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]

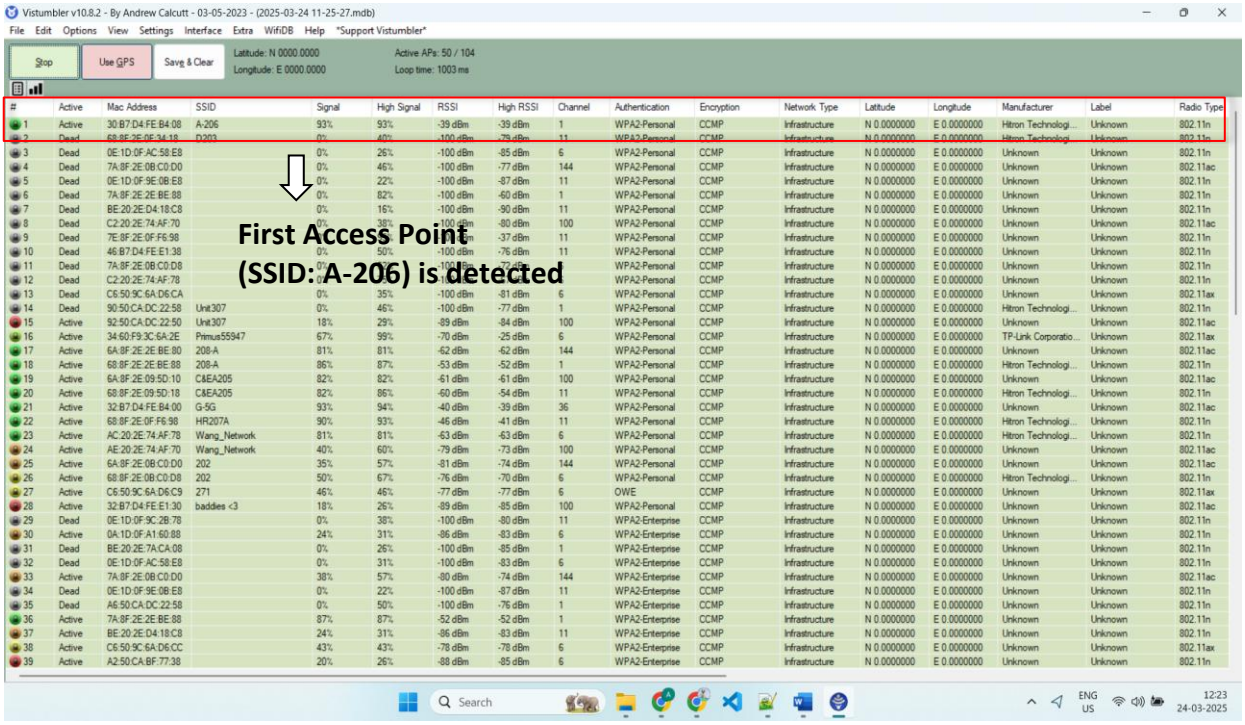
✓ **Output #1 – WLAN Access Point Information (from Vistumbler Scan)**

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.

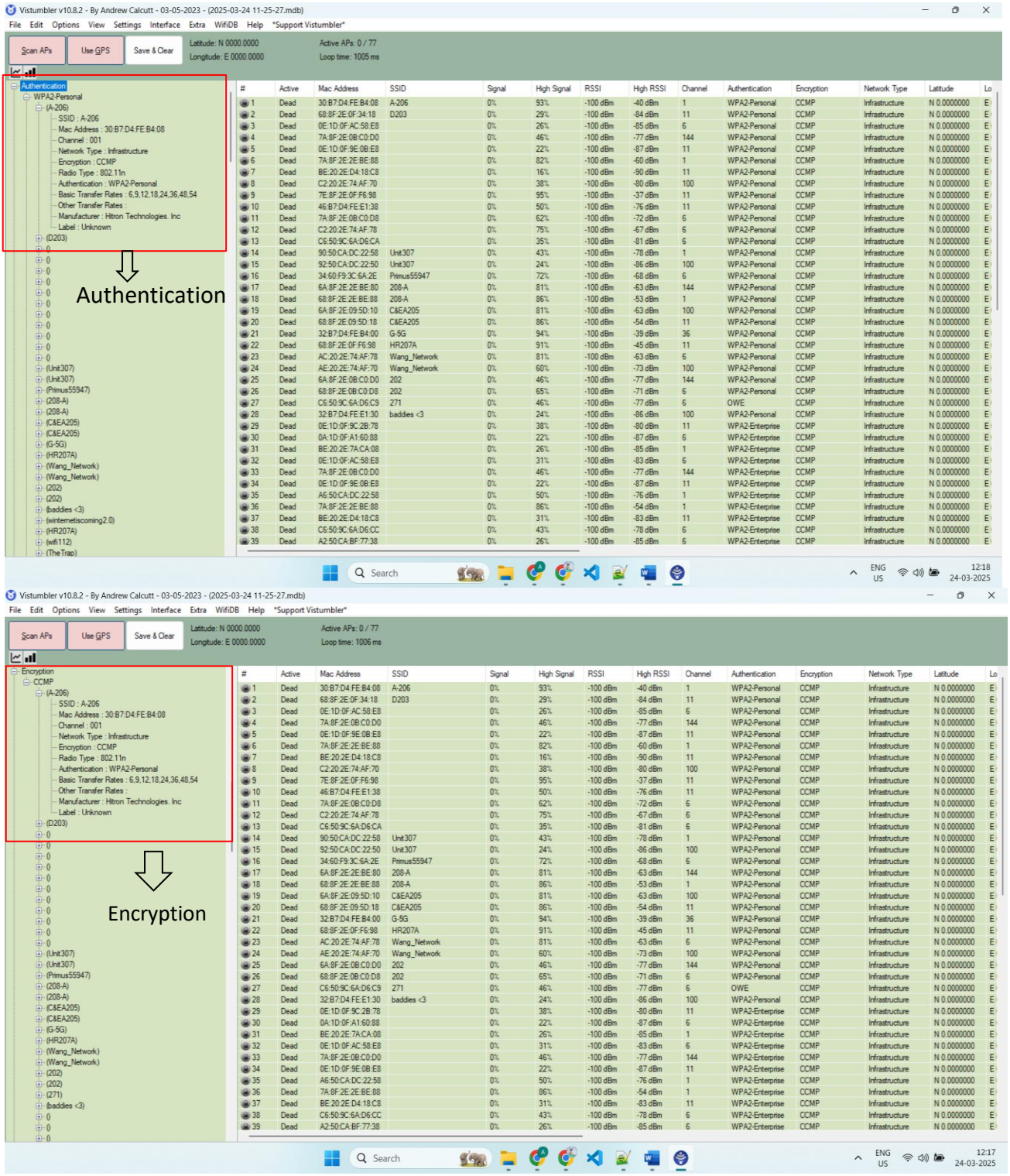


4. Expand the Authentication and Encryption categories for the selected AP in the left pane and list the types, along with a brief explanation for each in **Output #2** (2 Marks).

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.

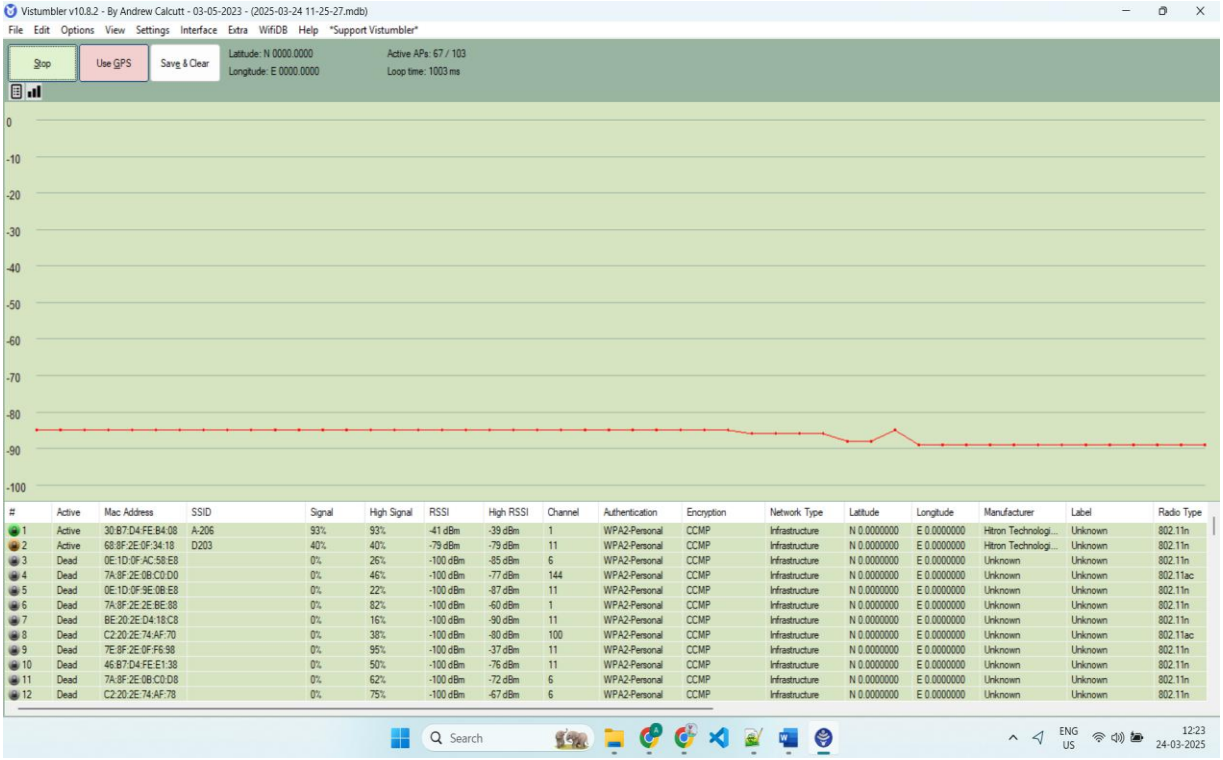
Output #2 – Authentication and Encryption Types with Descriptions



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

5. 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 supersede 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, forth 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.