Lab 8 – Netflow and Wireless Packet Capture Analysis

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Gina Marie

Date – 22nd July 2023

Week 8 Discussion:

Difference between Express Forwarding, IPFIX standard, and Netflow. What are each used for and what are their pros and cons?

- Express forwarding, IPFIX, and Netflow these three technologies are used in network monitoring and traffic analysis. Each has different features and differs in the way of implementation.
- **Express Forwarding:** This is the default packet-switching technique for most routing platforms such as Cisco. It uses a high-speed data structure, such as a Forwarding Information Base (FIB) or a Content-Addressable Memory (CAM), to perform rapid lookups for destination IP addresses and determine the outgoing interface for packet forwarding. This functionality is mainly an internal mechanism in network devices. [3]

- **IPFIX:** It stands for IP flow information export. It is designed for the collection and analysis of flow data from supported network devices such as routers, switches, etc. IPFIX is based on the same concept as Netflow v9. [1][2]
- **Netflow:** Netflow v9 is developed by Cisco and it is designed to collect information on network traffic. Netflow is able to gather and analyze packets through this. It provides information about the traffic flows in a network, including source/destination IP addresses, ports, protocols, and data volume. [1][2]

Technology	**Pros**	**Cons**
Express Forwarding	• Performance improvement. • Provides network resilience. • Flexibility and scalability. • mainly used to increase packet switching speed by reducing the overhead and delays introduced by other routing techniques [3]	• Not used for traffic analysis or flow monitoring
IPFIX	• IPFIX listens on UDP port 4739 • IPFIX is an open standard and is supported by many networking vendors apart from Cisco • IPFIX is sometimes even referred to as “NetFlow v10”. [1][2]	• NetFlow v9 tends to listen on 2055, 2056, 4432, 4739, 9995, 9996, and several others • Requires additional setup and configuration while exporting [1][2]
Netflow	• Simplifies network traffic analysis • Provides insights into traffic patterns [1][2]	• Older versions may have limitations in data granularity • Proprietary to Cisco devices, limited interoperability with non-Cisco equipment [1][2]

Citations –

1. Kumarsamy, S. (2019, September 17). IPFIX vs. NetFlow. Gigamon Blog. https://blog.gigamon.com/2019/09/17/ipfix-vs-netflow/
2. Grimmick, R. (2021, June 17). Flow Monitoring: What is It and Why Do You Need It? Varonis Blog. https://www.varonis.com/blog/flow-monitoring#:~:text=The%20primary%20difference%20between%20the,to%20as%20%E2%80%9CNetFlow%20v10%E2%80%9D
3. Study CCNP. (n.d.). Cisco Express Forwarding (CEF) Overview. Study CCNP. https://study-ccnp.com/cisco-express-forwarding-cef-overview/

Scenario - In this fictitious scenario, you'll be provided a packet capture file in an effort to assist an investigation. Inter0ptic is on the lam and is pinned down. The area is crawling with cops, and so he must stay put. He desperately needs to be able to get a message out to Ann and Mr. X. Luckily for him, he detects a wireless access point (WAP) in the building next door that he might be able to use. Meanwhile next door, Joe is a sysadmin for HackMe, Inc. He runs the IT infrastructure, including a WAP that is used pretty much exclusively by him. He’s trying to use it now and has discovered that he’s begun to get dropped. He captured some traffic but doesn’t know how to interpret it. Suddenly he discovered he can’t even login to administer his WAP at all. Joe has provided us with a packet capture and permission to inspect it in any way you need. He tells us his own MAC address is 00:11:22:33:44:55 and reiterates that no one else should be using this WAP. Wlan.pcap is stored in Evidence Drive, under "Wireless Packet Capture Analysis". (Linux or Windows)

Introduction - Joe sysadmin for HackMe who runs IT infrastructure has provided wlan.pcap file and his MAC address details and we have to carry out packet capture analysis to better understand what happened with WAP and who the attacker in this scenario is.

Pre-Lab – For this, I am using a Windows machine and Wireshark to analyze wlan.pcap file. We have given wlan.pcap file and MAC address of Joe 00:11:22:33:44:55 We will be using multiple Wireshark commands to filter packets and analyze network traffic and perform packet analysis.

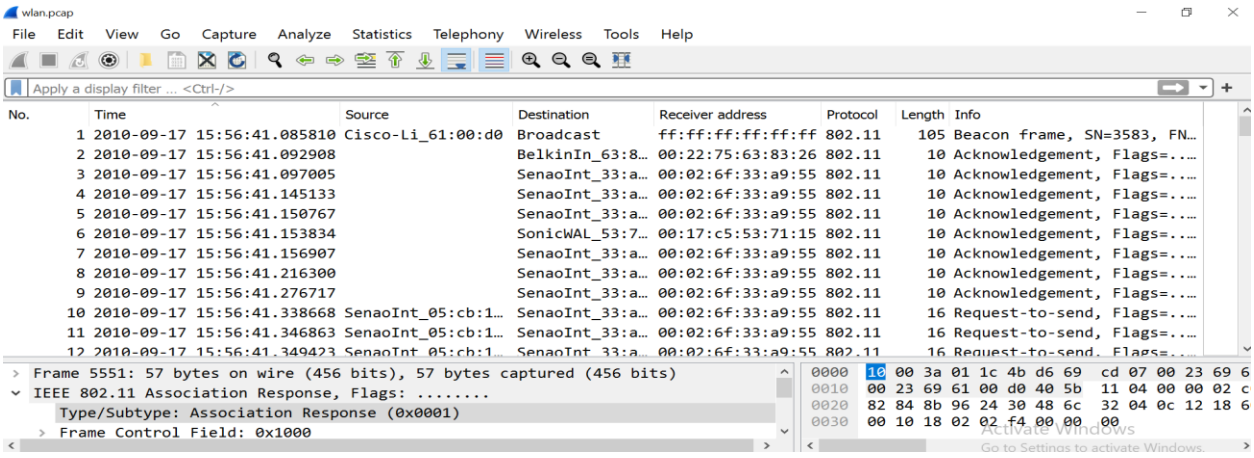
Analysis –

Wireless Packet Capture Analysis

Your team got a tip that Inter0ptic might be in the area.

1. Can you figure out what's going on and track the attacker's activities?

- We have provided wlan.pcap file and as stated by Joe (Admin Guy) his MAC address is 00:11:22:33:44:55. Open pcap file. We are seeing MAC addresses other than legit MAC address as well. But have to analyze all packets carefully to come to any conclusion. Let's start the analysis of packets and different requests which has sent in each frame.



2. What are the BSSID and SSID of the WAP of interest?

- SSID is the network "name" that you see when you try and connect
  BSSID: An access point MAC (hardware) address. The BSSIDs are used to identify the access points and keep them separate from one another. [4]

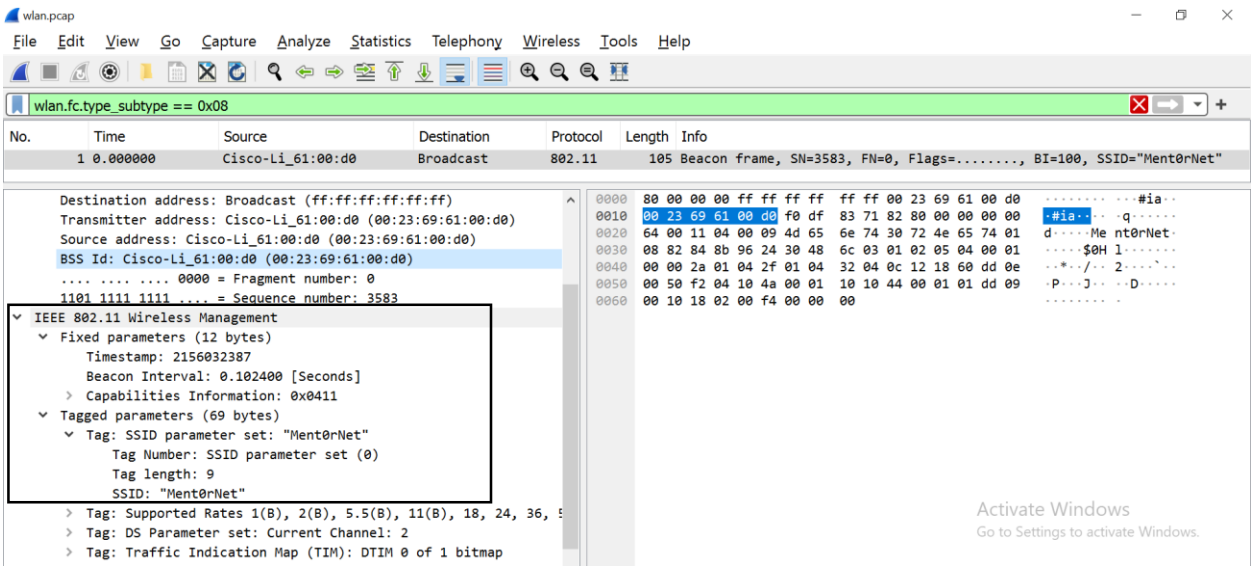
  To check the BSSID and SSID of WAP interest use the below query

  The Wireshark display filter for Beacon packets is “wlan.fc.type_subtype == 0x08” [1]

  BSSID: 00:23:69:61:00:d0, SSID: Ment0rNet

- SSID parameter set: The SSID (Ment0rNet) broadcasted by the access point

- The **beacon frame** is one of the most information-dense wireless packets. The access point sends a beacon frame as a broadcast to announce its presence to any wireless clients. It relays information about the parameters that must be set on the client side in order to connect to it.



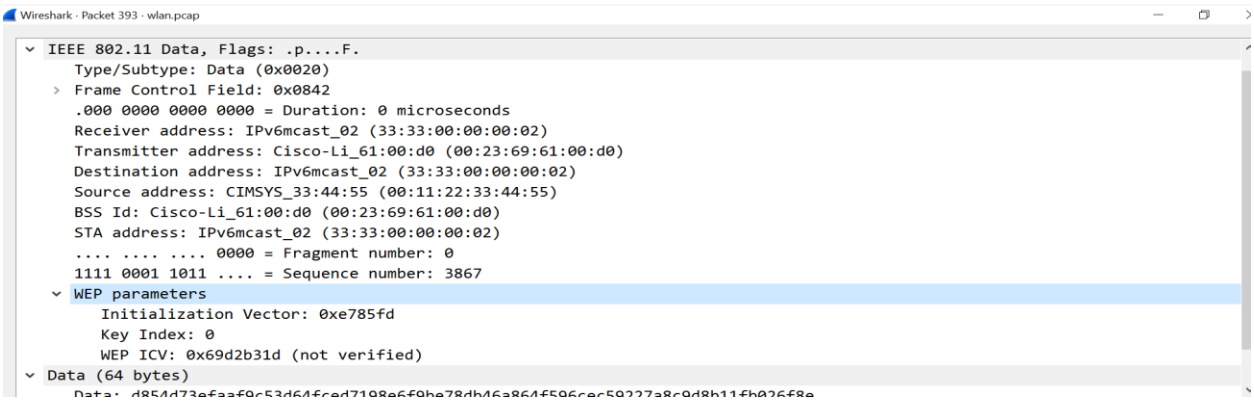
3. Is the WAP of interest using encryption?

- WEP encryption is being used here. Initialization Vector: 0xe785fd

  The IV is combined with the encryption key to create a unique encryption key for each packet, enhancing security.

- **WEP encryption** has significant vulnerabilities that make it easy to crack, making it highly susceptible to various attacks, such as the "chop-chop" attack, "IV attack," , WEP and "FMS attack."

  Note - WEP only provides encryption and lacks proper user authentication, making it vulnerable to unauthorized access.



4. What stations are interacting with the WAP and/or other stations on the WLAN?

- To identify the stations interacting with the WAP and other stations on the WLAN:

  Command - wlan.fc.type_subtype == 0x00 || wlan.fc.type_subtype == 0x01 || wlan.fc.type_subtype == 0x02 (This filter shows management frames like Probe Request, Probe Response, Association Request, and Association Response.).

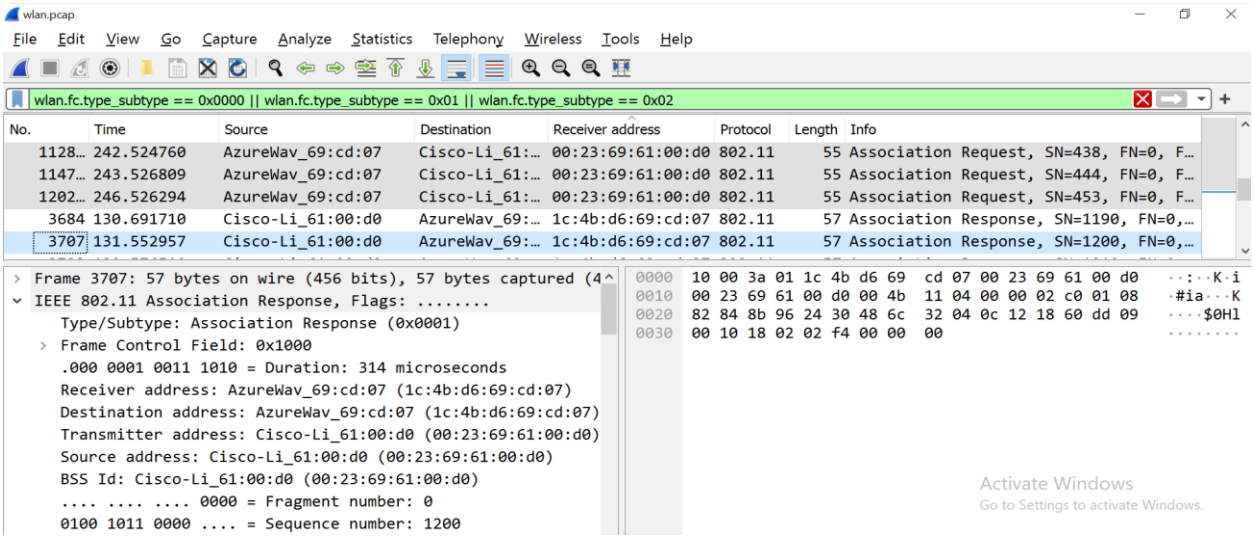
  After applying filter click on Statistics → Endpoints. This will show all the station's communicating with WAP and other stations. Below are the details:

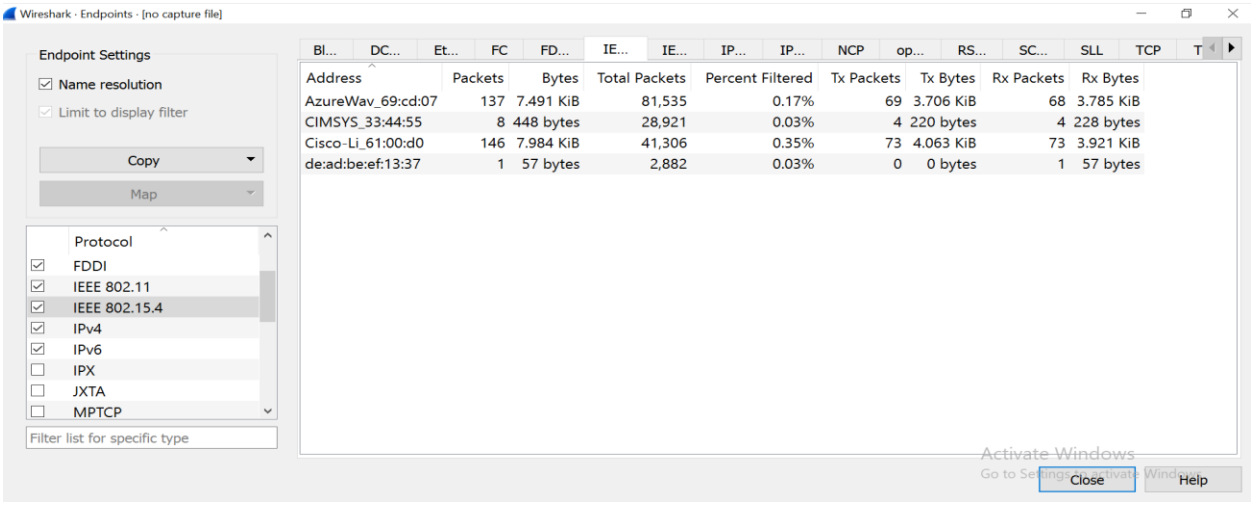
  Cisco-Li_61:00:d0 (00:23:69:61:00:d0)

  AzureWav_69:cd:07 (1c:4b:d6:69:cd:07)

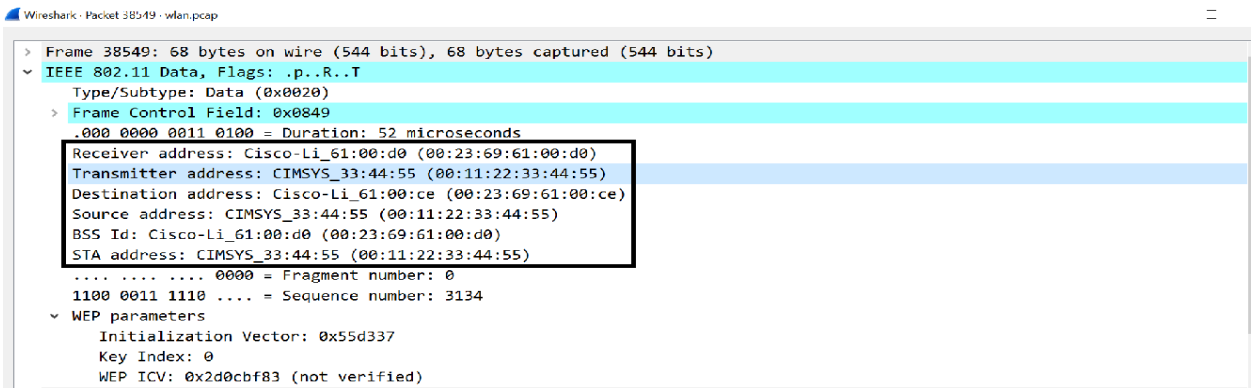
CIMSYS_33:44:55 (00:11:22:33:44:55)

de:ad:be:ef:13:37 (de:ad:be:ef:13:37)





- From the details provided by Joe (The sysadmin) we know that “00:11:22:33:44:55” is his Mac address. Also Mac address “00:23:69:61:00:d0” is the BSS ID.

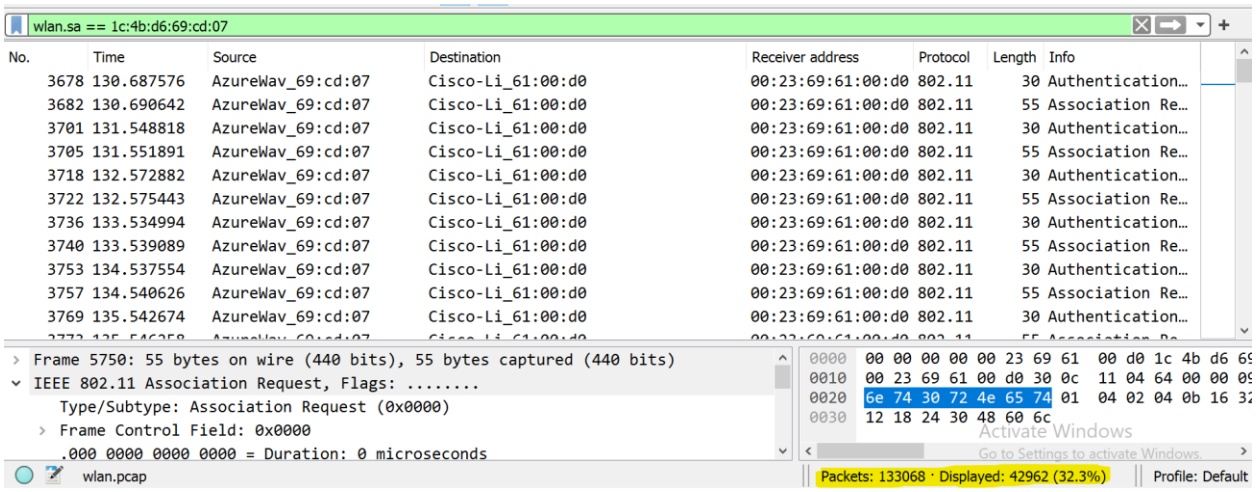


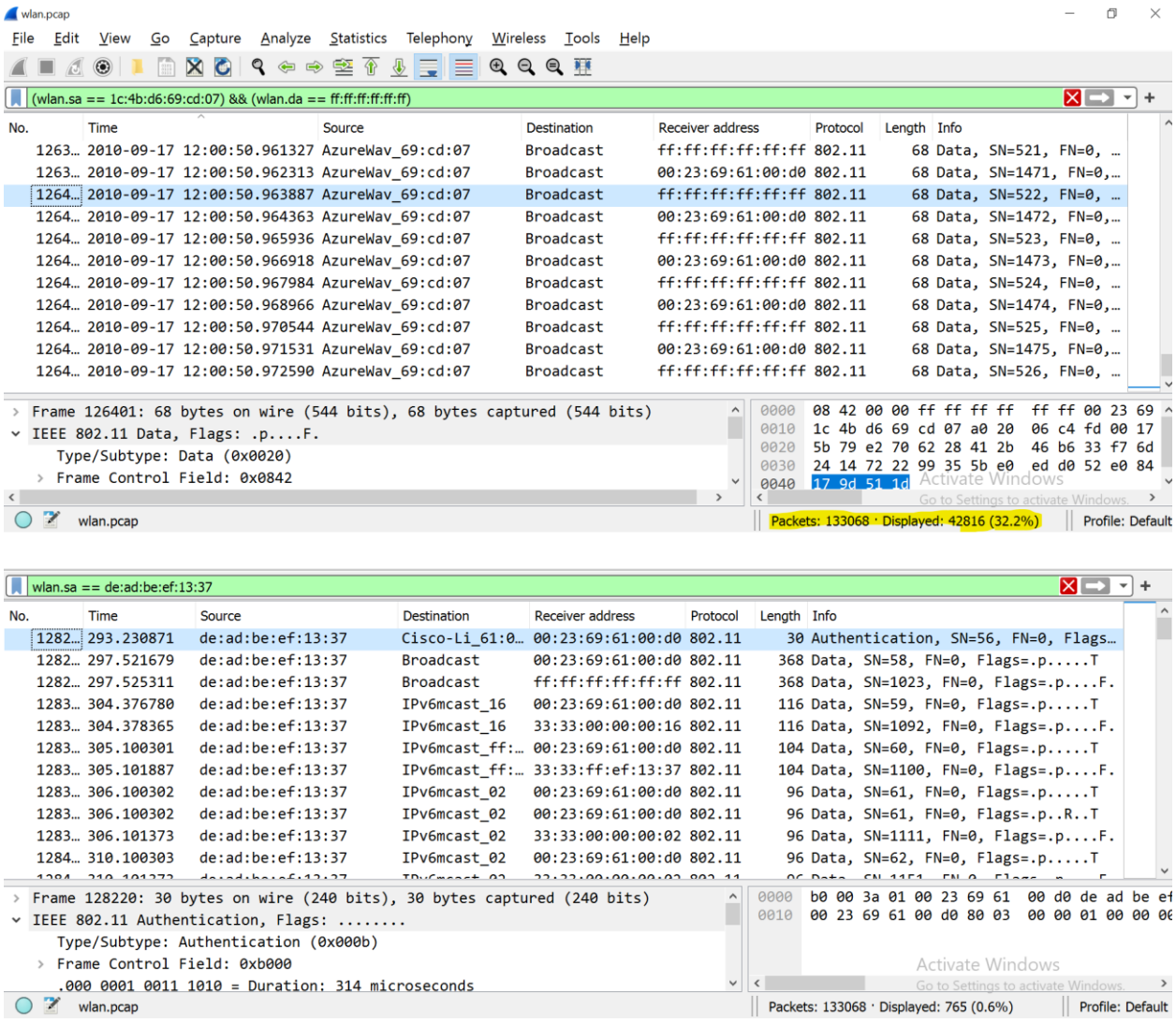
5. Are there patterns of activity that seem anomalous?

- After searching endpoints we know two endpoints Joe's MAC address - "00:11:22:33:44:55" and BSSID - 00:23:69:61:00:d0. However, other two endpoints seems suspicious which are - AzureWav_69:cd:07 (1c:4b:d6:69:cd:07), de:ad:be:ef:13:37 (de:ad:be:ef:13:37)

6. How are they anomalous: Consistent with malfunction?

- Total 42962 packets were sent from station AzureWav_69:cd:07 (1c:4b:d6:69:cd:07) out of which 42816 frames were broadcast frames which are all data frames.
- Total 765 packets were sent from de:ad:be:ef:13:37 out of which only 4 are broadcast frames
- This frame count is huge and sent within a shorter time duration which looks suspicious.



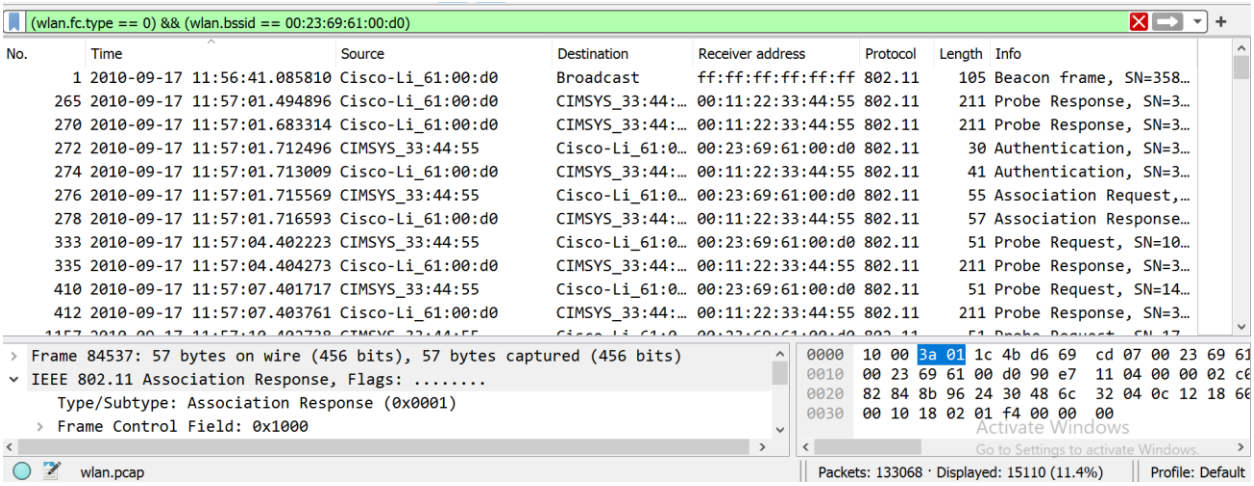


-

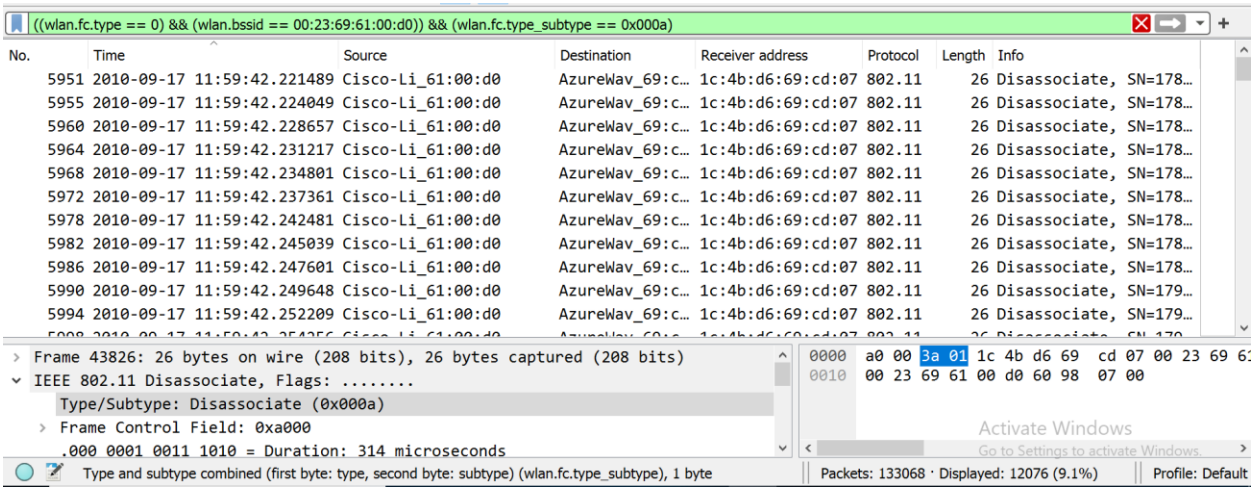
7. Consistent with maliciousness?

- As previously confirmed by Joe only he use this WAP. But now we have seen huge traffic from unknown data frames out of which 42816 are data frames from AzureWav_69:cd:07 (1c:4b:d6:69:cd:07) endpoint which looks malicious. The other odd station, de:ad:be:ef:13:37, also communicated with the WAP and has sent a lot of data frames.
- Also WEP encryption is being used which is vulnerable to many attacks

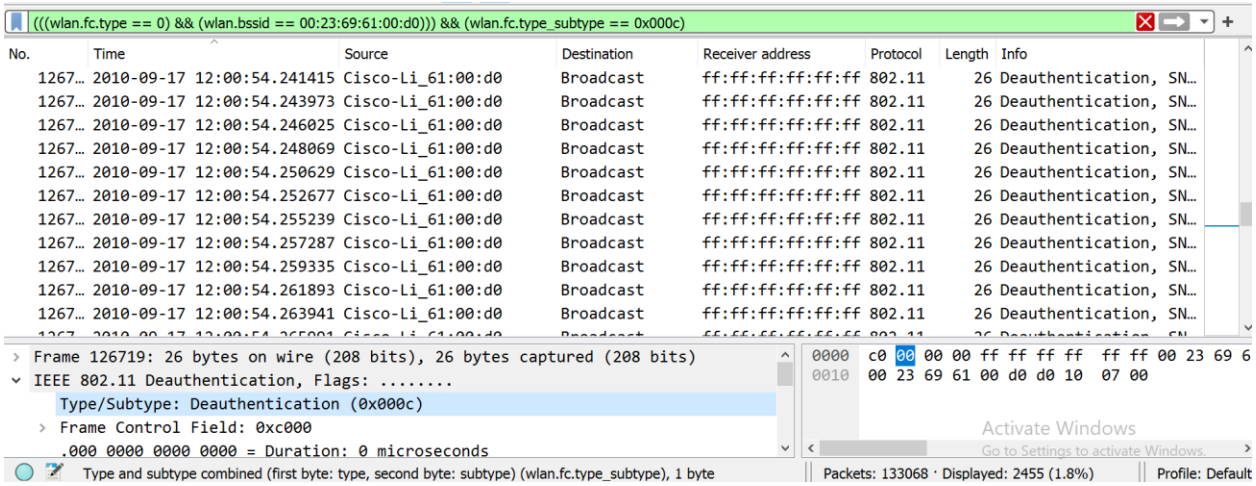
- Now, to further search for management frames from BSSID we have used the command (wlan.fc.type == 0) && (wlan.bssid == 00:23:69:61:00:d0). A total of ‘15110’ are management frames. Management frames enable stations to establish and maintain communication. Management packets are used for authentication, association, and synchronization.



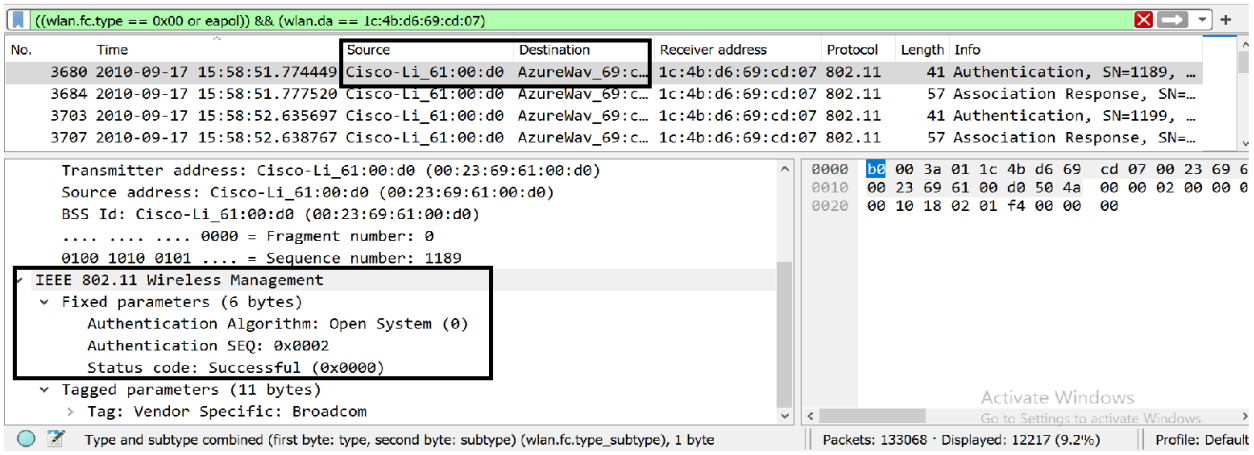
- Out of which 12076 are Disassociate frames from BSSID. To check this we have used subtype (wlan.fc.type_subtype == 0x000a). The WAP told the unknown MAC, 1c:4b:d6:69:cd:07, to Disassociate 12,076 in 65 seconds. Dissociation frames are sent to terminate the connection.



- A total of 2455 are Deauthentication frames from BSSID. To check this we have used (wlan.fc.type_subtype == 0x000c). The WAP broadcasted 2455 Deauthentication messages in the same time. 802.11 does not include a mechanism for verifying the authenticity of the sender and can likely be spoofed. WAP sends this frame as an announcement by a station that sends a de-authentication frame to another station if it wishes to terminate secure communications.



- The complete client authentication process can be seen using the command ((wlan.fc.type == 0x00 or eapol)) && (wlan.da == 1c:4b:d6:69:cd:07)



[1]

8. Can we identify any potentially bad actors?

- After carefully investigating all packets it is concluded that AzureWav_69:cd:07 (1c:4b:d6:69:cd:07) is an attacker. He sent Authentication and association packets at start to get authenticated with WAP and then started sending data packets. It seems WAP's de-authentication and disassociates packets were an indication for an attacker if it wishes to terminate secure communication and to stop sending data frames and stop authentication and association requests. This seems to be a WEP cracking attack and has taken advantage of WEP vulnerabilities. It is confirmed that WEP is compromised. [1]
- What is WEP cracking: WEP cracking is a method used for a security breach in wireless networks. Aircrack-ng is mostly used to crack the WEP key. [3]

9. Can we determine if a bad actor successfully executed an attack?

- From above all analysis we can conclude that AzureWav_69:cd:07 (1c:4b:d6:69:cd:07) is an attacker and have taken advantage of vulnerable WEP encryption used in WAP and have successfully executed the attack and have send messages to Ann through data packets.

Citations -

1. Meraki. (2020, October 5). Analyzing Wireless Packet Captures. Meraki Documentation. https://documentation.meraki.com/General_Administration/Tools_and_Troubleshooting/Analyzing_Wireless_Packet_Captures
2. Semfi Networks. (2021, April). Wireshark 802.11 Filters - Reference Sheet. Semfi Networks. https://semfionetworks.com/wp-content/uploads/2021/04/wireshark_802.11_filters_-_reference_sheet.pdf
3. Lamgadey, V. (2021, July). Re: Define WEP Cracking. Board Infinity Discuss. Message posted to https://discuss.boardinfinity.com/t/define-wep-cracking/10187
4. Cohen, D. B. (2022, January 18). Computer Terms Unwrapped: What is BSSID? Atera Blog. https://www.atera.com/blog/computer-terms-unwrapped-what-is-bssid/#:~:text=The%20BSSIDs%20are%20used%20to,address%20for%20each%20access%20point.