Lab 8

NIDS_NIPS and Web Proxy Analysis

Mina Salehi

University of Maryland Baltimore County

CYBR 642 Introduction to Digital Forensics

Presented to: Gina Scaldaferri

04/16/2025

Introduction

NetFlow is a network protocol originally developed by Cisco that captures metadata about IP traffic flows across routers and switches. It is widely used in network forensics for its ability to provide a high-level overview of network activity, including source and destination IP addresses, ports, protocol types, and volume of traffic (Cisco, 2020). One of the main advantages of NetFlow is its scalability—it can monitor large volumes of traffic efficiently without the storage demands of full packet capture. Additionally, NetFlow enables anomaly detection, helping investigators identify suspicious traffic patterns, unauthorized communications, or data exfiltration attempts (Flowmon, 2021).

However, NetFlow also has its limitations. A key drawback is that it does not capture payload data, meaning analysts cannot view the content of communications—only metadata (Flowmon, 2021). This restricts the ability to reconstruct sessions or inspect files, which is often necessary for legal or incident response purposes. Another concern is sampling, where only a subset of traffic is recorded to reduce load, potentially missing short-lived or low-volume malicious activity. Moreover, NetFlow may not offer sufficient insight into encrypted traffic, which further obscures malicious behavior. Despite these limitations, when combined with other tools like packet capture and endpoint monitoring, NetFlow remains a powerful and efficient component of network investigations.

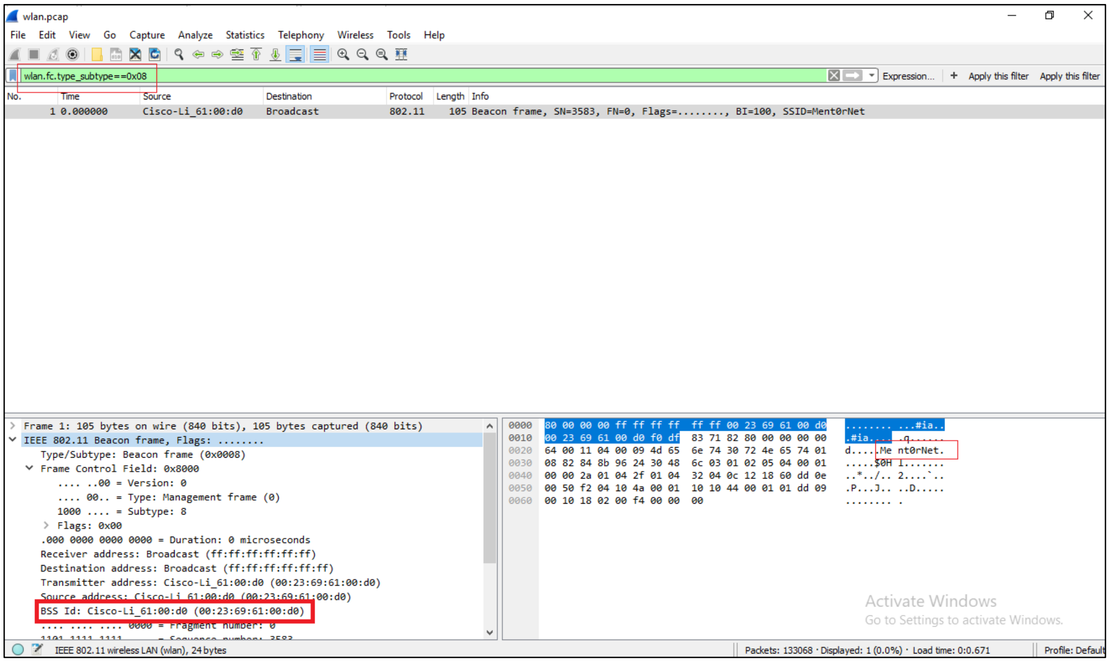
Pre-Analysis

Lab 8 involves a fugitive, Inter0ptic, who is attempting to send a message to known associates, Ann and Mr. X, while evading law enforcement. To do so, Inter0ptic identifies a wireless access point (WAP) in a neighboring building belonging to HackMe, Inc. The system administrator, Joe, who manages the IT infrastructure and the WAP, has begun experiencing network disruptions, including dropped connections and the inability to access his WAP for administrative purposes. In response, Joe captured wireless traffic and provided the packet capture (PCAP) file for forensic analysis.

This lab will involve analyzing the provided PCAP file, to determine if unauthorized access occurred and to identify any communication attempts made by Inter0ptic. The analysis will focus on examining wireless traffic, identifying anomalies, and reconstructing events based on captured data. Tools such as Wireshark are commonly used in wireless forensics for examining packet captures, identifying devices by their Media Access Control (MAC) addresses, and detecting suspicious activity within wireless environments. (Infosec Institute, 2021).

Wireless Packet Capture Analysis

1. **What are the BSSID and SSID of the WAP of interest?**
    - Wireshark Filter: wlan.fc.type_subtype==0x08
    - This filter targets Beacon frames, which advertise the SSID and BSSID of a wireless network
    - SSID (Network Name): Ment0rnet
    - BSS Id (MAC Address of AP): Cisco-Li_61:00:d0 (00:23:69:61:00:d0)



2. **Is the WAP of interest using encryption?**

   - Wireshark command: wlan.fc.type_subtype==0x20 && wlan.bssid==00:23:69:61:00:d0
   - Useful for analyzing which devices are sending/receiving encrypted data during a session.
   - The packets associated with the WAP have the Protected flag set to 1, indicating the use of encryption

```
.... 10.. = Type: Data frame (2)
0000 .... = Subtype: 0
Flags: 0x42
    .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS:
    .... .0.. = More Fragments: This is the last fragment
    .... 0... = Retry: Frame is not being retransmitted
    ...0 .... = PWR MGT: STA will stay up
    ..0. .... = More Data: No data buffered
    .1.. .... = Protected flag: Data is protected
    0... .... = Order flag: Not strictly ordered
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Destination address: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Transmitter address: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)
Source address: Cisco-Li_61:00:c0 (00:23:69:61:00:c0)
```

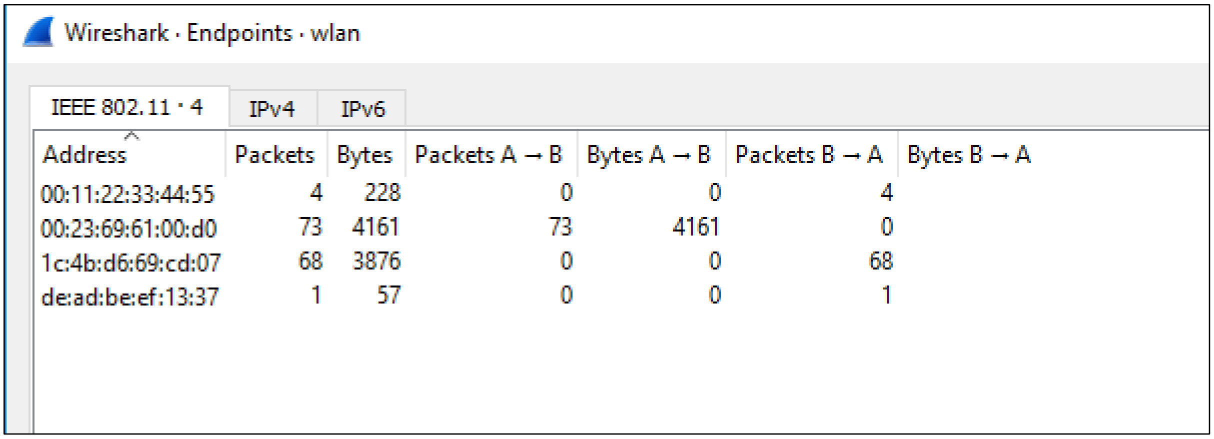
3. What stations are interacting with the WAP and/or other stations on the WLAN?

- (wlan.fc.type_subtype==0x01) && (wlan_mgt.fixed.status_code==0x0000)
- Statistics -> Endpoints -> Endpoint Types: IEEE 801.11
- Several MAC addresses were observed interacting with the WAP, including:
    - 1c:4b:d6:69:cd:07 - suspicious
    - de:ad:be:ef:13:37 – Malicious
    - 00:11:22:33:44:55 – legit

(wlan.fc.type_subtype == 0x01)&&(wlan_mgt.fixed.status_code==0x0000) Expression... + Apply this filter Apply this filter

Packet list Narrow & Wide Case sensitive Display filter Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
98210	234.528892	Cisco-Li_61:00:d0	Azurewav_69:cd:07	802.11	57	Association Response, SN=2814, FN=0, Flags=........
1000…	235.530943	Cisco-Li_61:00:d0	Azurewav_69:cd:07	802.11	57	Association Response, SN=3198, FN=0, Flags=........
1018…	236.531455	Cisco-Li_61:00:d0	Azurewav_69:cd:07	802.11	57	Association Response, SN=3585, FN=0, Flags=........
1037…	237.530943	Cisco-Li_61:00:d0	Azurewav_69:cd:07	802.11	57	Association Response, SN=3976, FN=0, Flags=........
1055…	238.528383	Cisco-Li_61:00:d0	Azurewav_69:cd:07	802.11	57	Association Response, SN=261, FN=0, Flags=........
1110…	241.527869	Cisco-Li_61:00:d0	Azurewav_69:cd:07	802.11	57	Association Response, SN=1394, FN=0, Flags=........
1128…	242.525820	Cisco-Li_61:00:d0	Azurewav_69:cd:07	802.11	57	Association Response, SN=1775, FN=0, Flags=........
1147…	243.527869	Cisco-Li_61:00:d0	Azurewav_69:cd:07	802.11	57	Association Response, SN=2164, FN=0, Flags=........
1202…	246.527358	Cisco-Li_61:00:d0	Azurewav_69:cd:07	802.11	57	Association Response, SN=3323, FN=0, Flags=........
1282…	293.235005	Cisco-Li_61:00:d0	de:ad:be:ef:13:37	802.11	57	Association Response, SN=980, FN=0, Flags=........
1302…	340.025599	Cisco-Li_61:00:d0	CimsysIn_33:44:55	802.11	57	Association Response, SN=1716, FN=0, Flags=........



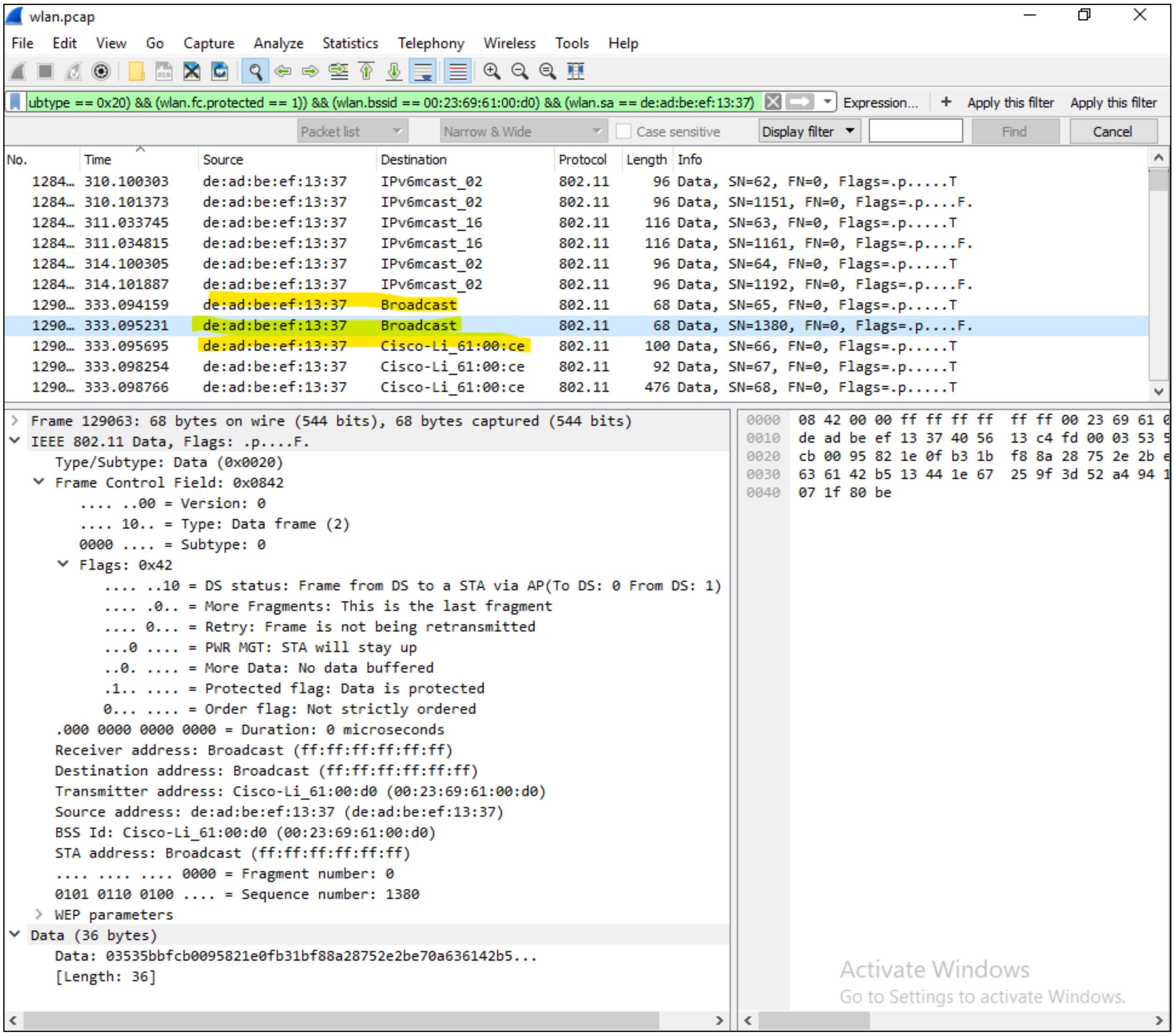
Wireshark · Endpoints · wlan

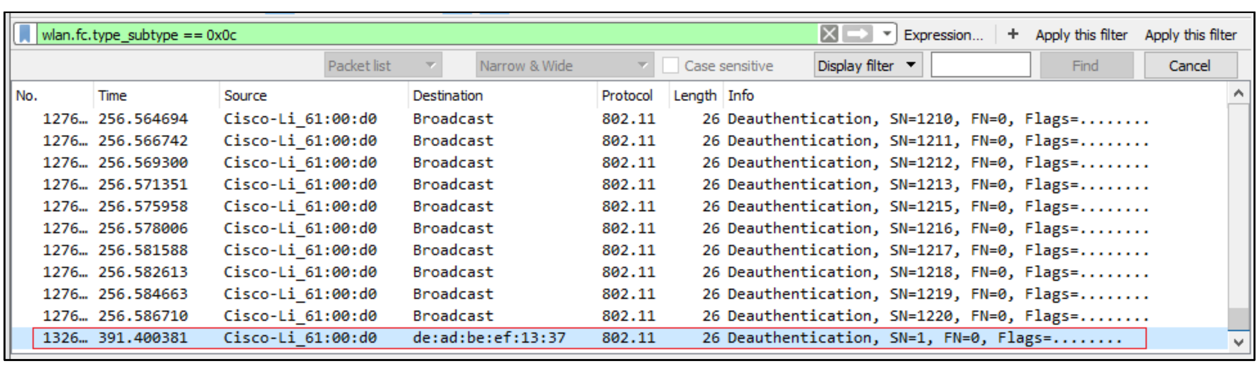
IEEE 802.11 · 4 | IPv4 | IPv6

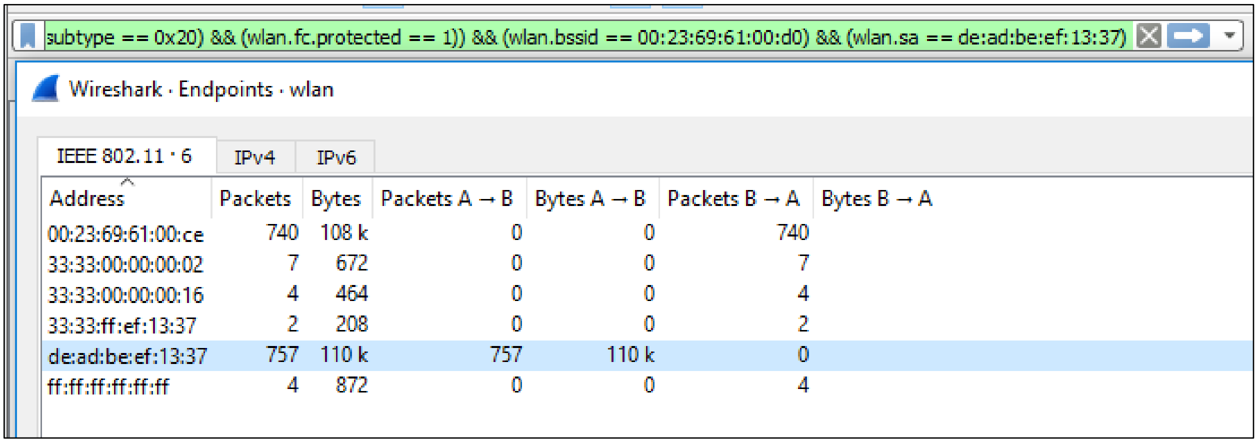
Address	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
00:11:22:33:44:55	4	228	0	0	4	
00:23:69:61:00:d0	73	4161	73	4161	0	
1c:4b:d6:69:cd:07	68	3876	0	0	68	
de:ad:be:ef:13:37	1	57	0	0	1	

4. **Are there patterns of activity that seem anomalous?**

    - Wireshark commands:
        - wlan.fc.type_subtype == 0x0c || wlan.fc.type_subtype == 0x0a
            - 0x0c → Deauthentication frames
            - 0x0a → Disassociation frames
    - ((wlan.fc.type_subtype == 0x20) && (wlan.fc.protected == 1)) && (wlan.bssid == 00:23:69:61:00:d0) && (wlan.sa == de:ad:be:ef:13:37)
    - Yes, de:ad:be:ef:13:37 sending packets and broadcasting to the AP
    - 1c:4b:d6:69:cd:07 – Authenticated but never seen acquiring IP address (likely failed probe)


wlan.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ubtype == 0x20) && (wlan.fc.protected == 1)) && (wlan.bssid == 00:23:69:61:00:d0) && (wlan.sa == de:ad:be:ef:13:37)
Expression... + Apply this filter Apply this filter
Packet list Narrow & Wide Case sensitive Display filter Find Cancel
No. Time Source Destination Protocol Length Info
1284… 310.100303 de:ad:be:ef:13:37 IPv6mcast_02 802.11 96 Data, SN=62, FN=0, Flags=.p.....T
1284… 310.101373 de:ad:be:ef:13:37 IPv6mcast_02 802.11 96 Data, SN=1151, FN=0, Flags=.p....F.
1284… 311.033745 de:ad:be:ef:13:37 IPv6mcast_16 802.11 116 Data, SN=63, FN=0, Flags=.p.....T
1284… 311.034815 de:ad:be:ef:13:37 IPv6mcast_16 802.11 116 Data, SN=1161, FN=0, Flags=.p....F.
1284… 314.100305 de:ad:be:ef:13:37 IPv6mcast_02 802.11 96 Data, SN=64, FN=0, Flags=.p.....T
1284… 314.101887 de:ad:be:ef:13:37 IPv6mcast_02 802.11 96 Data, SN=1192, FN=0, Flags=.p....F.
1290… 333.094159 de:ad:be:ef:13:37 Broadcast 802.11 68 Data, SN=65, FN=0, Flags=.p.....T
1290… 333.095231 de:ad:be:ef:13:37 Broadcast 802.11 68 Data, SN=1380, FN=0, Flags=.p....F.
1290… 333.095695 de:ad:be:ef:13:37 Cisco-Li_61:00:ce 802.11 100 Data, SN=66, FN=0, Flags=.p.....T
1290… 333.098254 de:ad:be:ef:13:37 Cisco-Li_61:00:ce 802.11 92 Data, SN=67, FN=0, Flags=.p.....T
1290… 333.098766 de:ad:be:ef:13:37 Cisco-Li_61:00:ce 802.11 476 Data, SN=68, FN=0, Flags=.p.....T
Frame 129063: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
IEEE 802.11 Data, Flags: .p....F.
Type/Subtype: Data (0x0020)
Frame Control Field: 0x0842
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
0000 .... = Subtype: 0
Flags: 0x42
.... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.1.. .... = Protected flag: Data is protected
0... .... = Order flag: Not strictly ordered
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)
Source address: de:ad:be:ef:13:37 (de:ad:be:ef:13:37)
BSS Id: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)
STA address: Broadcast (ff:ff:ff:ff:ff:ff)
.... 0000 = Fragment number: 0
0101 0110 0100 .... = Sequence number: 1380
WEP parameters
Data (36 bytes)
Data: 03535bbfcb0095821e0fb31bf88a28752e2be70a636142b5...
[Length: 36]
0000 08 42 00 00 ff ff ff ff ff ff 00 23 69 61
0010 de ad be ef 13 37 40 56 13 c4 fd 00 03 53
0020 cb 00 95 82 1e 0f b3 1b f8 8a 28 75 2e 2b
0030 63 61 42 b5 13 44 1e 67 25 9f 3d 52 a4 94
0040 07 1f 80 be
Activate Windows
Go to Settings to activate Windows.


wlan.fc.type_subtype == 0x0c
Expression... + Apply this filter Apply this filter
Packet list Narrow & Wide Case sensitive Display filter Find Cancel
No. Time Source Destination Protocol Length Info
1276… 256.564694 Cisco-Li_61:00:d0 Broadcast 802.11 26 Deauthentication, SN=1210, FN=0, Flags=........
1276… 256.566742 Cisco-Li_61:00:d0 Broadcast 802.11 26 Deauthentication, SN=1211, FN=0, Flags=........
1276… 256.569300 Cisco-Li_61:00:d0 Broadcast 802.11 26 Deauthentication, SN=1212, FN=0, Flags=........
1276… 256.571351 Cisco-Li_61:00:d0 Broadcast 802.11 26 Deauthentication, SN=1213, FN=0, Flags=........
1276… 256.575958 Cisco-Li_61:00:d0 Broadcast 802.11 26 Deauthentication, SN=1215, FN=0, Flags=........
1276… 256.578006 Cisco-Li_61:00:d0 Broadcast 802.11 26 Deauthentication, SN=1216, FN=0, Flags=........
1276… 256.581588 Cisco-Li_61:00:d0 Broadcast 802.11 26 Deauthentication, SN=1217, FN=0, Flags=........
1276… 256.582613 Cisco-Li_61:00:d0 Broadcast 802.11 26 Deauthentication, SN=1218, FN=0, Flags=........
1276… 256.584663 Cisco-Li_61:00:d0 Broadcast 802.11 26 Deauthentication, SN=1219, FN=0, Flags=........
1276… 256.586710 Cisco-Li_61:00:d0 Broadcast 802.11 26 Deauthentication, SN=1220, FN=0, Flags=........
1326… 391.400381 Cisco-Li_61:00:d0 de:ad:be:ef:13:37 802.11 26 Deauthentication, SN=1, FN=0, Flags=........



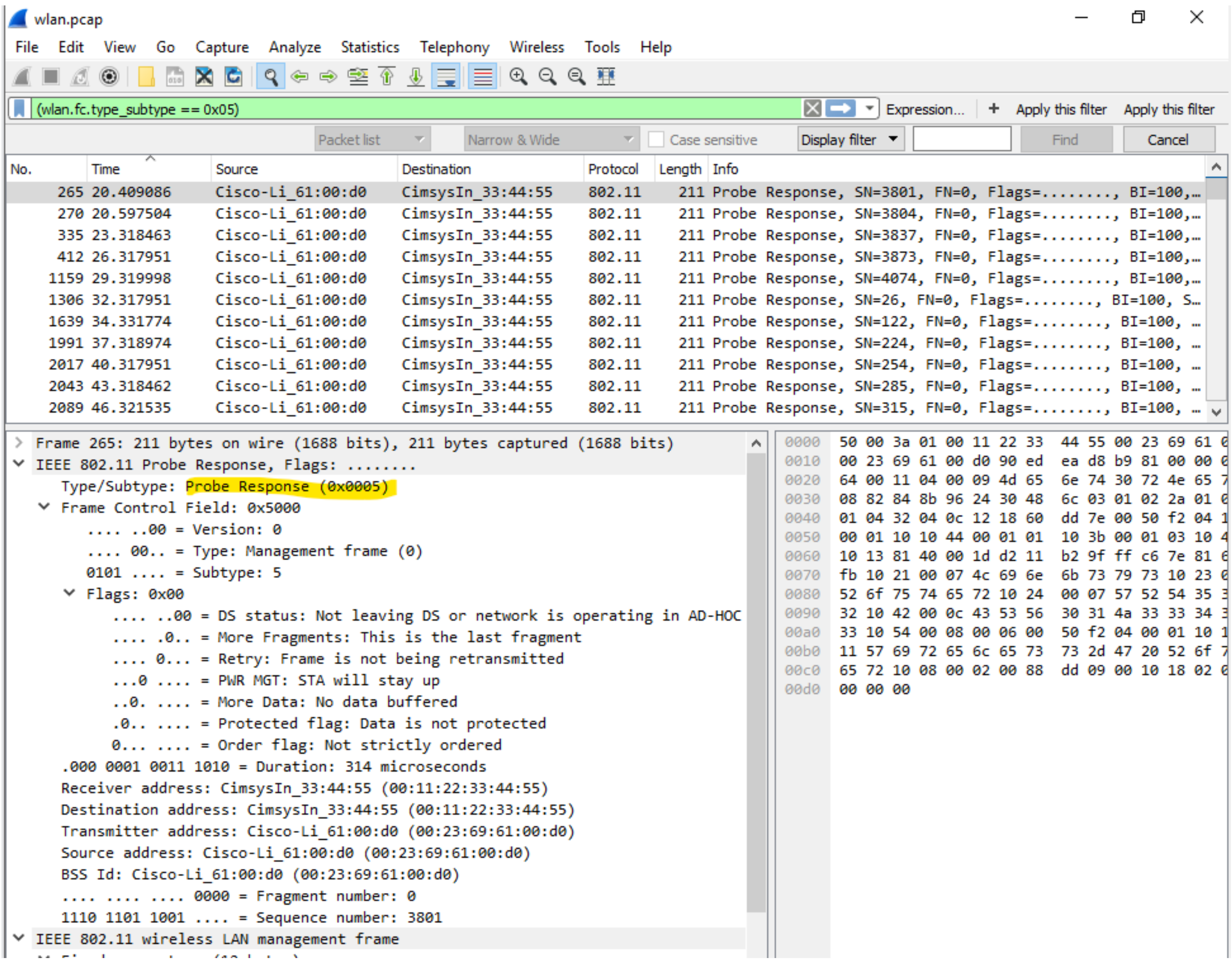
Address	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
00:23:69:61:00:ce	740	108 k	0	0	740	
33:33:00:00:00:02	7	672	0	0	7	
33:33:00:00:00:16	4	464	0	0	4	
33:33:ff:ef:13:37	2	208	0	0	2	
de:ad:be:ef:13:37	757	110 k	757	110 k	0	
ff:ff:ff:ff:ff:ff	4	872	0	0	4	

5. **How are they anomalous: Consistent with malfunction or consistent with maliciousness?**

Consistent with maliciousness.

(wlan.fc.type_subtype == 0x05) : Probe responses can indicate reconnaissance or spoofing attempts (Cisco Systems. (n.d.)).

The volume and timing of deauthentication frames suggest a deliberate attempt to disconnect users, a known tactic in wireless attacks (e.g., ARP replay or deauth attacks using tools like Aircrack-ng)



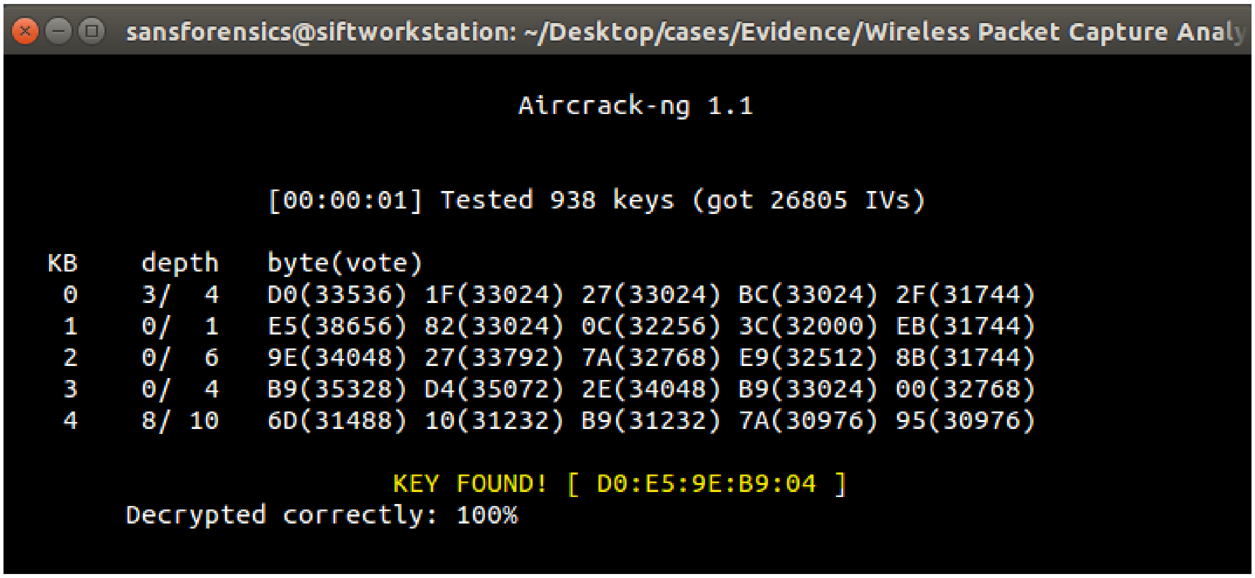
6. **Can you identify any potentially bad actors?**

   - de:ad:be:ef:13:37 stands out as a spoofed or confirmed cracked the WEP and it is malicious
   - 1c:4b:d6:69:cd:07 – suspicious , could not find any malicious activity

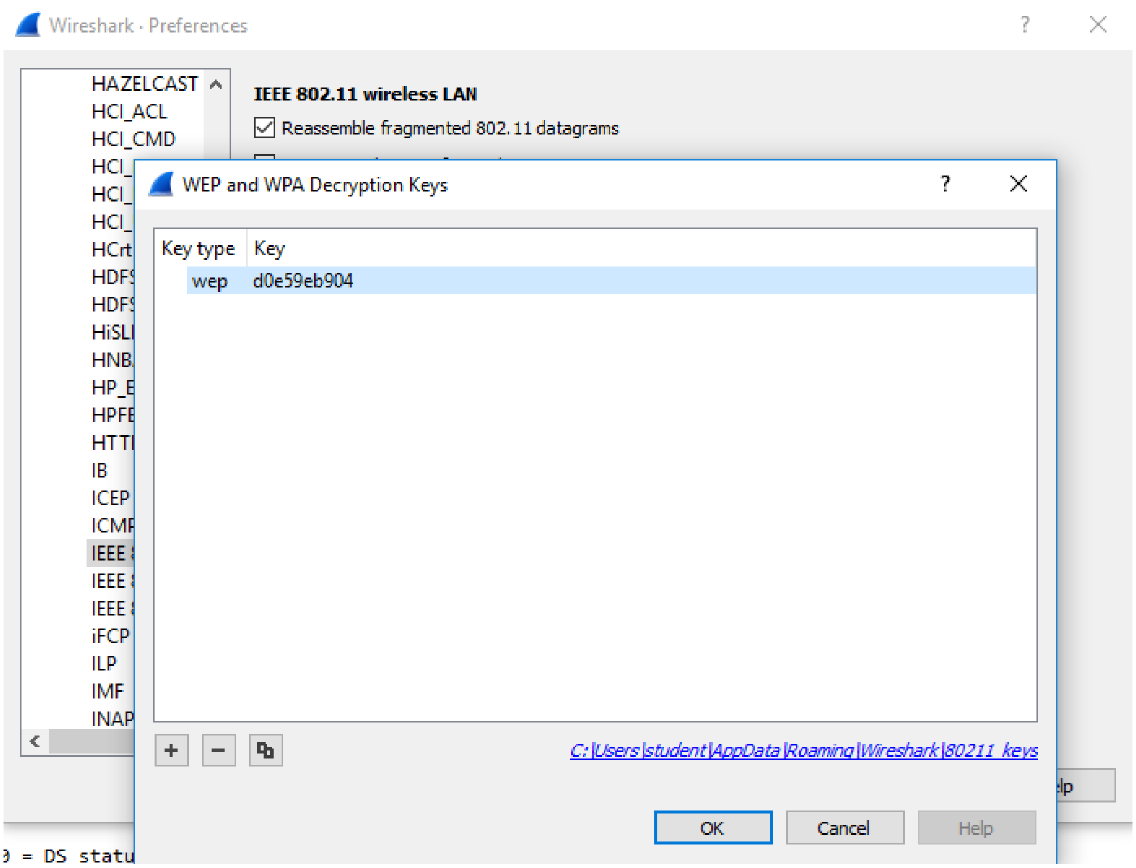
7. **Can you determine if a bad actor successfully executed an attack?**

Yes, attacker was able to find the WEP key using aircrack-ng

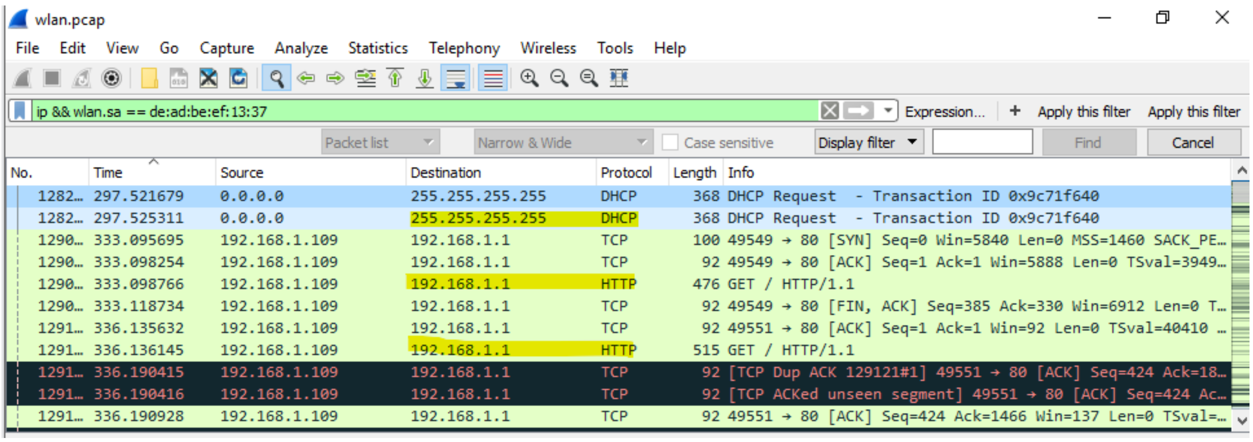
Deauths sent → reauthentication observed → encrypted traffic bursts



Wireshark -> Preferences -> Protocols -> IEEE 802.11 -> Decryption Keys ->Edit



Wireshark Command: ip && wlan.sa == de:ad:be:ef:13:37

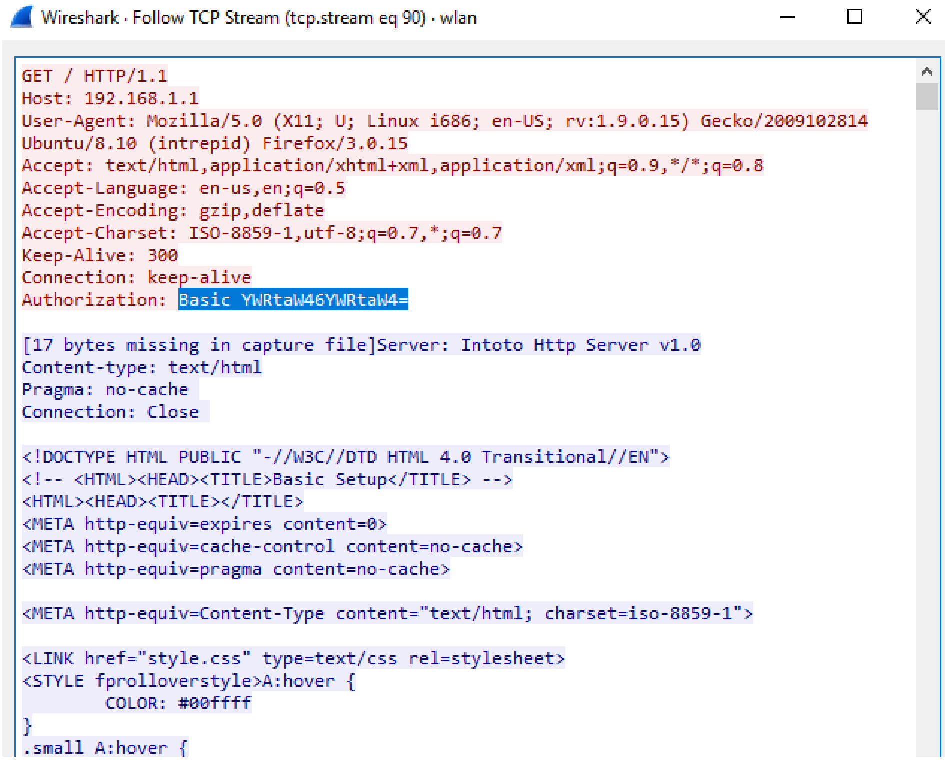


8. **Can you figure out what's going on explain it to Joe and track the attacker's activities in a timeline?**

An attacker connected to a wireless network named Ment0rNet (BSSID 00:23:69:61:00:d0) and began sending deauthentication frames to force legitimate users off the network. By doing so, the attacker could capture encrypted packets repeatedly and potentially execute a WEP cracking. Also, attacker took advantage of vulnerability of weak password and changed the password

One suspicious device (de:ad:be:ef:13:37) was observed generating these anomalies.

- Timeline: 297.521679 IP address was assigned to the malicious MAC address

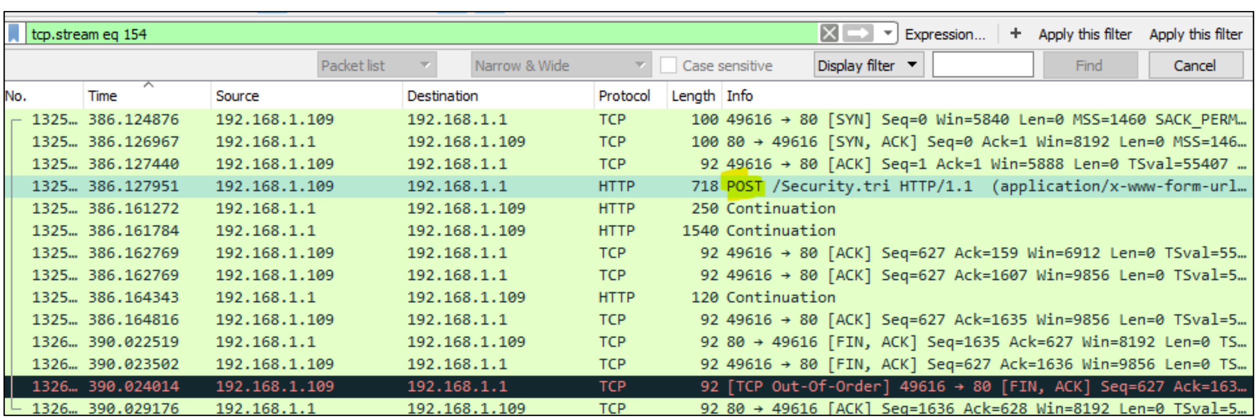


Wireshark · Follow TCP Stream (tcp.stream eq 90) · wlan

```
GET / HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.15) Gecko/2009102814
Ubuntu/8.10 (intrepid) Firefox/3.0.15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Authorization: Basic YWRtaW46YWRtaW4=

[17 bytes missing in capture file]Server: Intoto Http Server v1.0
Content-type: text/html
Pragma: no-cache
Connection: Close

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- <HTML><HEAD><TITLE>Basic Setup</TITLE> -->
<HTML><HEAD><TITLE></TITLE>
<META http-equiv=expires content=0>
<META http-equiv=cache-control content=no-cache>
<META http-equiv=pragma content=no-cache>

<META http-equiv=Content-Type content="text/html; charset=iso-8859-1">

<LINK href="style.css" type=text/css rel=stylesheet>
<STYLE fprolloverstyle>A:hover {
        COLOR: #00ffff
}
.small A:hover {
```

```php
echo base64_encode('admin:admin') // YWRtaW46YWRtaW4=
echo base64_decode('YWRtaW46YWRtaW4=') // admin:admin
```

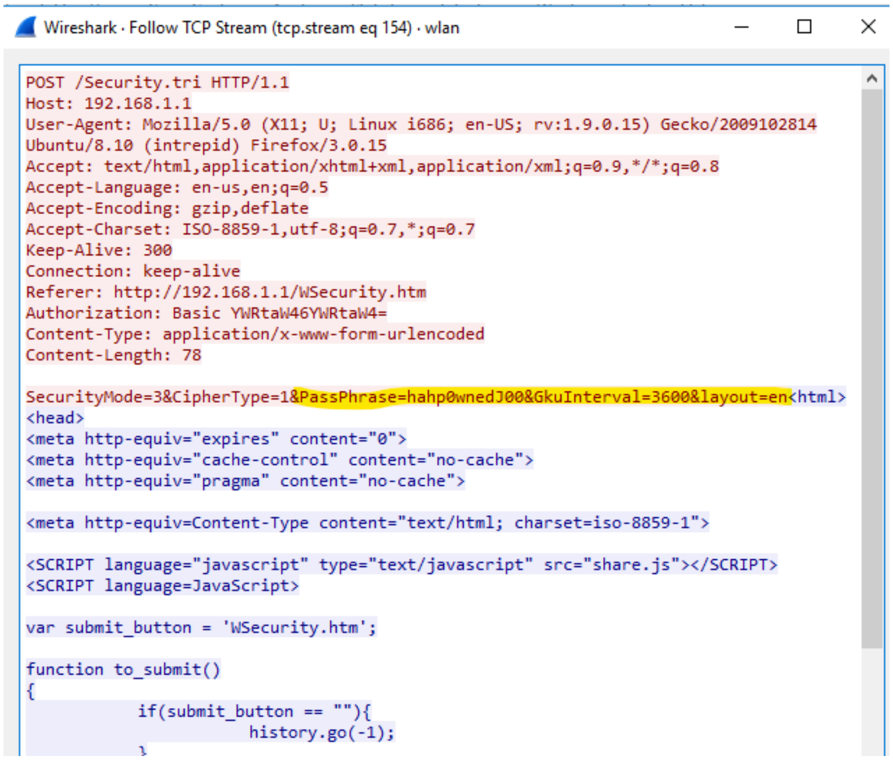
Tc



tcp.stream eq 154 | Expression… | + | Apply this filter | Apply this filter

Packet list | Narrow & Wide | Case sensitive | Display filter | Find | Cancel

No.	Time	Source	Destination	Protocol	Length	Info
1325…	386.124876	192.168.1.109	192.168.1.1	TCP	100	49616 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM…
1325…	386.126967	192.168.1.1	192.168.1.109	TCP	100	80 → 49616 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=146…
1325…	386.127440	192.168.1.109	192.168.1.1	TCP	92	49616 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=55407 …
1325…	386.127951	192.168.1.109	192.168.1.1	HTTP	718	POST /Security.tri HTTP/1.1 (application/x-www-form-url…
1325…	386.161272	192.168.1.1	192.168.1.109	HTTP	250	Continuation
1325…	386.161784	192.168.1.1	192.168.1.109	HTTP	1540	Continuation
1325…	386.162769	192.168.1.109	192.168.1.1	TCP	92	49616 → 80 [ACK] Seq=627 Ack=159 Win=6912 Len=0 TSval=55…
1325…	386.162769	192.168.1.109	192.168.1.1	TCP	92	49616 → 80 [ACK] Seq=627 Ack=1607 Win=9856 Len=0 TSval=5…
1325…	386.164343	192.168.1.1	192.168.1.109	HTTP	120	Continuation
1325…	386.164816	192.168.1.109	192.168.1.1	TCP	92	49616 → 80 [ACK] Seq=627 Ack=1635 Win=9856 Len=0 TSval=5…
1326…	390.022519	192.168.1.1	192.168.1.109	TCP	92	80 → 49616 [FIN, ACK] Seq=1635 Ack=627 Win=8192 Len=0 TS…
1326…	390.023502	192.168.1.109	192.168.1.1	TCP	92	49616 → 80 [FIN, ACK] Seq=627 Ack=1636 Win=9856 Len=0 TS…
1326…	390.024014	192.168.1.109	192.168.1.1	TCP	92	[TCP Out-Of-Order] 49616 → 80 [FIN, ACK] Seq=627 Ack=163…
1326…	390.029176	192.168.1.1	192.168.1.109	TCP	92	80 → 49616 [ACK] Seq=1636 Ack=628 Win=8192 Len=0 TSval=5…



Conclusion

Lab 8 provided practical experience in analyzing wireless traffic to detect potentially malicious activity within a network. Through the use of Wireshark, we identified critical components of wireless communications, such as BSSID, SSID, encryption indicators, and the behaviors of associated stations. The wireless capture revealed anomalous patterns consistent with a deauthentication-based attack. Additionally, the lab demonstrated how protected frames and management subtypes can expose unauthorized activity even when payloads are encrypted. This exercise reinforced key concepts in network forensics, including traffic pattern recognition, timeline reconstruction, and attacker attribution. The findings highlight the importance of proactive wireless monitoring and the value of packet-level inspection in identifying security threats.

Glossary

NetFlow: A protocol that collects and monitors metadata about IP traffic flows across network devices.

Metadata: Descriptive information about data traffic, including IP addresses, ports, and timestamps, but not the actual content.

Packet Payload: The portion of a packet that contains the actual data being transmitted.

Sampling: A technique where only a portion of network traffic is analyzed to reduce resource use, possibly missing some traffic.

Anomaly Detection: Identifying unusual network behavior that may signal a cyberattack or policy violation.

Packet Capture (PCAP): A file format used to store network traffic data captured from a network interface for forensic analysis.

Wireless Access Point (WAP): A network hardware device that allows wireless devices to connect to a wired network using Wi-Fi technology.

MAC Address: A unique hardware identifier assigned to network interfaces for communications on the physical network segment.

References

Cisco. (2020). *Introduction to NetFlow*. Cisco Systems. Retrieved from https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html

Cisco Systems. (n.d.). *802.11 Sniffer Capture Analysis: Management Frames and Open Authentication*. Cisco Community. Retrieved April 15, 2025, from https://community.cisco.com/t5/wireless-mobility-knowledge-base/802-11-sniffer-capture-analysis-management-frames-and-open-auth/ta-p/3120622

Flowmon. (2021). *Why NetFlow is crucial for network security monitoring*. Retrieved from https://www.flowmon.com/en/blog/netflow-crucial-for-network-security-monitoring

Infosec Institute. (2021, Jan 11). *PCAP analysis basics with Wireshark [updated 2021]*. https://www.infosecinstitute.com/resources/network-security-101/pcap-analysis-basics-with-wireshark/