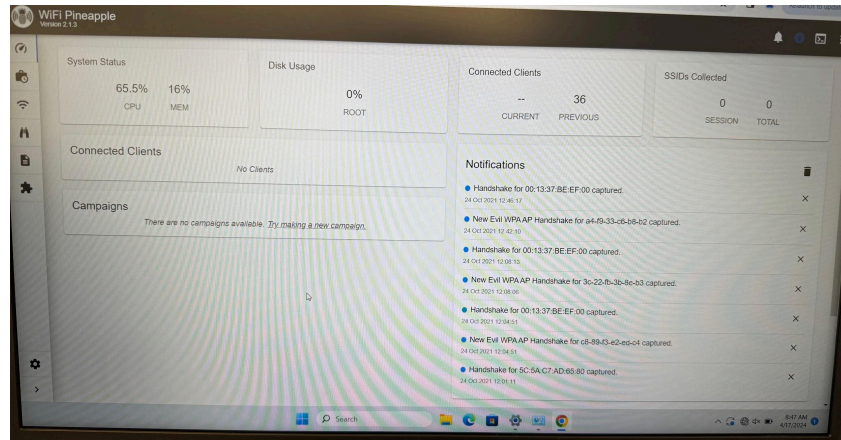


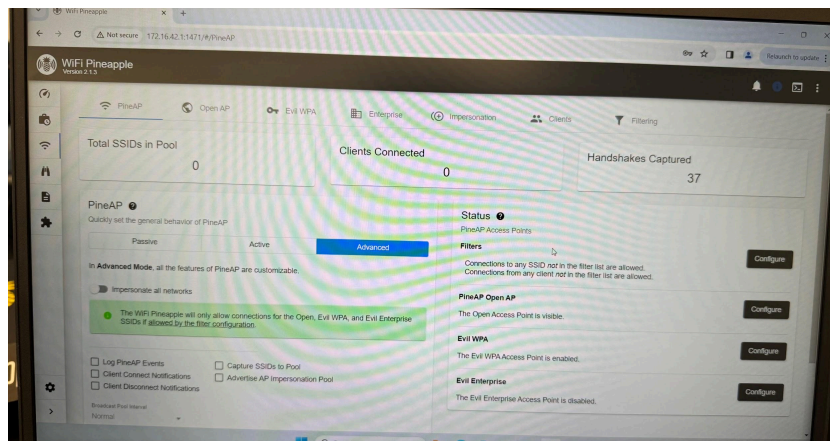
Karina Jadia | 172.16.50.127 | Team 2

Q1:  
dashboard:



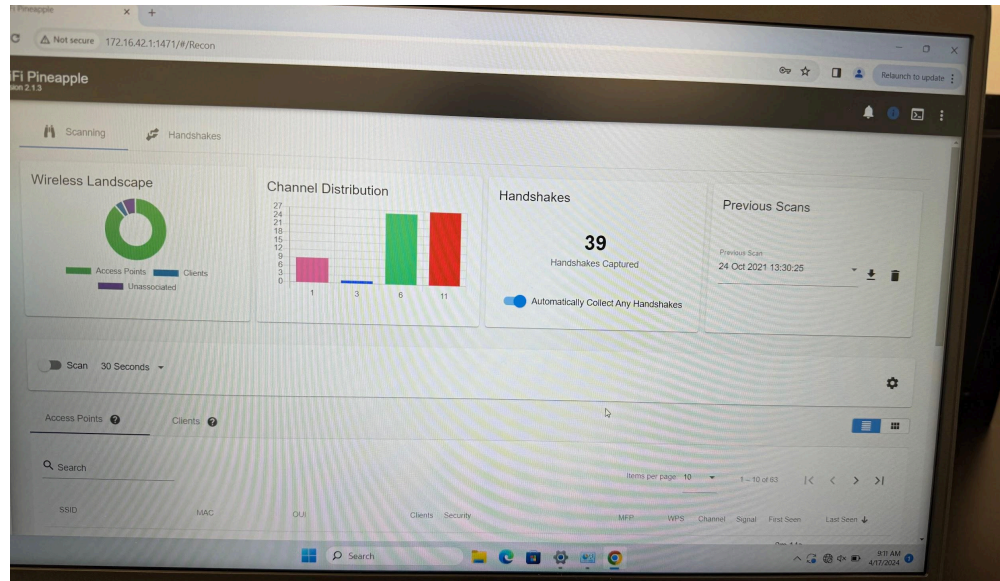
The dashboard is where we can view information about the system. The top row shows the statuses of the system, including CPU, RAM, and disk usage, and information about the clients currently and previously connected to the Pineapple. The SSIDs Collected section tells how many SSID values were picked up from the clients by the Pineapple. The connected clients section, the MAC address as well as the IP Address of connected clients will show up when clients connect to the non-management server. The notification section is what the system uses to notify the user when there's a change in status or update in the system. Campaigns specify engagement; when there is a campaign available the name, status, and type of campaign would show up. The Wireless Landscape section gives the general overview statistics on the recon scan that is done.

wifi console:



The Wifi Administration Page is similar to the dashboard in that the top three boxes are the number of SSIDs found from clients, number of clients connected, and number of handshakes captured. Handshakes signify when a client joins or refreshes a network. The PineAP section gives us different options for how the system is able to scan, for example by impersonating access points and controlling access with filters. The interface name used is "wlan2," a WLAN is basically any network. Wifi is an example of a WLAN.

Q2:  
scan tab:



This is the scan tab after doing a single 30 second scan. The wireless landscape card gives a general overview of the scan that was done. The handshake card picks up handshakes (joining, refreshing – normal wifi traffic). Under these cards, it displays the access points being picked up by the Pineapple and the available clients for each access point.

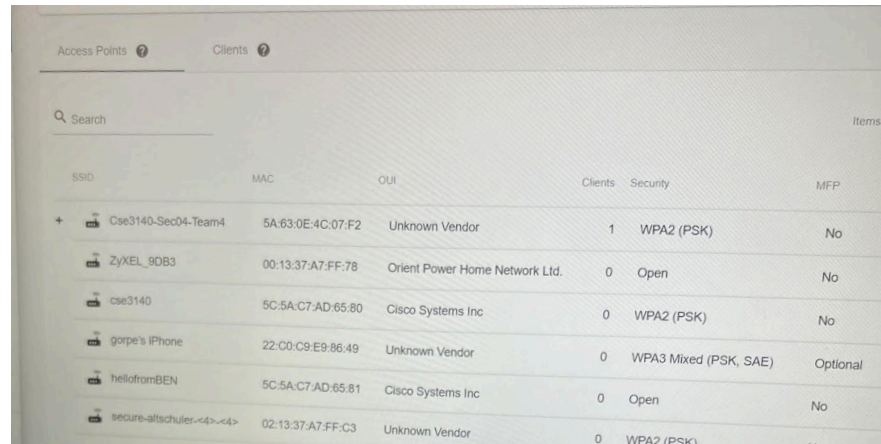
handshakes tab:

The screenshot shows the 'Handshakes' tab of the WiFi Pineapple interface, displaying a table of 'Captured WPA Handshakes'. The table has columns for BSSID, Client, Source, Type, Captured, Message 1, Message 2, Message 3, Message 4, and Beacon Frame. The data rows show various handshakes captured by the system, including those from Recon, Evil WPA2 Twin, and Evil WPA2 Hashcat sources.

BSSID	Client	Source	Type	Captured	Message 1	Message 2	Message 3	Message 4	Beacon Frame
0E:E1:99:97:7F:10	E0:0A:F6:89:EC:3B	Recon	Full Hashcat	6h 41m ago	✓	✓	✓	✓	✓
54:14:F3:A9:F5:D0	EVILTWIN.PCAP	Evil WPA2 Twin	Eviltwin PCAP	2h 28m ago	?	?	?	?	?
FE:0B:58:56:3A:08	EVILTWIN.22000	Evil WPA2 Twin	Eviltwin Hashcat	6h 17m ago	?	?	?	?	?
BE:F5:33:B6:00:E1	2C:8D:51:71:62:BD	Recon	Full PCAP	7h 44m ago	✗	✓	✓	✓	✓
0C:EF:AF:CD:E9:01	EVILTWIN.22000	Evil WPA2 Twin	Eviltwin Hashcat	2h 22m ago	?	?	?	?	?
3C:22:FB:3B:8E:B3	EVILTWIN.PCAP	Evil WPA2 Twin	Eviltwin PCAP	1h 23m ago	?	?	?	?	?
50:2F:A8:12:E5:03	3C:22:FB:CD:67:7D	Recon	Partial PCAP	2h 2m ago	✓	✓	✓	✗	✓
BE:F5:33:B6:00:E1	2C:8D:51:71:62:BD	Recon	Full Hashcat	7h 44m ago	✗	✓	✓	✓	✓
00:13:37:BE:EF:00	3C:A6:F6:3F:EAC3	Recon	Partial Hashcat	7h 40m ago	✓	✓	✓	✗	✓
AD:90	EVILTWIN.22000	Evil WPA2 Twin	Eviltwin Hashcat	2h 29m ago	?	?	?	?	?

This shows the details for every handshake the system got, specifically the SSID, the client, the source, type, the time the handshake was captured and the different statistics that show the validity of the connection created.

Q3:



Access Points ?		Clients ?				
Search						
SSID	MAC	OUI	Clients	Security	MFP	
+ Cse3140-Sec04-Team4	5A:63:0E:4C:07:F2	Unknown Vendor	1	WPA2 (PSK)	No	
ZyXEL_9DB3	00:13:37:A7:FF:78	Orient Power Home Network Ltd.	0	Open	No	
cse3140	5C:5A:C7:AD:65:80	Cisco Systems Inc	0	WPA2 (PSK)	No	
gorpe's iPhone	22:C0:C9:E9:86:49	Unknown Vendor	0	WPA3 Mixed (PSK, SAE)	Optional	
hellotromBEN	5C:5A:C7:AD:65:81	Cisco Systems Inc	0	Open	No	
secure-altshuler<4><4>	02:13:37:A7:FF:C3	Unknown Vendor	0	WPA2 (PSK)	No	

I was unable to connect my phone, however I got my friend to rename and share her hotspot. It is the first one under access points.

The SSID tab tells the name of the network. The MAC tab shows the unique identifier assigned to each Network Interface Controller. The OUI tab shows the vendor of the network adapter (when the Pineapple is able to find that information). The clients tab shows how many clients are connected to each network. The security tab names the type of security each network uses. MFP is an extra layer of security and the system displays whether the network has it.

### Can you find this access point?

Yes, I was able to find the access point, which is a mobile hotspot on my friend's phone.

### Can we see the users connected to the access point?

I could see clients on my specific access point. When I pressed the + button on the left side of the access point, I could see the information about the client connected to the access point.

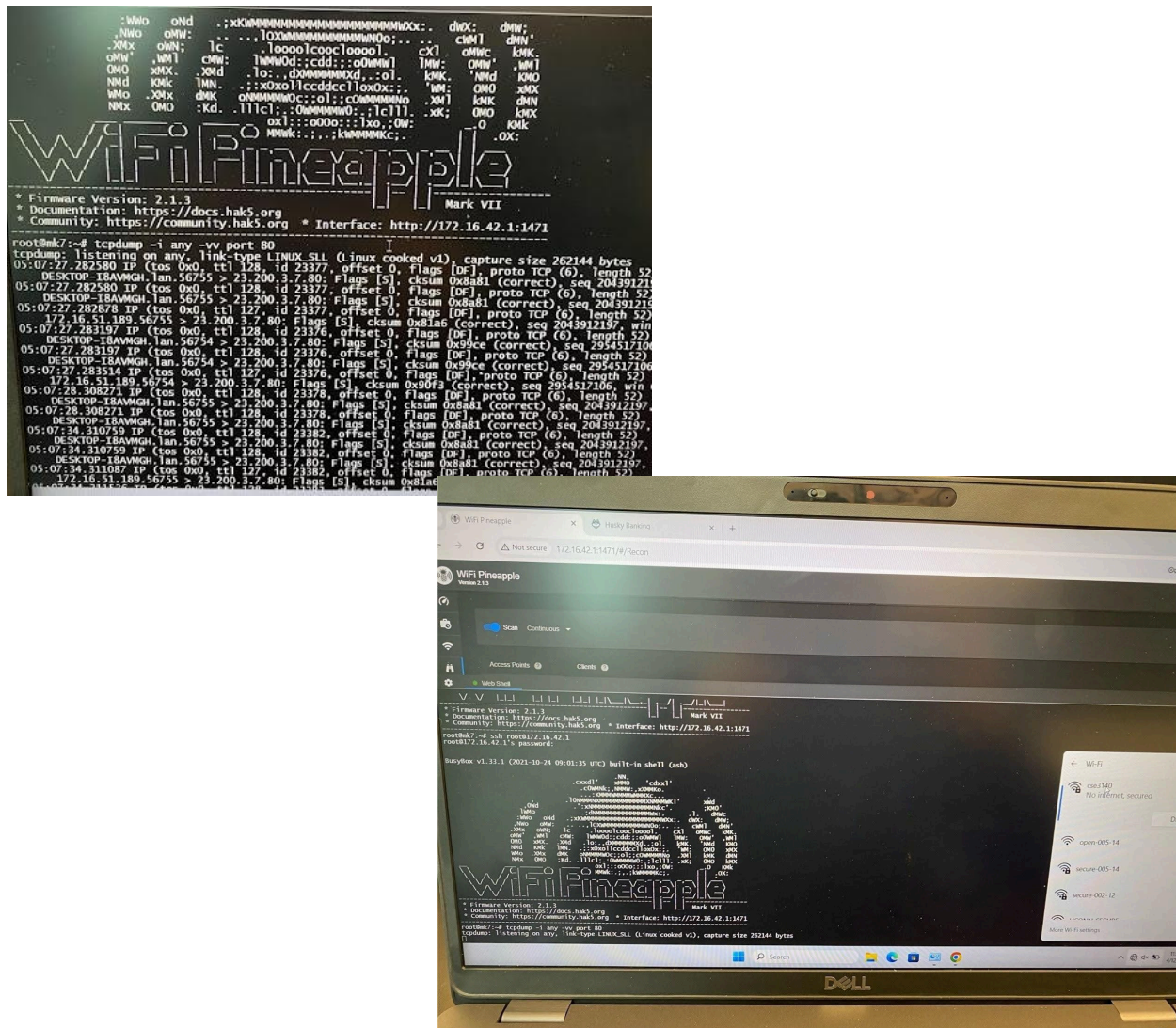
### What kind of security is the cse3140 network using?

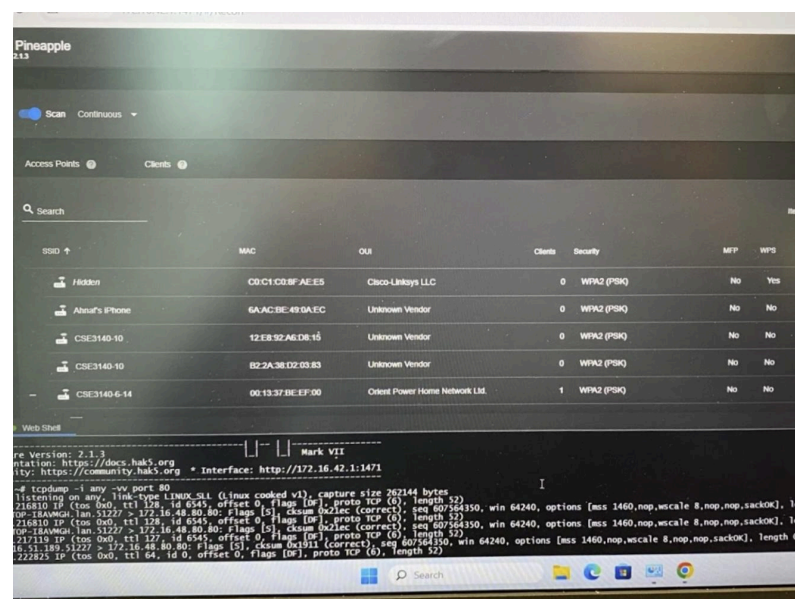
The cse3140 network is using WPA2(PSK) security.



Q4:

When you connect to an unsecured network, you see traffic because it is un-encrypted. The traffic came from DESKTOP-I8AVMGH, which was the laptop used in the lab. When I connected to the protected network, there was no visible traffic because of security protocols that encrypted the data. This shows that information is easier to find on unsecured networks than secured networks.



[illegible]

Q6:

Client	Security	WPA2	WPS	Channel	Signal
Cisco Systems Inc.	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	1	
Cisco Systems Inc.	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	6	
Cisco Systems Inc.	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	6	
Cisco Systems Inc.	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	6	
Cisco Systems Inc.	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	11	
Cisco Systems Inc.	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	11	
Cisco Systems Inc.	WPA2 (802.1X Enterprise, 802.1X Enterprise FT)	Optional	No	11	
Cisco Systems Inc.	WPA2 (PSK)	No	No	11	
Client Power Home Network Ltd.	WPA2 (PSK)	No	Yes	6	
Unknown Vendor	WPA2 (PSK)	No	No	6	
Cisco Systems Inc.	WPA2 (PSK)	No	No	6	

SSID	MAC	Out	Client	Security	WPA2	WPS	Channel	Signal	First Seen
Molekule_0808	10:8E:BA:06:3A:0F	Molekule	0	Open	No	No	1		0m 35s ago
UCONN-GUEST	00:27:E3:37:45:E2	Cisco Systems Inc.	0	Open	No	No	11		0m 37s ago
UCONN-GUEST	00:27:E3:3E:0D:D2	Cisco Systems Inc.	0	Open	No	No	11		0m 37s ago
UCONN-GUEST	00:27:E3:33:CD:C2	Cisco Systems Inc.	0	Open	No	No	6		0m 29s ago
UCONN-GUEST	00:27:E3:33:CF:02	Cisco Systems Inc.	0	Open	No	No	6		0m 29s ago
UCONN-GUEST	00:27:E3:34:1A:C2	Cisco Systems Inc.	0	Open	No	No	6		0m 35s ago
UCONN-GUEST	00:27:E3:30:02:02	Cisco Systems Inc.	0	Open	No	No	1		0m 39s ago
UCONN-GUEST	00:27:E3:30:04:C2	Cisco Systems Inc.	0	Open	No	No	5		0m 39s ago
UCONN-GUEST	50:2F:A8:12:E5:01	Cisco Systems Inc.	0	Open	No	No	6		0m 40s ago

**What wireless networks are visible? Each row is a separate network.**

The wireless networks visible are UCONN-GUEST, Molekule\_0808, UCONN-SECURE, and numerous others.

**Can you identify an access point that announces more than one network? How do you know?**

UCONN-SECURE and UCONN-GUEST were listed many times. For example each time UCONN-SECURE was listed, it had different values in the MAC column, while the other columns were the same between the two versions.

**In the security column, what are the different values listed? (e.g. WPA2, Open, etc)**

Open, WEP, WPA2(PSK) (used by the cse3140 network), and WPA2(802.1X Enterprise, 802.1X Enterprise FT) which is used for the UCONN-SECURE network.

Q7: video (worked with Rohit and Faiyhaa because my phone wasn't working)

[https://drive.google.com/file/d/1Fnlije8O9Bnbx1H2f5PQ2RRi\\_QGeaTB/view?usp=drive\\_link](https://drive.google.com/file/d/1Fnlije8O9Bnbx1H2f5PQ2RRi_QGeaTB/view?usp=drive_link)

We connected another laptop to the CSE3140-Sec005-Team14, then went to the terminal and typed in the route at root@172.16.42.1. We were able to connect to the IP address mentioned within the instructions by sshing from the terminal, using the interface name "any" which allowed us to see who was connected to the network; but since it was secure we were not able to retrieve the same client information we were able to in 4.

Q8: I have an iPhone :(