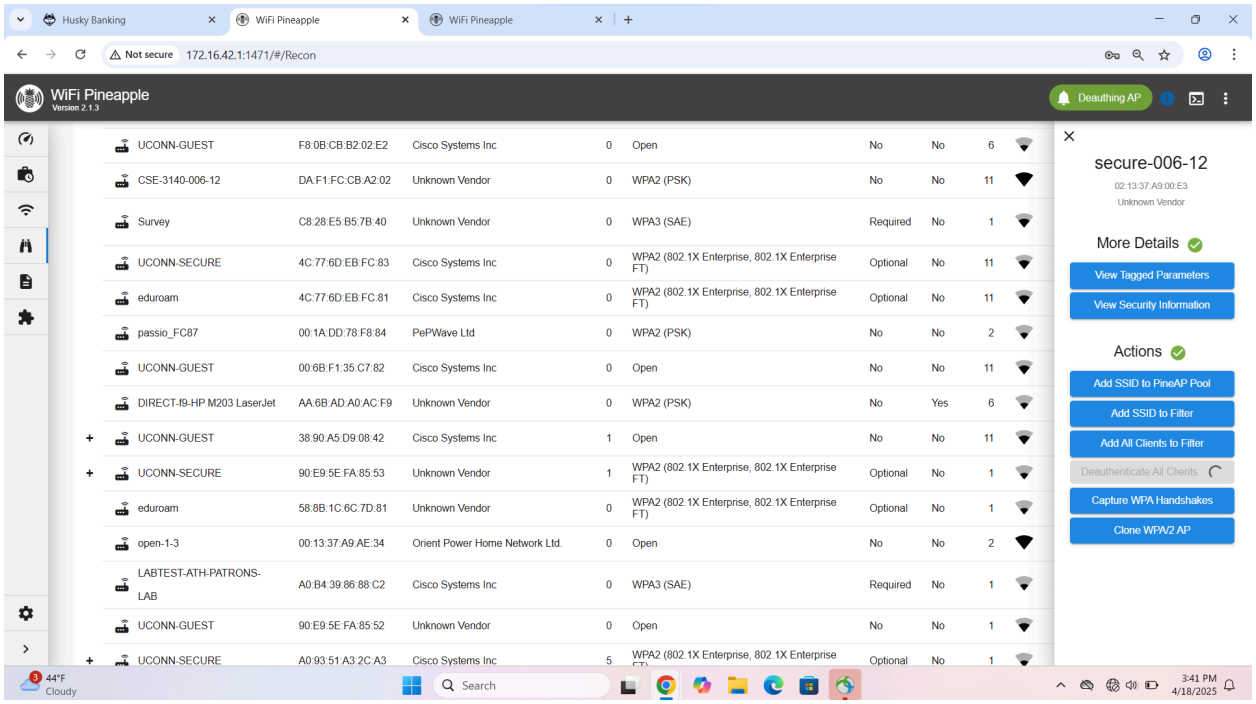



I Did this on the lab computer unable to screen record but recorded through screenshots I was able to connect and then I went to the terminal typed in the root number and was able to connect to the IP Address.

Q8. For Q8 I record through my phone and screenshots as this was done through lab computer


Not secure
172.16.42.1:1471/#/Recon
WiFi Pineapple
Version 2.1.3
CSE3140-004-014 22:28:AD:06:A1:1D Unknown Vendor 0 WPA (PSK) No No 11
Survey 58:8B:1C:6C:7D:80 Unknown Vendor 0 WPA3 (SAE) Required No 1
Survey 90:E9:5E:FA:85:50 Unknown Vendor 0 WPA3 (SAE) Required No 1
Survey
UCONN-GUEST
UCONN-SECURE
open-005-12
open-007-00 00:13:37:A9:AE:82 Orient Power Home Network Ltd. 0 Open No No 11
open-sect6-team9 00:13:37:A9:AE:68 Orient Power Home Network Ltd. 0 Open No No 11
secure-007-0 02:13:37:A9:AE:82 Unknown Vendor 0 WPA2 (PSK) No No 11
CSE-3140-006-12 DA:F1:FC:CB:A2:02 Unknown Vendor 0 WPA2 (PSK) No No 11
Network CSE-3140-006-12 (DA:F1:FC:CB:A2:02)
CSE-3140-006-12 (DA:F1:FC:CB:A2:02) has no clients.
There do not appear to be any clients on this access point. You can still try to deauthenticate hidden clients, but there may be no users on this network.
Deauthenticate
Close
CSE-3140-006-12
DA:F1:FC:CB:A2:02
Unknown Vendor
More Details
View Tagged Parameters
View Security Information
Actions
Add SSID to PineAP Pool
Add SSID to Filter
Add All Clients to Filter
Deauthenticate All Clients
Capture WPA Handshakes
Clone WPA/2 AP




Captured WPA Handshakes

| BSSID | Client | Source | Type | Captured | Message 1 | Message 2 | Message 3 | Message 4 | Beacon Frame |
|---|---|---|---|---|---|---|---|---|---|
| 02:13:37:A9:AE:67 | 9C:FC:E8:CF:46:E4 | Recon | Full PCAP | 4h 24m ago | ✓ | ✓ | ✓ | ✓ | ✓ |
| 02:13:37:A9:AE:C7 | 9C:FC:E8:CF:55:30 | Recon | Full PCAP | 4h 28m ago | ✓ | ✓ | ✓ | ✓ | ✓ |
| 5E:B1:16:6F:67:F0 | EVILTWIN.22000 | Evil WPA/2 Twin | Eviltwin Hashcat | 5h 48m ago | ? | ? | ? | ? | ? |
| 9C:FC:E8:CF:63:AE | EVILTWIN.22000 | Evil WPA/2 Twin | Eviltwin Hashcat | 1h 16m ago | ? | ? | ? | ? | ? |
| CA:25:65:2B:BD:BB | EVILTWIN.22000 | Evil WPA/2 Twin | Eviltwin Hashcat | 7h 31m ago | ? | ? | ? | ? | ? |
| 00:13:37:BE:EF:00 | 9C:FC:E8:CF:55:76 | Recon | Partial Hashcat | 4h 30m ago | ✓ | ✓ | ✓ | ✓ | ✓ |
| 02:13:37:A9:00:E3 | 9C:FC:E8:CF:55:30 | Recon | Full Hashcat | 9h 27m ago | ✓ | ✓ | ✓ | ✓ | ✓ |
| 02:13:37:A9:01:31 | 84:FD:D1:54:E4:85 | Recon | Full Hashcat | 10h 42m ago | ✓ | ✓ | ✓ | ✓ | ✓ |
| 02:13:37:A9:AE:82 | 84:FD:D1:59:FA:2E | Recon | Partial PCAP | 6h 2m ago | ✓ | ✓ | ✗ | ✓ | ✓ |
| 24:EE:9A:D9:D0:3C | EVILTWIN.22000 | Evil WPA/2 Twin | Eviltwin Hashcat | 7h 51m ago | ? | ? | ? | ? | ? |
| 4A:CA:8D:7D:E5:52 | EVILTWIN.PCAP | Evil WPA/2 Twin | Eviltwin PCAP | 7h 42m ago | ? | ? | ? | ? | ? |

I was able to observe that one the d'authentification happened traffic was able to be seen through the secure network even through encryption.

Q9. Pineapple's DNS records were configured for rerouting towards bank.com to the VM static ip address and was done by editing /etc/host files with entries. But despite DNS being successful, the Pineapple device failed to forward these connections to test machines leaving me unable to finish this part entirely.