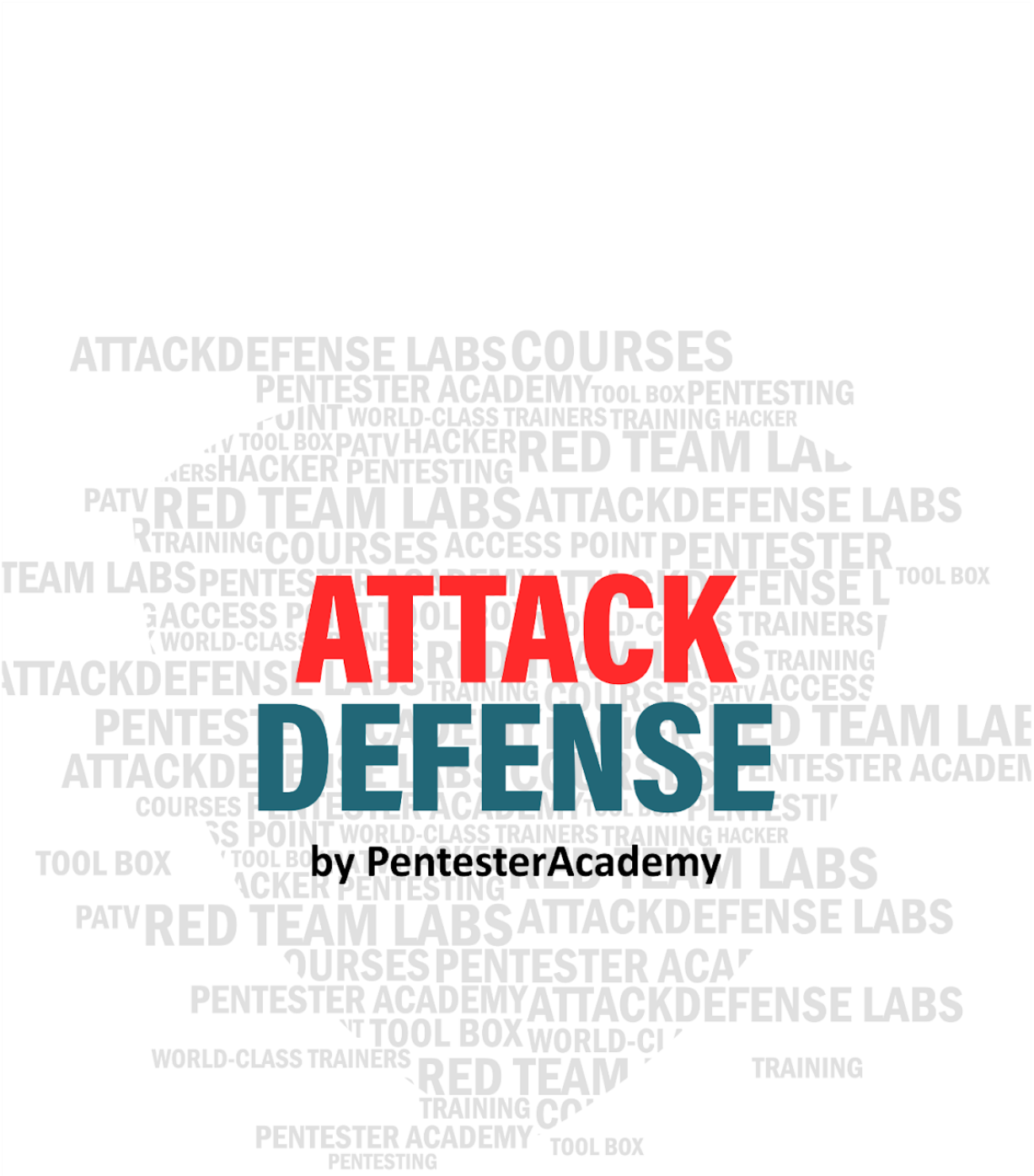

ATTACK
DEFENSE
by PentesterAcademy

Name	Breach Investigation
URL	https://www.attackdefense.com/challengedetails?cid=70
Type	Forensics : WiFi

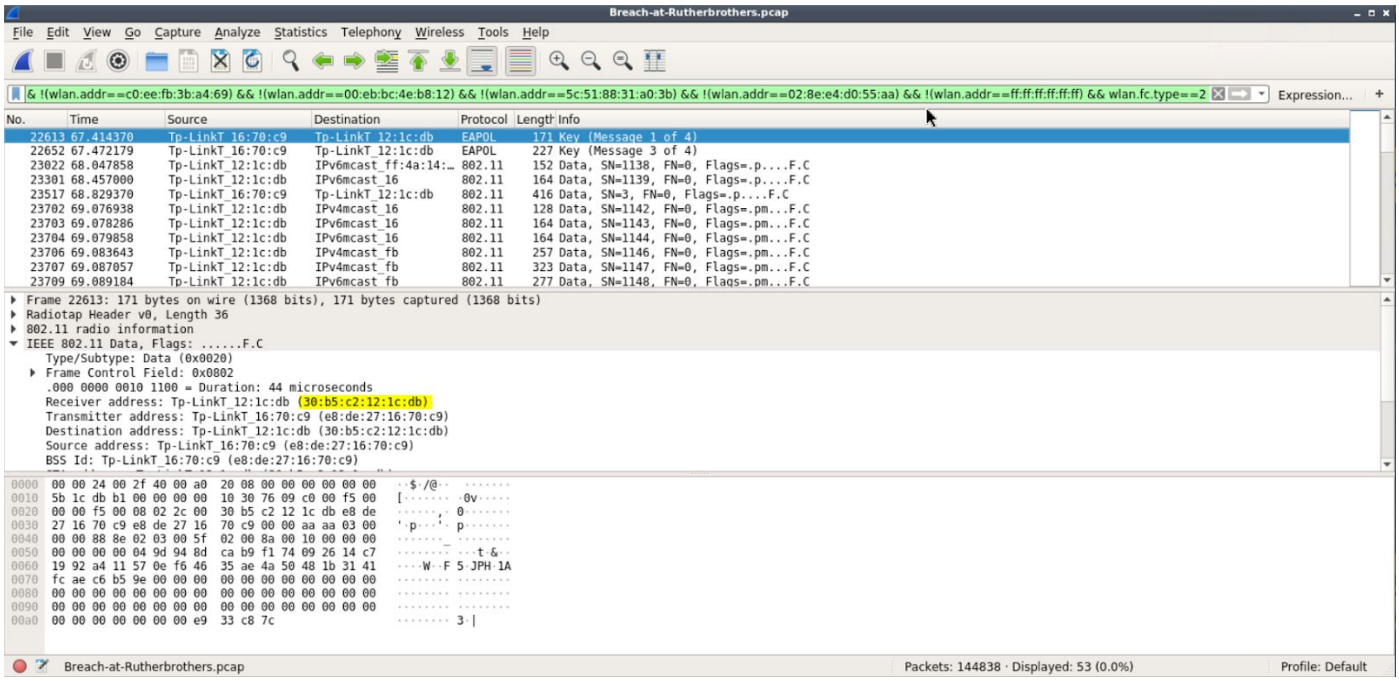
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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



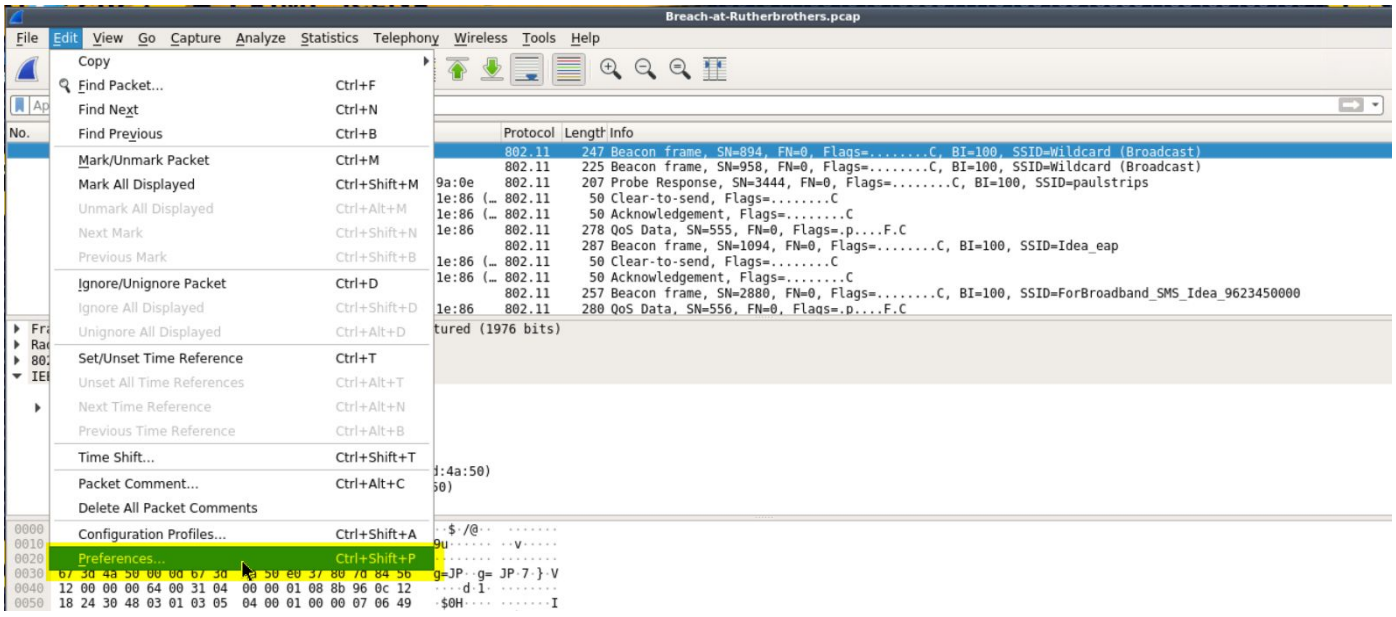
Answer: 30:b5:c2:12:1c:db

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

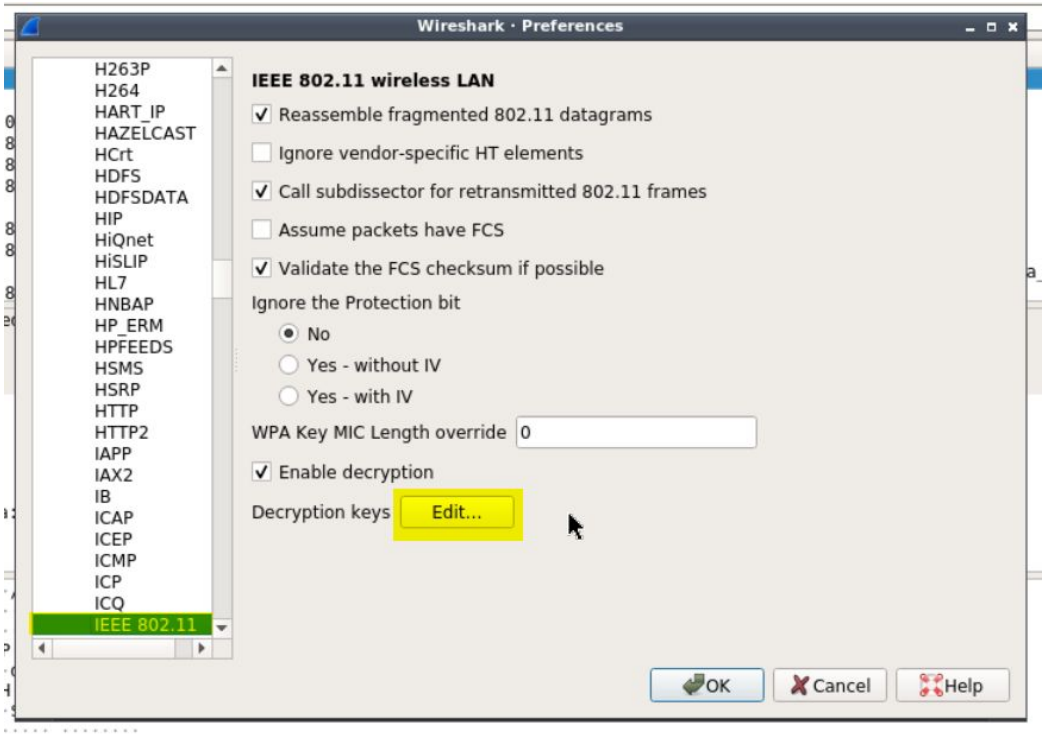
Solution

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

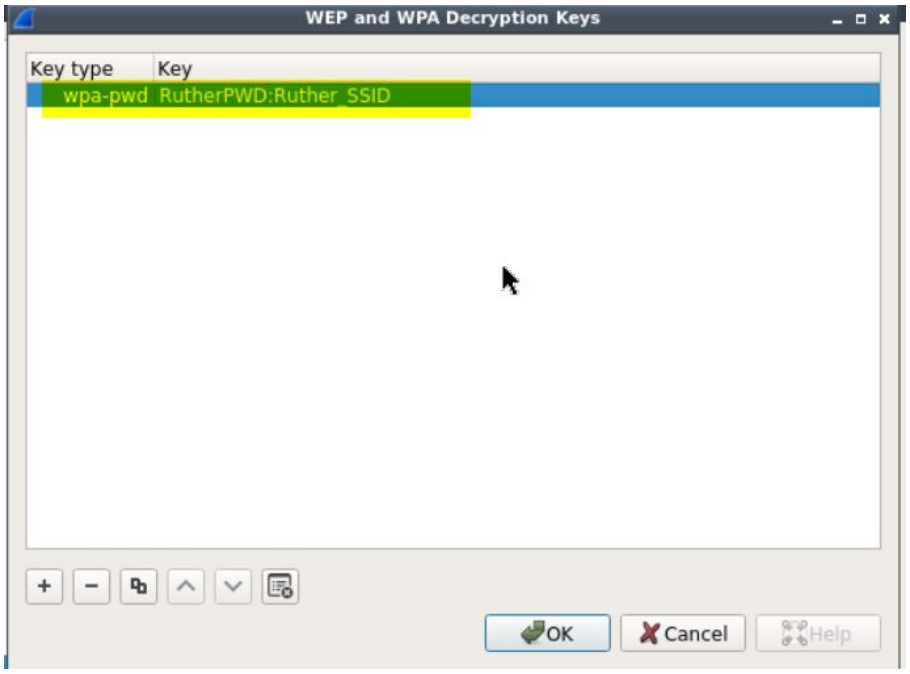
First, Open Edit > Preferences



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

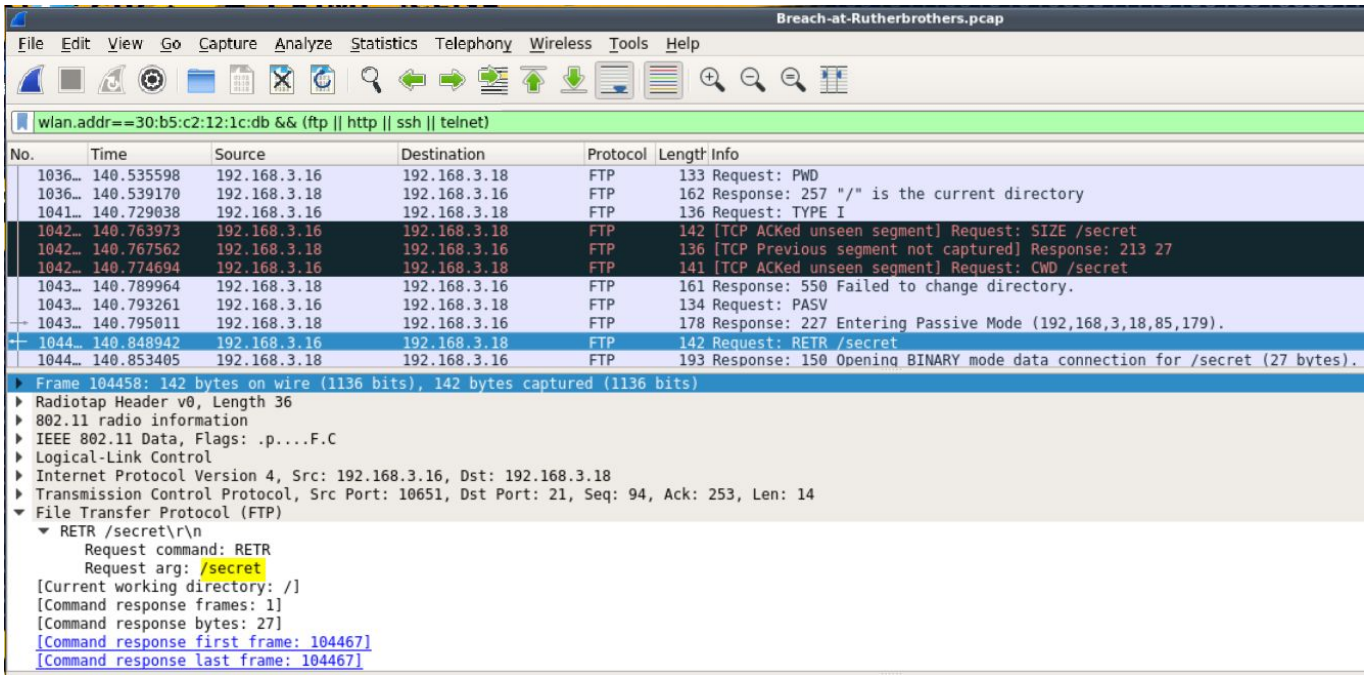


The record is added in the following format <Shared_sercet>:<SSID_name>. WPA-PWD denotes WPA secret passphrase.



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)



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

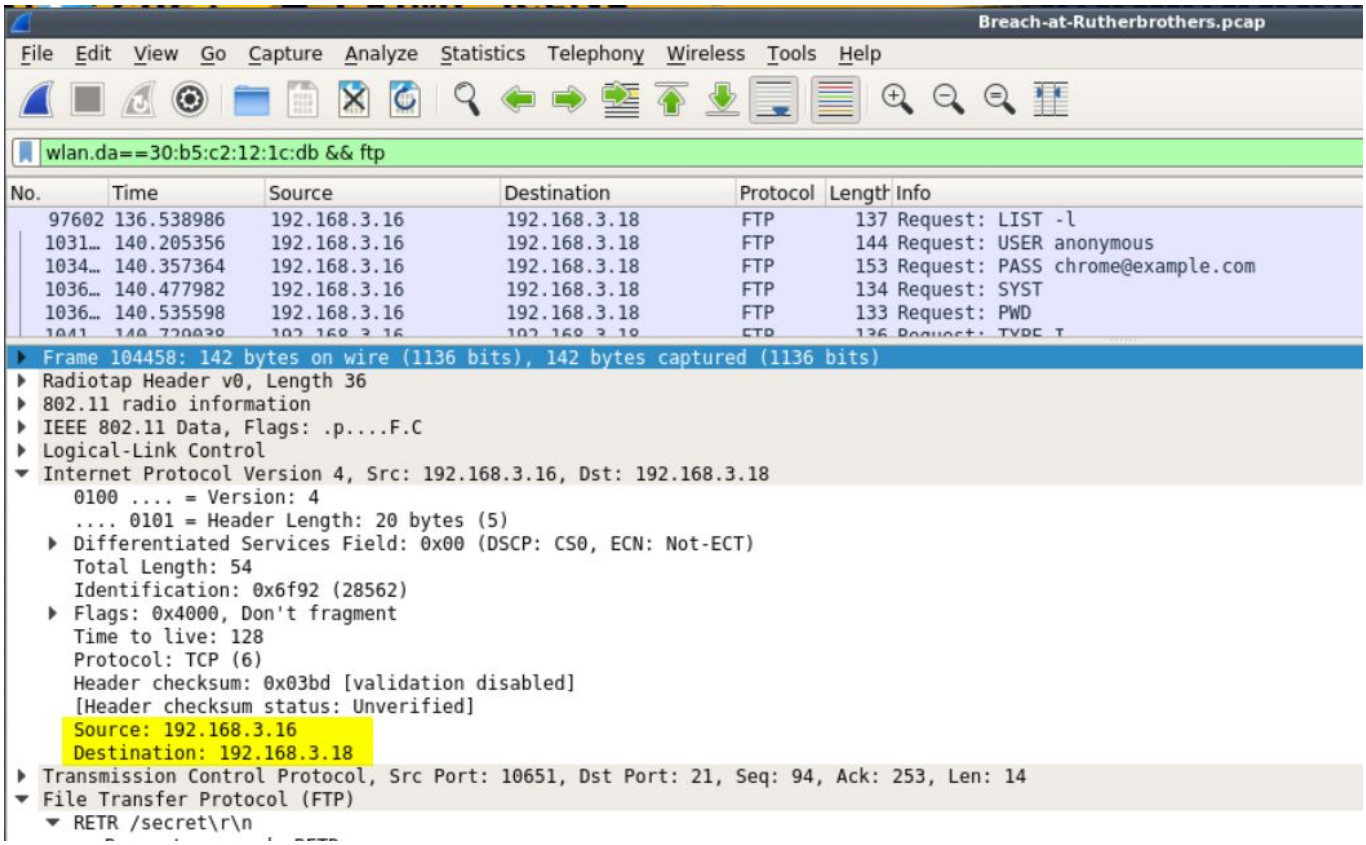
Answer: Intruder downloaded a file named “secret” from the target machine.

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



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)