NETFLOW AND WIRELESS PACKET CAPTURE ANALYSIS

Introduction

The new age of technology has led to the complexity of networks in today's world. This has aided the emergence of network monitoring approaches as the need to maintain the health of the network rises. Different approaches have been adopted to serve these purposes and can be classified as active or passive. This paper we delve into one of the basic protocols utilized for flow export of networks called NetFlow. It is vital to understand that a flow is defined as " a set of Internet Protocol packets passing an observation point in the network during a certain time interval, such that all packets belonging to a particular flow have a set of common properties" (Claise, B.Trammell, & P.Aitken, 2013).

NetFlow was developed by Cisco as their flow export technology and patented it back in 1996.This feature has been utilized to capture IP network traffic which can be analyzed based on common attributes such as source and destination addresses, port numbers, packet contents et cetera (Nevil, 2011).

NetFlow, just like any other feature has its cons and pros, though there are more benefits to be gained from using NetFlow. These benefits include easy network bandwidth and traffic monitoring, fast network troubleshooting which aids the improvement of user experience, gaining quick insights from bandwidth reports and finally network security reports that heighten cybersecurity protection. NetFlow shortcomings include the high usage of bandwidth that negatively impacts the device performance, forwarding results to a limited number of recipients which slows network management and troubleshooting and lastly NetFlow does not have the capacity to provide user identities e.g. login information after identifying a device (IBM, n.d.).

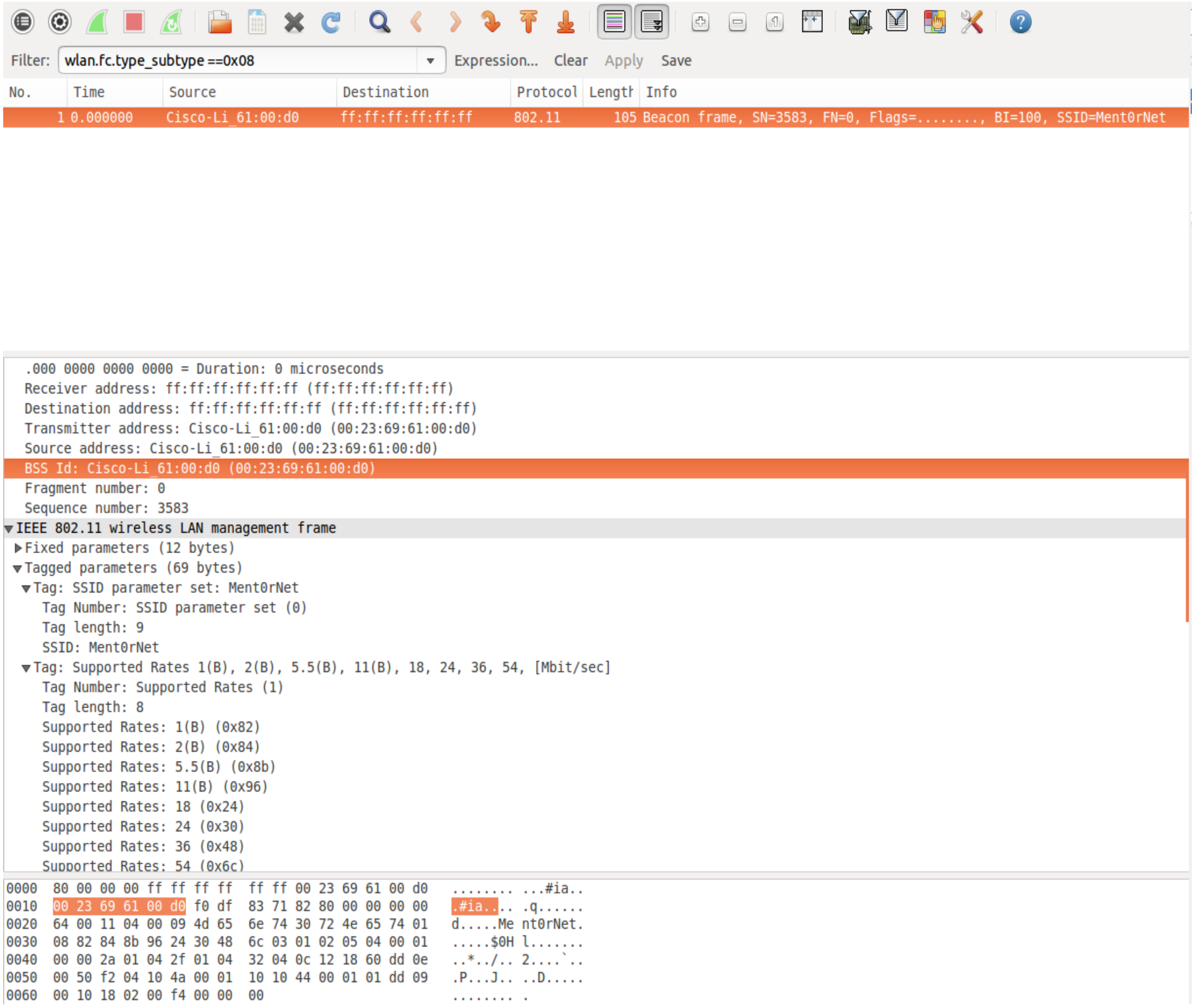
Wireless Packet Capture Analysis

This section involves the investigation of a packet capture file provided by Joe (a victim) that we will analysis and interpret to gain insights for any anomalies given the fact that Joe should be the one using his WAP (Wireless Access Point) where the packet file was derived from.

1.BSSID AND SSID

BSSID stands for basic service set identifier and it is the MAC (Media Access Control) physical address of a given access point or wireless router used for wi-fi connection (Atera, 2024). SSID on the other hand stands for service set identifier and this is the name used for a wireless network (Chris & Jordan, 2024).It is vital to note that SSID can be changed anytime unlike BSSID.

The figure below shows the BSSID as 00:23:69:00:d0 and the SSID as ment0rNet.



Filter: wlan.fc.type_subtype ==0x08

```
No.   Time       Source             Destination         Protocol  Length Info
    1 0.000000   Cisco-Li_61:00:d0  ff:ff:ff:ff:ff:ff   802.11       105 Beacon frame, SN=3583, FN=0, Flags=........, BI=100, SSID=Ment0rNet
```

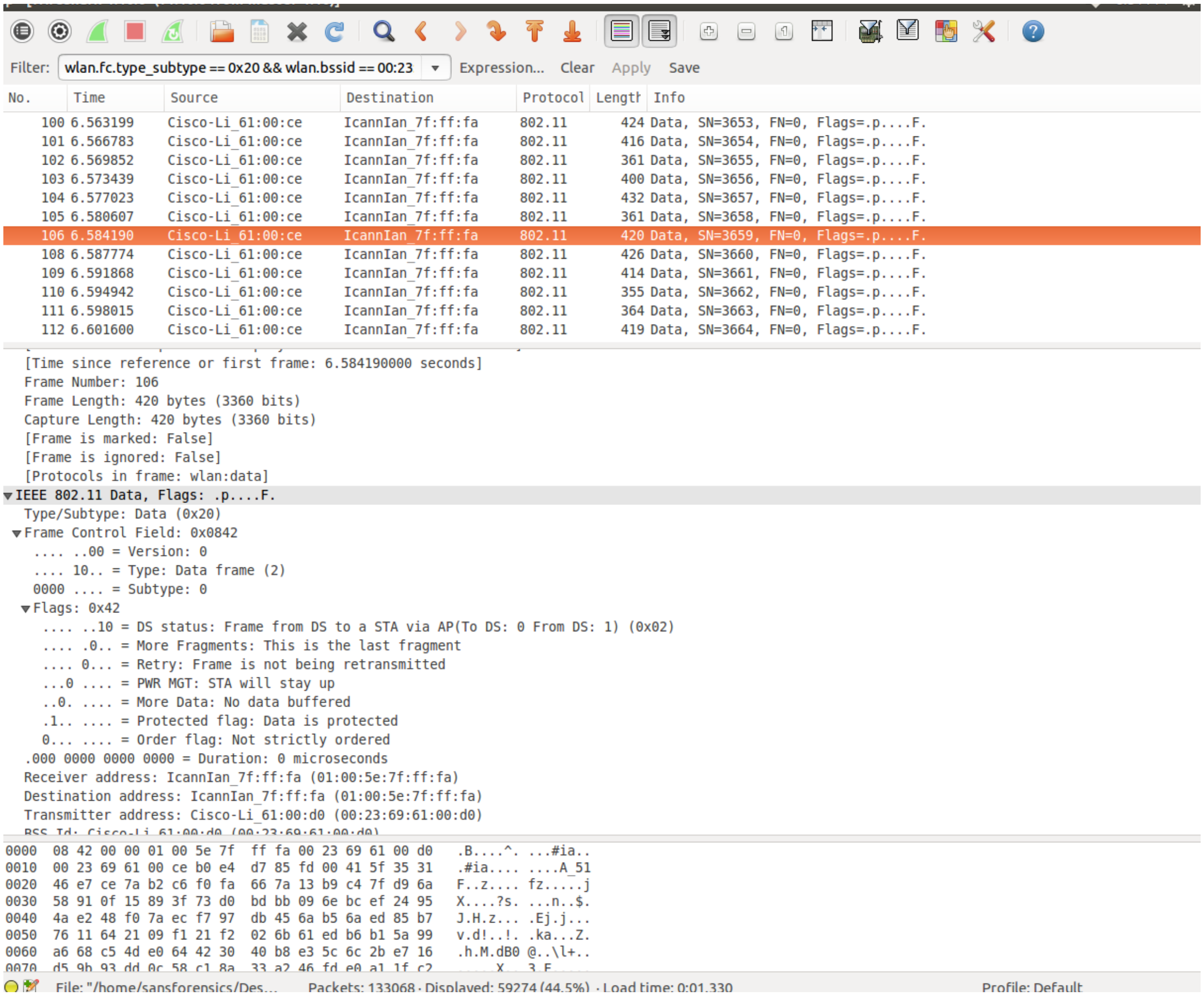
```
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
  Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
  Transmitter address: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)
  Source address: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)
  BSS Id: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)
  Fragment number: 0
  Sequence number: 3583
▼IEEE 802.11 wireless LAN management frame
 ▶Fixed parameters (12 bytes)
 ▼Tagged parameters (69 bytes)
  ▼Tag: SSID parameter set: Ment0rNet
     Tag Number: SSID parameter set (0)
     Tag length: 9
     SSID: Ment0rNet
  ▼Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
     Tag Number: Supported Rates (1)
     Tag length: 8
     Supported Rates: 1(B) (0x82)
     Supported Rates: 2(B) (0x84)
     Supported Rates: 5.5(B) (0x8b)
     Supported Rates: 11(B) (0x96)
     Supported Rates: 18 (0x24)
     Supported Rates: 24 (0x30)
     Supported Rates: 36 (0x48)
     Supported Rates: 54 (0x6c)
```

```
0000  80 00 00 00 ff ff ff ff  ff ff 00 23 69 61 00 d0   ........ ...#ia..
0010  00 23 69 61 00 d0 f0 df  83 71 82 80 00 00 00 00   .#ia.... .q......
0020  64 00 11 04 00 09 4d 65  6e 74 30 72 4e 65 74 01   d.....Me nt0rNet.
0030  08 82 84 8b 96 24 30 48  6c 03 01 02 05 04 00 01   .....$0H l.......
0040  00 00 2a 01 04 2f 01 04  32 04 0c 12 18 60 dd 0e   ..*../.. 2....`..
0050  00 50 f2 04 10 4a 00 01  10 10 44 00 01 01 dd 09   .P...J.. ..D.....
0060  00 10 18 02 00 f4 00 00  00                        ........ .
```

Figure 1/BSSID and SSID

2.WAP

In the section we investigate if the WAP above uses encryption which is evidence that it does have an encryption following the flags that have been shown in the screenshot below. The flag on data protection shows that there is protection, and it is indicated with a 1.



```
Filter: wlan.fc.type_subtype == 0x20 && wlan.bssid == 00:23

No.  Time       Source             Destination         Protocol Length Info
 100 6.563199   Cisco-Li_61:00:ce  IcannIan_7f:ff:fa   802.11      424 Data, SN=3653, FN=0, Flags=.p....F.
 101 6.566783   Cisco-Li_61:00:ce  IcannIan_7f:ff:fa   802.11      416 Data, SN=3654, FN=0, Flags=.p....F.
 102 6.569852   Cisco-Li_61:00:ce  IcannIan_7f:ff:fa   802.11      361 Data, SN=3655, FN=0, Flags=.p....F.
 103 6.573439   Cisco-Li_61:00:ce  IcannIan_7f:ff:fa   802.11      400 Data, SN=3656, FN=0, Flags=.p....F.
 104 6.577023   Cisco-Li_61:00:ce  IcannIan_7f:ff:fa   802.11      432 Data, SN=3657, FN=0, Flags=.p....F.
 105 6.580607   Cisco-Li_61:00:ce  IcannIan_7f:ff:fa   802.11      361 Data, SN=3658, FN=0, Flags=.p....F.
 106 6.584190   Cisco-Li_61:00:ce  IcannIan_7f:ff:fa   802.11      420 Data, SN=3659, FN=0, Flags=.p....F.
 108 6.587774   Cisco-Li_61:00:ce  IcannIan_7f:ff:fa   802.11      426 Data, SN=3660, FN=0, Flags=.p....F.
 109 6.591868   Cisco-Li_61:00:ce  IcannIan_7f:ff:fa   802.11      414 Data, SN=3661, FN=0, Flags=.p....F.
 110 6.594942   Cisco-Li_61:00:ce  IcannIan_7f:ff:fa   802.11      355 Data, SN=3662, FN=0, Flags=.p....F.
 111 6.598015   Cisco-Li_61:00:ce  IcannIan_7f:ff:fa   802.11      364 Data, SN=3663, FN=0, Flags=.p....F.
 112 6.601600   Cisco-Li_61:00:ce  IcannIan_7f:ff:fa   802.11      419 Data, SN=3664, FN=0, Flags=.p....F.
```

```
  [Time since reference or first frame: 6.584190000 seconds]
  Frame Number: 106
  Frame Length: 420 bytes (3360 bits)
  Capture Length: 420 bytes (3360 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: wlan:data]
▼IEEE 802.11 Data, Flags: .p....F.
  Type/Subtype: Data (0x20)
 ▼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) (0x02)
    .... .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: IcannIan_7f:ff:fa (01:00:5e:7f:ff:fa)
  Destination address: IcannIan_7f:ff:fa (01:00:5e:7f:ff:fa)
  Transmitter address: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)
  BSS Id: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)
```

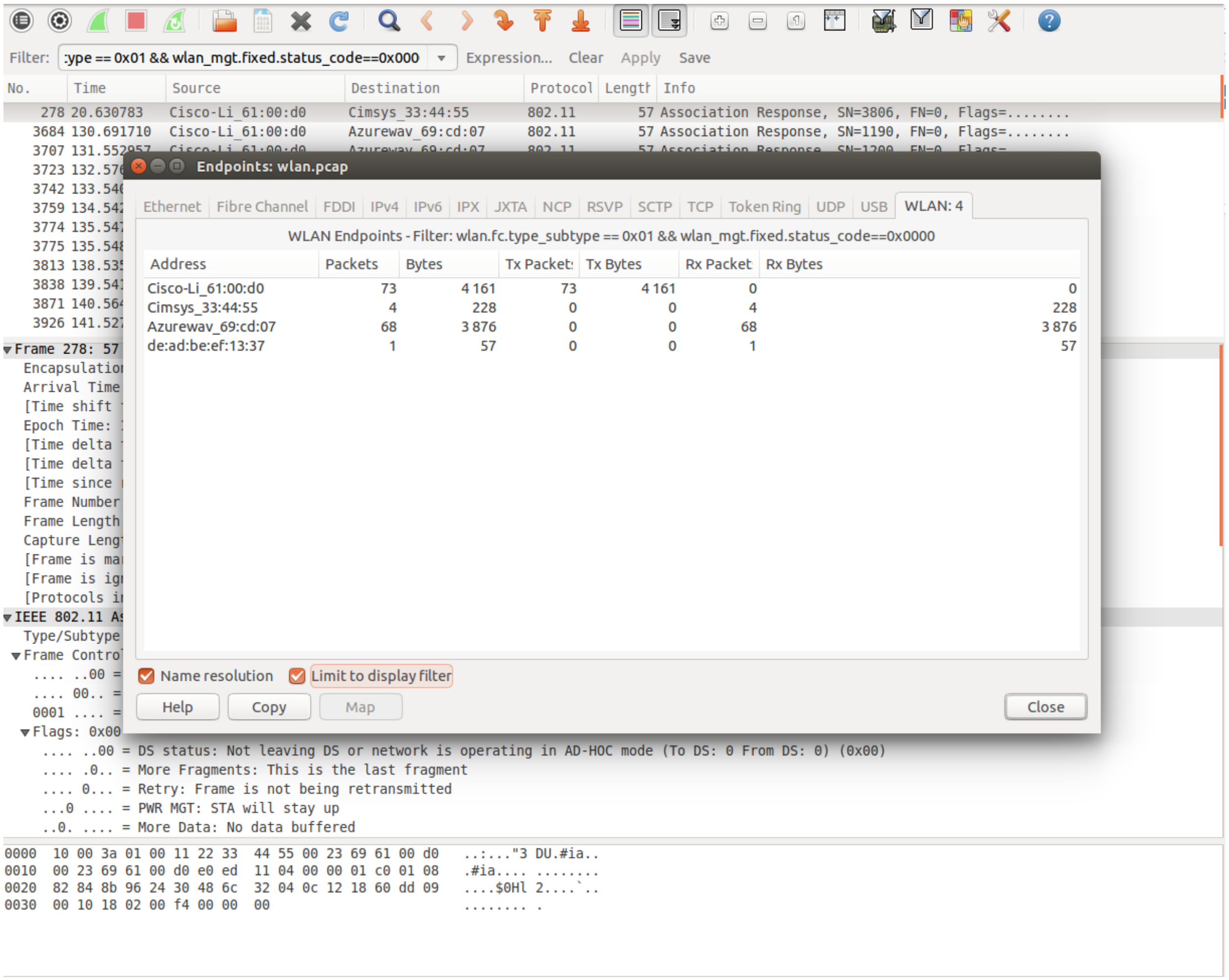
```
0000  08 42 00 00 01 00 5e 7f  ff fa 00 23 69 61 00 d0   .B....^. ...#ia..
0010  00 23 69 61 00 ce b0 e4  d7 85 fd 00 41 5f 35 31   .#ia.... ....A_51
0020  46 e7 ce 7a b2 c6 f0 fa  66 7a 13 b9 c4 7f d9 6a   F..z.... fz.....j
0030  58 91 0f 15 89 3f 73 d0  bd bb 09 6e bc ef 24 95   X....?s. ...n..$.
0040  4a e2 48 f0 7a ec f7 97  db 45 6a b5 6a ed 85 b7   J.H.z... .Ej.j...
0050  76 11 64 21 09 f1 21 f2  02 6b 61 ed b6 b1 5a 99   v.d!..!. .ka...Z.
0060  a6 68 c5 4d e0 64 42 30  40 b8 e3 5c 6c 2b e7 16   .h.M.dB0 @..\l+..
0070  d5 9b 93 dd 0c 58 c1 8a  33 a2 46 fd e0 a1 1f c2   .....X.. 3.F.....
```

File: "/home/sansforensics/Des... Packets: 133068 · Displayed: 59274 (44.5%) · Load time: 0:01.330 Profile: Default

Figure 2/Wap encryption

3.Stations

The stations which can be termed as the devices that were associated with our WAP above were listed in the screenshot below as we filtered for only the endpoints that had connected to the access point. The screenshot below shows also the number of packets that were sent and received.



```
No.   Time         Source             Destination        Protocol Lengtł Info
  278 20.630783    Cisco-Li_61:00:d0  Cimsys_33:44:55    802.11       57 Association Response, SN=3806, FN=0, Flags=........
 3684 130.691710   Cisco-Li_61:00:d0  Azurewav_69:cd:07  802.11       57 Association Response, SN=1190, FN=0, Flags=........
 3707 131.552957   Cisco-Li_61:00:d0  Azurewav_69:cd:07  802.11       57 Association Response, SN=1200, FN=0, Flags=
 3723 132.576
 3742 133.546
 3759 134.542
 3774 135.547
 3775 135.548
 3813 138.535
 3838 139.541
 3871 140.564
 3926 141.527
```

WLAN Endpoints - Filter: wlan.fc.type_subtype == 0x01 && wlan_mgt.fixed.status_code==0x0000

Address	Packets	Bytes	Tx Packet:	Tx Bytes	Rx Packet	Rx Bytes
Cisco-Li_61:00:d0	73	4 161	73	4 161	0	0
Cimsys_33:44:55	4	228	0	0	4	228
Azurewav_69:cd:07	68	3 876	0	0	68	3 876
de:ad:be:ef:13:37	1	57	0	0	1	57

☑ Name resolution ☑ Limit to display filter

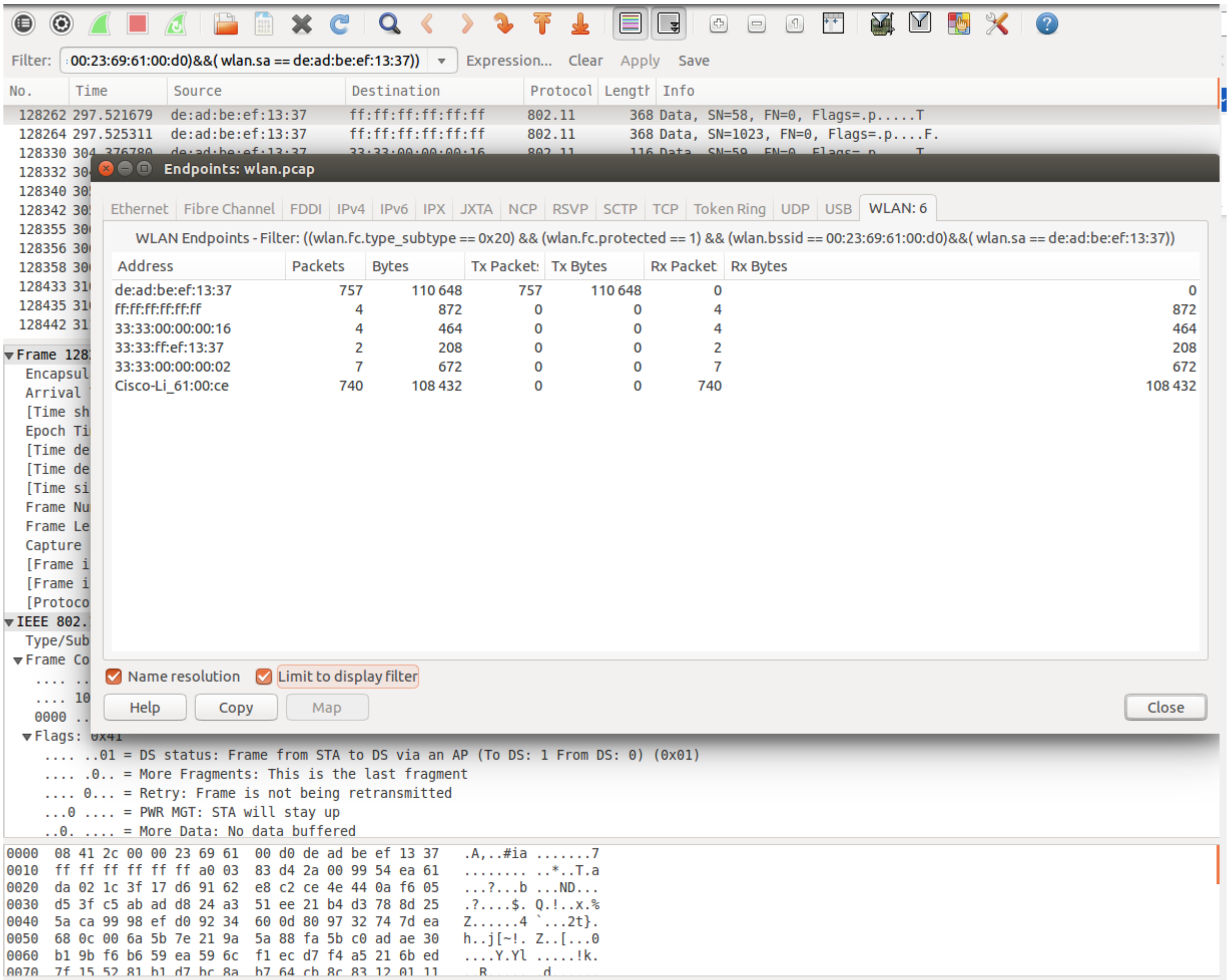
```
▼Frame 278: 57
  Encapsulatio
  Arrival Time
  [Time shift
  Epoch Time:
  [Time delta
  [Time delta
  [Time since
  Frame Number
  Frame Length
  Capture Leng
  [Frame is ma
  [Frame is ig
  [Protocols i
▼IEEE 802.11 A
  Type/Subtype
 ▼Frame Contro
    .... ..00 =
    .... 00.. =
    0001 .... =
  ▼Flags: 0x00
     .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
     .... .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
```

```
0000  10 00 3a 01 00 11 22 33  44 55 00 23 69 61 00 d0   ..:..."3 DU.#ia..
0010  00 23 69 61 00 d0 e0 ed  11 04 00 00 01 c0 01 08   .#ia.... ........
0020  82 84 8b 96 24 30 48 6c  32 04 0c 12 18 60 dd 09   ....$0Hl 2....`..
0030  00 10 18 02 00 f4 00 00  00                        ........ .
```

Figure 3/Stations

4.Patterns

The patterns that seemed to be anomalous simply mean that some endpoints generated suspicious traffic unlike the expected traffic from Joe. The screenshot below shows that there was abnormal traffic from one of the stations that was flagged.



```
Filter: 00:23:69:61:00:d0)&&( wlan.sa == de:ad:be:ef:13:37))

No.    Time       Source             Destination        Protocol Length Info
128262 297.521679 de:ad:be:ef:13:37  ff:ff:ff:ff:ff:ff  802.11      368 Data, SN=58, FN=0, Flags=.p.....T
128264 297.525311 de:ad:be:ef:13:37  ff:ff:ff:ff:ff:ff  802.11      368 Data, SN=1023, FN=0, Flags=.p....F.
128330 304.376780 de:ad:be:ef:13:37  33:33:00:00:00:16  802.11      116 Data, SN=59, FN=0, Flags=.p.....T
128332 30
128340 30
128342 30
128355 30
128356 30
128358 30
128433 31
128435 31
128442 31
```

Endpoints: wlan.pcap

WLAN Endpoints - Filter: ((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))

Address	Packets	Bytes	Tx Packet:	Tx Bytes	Rx Packet	Rx Bytes
de:ad:be:ef:13:37	757	110 648	757	110 648	0	0
ff:ff:ff:ff:ff:ff	4	872	0	0	4	872
33:33:00:00:00:16	4	464	0	0	4	464
33:33:ff:ef:13:37	2	208	0	0	2	208
33:33:00:00:00:02	7	672	0	0	7	672
Cisco-Li_61:00:ce	740	108 432	0	0	740	108 432

☑ Name resolution ☑ Limit to display filter

```
▼Frame 128
   Encapsul
   Arrival
   [Time sh
   Epoch Ti
   [Time de
   [Time de
   [Time si
   Frame Nu
   Frame Le
   Capture
   [Frame i
   [Frame i
   [Protoco
▼IEEE 802.
   Type/Sub
 ▼Frame Co
    .... ..
    .... 10
    0000 ..
  ▼Flags: 0x41
     .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x01)
     .... .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
```

```
0000  08 41 2c 00 00 23 69 61  00 d0 de ad be ef 13 37   .A,..#ia .......7
0010  ff ff ff ff ff ff a0 03  83 d4 2a 00 99 54 ea 61   ........ ..*..T.a
0020  da 02 1c 3f 17 d6 91 62  e8 c2 ce 4e 44 0a f6 05   ...?...b ...ND...
0030  d5 3f c5 ab ad d8 24 a3  51 ee 21 b4 d3 78 8d 25   .?....$. Q.!..x.%
0040  5a ca 99 98 ef d0 92 34  60 0d 80 97 32 74 7d ea   Z......4 `...2t}.
0050  68 0c 00 6a 5b 7e 21 9a  5a 88 fa 5b c0 ad ae 30   h..j[~!. Z..[...0
0060  b1 9b f6 b6 59 ea 59 6c  f1 ec d7 f4 a5 21 6b ed   ....Y.Yl .....!k.
0070  7f 15 52 81 b1 d7 bc 8a  b7 64 cb 8c 83 12 01 11   ..R..... .d......
```

Figure 4/Patterns

5.Anomality

The stations identified to have anomalous traffic above can be categorized under the types of attacks described below:

5.1 WEP cracking attack

This is an attack that is used to exploit the vulnerabilities of the wired equivalent privacy protocol. This was successful since WEP was an early encryption method used for wireless networks security where over the years methods have been invented to crack it (NordVPN, n.d.).

5.2 ARP replay attack

This attack occurs when a hacker listens to network traffic to intercept an ARP request, then inserts a spoofed ARP reply before the legitimate device can respond. The reply contains the hackers MAC address instead of the intended device’s MAC address. Then the hacker can obtain data belonging to the legitimate user (s3CloudHub, 2024).

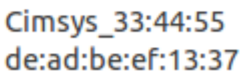
5.3 Denial of Service

This “attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor” (CISA, 2021).This is achieved by flooding the targeted host with traffic to a point that the device cannot handle the request and therefore crashes causing services to be inaccessible.

In conclusion the three attacks explained all took part in this investigation since the WAP had a WEP encryption which was possibly cracked and then ARP replies were transmitted using the Cimsys hence the denial of service where the traffic was overwhelmed and Joe was not able to reach his Wi-Fi services.

6.Stations

The stations that have displayed consistent anomalies and are suspicious are shown on the screenshot below.

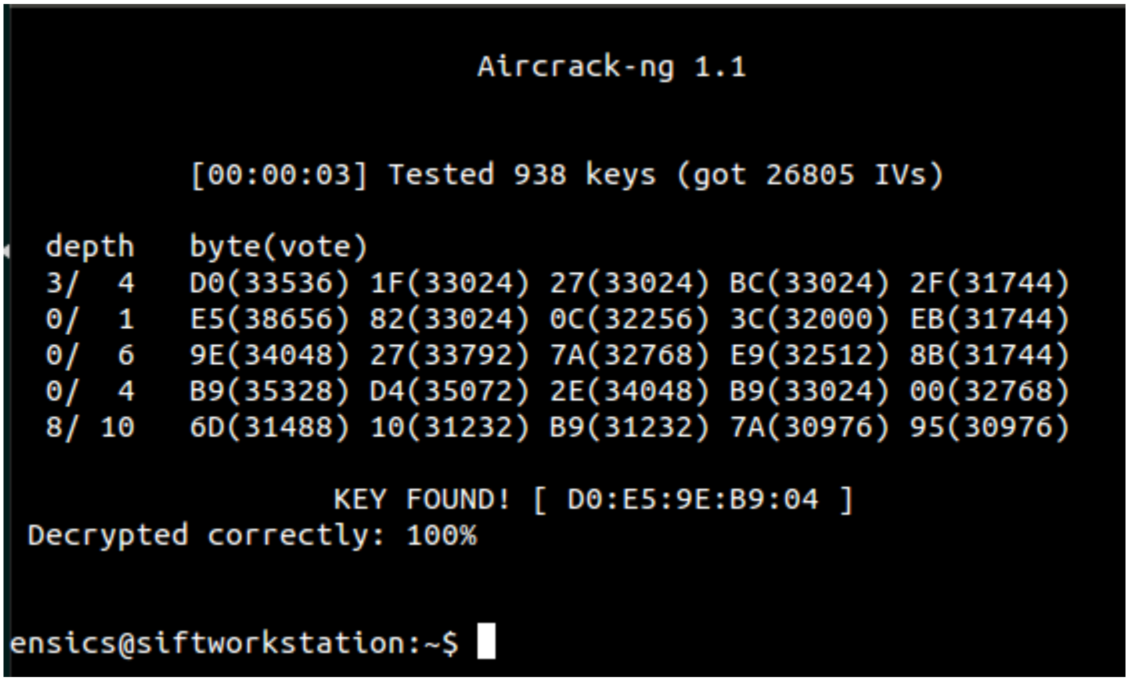


```
Cimsys_33:44:55
de:ad:be:ef:13:37
```

Figure 5/Stations

7.Unknown

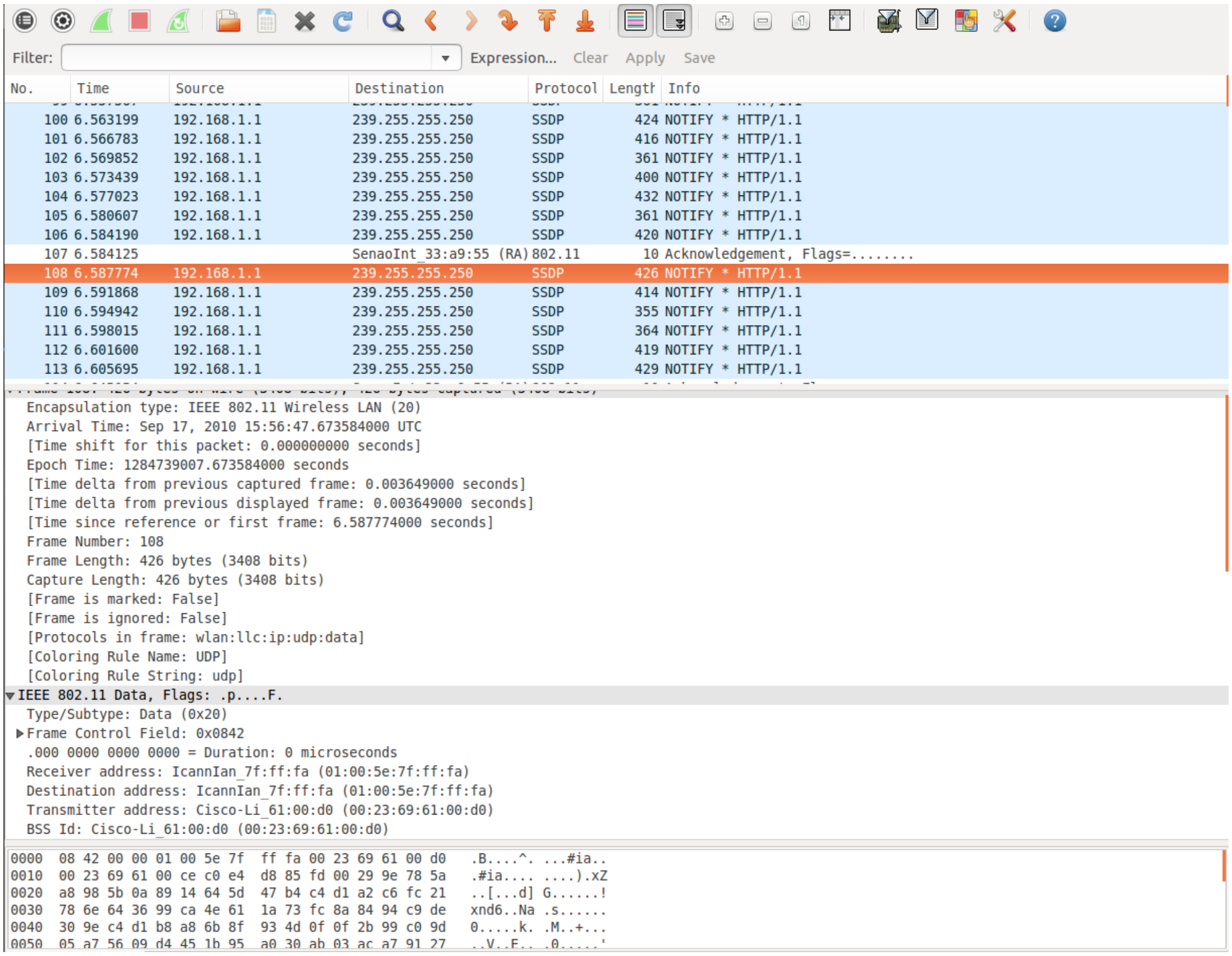
We cracked the WEP key using Aircrack-ng where we obtained the key that we used to discover the WEP key as shown in the figure below.



```
                           Aircrack-ng 1.1


          [00:00:03] Tested 938 keys (got 26805 IVs)

  depth   byte(vote)
  3/  4   D0(33536) 1F(33024) 27(33024) BC(33024) 2F(31744)
  0/  1   E5(38656) 82(33024) 0C(32256) 3C(32000) EB(31744)
  0/  6   9E(34048) 27(33792) 7A(32768) E9(32512) 8B(31744)
  0/  4   B9(35328) D4(35072) 2E(34048) B9(33024) 00(32768)
  8/ 10   6D(31488) 10(31232) B9(31232) 7A(30976) 95(30976)

                  KEY FOUND! [ D0:E5:9E:B9:04 ]
 Decrypted correctly: 100%


ensics@siftworkstation:~$ 
```

Figure 6/WEP key

Then we applied to decrypt the pcap file which displayed the unknown endpoint IcannIan_7f:ff:fa (01:00:5e:7f:ff:fa) that was used to retransmit and authentication.



```
No.   Time      Source         Destination             Protocol Length Info
  100 6.563199  192.168.1.1    239.255.255.250         SSDP      424 NOTIFY * HTTP/1.1
  101 6.566783  192.168.1.1    239.255.255.250         SSDP      416 NOTIFY * HTTP/1.1
  102 6.569852  192.168.1.1    239.255.255.250         SSDP      361 NOTIFY * HTTP/1.1
  103 6.573439  192.168.1.1    239.255.255.250         SSDP      400 NOTIFY * HTTP/1.1
  104 6.577023  192.168.1.1    239.255.255.250         SSDP      432 NOTIFY * HTTP/1.1
  105 6.580607  192.168.1.1    239.255.255.250         SSDP      361 NOTIFY * HTTP/1.1
  106 6.584190  192.168.1.1    239.255.255.250         SSDP      420 NOTIFY * HTTP/1.1
  107 6.584125                 SenaoInt_33:a9:55 (RA) 802.11     10 Acknowledgement, Flags=........
  108 6.587774  192.168.1.1    239.255.255.250         SSDP      426 NOTIFY * HTTP/1.1
  109 6.591868  192.168.1.1    239.255.255.250         SSDP      414 NOTIFY * HTTP/1.1
  110 6.594942  192.168.1.1    239.255.255.250         SSDP      355 NOTIFY * HTTP/1.1
  111 6.598015  192.168.1.1    239.255.255.250         SSDP      364 NOTIFY * HTTP/1.1
  112 6.601600  192.168.1.1    239.255.255.250         SSDP      419 NOTIFY * HTTP/1.1
  113 6.605695  192.168.1.1    239.255.255.250         SSDP      429 NOTIFY * HTTP/1.1
```

```
  Encapsulation type: IEEE 802.11 Wireless LAN (20)
  Arrival Time: Sep 17, 2010 15:56:47.673584000 UTC
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1284739007.673584000 seconds
  [Time delta from previous captured frame: 0.003649000 seconds]
  [Time delta from previous displayed frame: 0.003649000 seconds]
  [Time since reference or first frame: 6.587774000 seconds]
  Frame Number: 108
  Frame Length: 426 bytes (3408 bits)
  Capture Length: 426 bytes (3408 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: wlan:llc:ip:udp:data]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
▼IEEE 802.11 Data, Flags: .p....F.
  Type/Subtype: Data (0x20)
 ▶Frame Control Field: 0x0842
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: IcannIan_7f:ff:fa (01:00:5e:7f:ff:fa)
  Destination address: IcannIan_7f:ff:fa (01:00:5e:7f:ff:fa)
  Transmitter address: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)
  BSS Id: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)
```

```
0000  08 42 00 00 01 00 5e 7f  ff fa 00 23 69 61 00 d0   .B....^. ...#ia..
0010  00 23 69 61 00 ce c0 e4  d8 85 fd 00 29 9e 78 5a   .#ia.... ....).xZ
0020  a8 98 5b 0a 89 14 64 5d  47 b4 c4 d1 a2 c6 fc 21   ..[...d] G......!
0030  78 6e 64 36 99 ca 4e 61  1a 73 fc 8a 84 94 c9 de   xnd6..Na .s......
0040  30 9e c4 d1 b8 a8 6b 8f  93 4d 0f 0f 2b 99 c0 9d   0.....k. .M..+...
0050  05 a7 56 09 d4 45 1b 95  a0 30 ab 03 ac a7 91 27   ..V..E.. .0.....'
```

Figure 7/unknown

8.Conclusion

Joe’s wireless access point issues started when a WEP key was cracked, and the attacker used a transmitter to disrupt the ARP replies that were directed to the attacker’s device that were intended to be Joe’s. This is when Joe realized that he was getting dropped since his device wasn’t receiving any replies from his WAP. The attacker was able to pick up an IP address and could authenticate the devices since Joe was completely locked out after the transmission was successful.

Glossary

ARP – Stands for Address Resolution Protocol which connects an ever-changing internet protocol address to a specific Media Access Control (MAC) address in a local area network (LAN) (Fortinet, 2024).

WAP – Stands for Wireless Access Point which is a networking hardware device that allows other WIFI devices to connect to a wired network (Chris, 2016).

WLAN – stands for wireless local area network which is a group of computers or network devices that are collocated and form a network based on radio transmissions rather than wired connections (Bradley, 2024).

References

Atera. (2024, August 18). *Atera Group*. Retrieved from computer terms unwrapped: what is BSSID?: https://www.atera.com/blog/computer-terms-unwrapped-what-is-bssid/

Bradley, M. (2024, september 16). *What is WLAN(Wireless LAN)*. Retrieved from Lifewire tech for humans: https://www.lifewire.com/wlan-816565

Chris, H. (2016, september 22). *whats-the-difference-between-ad-hoc-and-infrastructure-mode*. Retrieved from How-To-Geek: https://www.howtogeek.com/180649/htg-explains-whats-the-difference-between-ad-hoc-and-infrastructure-mode/

Chris, H., & Jordan, G. (2024, September 13). *What is an SSID?* Retrieved from How-To-Geek: https://www.howtogeek.com/334935/what-is-an-ssid-or-service-set-identifier/

CISA. (2021, February 2021). *Understanding Denial-of-Service Attacks*. Retrieved from America's Cyber Defense Agency: https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

Claise, B., B.Trammell, & P.Aitken. (2013). Specification of the IP Flow Information Export(IPFIX) Protocol for the Exchange of Flow Information. *RFC 7011 (Internet Standard) Internet Engineering Task Force(IEFT)*.

Fortinet. (2024). *What is Address Resolution Protocol(ARP)?* Retrieved from Fortinet: https://www.fortinet.com/resources/cyberglossary/what-is-arp

IBM. (n.d.). *What is NetFlow?* Retrieved from IBM: https://www.ibm.com/topics/netflow

Nevil, B. (2011). Flow-based measurement: IPFIX development and deployment . *IEICE Trans communication vol 94*, 2190-2198.

NordVPN. (n.d.). *WEP crack*. Retrieved from NordVPN: https://nordvpn.com/cybersecurity/glossary/wep-crack/?msockid=0a985238a4ff638024ce461fa584626e

s3CloudHub. (2024, October 18). *ARP Request & Replay Attack:How Hackers Hijack Networks*. Retrieved from DEV: https://dev.to/s3cloudhub/arp-request-replay-attack-how-hackers-hijack-networks-6bd