ATTACK DEFENSE

by PentesterAcademy

Name	Evil Twin Detection
URL	https://www.attackdefense.com/challengedetails?cid=1144
Type	WiFi Pentesting: Traffic Analysis

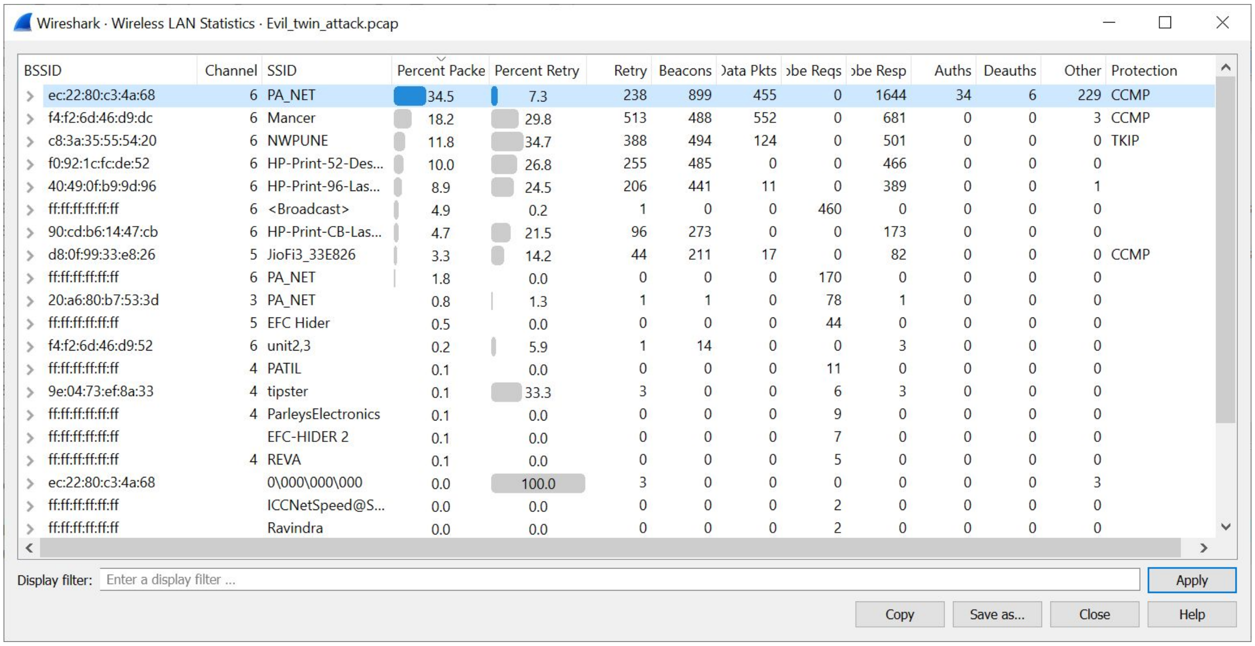
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. What is the SSID of the evil twin?

A. PA_NET

Solution:

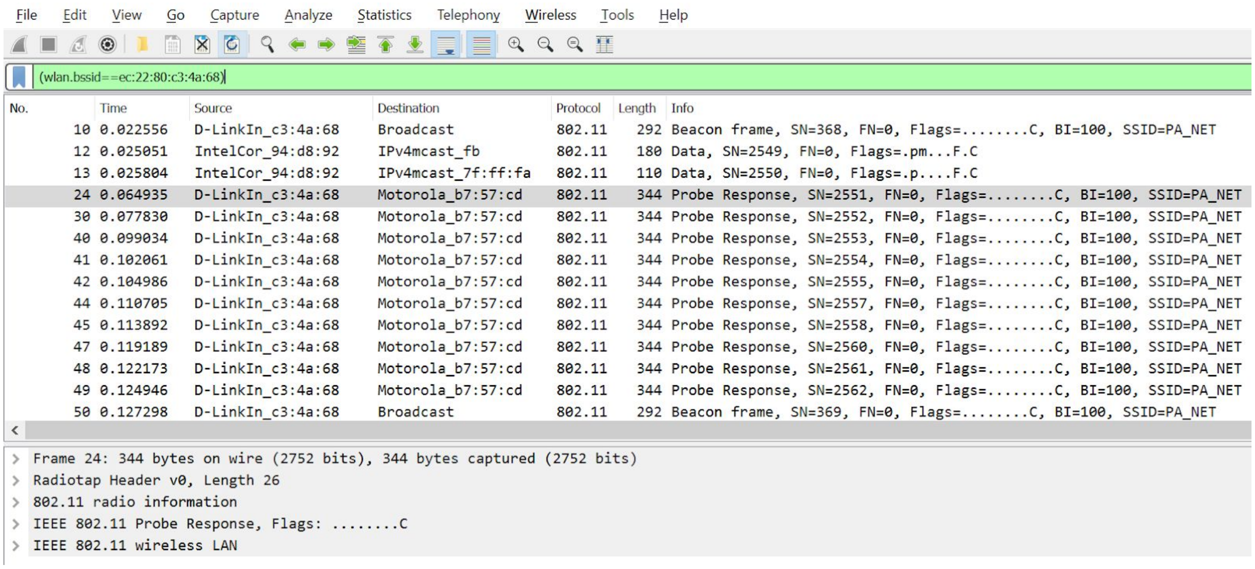
PA_NET has the majority packets in the capture, so it is a good choice to start investigation.


Wireshark · Wireless LAN Statistics · Evil_twin_attack.pcap
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close
Help

BSSID	Channel	SSID	Percent Packe	Percent Retry	Retry	Beacons	)ata Pkts	›be Reqs	›be Resp	Auths	Deauths	Other	Protection
ec:22:80:c3:4a:68	6	PA_NET	34.5	7.3	238	899	455	0	1644	34	6	229	CCMP
f4:f2:6d:46:d9:dc	6	Mancer	18.2	29.8	513	488	552	0	681	0	0	3	CCMP
c8:3a:35:55:54:20	6	NWPUNE	11.8	34.7	388	494	124	0	501	0	0	0	TKIP
f0:92:1c:fc:de:52	6	HP-Print-52-Des...	10.0	26.8	255	485	0	0	466	0	0	0	
40:49:0f:b9:9d:96	6	HP-Print-96-Las...	8.9	24.5	206	441	11	0	389	0	0	1	
ff:ff:ff:ff:ff:ff	6	<Broadcast>	4.9	0.2	1	0	0	460	0	0	0	0	
90:cd:b6:14:47:cb	6	HP-Print-CB-Las...	4.7	21.5	96	273	0	0	173	0	0	0	
d8:0f:99:33:e8:26	5	JioFi3_33E826	3.3	14.2	44	211	17	0	82	0	0	0	CCMP
ff:ff:ff:ff:ff:ff	6	PA_NET	1.8	0.0	0	0	0	170	0	0	0	0	
20:a6:80:b7:53:3d	3	PA_NET	0.8	1.3	1	1	0	78	1	0	0	0	
ff:ff:ff:ff:ff:ff	5	EFC Hider	0.5	0.0	0	0	0	44	0	0	0	0	
f4:f2:6d:46:d9:52	6	unit2,3	0.2	5.9	1	14	0	0	3	0	0	0	
ff:ff:ff:ff:ff:ff	4	PATIL	0.1	0.0	0	0	0	11	0	0	0	0	
9e:04:73:ef:8a:33	4	tipster	0.1	33.3	3	0	0	6	3	0	0	0	
ff:ff:ff:ff:ff:ff	4	ParleysElectronics	0.1	0.0	0	0	0	9	0	0	0	0	
ff:ff:ff:ff:ff:ff		EFC-HIDER 2	0.1	0.0	0	0	0	7	0	0	0	0	
ff:ff:ff:ff:ff:ff	4	REVA	0.1	0.0	0	0	0	5	0	0	0	0	
ec:22:80:c3:4a:68		0\000\000\000	0.0	100.0	3	0	0	0	0	0	0	3	
ff:ff:ff:ff:ff:ff		ICCNetSpeed@S...	0.0	0.0	0	0	0	2	0	0	0	0	
ff:ff:ff:ff:ff:ff		Ravindra	0.0	0.0	0	0	0	2	0	0	0	0	

Filter all traffic related to the BSSID ec:22:80:c3:4a:68

Filter: wlan.bssid==ec:22:80:c3:4a:68



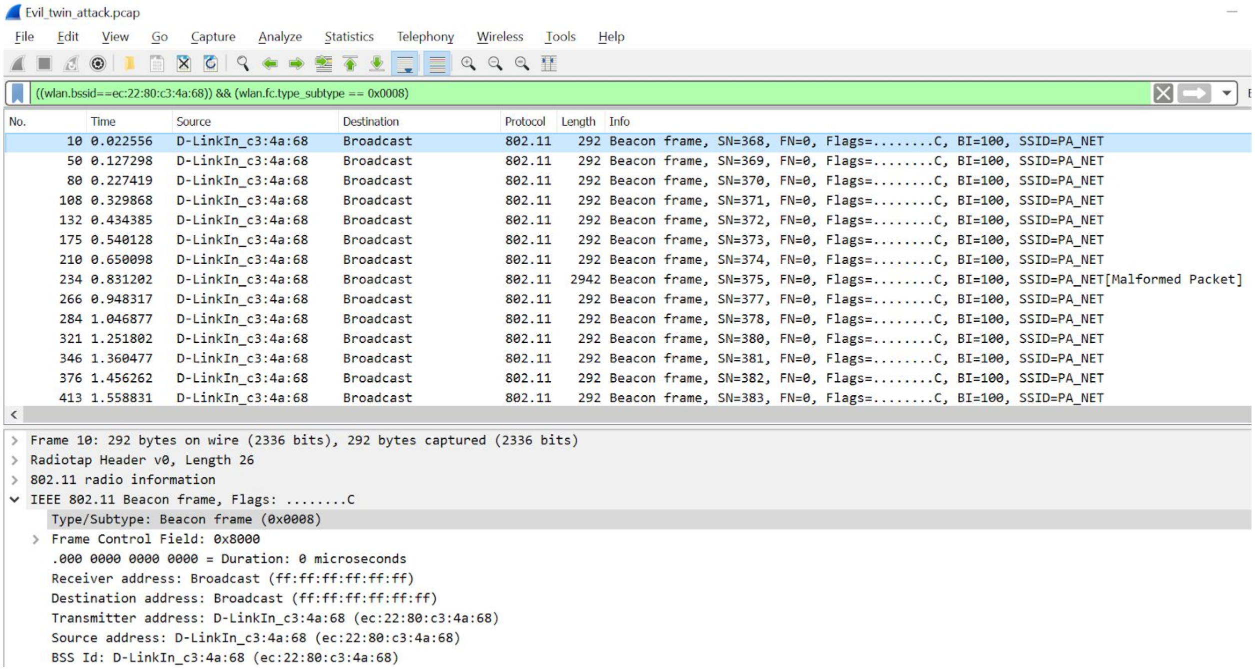
(wlan.bssid==ec:22:80:c3:4a:68)

```
No.     Time      Source            Destination        Protocol Length Info
     10 0.022556  D-LinkIn_c3:4a:68 Broadcast          802.11    292 Beacon frame, SN=368, FN=0, Flags=........C, BI=100, SSID=PA_NET
     12 0.025051  IntelCor_94:d8:92 IPv4mcast_fb       802.11    180 Data, SN=2549, FN=0, Flags=.pm...F.C
     13 0.025804  IntelCor_94:d8:92 IPv4mcast_7f:ff:fa 802.11    110 Data, SN=2550, FN=0, Flags=.p....F.C
     24 0.064935  D-LinkIn_c3:4a:68 Motorola_b7:57:cd  802.11    344 Probe Response, SN=2551, FN=0, Flags=........C, BI=100, SSID=PA_NET
     30 0.077830  D-LinkIn_c3:4a:68 Motorola_b7:57:cd  802.11    344 Probe Response, SN=2552, FN=0, Flags=........C, BI=100, SSID=PA_NET
     40 0.099034  D-LinkIn_c3:4a:68 Motorola_b7:57:cd  802.11    344 Probe Response, SN=2553, FN=0, Flags=........C, BI=100, SSID=PA_NET
     41 0.102061  D-LinkIn_c3:4a:68 Motorola_b7:57:cd  802.11    344 Probe Response, SN=2554, FN=0, Flags=........C, BI=100, SSID=PA_NET
     42 0.104986  D-LinkIn_c3:4a:68 Motorola_b7:57:cd  802.11    344 Probe Response, SN=2555, FN=0, Flags=........C, BI=100, SSID=PA_NET
     44 0.110705  D-LinkIn_c3:4a:68 Motorola_b7:57:cd  802.11    344 Probe Response, SN=2557, FN=0, Flags=........C, BI=100, SSID=PA_NET
     45 0.113892  D-LinkIn_c3:4a:68 Motorola_b7:57:cd  802.11    344 Probe Response, SN=2558, FN=0, Flags=........C, BI=100, SSID=PA_NET
     47 0.119189  D-LinkIn_c3:4a:68 Motorola_b7:57:cd  802.11    344 Probe Response, SN=2560, FN=0, Flags=........C, BI=100, SSID=PA_NET
     48 0.122173  D-LinkIn_c3:4a:68 Motorola_b7:57:cd  802.11    344 Probe Response, SN=2561, FN=0, Flags=........C, BI=100, SSID=PA_NET
     49 0.124946  D-LinkIn_c3:4a:68 Motorola_b7:57:cd  802.11    344 Probe Response, SN=2562, FN=0, Flags=........C, BI=100, SSID=PA_NET
     50 0.127298  D-LinkIn_c3:4a:68 Broadcast          802.11    292 Beacon frame, SN=369, FN=0, Flags=........C, BI=100, SSID=PA_NET
```

```
> Frame 24: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits)
> Radiotap Header v0, Length 26
> 802.11 radio information
> IEEE 802.11 Probe Response, Flags: ........C
> IEEE 802.11 wireless LAN
```

Looking for sequence number and packet size based anomalies will make more sense if we do it on

Filter: ((wlan.bssid==ec:22:80:c3:4a:68)) && (wlan.fc.type_subtype == 0x0008)

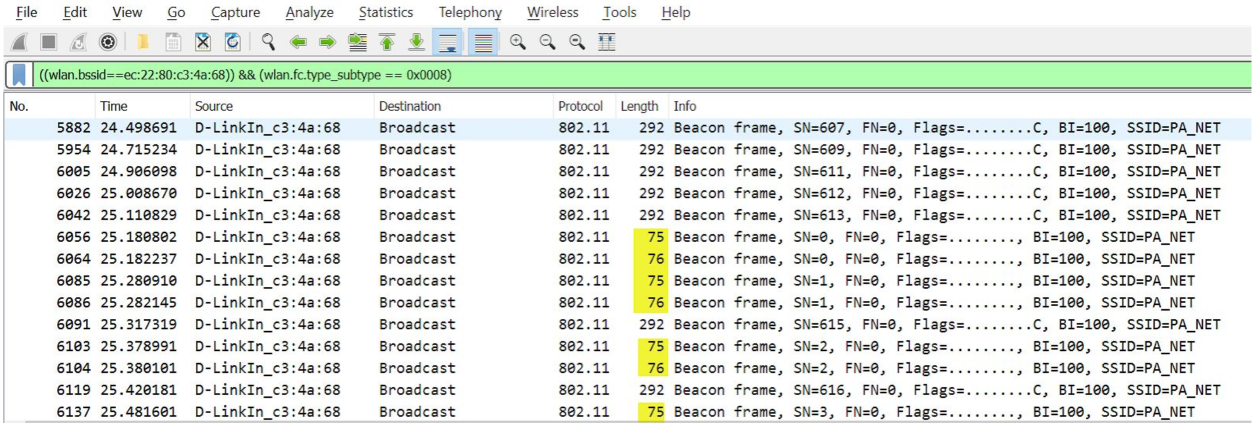

Evil_twin_attack.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
((wlan.bssid==ec:22:80:c3:4a:68)) && (wlan.fc.type_subtype == 0x0008)
```

```
No.  Time      Source              Destination  Protocol Length Info
  10 0.022556  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=368, FN=0, Flags=........C, BI=100, SSID=PA_NET
  50 0.127298  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=369, FN=0, Flags=........C, BI=100, SSID=PA_NET
  80 0.227419  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=370, FN=0, Flags=........C, BI=100, SSID=PA_NET
 108 0.329868  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=371, FN=0, Flags=........C, BI=100, SSID=PA_NET
 132 0.434385  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=372, FN=0, Flags=........C, BI=100, SSID=PA_NET
 175 0.540128  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=373, FN=0, Flags=........C, BI=100, SSID=PA_NET
 210 0.650098  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=374, FN=0, Flags=........C, BI=100, SSID=PA_NET
 234 0.831202  D-LinkIn_c3:4a:68   Broadcast    802.11   2942  Beacon frame, SN=375, FN=0, Flags=........C, BI=100, SSID=PA_NET[Malformed Packet]
 266 0.948317  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=377, FN=0, Flags=........C, BI=100, SSID=PA_NET
 284 1.046877  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=378, FN=0, Flags=........C, BI=100, SSID=PA_NET
 321 1.251802  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=380, FN=0, Flags=........C, BI=100, SSID=PA_NET
 346 1.360477  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=381, FN=0, Flags=........C, BI=100, SSID=PA_NET
 376 1.456262  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=382, FN=0, Flags=........C, BI=100, SSID=PA_NET
 413 1.558831  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=383, FN=0, Flags=........C, BI=100, SSID=PA_NET
```

```
> Frame 10: 292 bytes on wire (2336 bits), 292 bytes captured (2336 bits)
> Radiotap Header v0, Length 26
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    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: D-LinkIn_c3:4a:68 (ec:22:80:c3:4a:68)
    Source address: D-LinkIn_c3:4a:68 (ec:22:80:c3:4a:68)
    BSS Id: D-LinkIn_c3:4a:68 (ec:22:80:c3:4a:68)
```

On scrolling down, we can observe size based difference. Now this clearly indicates that there are two different machines/interfaces/setups for SSID PA_NET.

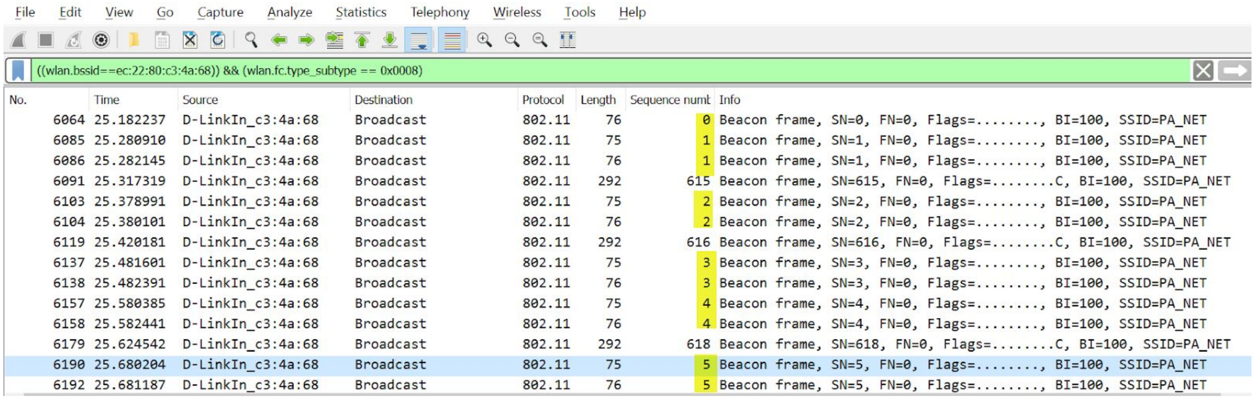

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
((wlan.bssid==ec:22:80:c3:4a:68)) && (wlan.fc.type_subtype == 0x0008)
```

```
No.   Time       Source              Destination  Protocol Length Info
 5882 24.498691  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=607, FN=0, Flags=........C, BI=100, SSID=PA_NET
 5954 24.715234  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=609, FN=0, Flags=........C, BI=100, SSID=PA_NET
 6005 24.906098  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=611, FN=0, Flags=........C, BI=100, SSID=PA_NET
 6026 25.008670  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=612, FN=0, Flags=........C, BI=100, SSID=PA_NET
 6042 25.110829  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=613, FN=0, Flags=........C, BI=100, SSID=PA_NET
 6056 25.180802  D-LinkIn_c3:4a:68   Broadcast    802.11     75  Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=PA_NET
 6064 25.182237  D-LinkIn_c3:4a:68   Broadcast    802.11     76  Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=PA_NET
 6085 25.280910  D-LinkIn_c3:4a:68   Broadcast    802.11     75  Beacon frame, SN=1, FN=0, Flags=........, BI=100, SSID=PA_NET
 6086 25.282145  D-LinkIn_c3:4a:68   Broadcast    802.11     76  Beacon frame, SN=1, FN=0, Flags=........, BI=100, SSID=PA_NET
 6091 25.317319  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=615, FN=0, Flags=........C, BI=100, SSID=PA_NET
 6103 25.378991  D-LinkIn_c3:4a:68   Broadcast    802.11     75  Beacon frame, SN=2, FN=0, Flags=........, BI=100, SSID=PA_NET
 6104 25.380101  D-LinkIn_c3:4a:68   Broadcast    802.11     76  Beacon frame, SN=2, FN=0, Flags=........, BI=100, SSID=PA_NET
 6119 25.420181  D-LinkIn_c3:4a:68   Broadcast    802.11    292  Beacon frame, SN=616, FN=0, Flags=........C, BI=100, SSID=PA_NET
 6137 25.481601  D-LinkIn_c3:4a:68   Broadcast    802.11     75  Beacon frame, SN=3, FN=0, Flags=........, BI=100, SSID=PA_NET
```

To confirm this, add sequence number as a column to the wireshark. We can observe two different sequence number running in parallel which confirms the suspicion

.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
((wlan.bssid==ec:22:80:c3:4a:68)) && (wlan.fc.type_subtype == 0x0008)

No.    Time       Source             Destination  Protocol  Length  Sequence numt  Info
 6064 25.182237  D-LinkIn_c3:4a:68  Broadcast    802.11    76        0  Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=PA_NET
 6085 25.280910  D-LinkIn_c3:4a:68  Broadcast    802.11    75        1  Beacon frame, SN=1, FN=0, Flags=........, BI=100, SSID=PA_NET
 6086 25.282145  D-LinkIn_c3:4a:68  Broadcast    802.11    76        1  Beacon frame, SN=1, FN=0, Flags=........, BI=100, SSID=PA_NET
 6091 25.317319  D-LinkIn_c3:4a:68  Broadcast    802.11    292     615  Beacon frame, SN=615, FN=0, Flags=........C, BI=100, SSID=PA_NET
 6103 25.378991  D-LinkIn_c3:4a:68  Broadcast    802.11    75        2  Beacon frame, SN=2, FN=0, Flags=........, BI=100, SSID=PA_NET
 6104 25.380101  D-LinkIn_c3:4a:68  Broadcast    802.11    76        2  Beacon frame, SN=2, FN=0, Flags=........, BI=100, SSID=PA_NET
 6119 25.420181  D-LinkIn_c3:4a:68  Broadcast    802.11    292     616  Beacon frame, SN=616, FN=0, Flags=........C, BI=100, SSID=PA_NET
 6137 25.481601  D-LinkIn_c3:4a:68  Broadcast    802.11    75        3  Beacon frame, SN=3, FN=0, Flags=........, BI=100, SSID=PA_NET
 6138 25.482391  D-LinkIn_c3:4a:68  Broadcast    802.11    76        3  Beacon frame, SN=3, FN=0, Flags=........, BI=100, SSID=PA_NET
 6157 25.580385  D-LinkIn_c3:4a:68  Broadcast    802.11    75        4  Beacon frame, SN=4, FN=0, Flags=........, BI=100, SSID=PA_NET
 6158 25.582441  D-LinkIn_c3:4a:68  Broadcast    802.11    76        4  Beacon frame, SN=4, FN=0, Flags=........, BI=100, SSID=PA_NET
 6179 25.624542  D-LinkIn_c3:4a:68  Broadcast    802.11    292     618  Beacon frame, SN=618, FN=0, Flags=........C, BI=100, SSID=PA_NET
 6190 25.680204  D-LinkIn_c3:4a:68  Broadcast    802.11    75        5  Beacon frame, SN=5, FN=0, Flags=........, BI=100, SSID=PA_NET
 6192 25.681187  D-LinkIn_c3:4a:68  Broadcast    802.11    76        5  Beacon frame, SN=5, FN=0, Flags=........, BI=100, SSID=PA_NET
```

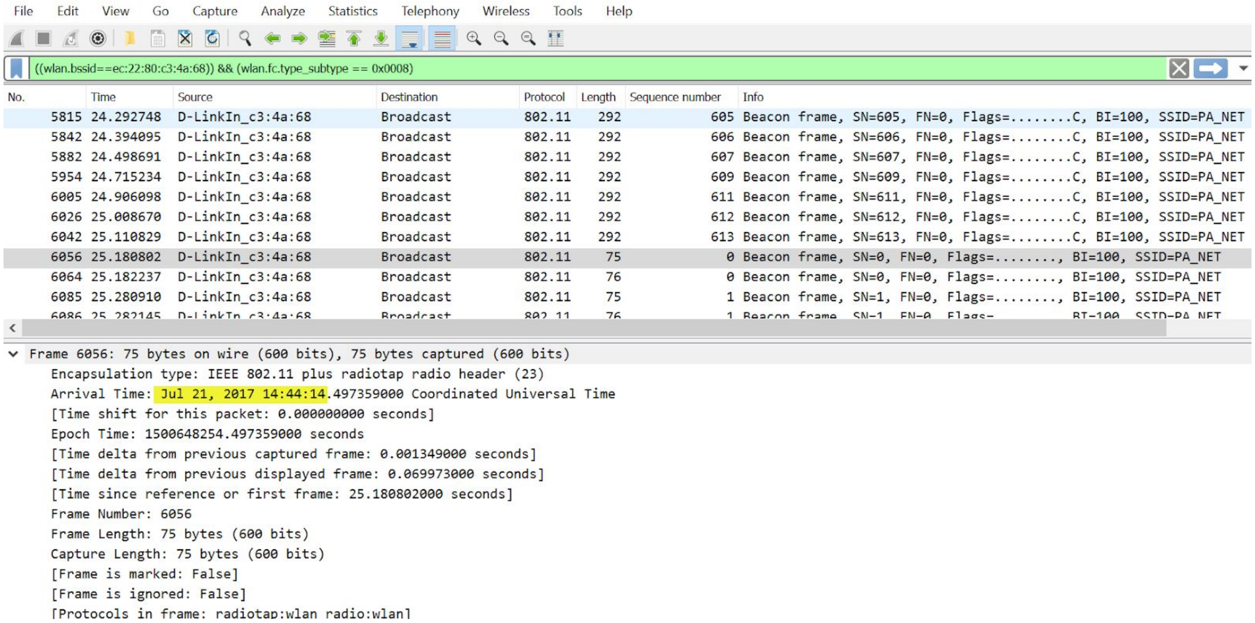
Q2. When did the evil twin AP started operating? Provide UTC time in DD-MM-YYYY HH:MM:SS format.

A. 21-07-2017 14:44:14

Solution:

Read the timestamp of the first beacon packet of that network.

Filter: ((wlan.bssid==ec:22:80:c3:4a:68)) && (wlan.fc.type_subtype == 0x0008)


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
((wlan.bssid==ec:22:80:c3:4a:68)) && (wlan.fc.type_subtype == 0x0008)

No.    Time       Source             Destination  Protocol  Length  Sequence number  Info
 5815 24.292748  D-LinkIn_c3:4a:68  Broadcast    802.11    292     605  Beacon frame, SN=605, FN=0, Flags=........C, BI=100, SSID=PA_NET
 5842 24.394095  D-LinkIn_c3:4a:68  Broadcast    802.11    292     606  Beacon frame, SN=606, FN=0, Flags=........C, BI=100, SSID=PA_NET
 5882 24.498691  D-LinkIn_c3:4a:68  Broadcast    802.11    292     607  Beacon frame, SN=607, FN=0, Flags=........C, BI=100, SSID=PA_NET
 5954 24.715234  D-LinkIn_c3:4a:68  Broadcast    802.11    292     609  Beacon frame, SN=609, FN=0, Flags=........C, BI=100, SSID=PA_NET
 6005 24.906098  D-LinkIn_c3:4a:68  Broadcast    802.11    292     611  Beacon frame, SN=611, FN=0, Flags=........C, BI=100, SSID=PA_NET
 6026 25.008670  D-LinkIn_c3:4a:68  Broadcast    802.11    292     612  Beacon frame, SN=612, FN=0, Flags=........C, BI=100, SSID=PA_NET
 6042 25.110829  D-LinkIn_c3:4a:68  Broadcast    802.11    292     613  Beacon frame, SN=613, FN=0, Flags=........C, BI=100, SSID=PA_NET
 6056 25.180802  D-LinkIn_c3:4a:68  Broadcast    802.11    75        0  Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=PA_NET
 6064 25.182237  D-LinkIn_c3:4a:68  Broadcast    802.11    76        0  Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=PA_NET
 6085 25.280910  D-LinkIn_c3:4a:68  Broadcast    802.11    75        1  Beacon frame, SN=1, FN=0, Flags=........, BI=100, SSID=PA_NET
 6086 25.282145  D-LinkIn_c3:4a:68  Broadcast    802.11    76        1  Beacon frame, SN=1, FN=0, Flags=........, BI=100, SSID=PA_NET

Frame 6056: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Jul 21, 2017 14:44:14.497359000 Coordinated Universal Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1500648254.497359000 seconds
    [Time delta from previous captured frame: 0.001349000 seconds]
    [Time delta from previous displayed frame: 0.069973000 seconds]
    [Time since reference or first frame: 25.180802000 seconds]
    Frame Number: 6056
    Frame Length: 75 bytes (600 bits)
    Capture Length: 75 bytes (600 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan]
```

References:

1. Wireshark (https://www.wireshark.org/)
2. Pentester Academy WiFi course (https://www.pentesteracademy.com/course?id=9)