Case Name: WK2

[redacted]

Examiner Name: Candace [redacted]

Table of Contents

List of Illustrative Materials

Tables

Figures

Executive Summary

Background

A systems administrator at HackMe, Inc. recently captured some suspicious traffic on his small company's wireless network before losing administrative access. As Inter0ptic is known to be in the area, the capture has become a potential lead in law enforcement's search for his whereabouts.

Request

The examiner was requested to analyze the contents of the packet capture to determine a possible connection between Inter0ptic's activities and the HackMe, Inc wireless access point. The following questions should be addressed:

- What are the BSSID and SSID of the WAP of interest?
- Is the WAP of interest using encryption?
- What stations are interacting with the WAP and/or other stations on the WLAN?
- Are there patterns of activity that seem anomalous?
- How are they anomalous: Consistent with malfunction? Consistent with maliciousness?
- Can we identify any potentially bad actors?
- Can we determine if a bad actor successfully executed an attack?

Findings

The BSSID and SSID of the WAP were 00:23:69:61:00:d0 and Ment0rNet, respectively. The WAP was using encryption on every packet. Three stations were communicating with the WAP: 00:11:22:33:44:55 (Joe), unknown station 1c:4b:d6:69:cd:07, and de:ad:be:ef:13:37. Several anomalous patterns were discovered. Most notable was a flood of data frames coming from station 1c:4b:d6:69:cd:07 that coincided with a spike in unique IVs being sent from the WAP, indicative of a WEP password cracking attempt. The successful association of station de:ad:be:ef:13:37 afterwards indicates the attack was successful. Both unknown stations should be considered bad actors.

Evidence

Table 1 outlines the evidence items of this case.

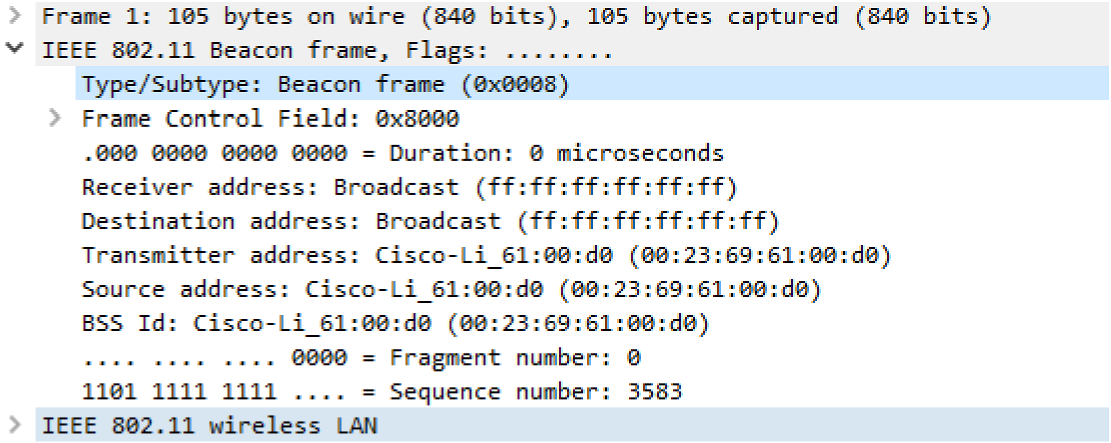
Description	Designation	Filename	MD5 Hash
Evidence Provided	Preservation Copy	Ch6-Wireless.zip	2E5E96A1D795C10597D0CB21B730487C
Evidence Created	Working Copy	Ch6-WirelessXX	2E5E96A1D795C10597D0CB21B730487C

Evidence Examined	Working Copy	Ch6-WirelessXX	2E5E96A1D795C10597D0CB21B730487C

Table 1: Case Evidence Items

Analysis

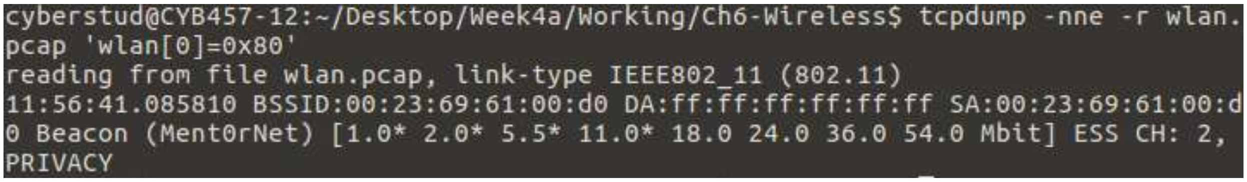
Examiner started Wireshark and opened the packet capture file *wlan.pcap*, then applied display filter “wlan.fc.type_subtype==0x08”. One frame was displayed, as shown in figure 1, indicating that this WAP was not configured to not send beacon frames. The BSSID in the frame (00:23:69:61:00:d0) is that of the wireless access point.



```
> Frame 1: 105 bytes on wire (840 bits), 105 bytes captured (840 bits)
v IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .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: 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 = Fragment number: 0
    1101 1111 1111 .... = Sequence number: 3583
> IEEE 802.11 wireless LAN
```

Figure 1: Beacon frame viewed in Wireshark

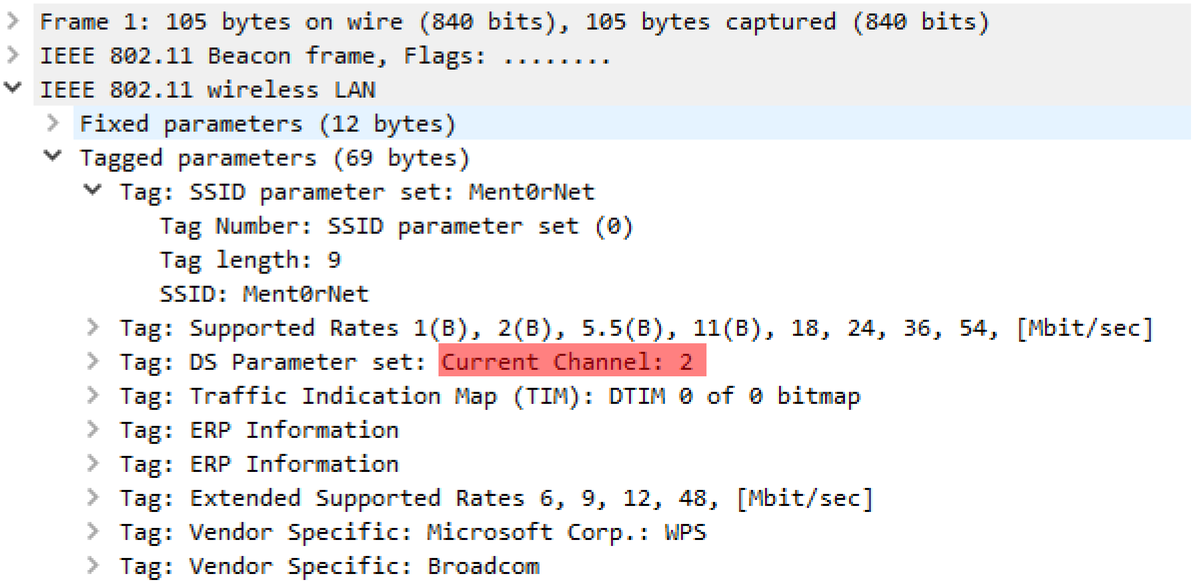
Examiner entered command “tcpdump -nne -r wlan.pcap ‘wlan[0]=0x80’” in a terminal in the *Desktop/Week4a/Working/Ch6-Wireless* directory. The output revealed similar information to that of Wireshark, as seen in figure 2, with additional information such as the SSID Ment0rnet.



```
cyberstud@CYB457-12:~/Desktop/Week4a/Working/Ch6-Wireless$ tcpdump -nne -r wlan.
pcap 'wlan[0]=0x80'
reading from file wlan.pcap, link-type IEEE802_11 (802.11)
11:56:41.085810 BSSID:00:23:69:61:00:d0 DA:ff:ff:ff:ff:ff:ff SA:00:23:69:61:00:d
0 Beacon (Ment0rNet) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] ESS CH: 2,
PRIVACY
```

Figure 2: Beacon frame viewed in tcpdump

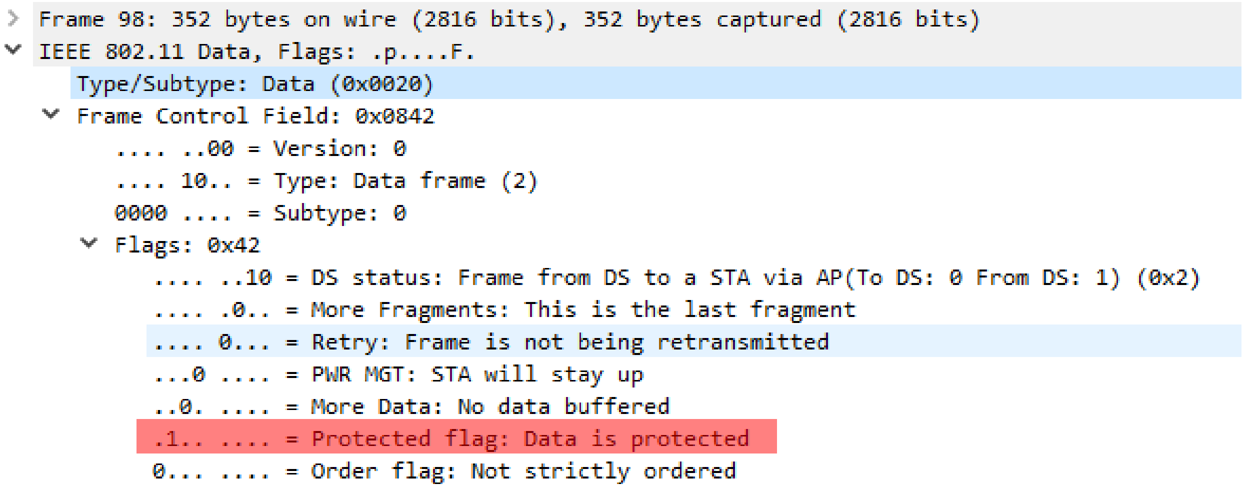
Examiner returned to Wireshark to view additional details provided by the beacon frame: the WAP was operating on channel 2 (see figure 3).



```
> Frame 1: 105 bytes on wire (840 bits), 105 bytes captured (840 bits)
> IEEE 802.11 Beacon frame, Flags: ........
v IEEE 802.11 wireless LAN
  > Fixed parameters (12 bytes)
  v Tagged parameters (69 bytes)
    v 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: DS Parameter set: Current Channel: 2
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    > Tag: ERP Information
    > Tag: ERP Information
    > Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    > Tag: Vendor Specific: Microsoft Corp.: WPS
    > Tag: Vendor Specific: Broadcom
```

Figure 3: WAP operating channel

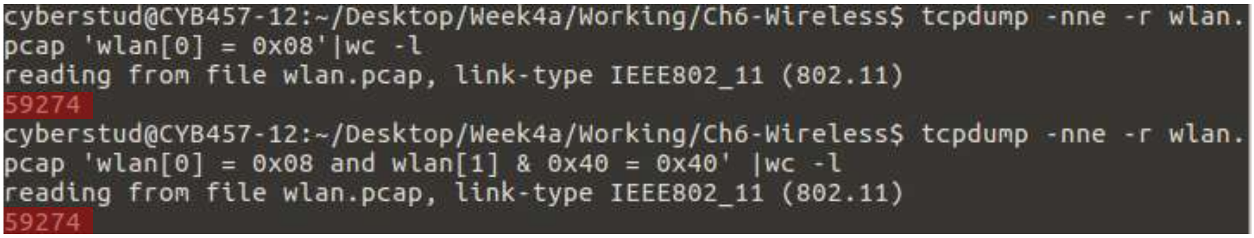
Examiner entered display filter “wlan.fc.type_subtype==0x20” in Wireshark to view data frames, then expanded the details of frame 98. Figure 4 shows that the data of this packet is protected (see figure 4).



```
> Frame 98: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits)
v IEEE 802.11 Data, Flags: .p....F.
    Type/Subtype: Data (0x0020)
  v Frame Control Field: 0x0842
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0000 .... = Subtype: 0
    v Flags: 0x42
        .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
        .... .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
```

Figure 4: Frame viewed is encrypted

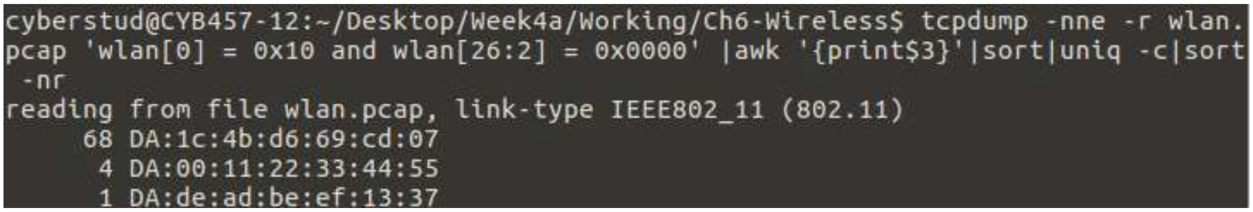
Examiner entered command “tcpdump -nne -r wlan.pcap ‘wlan[0] = 0x08’|wc -l” in a terminal in the *Desktop/Week4a/Working/Ch6-Wireless* directory to count all data frames in the capture. Then command “tcpdump -nne -r wlan.pcap ‘wlan[0] = 0x08 and wlan[1] & 0x40 = 0x40’ | wc -l” was entered to count all of the encrypted data frames. The number of frames (as seen in figure 5) were the same, meaning all data frames in the capture were encrypted.



```
cyberstud@CYB457-12:~/Desktop/Week4a/Working/Ch6-Wireless$ tcpdump -nne -r wlan.
pcap 'wlan[0] = 0x08'|wc -l
reading from file wlan.pcap, link-type IEEE802_11 (802.11)
59274
cyberstud@CYB457-12:~/Desktop/Week4a/Working/Ch6-Wireless$ tcpdump -nne -r wlan.
pcap 'wlan[0] = 0x08 and wlan[1] & 0x40 = 0x40' |wc -l
reading from file wlan.pcap, link-type IEEE802_11 (802.11)
59274
```

Figure 5: Number of data frames and number of encrypted data frames

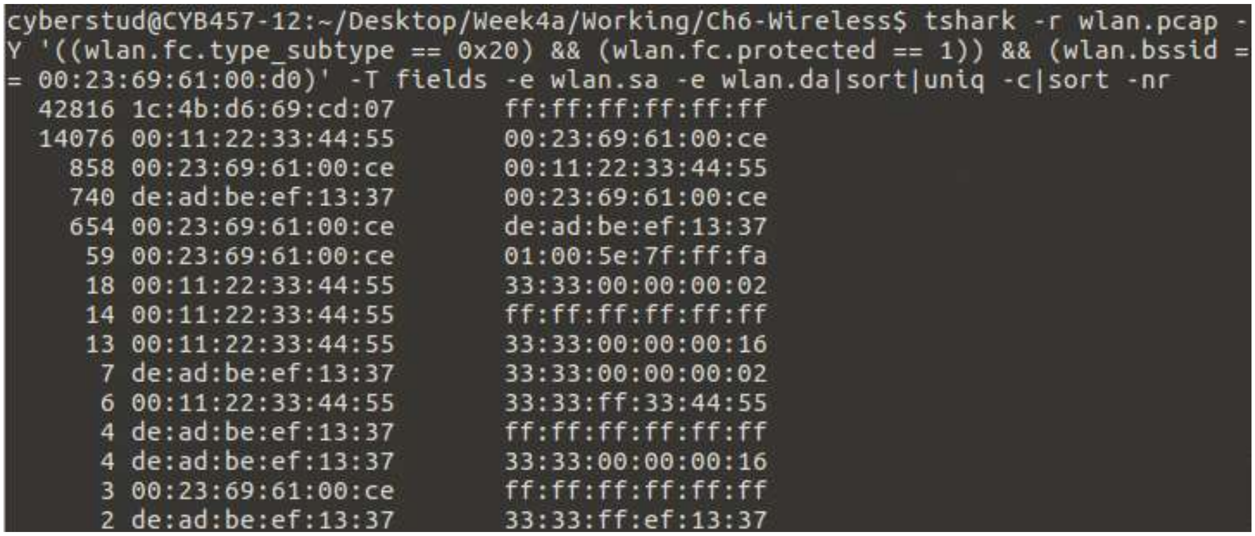
Examiner entered command "tcpdump -nne -r wlan.pcap 'wlan[0] = 0x10 and wlan[26:2] = 0x0000' | awk '{print $3}'|sort|uniq -c|sort -nr" in terminal to show stations that successfully connected with the wireless access point. Joe, the systems administrator of the wireless access point's mac address is 00:11:22:33:44:55, so these results indicated he connected four times during this capture (shown in figure 6). The results also indicate that unknown station de:ad:be:ef:13:37 successfully associated once, and another unknown station 1c:4b:d6:69:cd:07 successfully associated 68 times.



```
cyberstud@CYB457-12:~/Desktop/Week4a/Working/Ch6-Wireless$ tcpdump -nne -r wlan.
pcap 'wlan[0] = 0x10 and wlan[26:2] = 0x0000' |awk '{print$3}'|sort|uniq -c|sort
 -nr
reading from file wlan.pcap, link-type IEEE802_11 (802.11)
     68 DA:1c:4b:d6:69:cd:07
      4 DA:00:11:22:33:44:55
      1 DA:de:ad:be:ef:13:37
```

Figure 6: Successful associations to the WAP

To view the number of encrypted data frames transmitted from each of these stations to specific addresses, examiner entered command "tshark -r wlan.pcap -Y '((wlan.fc.type_subtype == 0x20) && (wlan.fc.protected == 1)) && (wlan.bssid == 00:23:69:61:00:d0)' -T fields -e wlan.sa -e wlan.da|sort|uniq -c|sort -nr" in terminal. Figure 7 shows the output. The number of frames sent by unknown station 1c:4b:d6:69:cd:07 to broadcast address ff:ff:ff:ff:ff:ff suggests some type of WEP-cracking attack took place.

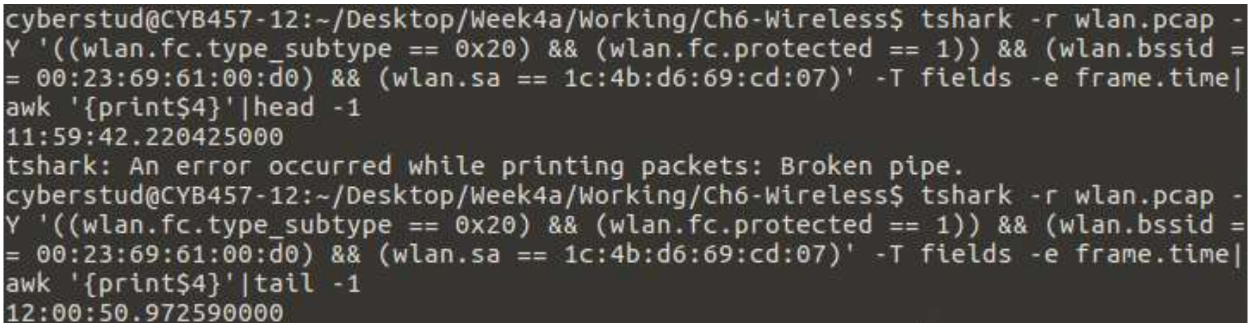


```
cyberstud@CYB457-12:~/Desktop/Week4a/Working/Ch6-Wireless$ tshark -r wlan.pcap -
Y '((wlan.fc.type_subtype == 0x20) && (wlan.fc.protected == 1)) && (wlan.bssid =
= 00:23:69:61:00:d0)' -T fields -e wlan.sa -e wlan.da|sort|uniq -c|sort -nr
  42816 1c:4b:d6:69:cd:07       ff:ff:ff:ff:ff:ff
  14076 00:11:22:33:44:55       00:23:69:61:00:ce
    858 00:23:69:61:00:ce       00:11:22:33:44:55
    740 de:ad:be:ef:13:37       00:23:69:61:00:ce
    654 00:23:69:61:00:ce       de:ad:be:ef:13:37
     59 00:23:69:61:00:ce       01:00:5e:7f:ff:fa
     18 00:11:22:33:44:55       33:33:00:00:00:02
     14 00:11:22:33:44:55       ff:ff:ff:ff:ff:ff
     13 00:11:22:33:44:55       33:33:00:00:00:16
      7 de:ad:be:ef:13:37       33:33:00:00:00:02
      6 00:11:22:33:44:55       33:33:ff:33:44:55
      4 de:ad:be:ef:13:37       ff:ff:ff:ff:ff:ff
      4 de:ad:be:ef:13:37       33:33:00:00:00:16
      3 00:23:69:61:00:ce       ff:ff:ff:ff:ff:ff
      2 de:ad:be:ef:13:37       33:33:ff:ef:13:37
```

Figure 7: Source and destination of encrypted data packets

To view the time frame of this large number of packets, examiner entered "tshark -r wlan.pcap -Y '((wlan.fc.type_subtype == 0x20) && (wlan.fc.protected == 1)) && (wlan.bssid ==

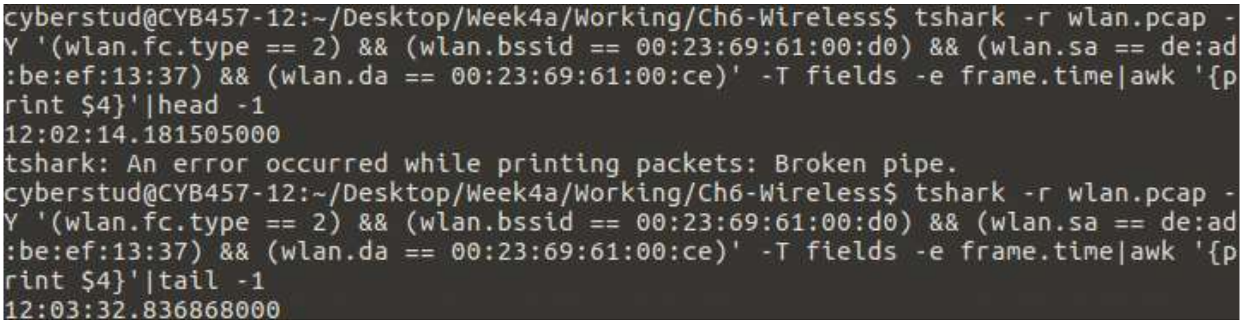
00:23:69:61:00:d0) && (wlan.sa == 1c:4b:d6:69:cd:07)’ -T fields -e frame.time|awk ‘{print $4}’|head -1” and “tshark -r wlan.pcap -Y ‘((wlan.fc.type_subtype == 0x20) && (wlan.fc.protected == 1)) && (wlan.bssid == 00:23:69:61:00:d0) && (wlan.sa == 1c:4b:d6:69:cd:07)’ -T fields -e frame.time|awk ‘{print $4}’|tail -1”. The difference between the two time stamps shown in figure 8 is less than 69 seconds.



```
cyberstud@CYB457-12:~/Desktop/Week4a/Working/Ch6-Wireless$ tshark -r wlan.pcap -
Y '((wlan.fc.type_subtype == 0x20) && (wlan.fc.protected == 1)) && (wlan.bssid =
= 00:23:69:61:00:d0) && (wlan.sa == 1c:4b:d6:69:cd:07)' -T fields -e frame.time|
awk '{print$4}'|head -1
11:59:42.220425000
tshark: An error occurred while printing packets: Broken pipe.
cyberstud@CYB457-12:~/Desktop/Week4a/Working/Ch6-Wireless$ tshark -r wlan.pcap -
Y '((wlan.fc.type_subtype == 0x20) && (wlan.fc.protected == 1)) && (wlan.bssid =
= 00:23:69:61:00:d0) && (wlan.sa == 1c:4b:d6:69:cd:07)' -T fields -e frame.time|
awk '{print$4}'|tail -1
12:00:50.972590000
```

Figure 8: Start and end time stamps of data sent from unknown station 1c:4b:d6:69:cd:07 to WAP

To view the time frame of packets sent by station de:ad:be:ef:13:37 to the WAP’s STA interface, examiner entered similar commands, as shown in figure 9.

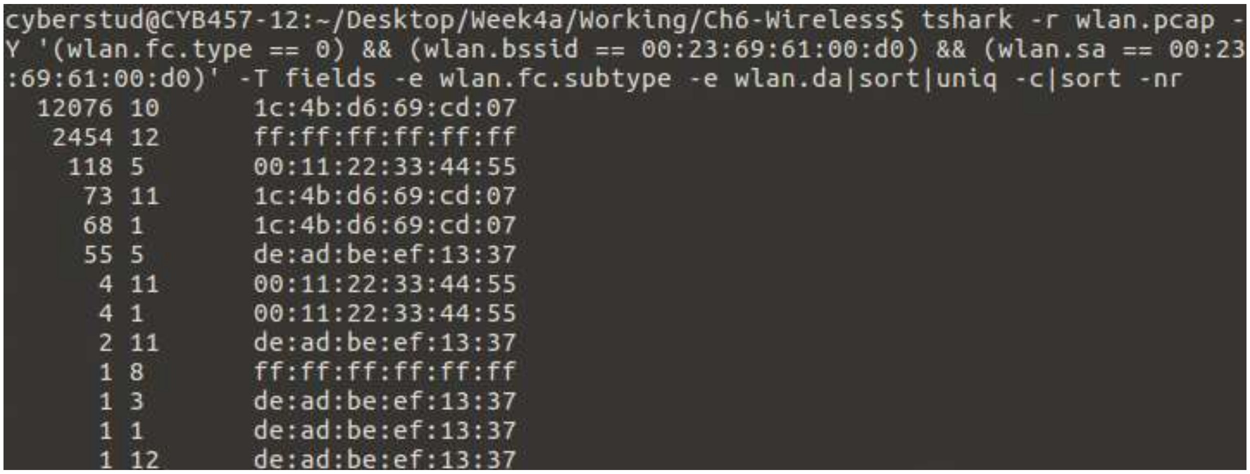


```
cyberstud@CYB457-12:~/Desktop/Week4a/Working/Ch6-Wireless$ tshark -r wlan.pcap -
Y '(wlan.fc.type == 2) && (wlan.bssid == 00:23:69:61:00:d0) && (wlan.sa == de:ad
:be:ef:13:37) && (wlan.da == 00:23:69:61:00:ce)' -T fields -e frame.time|awk '{p
rint $4}'|head -1
12:02:14.181505000
tshark: An error occurred while printing packets: Broken pipe.
cyberstud@CYB457-12:~/Desktop/Week4a/Working/Ch6-Wireless$ tshark -r wlan.pcap -
Y '(wlan.fc.type == 2) && (wlan.bssid == 00:23:69:61:00:d0) && (wlan.sa == de:ad
:be:ef:13:37) && (wlan.da == 00:23:69:61:00:ce)' -T fields -e frame.time|awk '{p
rint $4}'|tail -1
12:03:32.836868000
```

Figure 9: Start and end time stamps of data sent from unknown station de:ad:be:ef:13:37 to WAP’s STA interface

After adjusting for time differences, it was determined that these packets were sent toward the end of the capture (approximately 10:02:14 to 10:03:33).

To see the number of management frames sent by the WAP and their subtypes, examiner entered: “tshark -r wlan.pcap -Y ‘(wlan.fc.type == 0) && (wlan.bssid == 00:23:69:61:00:d0) && (wlan.sa == 00:23:69:61:00:d0)’ -T fields -e wlan.fc.subtype -e wlan.da|sort|uniq -c|sort -nr” in terminal. The results (see figure 10) show that the majority of management frames sent to unknown station 1c:4b:d6:69:cd:07 were subtype 10: disassociation. The next highest number of frames sent were subtype 12: deauthenticate. It is possible that an attacker was spoofing Joe’s WAP and sending these frames in order to knock stations off the network. It is important to note that de:ad:be:ef:13:37’s first data frame sent to the WAP’s STA interface occurred after this slew of disassociate/deauthenticate messages.



```
cyberstud@CYB457-12:~/Desktop/Week4a/Working/Ch6-Wireless$ tshark -r wlan.pcap -
Y '(wlan.fc.type == 0) && (wlan.bssid == 00:23:69:61:00:d0) && (wlan.sa == 00:23
:69:61:00:d0)' -T fields -e wlan.fc.subtype -e wlan.da|sort|uniq -c|sort -nr
  12076 10      1c:4b:d6:69:cd:07
   2454 12      ff:ff:ff:ff:ff:ff
    118 5       00:11:22:33:44:55
     73 11      1c:4b:d6:69:cd:07
     68 1       1c:4b:d6:69:cd:07
     55 5       de:ad:be:ef:13:37
      4 11      00:11:22:33:44:55
      4 1       00:11:22:33:44:55
      2 11      de:ad:be:ef:13:37
      1 8       ff:ff:ff:ff:ff:ff
      1 3       de:ad:be:ef:13:37
      1 1       de:ad:be:ef:13:37
      1 12      de:ad:be:ef:13:37
```

Figure 10: Management frames sent by WAP

Conclusion

The examiner was requested to identify the BSSID and SSID of the WAP of interest. They were 00:23:69:61:00:d0 and Ment0rNet, respectively. The examiner was asked to determine of the WAP was using encryption, which it was. The examiner was asked to identify which stations were interacting with the WAP and found three: 00:11:22:33:44:55 (Joe), unknown station 1c:4b:d6:69:cd:07, and de:ad:be:ef:13:37. Examiner also determined the anomalous activity surrounding the two unknown stations indicates that unknown station 1c:4b:d6:69:cd:07 carried out a successful WEP password cracking attempt, and that the retrieved credentials were used by unknown station de:ad:be:ef:13:37 to successfully connect to the WAP. The next steps to further understanding the possible actions of Inter0ptic would be to decrypt the packets and analyze the flow of data between de:ad:be:ef:13:37 and the WAP after the unknown station successfully connected to the network.

Appendix

Appendix A: Examiner Workstation Specifications

[redacted]

- System date/time is consistent with the time zone listed above, as verified by: http://nist.time.gov/.

Appendix B: Virtual Machine (VM) Specifications

- Virtual Machine Name: CYB457-12
- Operating System Name: Ubuntu
- System Make/Model: VMware, Inc. VMware Virtual Platform
- Virtual Machine Serial Number: VMware-42 1b 8a 7d d6 56 cd 16-8c 9a 80 0e 79 fb c8 f9
- VM’s Time Zone: Eastern Daylight Time
- System date and time are consistent with the time zone listed above, as verified by: http://nist.time.gov/.

Appendix C: Tools

- Wireshark v3.0.6
- Tshark v2.6.10
- Tcpdump v4.9.3

Appendix D: Evidence Copies

On 4/10/2020, the location of the week 4 lab files was made known to the examiner. The examiner created a new *Week4a* folder on the *Desktop*, then retrieved archive file *Ch6-Wireless.zip* via Mozilla Firefox from the CYB457 course shell to the *Week4a* folder.

Examiner used the online utility located at onlinemd5.com to obtain the md5 hash value of the downloaded archive file. No checksum for comparison was provided, so the examiner was unable to determine the purity of the preservation copy.

A new folder in *Week4a* was created called *Working*. Examiner created a working copy of the *Ch6-Wireless.zip* archive file in the *Working* folder called *Ch6-WirelessXX*. Onlinemd5.com was used to determine the hash value of the evidence created, which matched the preservation copy, confirming the integrity of the working copy.

Examiner unzipped the working copy archive, revealing file folder *Ch6-Wireless.*

Appendix E: Evidence Verification

Table 2 outlines the hashes obtained throughout the evidence verification process. Onlinemd5.com was used to calculate MD5 hashes.

Designation	Filename	MD5 Hash	Description
PRE-ANALYSIS			
Preservation Copy	Ch6-Wireless.zip	2E5E96A1D795C10597D0CB21B730487C	Archive file downloaded from Engage
Working Copy	Ch6-WirelessXX	2E5E96A1D795C10597D0CB21B730487C	Working Copy created from preservation copy. This copy was analyzed.
POST-ANALYSIS			
Preservation Copy	Ch6-Wireless.zip	2E5E96A1D795C10597D0CB21B730487C	Archive file downloaded from Engage
Working Copy	Ch6-WirelessXX	2E5E96A1D795C10597D0CB21B730487C	Working Copy created from preservation copy. This copy was analyzed.

Table 2: Evidence Verification Table