

Conestoga College

Course	INFO8965: Computer and Network Security
Activity	Wireless Network Security
Student Name	Twinkle Akhilesh Mishra
Date performed	24-March-2025

Objectives

- Explore WLAN security information using Vistumbler
- Learn about the enhanced security features in WPA3

Resources

- Hardware: PC/Laptop with wireless network capability
- Software: Vistumbler - Available at <https://www.vistumbler.net/>

(A) View WLAN Security Information with Vistumbler

1. Install and Set Up Vistumbler
 - Download and install Vistumbler from www.vistumbler.net using default settings.
 - Launch Vistumbler and click Scan APs to start scanning for nearby Access Points (APs).
 - View Access Point Details
2. After scanning, select the first AP in the right pane. Create a table of the following captured values, along with their meanings. Add this completed table in **Output #1** [2 marks]

✓ **Output #1 – WLAN Access Point Information (from Vistumbler Scan)**

Field	Captured Value	Meaning
MAC Address	30:B7:D4:FE:B4:08	Unique hardware address of the wireless access point
SSID	A-206	Name of the wireless network being broadcast
Signal Strength	93%	Strong signal, excellent connectivity potential
RSSI	-39 dBm	Received Signal Strength Indicator; a very strong and stable signal
Channel	1	Wi-Fi channel in use (2.4 GHz band)
Authentication	WPA2-Personal	Uses a shared password for access; standard for home networks
Encryption	CCMP	AES-based encryption providing data confidentiality and integrity
Radio Type	802.11n	Wi-Fi standard in use, supports higher throughput and better performance

Details of the first Access Point (SSID: A-206) detected using Vistumbler

3. Explain how this information that you've collected could be used maliciously. Add your answer to **Output # 1** [1 mark].

Potential Misuse: Attackers can leverage this data for reconnaissance. Knowing the SSID, signal strength, and MAC address helps identify and potentially spoof the access point. The authentication and encryption type (WPA2/CCMP) informs the attacker whether it's feasible to attempt a password dictionary attack, especially if they can capture the handshake. A high signal strength like -39 dBm means the attacker is within good range to perform such activities.

Vistumbler v10.8.2 - By Andrew Calcutt - 03-05-2023 - (2025-03-24 11:25:27.mdb)

File Edit Options View Settings Interface Extra WiFiDB Help *Support Vistumbler*

Stop Use GPS Save & Clear Latitude: N 0000.0000 Longitude: E 0000.0000 Active APs: 50 / 104 Loop time: 1003 ms

#	Active	Mac Address	SSID	Signal	High Signal	RSSI	High RSSI	Channel	Authentication	Encryption	Network Type	Latitude	Longitude	Manufacturer	Label	Radio Type
1	Active	30:B7:D4:FE:B4:08	A-206	93%	93%	-39 dBm	-39 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Hicon Technolog...	Unknown	802.11n
2	Dead	68:8F:2E:0F:34:18	D303	0%	40%	-100 dBm	-75 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Hicon Technolog...	Unknown	802.11n
3	Dead	0E:1D:0F:AC:58:E8		0%	26%	-100 dBm	-85 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
4	Dead	7A:8F:2E:08:C0:D8		0%	46%	-100 dBm	-77 dBm	144	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ac
5	Dead	0E:1D:0F:9E:08:08		0%	22%	-100 dBm	-87 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
6	Dead	7A:8F:2E:2E:BE:88		0%	82%	-100 dBm	-46 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
7	Dead	BE:20:2E:D4:18:C8		0%	16%	-100 dBm	-90 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
8	Dead	C2:20:2E:74:AF:70		0%	38%	-100 dBm	-80 dBm	100	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ac
9	Dead	7E:8F:2E:0F:F6:98		0%	50%	-100 dBm	-76 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
10	Dead	46:87:D4:FE:E1:38		0%	50%	-100 dBm	-76 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
11	Dead	7A:8F:2E:08:C0:D8		0%	100 dBm	-75 dBm	-75 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
12	Dead	C2:20:2E:74:AF:78		0%	35%	-100 dBm	-81 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
13	Dead	C6:50:3C:6A:D6:CA	Unit307	0%	35%	-100 dBm	-81 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ac
14	Dead	90:50:CA:DC:22:58	Unit307	0%	46%	-100 dBm	-77 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Hicon Technolog...	Unknown	802.11n
15	Active	92:50:CA:DC:22:58	Unit307	18%	29%	-89 dBm	-84 dBm	100	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ac
16	Active	34:60:F9:3C:6A:2E	Pmus55947	67%	99%	-70 dBm	-35 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	TP-Link Corporatio...	Unknown	802.11ac
17	Active	6A:8F:2E:2E:BE:88	208-A	81%	81%	-62 dBm	-62 dBm	144	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ac
18	Active	68:8F:2E:2E:BE:88	208-A	86%	87%	-53 dBm	-52 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Hicon Technolog...	Unknown	802.11n
19	Active	6A:8F:2E:09:5D:10	C&EA205	82%	82%	-61 dBm	-61 dBm	100	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ac
20	Active	68:8F:2E:09:5D:18	C&EA205	82%	86%	-60 dBm	-54 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Hicon Technolog...	Unknown	802.11n
21	Active	32:B7:D4:FE:B4:08	G50	93%	94%	-40 dBm	-39 dBm	36	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ac
22	Active	68:8F:2E:0F:F6:98	HR207A	90%	93%	-46 dBm	-41 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Hicon Technolog...	Unknown	802.11n
23	Active	AC:20:2E:74:AF:78	Wang_Network	81%	81%	-63 dBm	-63 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Hicon Technolog...	Unknown	802.11n
24	Active	AE:20:2E:74:AF:70	Wang_Network	40%	60%	-79 dBm	-73 dBm	100	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ac
25	Active	6A:8F:2E:08:C0:D8	202	35%	57%	-81 dBm	-74 dBm	144	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ac
26	Active	68:8F:2E:08:C0:D8	202	50%	67%	-76 dBm	-70 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Hicon Technolog...	Unknown	802.11n
27	Active	C6:50:3C:6A:D6:C9	271	46%	46%	-77 dBm	-77 dBm	6	OWE		Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ac
28	Active	32:B7:D4:FE:E1:30	baddies <3	18%	26%	-89 dBm	-85 dBm	100	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ac
29	Dead	0E:1D:0F:9C:28:78		0%	38%	-100 dBm	-80 dBm	11	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
30	Active	0A:1D:0F:A1:60:88		24%	31%	-96 dBm	-83 dBm	6	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
31	Dead	BE:20:2E:7A:CA:08		0%	26%	-100 dBm	-85 dBm	1	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
32	Dead	0E:1D:0F:AC:58:E8		0%	31%	-100 dBm	-83 dBm	6	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
33	Active	7A:8F:2E:08:C0:D8		38%	57%	-80 dBm	-74 dBm	144	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ac
34	Dead	0E:1D:0F:9E:08:08		0%	22%	-100 dBm	-87 dBm	11	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
35	Dead	A6:50:CA:DC:22:58		0%	50%	-100 dBm	-76 dBm	1	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
36	Active	7A:8F:2E:2E:BE:88		87%	87%	-52 dBm	-52 dBm	1	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
37	Active	BE:20:2E:D4:18:C8		24%	31%	-86 dBm	-83 dBm	11	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
38	Active	C6:50:3C:6A:D6:CC		43%	43%	-78 dBm	-78 dBm	6	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ac
39	Active	A2:50:CA:BF:77:38		20%	26%	-88 dBm	-85 dBm	6	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n

First Access Point (SSID: A-206) is Detected

4. Expand the Authentication and Encryption categories for the selected AP in the left pane and list the types, along with a brief explanation for each in **Output #2** (2 Marks).

Authentication	WPA2-Personal	Requires a pre-shared key (password). Common in homes. Vulnerable to brute-force attacks if the password is weak.
Encryption	CCMP	AES-based encryption is used with WPA2 and WPA3. Provides strong confidentiality and integrity for data in transit.

Description: The selected AP "A-206" uses **WPA2-Personal** authentication and **CCMP** encryption, which are secure and standard for most home and small business networks. WPA2-Personal is based on a shared password, while CCMP uses AES encryption to protect transmitted data.

Output #2 – Authentication and Encryption Types with Descriptions

The screenshot displays the Vistumbler v10.8.2 interface. The left sidebar shows the 'Authentication' and 'Encryption' settings for the selected AP 'A-206'. The main table lists various detected APs with their details.

Authentication Settings for A-206:

- SSID: A-206
- Mac Address: 30:B7:D4:FE:B4:08
- Channel: 001
- Network Type: Infrastructure
- Encryption: CCMP
- Radio Type: 802.11n
- Authentication: WPA2-Personal
- Basic Transfer Rates: 6.9, 12, 18, 24, 36, 48, 54
- Other Transfer Rates:
- Manufacturer: Htton Technologies, Inc.
- Label: Unknown

Encryption Settings for A-206:

- SSID: A-206
- Mac Address: 30:B7:D4:FE:B4:08
- Channel: 001
- Network Type: Infrastructure
- Encryption: CCMP
- Radio Type: 802.11n
- Authentication: WPA2-Personal
- Basic Transfer Rates: 6.9, 12, 18, 24, 36, 48, 54
- Other Transfer Rates:
- Manufacturer: Htton Technologies, Inc.
- Label: Unknown

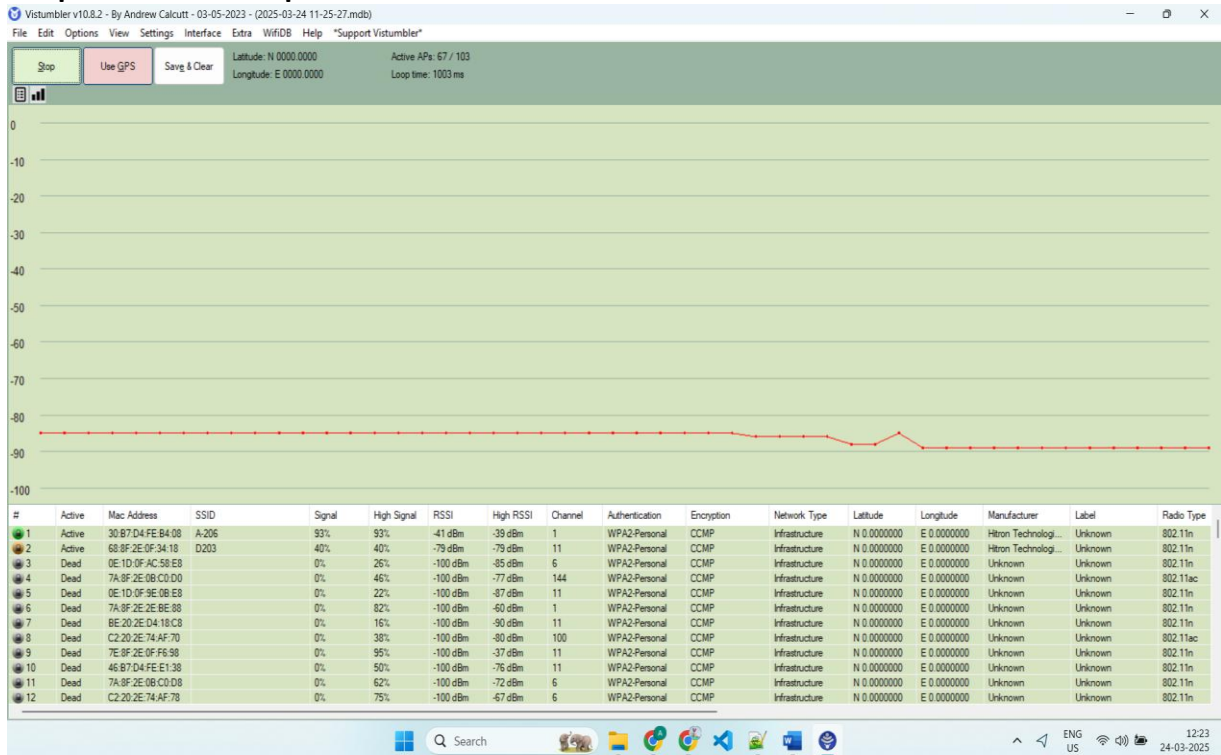
Table of Detected APs:

#	Active	Mac Address	SSID	Signal	High Signal	RSSI	High RSSI	Channel	Authentication	Encryption	Network Type	Latitude	Longitude
1	Dead	30:B7:D4:FE:B4:08	A-206	0%	53%	-100 dBm	-40 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
2	Dead	68:8F:2E:0F:34:18	D203	0%	29%	-100 dBm	-84 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
3	Dead	0E:1D:0F:AC:58:E8		0%	26%	-100 dBm	-85 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
4	Dead	7A:8F:2E:08:C0:D0		0%	46%	-100 dBm	-77 dBm	144	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
5	Dead	0E:1D:0F:9E:08:E8		0%	22%	-100 dBm	-87 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
6	Dead	7A:8F:2E:2E:BE:88		0%	82%	-100 dBm	-60 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
7	Dead	BE:20:2E:D4:18:C8		0%	16%	-100 dBm	-90 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
8	Dead	C2:20:2E:74:AF:78		0%	38%	-100 dBm	-80 dBm	100	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
9	Dead	7E:8F:2E:0F:F6:98		0%	95%	-100 dBm	-37 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
10	Dead	46:87:D4:FE:E1:30		0%	50%	-100 dBm	-76 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
11	Dead	7A:8F:2E:08:C0:D0		0%	62%	-100 dBm	-72 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
12	Dead	C2:20:2E:74:AF:78		0%	75%	-100 dBm	-67 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
13	Dead	C6:50:3C:6A:D6:CA		0%	35%	-100 dBm	-81 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
14	Dead	90:50:CA:DC:22:58	Unit307	0%	43%	-100 dBm	-78 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
15	Dead	92:50:CA:DC:22:50	Unit307	0%	24%	-100 dBm	-86 dBm	100	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
16	Dead	34:60:F9:3C:6A:2E	Primus55947	0%	72%	-100 dBm	-68 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
17	Dead	6A:8F:2E:2E:BE:80	208-A	0%	81%	-100 dBm	-63 dBm	144	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
18	Dead	68:8F:2E:2E:BE:88	208-A	0%	86%	-100 dBm	-53 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
19	Dead	6A:8F:2E:09:5D:10	C8EA205	0%	81%	-100 dBm	-63 dBm	100	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
20	Dead	68:8F:2E:09:5D:18	C8EA205	0%	86%	-100 dBm	-54 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
21	Dead	32:87:D4:FE:B4:00	G-5G	0%	94%	-100 dBm	-39 dBm	36	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
22	Dead	68:8F:2E:0F:F6:98	HR207A	0%	91%	-100 dBm	-45 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
23	Dead	AC:20:2E:74:AF:78	Wang_Network	0%	81%	-100 dBm	-63 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
24	Dead	AE:20:2E:74:AF:70	Wang_Network	0%	60%	-100 dBm	-73 dBm	100	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
25	Dead	6A:8F:2E:08:C0:D0	202	0%	46%	-100 dBm	-77 dBm	144	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
26	Dead	68:8F:2E:08:C0:D0	202	0%	65%	-100 dBm	-71 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
27	Dead	C6:50:3C:6A:D6:C9	271	0%	46%	-100 dBm	-77 dBm	6	OWE	CCMP	Infrastructure	N 0.0000000	E 0.0000000
28	Dead	32:87:D4:FE:E1:30	baddies <3	0%	24%	-100 dBm	-86 dBm	100	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000
29	Dead	0E:1D:0F:9E:2B:78		0%	38%	-100 dBm	-80 dBm	11	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000
30	Dead	0A:1D:0F:A1:60:88		0%	22%	-100 dBm	-87 dBm	6	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000
31	Dead	BE:20:2E:74:CA:08		0%	26%	-100 dBm	-85 dBm	1	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000
32	Dead	0E:1D:0F:AC:58:E8		0%	31%	-100 dBm	-83 dBm	6	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000
33	Dead	7A:8F:2E:08:C0:D0		0%	46%	-100 dBm	-77 dBm	144	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000
34	Dead	0E:1D:0F:9E:08:E8		0%	22%	-100 dBm	-87 dBm	11	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000
35	Dead	A6:50:CA:DC:22:58		0%	50%	-100 dBm	-76 dBm	1	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000
36	Dead	7A:8F:2E:2E:BE:88		0%	86%	-100 dBm	-54 dBm	1	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000
37	Dead	BE:20:2E:D4:18:C8		0%	31%	-100 dBm	-83 dBm	11	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000
38	Dead	C6:50:3C:6A:D6:CC		0%	43%	-100 dBm	-78 dBm	6	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000
39	Dead	A2:50:CA:BF:77:38		0%	26%	-100 dBm	-85 dBm	6	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.0000000

Authentication and encryption settings used by Access Point A-206, including WPA2-Personal and CCMP observed in Vistumbler's left panel

- With the first AP selected, go to View > Graph > Graph 1 to display the RSSI graph. Allow time to gather enough data for a full graph. Take a screenshot for **Output #3** (1 Marks) and explain what the graph displays.

Output #3 – RSSI Graph for AP A-206



Graph showing the RSSI (Received Signal Strength Indicator) of AP A-206 over time, used to analyze signal stability and strength.

- The graph depicts the variation in signal (RSSI) of the lifeline access point **A-206** over a certain duration of time. The red line marks the scans each point on the line indicates the signal strength at that time of the scan. In viewing the graph, it is noted that the line is relatively steady between **-90 dBm and -80 dBm**. This indicates that the signal was rather low during the scan period.
- There is a slight bump at one level, yet it plummets back down to where it originally was. Therefore, whatever led to that improvement did not last for a long duration. It could have been something such as a device getting closer to the router, or a small dip in interference, but as stated before, the signal overall remained feeble.
- After viewing the graph, it is easy to see that although the signal was not changing too much, which is good, it was also not strong enough to receive a stable connection or speed. Extremely stable RSSI levels could indicate that the access point is blocked by walls, placed too far from the device, or there is interference from nearby networks.
- In conclusion, the graph proves that while the signal was indeed poor, it was consistent and therefore could have severely impacted the Wi-Fi performance.

(B) WPA3 Security Features

Read about WPA3 from IEEE Spectrum:

<https://spectrum.ieee.org/everything-you-need-to-know-about-wpa3>

Summarize your understanding of the new features, specifically Simultaneous Authentication of Equals (SAE) and Opportunistic Wireless Encryption (OWE). Also explain how these features improve Wi-Fi security in **Output #4** (4 Marks)

Output #4 - WPA3 Security Features: SAE and OWE Summary

- WPA3 is the latest edition of a Wi-Fi security standard, superseding WPA2 due to the latter's security weaknesses over time. Two notable features are Simultaneous Authentication of Equals (SAE) and Opportunistic Wireless Encryption (OWE).
- Both have been implemented to provide protection to users, whether on public or private wifi networks, more efficiently.
- SAE supersedes Pre-shared Key (PSK), which was used in WPA2. With PSK, attackers were able to capture handshake data with relative ease and try to guess the password with much possibility of success. This was due to PSK being far too vulnerable.
- SAE solves this issue through their better and stronger connection establishment technique. Unlike the common handshake, both the device and the router's authentication is done independently, making it difficult for hackers to intercept the process and guess passwords.
- Additionally, forward secrecy is included meaning each session employs a new encryption key, making it far more secure. Even if a person were to figure out the passcode later on, their ability to decrypt older traffic is none.
- In contrast, OWE improves security at publicly accessible areas such as airports or cafes.
- Typically, these open networks are password-less which means anyone can connect to them and monitoring the activities of other users is a possibility.
- OWE solves this problem by autonomously encrypting the connection between the user's device and the networking hardware.
- Overall, SAE protects against password-related attacks on home or private networks, and OWE makes open networks safer for everyday use. These two features make WPA3 a big step forward for Wi-Fi security.