

**ATTACK**

**DEFENSE**

by PentesterAcademy

<b>Name</b>	Breach Investigation
<b>URL</b>	<a href="https://www.attackdefense.com/challengedetails?cid=70">https://www.attackdefense.com/challengedetails?cid=70</a>
<b>Type</b>	Forensics : WiFi

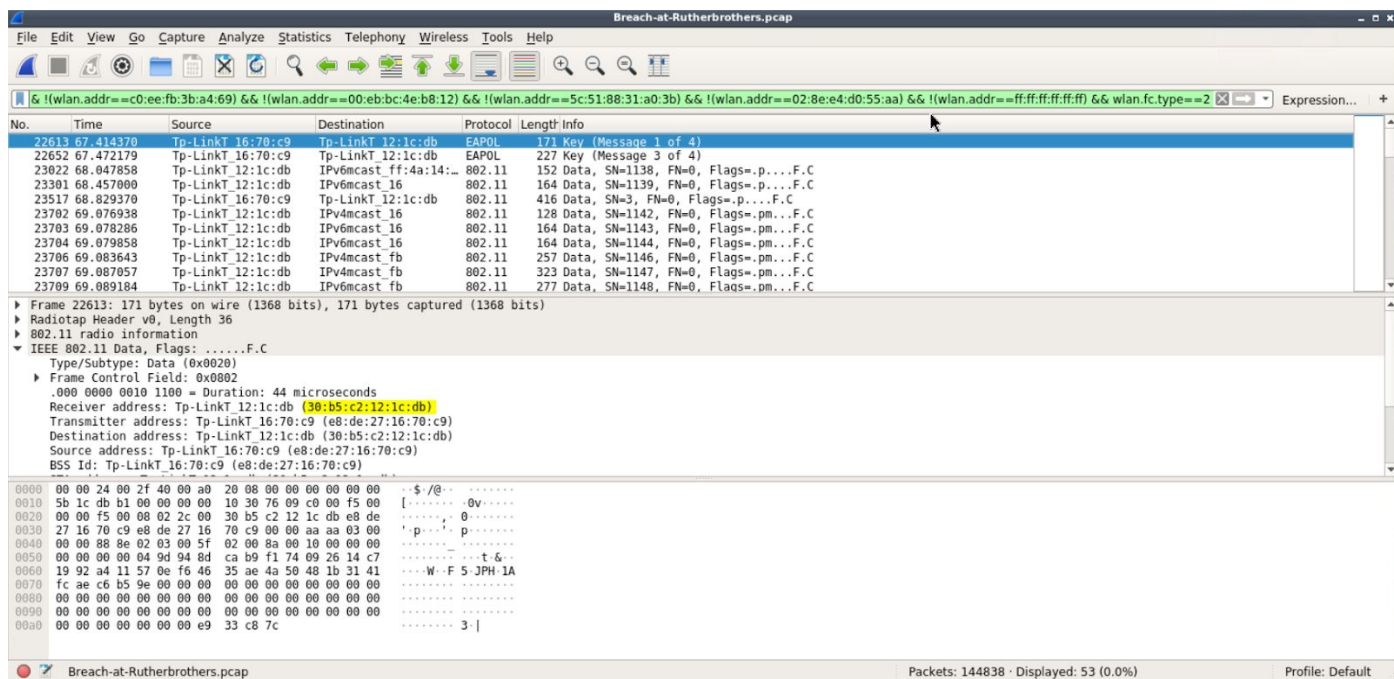
**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

**Question 1:** What is the MAC address of the suspect?

#### **Solution**

Exclude known client MAC addresses/broadcast address/Beacons/Probes and also add a filter for data packets to find out the alien addresses.

**Filter:** ((wlan.ta == e8:de:27:16:70:c9) && !(wlan.fc == 0x8000)) && !(wlan.fc.type\_subtype == 0x0005) && !(wlan.fc.type\_subtype == 0x0004) && !(wlan.addr == c0:ee:fb:3b:a4:69) && !(wlan.addr == 00:eb:bc:4e:b8:12) && !(wlan.addr == 5c:51:88:31:a0:3b) && !(wlan.addr == 02:8e:e4:d0:55:aa) && !(wlan.addr == ff:ff:ff:ff:ff:ff) && wlan.fc.type == 2



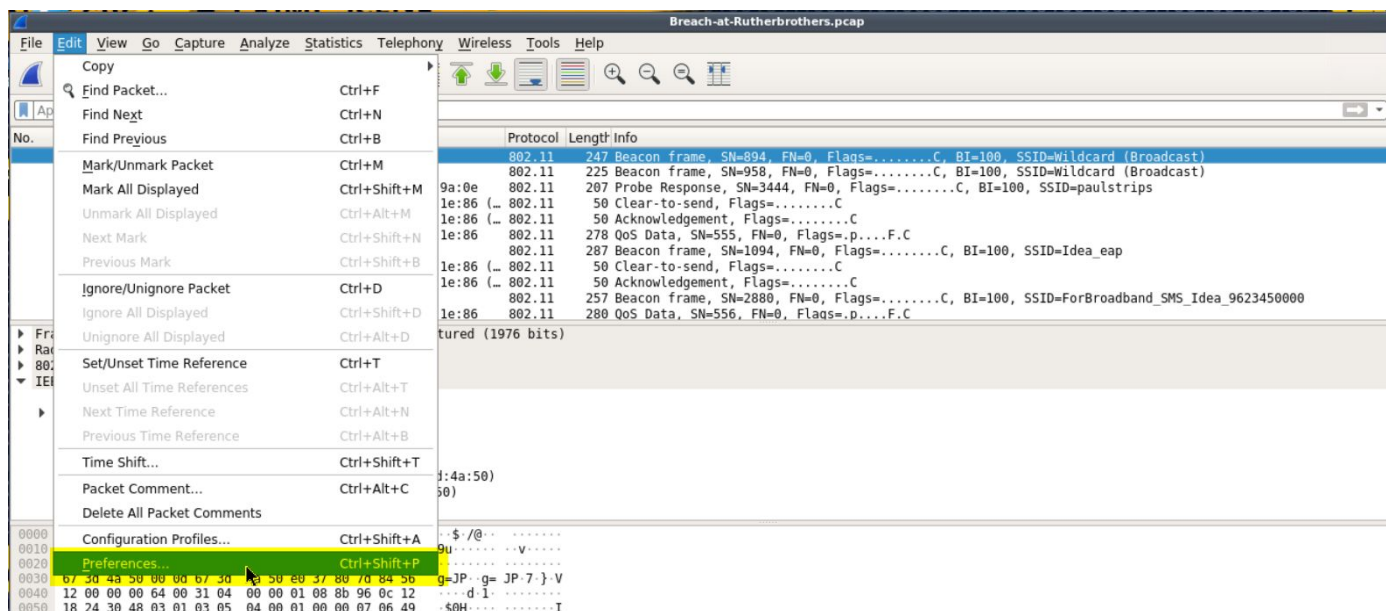
**Answer:** 30:b5:c2:12:1c:db

**Question 2:** What did the attacker do on the network?

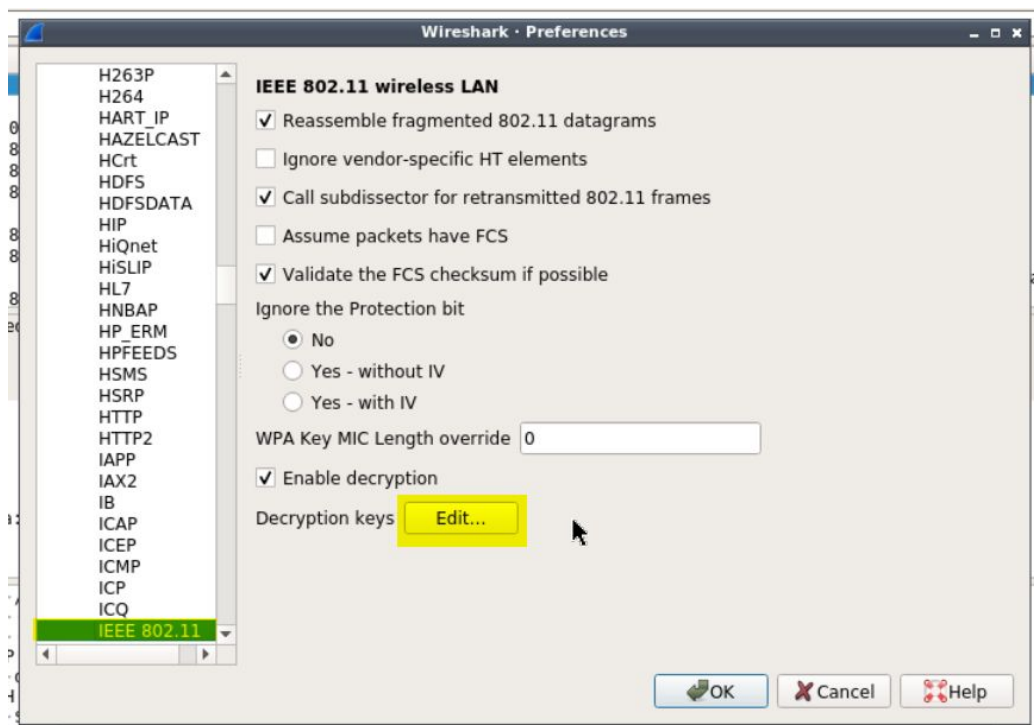
**Solution**

Decrypted WiFi traffic is needed. For that, add the WiFi network details to wireshark as shown below:

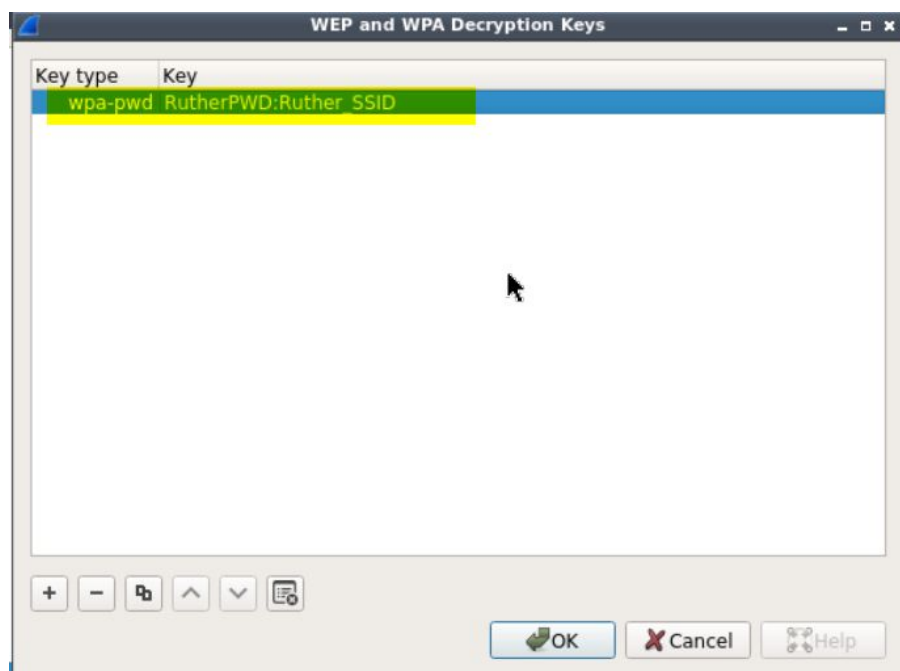
First, Open Edit > Preferences



From protocols, select IEEE802.11. To add the decryption keys, click the Edit button.



The record is added in the following format <Shared\_secret>:<SSID\_name>. WPA-PWD denotes WPA secret passphrase.



On saving the keys and closing the pop up, the traffic will be decrypted. Then, one can filter the packets of popular protocols associated with the MAC of attacker

**Filter:** wlan.addr==30:b5:c2:12:1c:db && (ftp || http || ssh || telnet)



Breach-at-Rutherbrothers.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.addr==30:b5:c2:12:1c:db && (ftp || http || ssh || telnet)

No.	Time	Source	Destination	Protocol	Length	Info
1036...	140.535598	192.168.3.16	192.168.3.18	FTP	133	Request: PWD
1036...	140.539170	192.168.3.18	192.168.3.16	FTP	162	Response: 257 "/" is the current directory
1041...	140.729038	192.168.3.16	192.168.3.18	FTP	136	Request: TYPE I
1042...	140.763973	192.168.3.16	192.168.3.18	FTP	142	[TCP ACKed unseen segment] Request: SIZE /secret
1042...	140.767562	192.168.3.18	192.168.3.16	FTP	136	[TCP Previous segment not captured] Response: 213 27
1042...	140.774694	192.168.3.16	192.168.3.18	FTP	141	[TCP ACKed unseen segment] Request: CWD /secret
1043...	140.789964	192.168.3.18	192.168.3.16	FTP	161	Response: 550 Failed to change directory.
1043...	140.793261	192.168.3.16	192.168.3.18	FTP	134	Request: PASV
1043...	140.795011	192.168.3.18	192.168.3.16	FTP	178	Response: 227 Entering Passive Mode (192,168,3,18,85,179).
1044...	140.848942	192.168.3.16	192.168.3.18	FTP	142	Request: RETR /secret
1044...	140.853405	192.168.3.18	192.168.3.16	FTP	193	Response: 150 Opening BINARY mode data connection for /secret (27 bytes).

Frame 104458: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits)

- ▶ Radiotap Header v0, Length 36
- ▶ 802.11 radio information
- ▶ IEEE 802.11 Data, Flags: .p....F.C
- ▶ Logical-Link Control
- ▶ Internet Protocol Version 4, Src: 192.168.3.16, Dst: 192.168.3.18
- ▶ Transmission Control Protocol, Src Port: 10651, Dst Port: 21, Seq: 94, Ack: 253, Len: 14
- ▼ File Transfer Protocol (FTP)
  - RETR /secret\r\n
    - Request command: RETR
    - Request arg: /secret

[Current working directory: /]  
 [Command response frames: 1]  
 [Command response bytes: 27]  
 [Command response first frame: 104467]  
 [Command response last frame: 104467]

A lot of activity is there for FTP protocol. Check it to get the information of exact actions.

**Answer:** Intruder downloaded a file named "secret" from the target machine.

**Question 3:** What is the MAC and IP address of the affected machine?

**Solution**

Check the IP address and MAC of the FTP server

**Filter:** wlan.da==30:b5:c2:12:1c:db && ftp

Breach-at-Rutherbrothers.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.da==30:b5:c2:12:1c:db && ftp

No.	Time	Source	Destination	Protocol	Length	Info
97602	136.538986	192.168.3.16	192.168.3.18	FTP	137	Request: LIST -l
1031...	140.205356	192.168.3.16	192.168.3.18	FTP	144	Request: USER anonymous
1034...	140.357364	192.168.3.16	192.168.3.18	FTP	153	Request: PASS chrome@example.com
1036...	140.477982	192.168.3.16	192.168.3.18	FTP	134	Request: SYST
1036...	140.535598	192.168.3.16	192.168.3.18	FTP	133	Request: PWD
1041...	140.720030	192.168.3.16	192.168.3.18	FTP	136	Request: TYPE T

▶ Frame 104458: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits)

- ▶ Radiotap Header v0, Length 36
- ▶ 802.11 radio information
- ▶ IEEE 802.11 Data, Flags: .p...F.C
- ▶ Logical-Link Control
- ▼ Internet Protocol Version 4, Src: 192.168.3.16, Dst: 192.168.3.18
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 54
  - Identification: 0x6f92 (28562)
  - ▶ Flags: 0x4000, Don't fragment
  - Time to live: 128
  - Protocol: TCP (6)
  - Header checksum: 0x03bd [validation disabled]
  - [Header checksum status: Unverified]
  - Source: 192.168.3.16
  - Destination: 192.168.3.18
- ▶ Transmission Control Protocol, Src Port: 10651, Dst Port: 21, Seq: 94, Ack: 253, Len: 14
- ▼ File Transfer Protocol (FTP)
  - RETR /secret\r\n

**Answer:** MAC: 02:8e:e4:d0:55:aa, IP address: 192.168.3.16

**Question 4:** Whose machine is it?

**Solution**

Cross reference the MAC address of the affected machine with employee details table.

**Answer:** Ms. Betty (Manager)