2.7. <https://attackdefense.com/challengedetails?cid=71>

You are a licensed Private Investigator (PI). UVW88 Inc is one of your old customers. They import electronics from abroad and sell the re-branded product. They asked you to look into Ron, one of their purchasing managers. They think that he is tipping off their competitors about the soon to be launched products in advance, giving the competition an edge over them. They checked his company issued phones and corporate email account but didn’t find anything suspicious. Hence, they brought in the big guns ( yes you :-) ). You follow him for 2 days but he isn’t meeting anyone. So, the next night you decide to wait outside his house in your car. While sitting outside, eating a burger, you notice his home WiFi network and you realize that he may be using this to communicate with the 3rd party. So, you capture his WiFi traffic and return to your office to analyze it.

##### The relevant details

The details of Ron's home WiFi network are given below:

* SSID: Ron\_Home
* BSSID: 30:b5:c2:11:de:2a
* Security: WPA2-PSK
* Phone MAC: 5c:51:88:31:a0:3b
* Laptop MAC: e8:de:27:16:70:c9

##### **Questions**

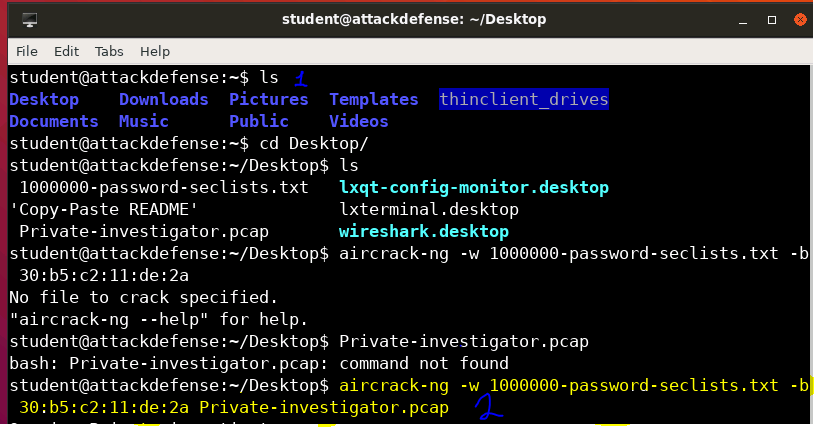
1. How he is communicating with the 3rd party?
2. What content did you recover from the communication intercepted (if any)?
3. Any contact information of the 3rd party (if any)?
4. Anything interesting that you observed during the analysis which could shed light on his other motives?

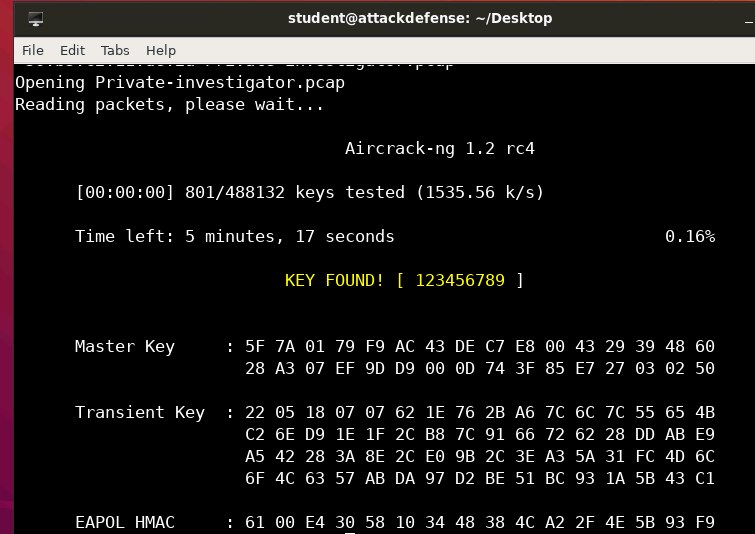
Solution.

Decrypted WiFi traffic is needed. And, the key is not known, use aircrack-ng to figure out the

passphrase using given dictionary.

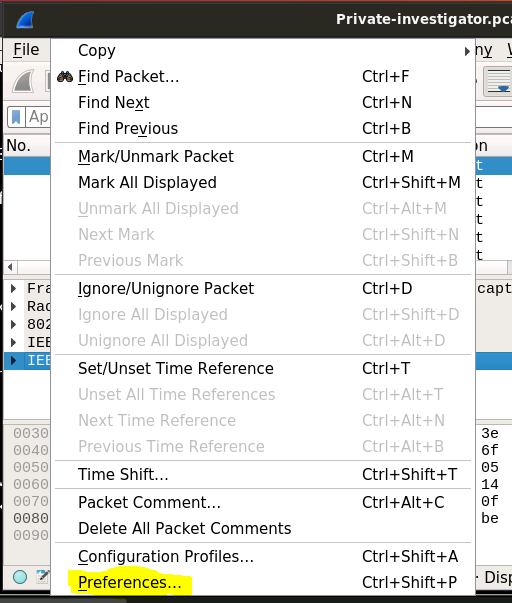
So after navigating my way to the desktop ran the Command: aircrack-ng -w 1000000-password-seclists.txt -b 30:b5:c2:11:de:2a Private-investigator.pcap



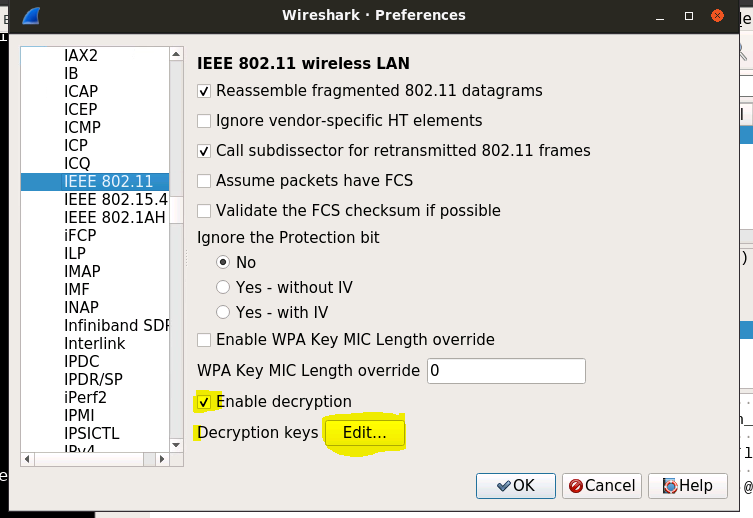


Found the pass key and processed to decrypt the traffic using passphrase. Add the WiFi network details to wireshark as shown below:

Open Edit > Preferences



From protocols, select IEEE802.11. 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

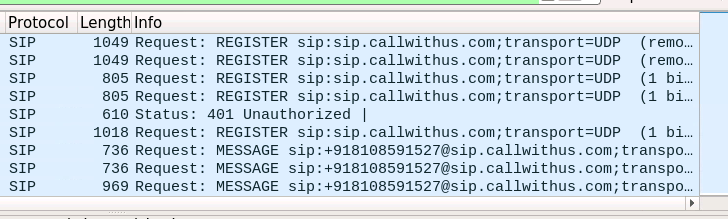


On saving the keys and closing the pop up, the traffic was decrypted. Once the traffic is

Decrypted, I looked for commonly used communication protocols e.g. imap, pop, sip, irc

Filter: imap || pop || sip || irc

SIP traffic is present.



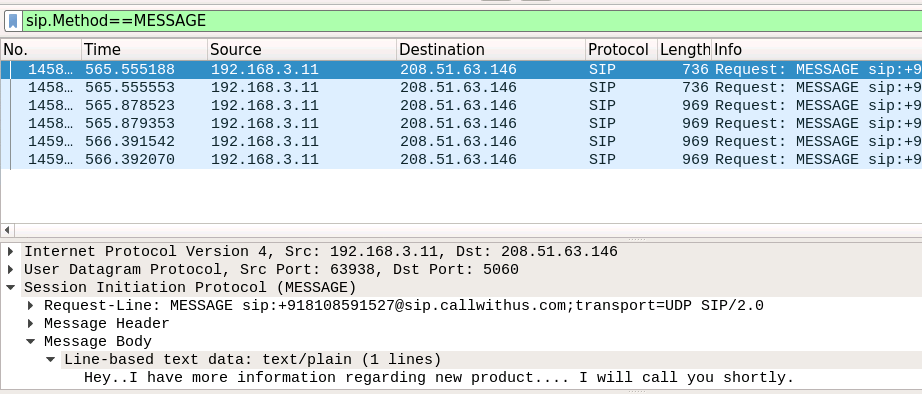
**Answer 1**: He is sending SMS (and tried to call) using VoIP service using his home WiFi.

**Question 2**: What content did you recovered from the communication intercepted (if any)?

Solution

Apllying the filter: sip.Method==MESSAGE

We can extract SIP messages from the traffic which revelled



**Answer 2**: He sent the following message other party’s cell phone.

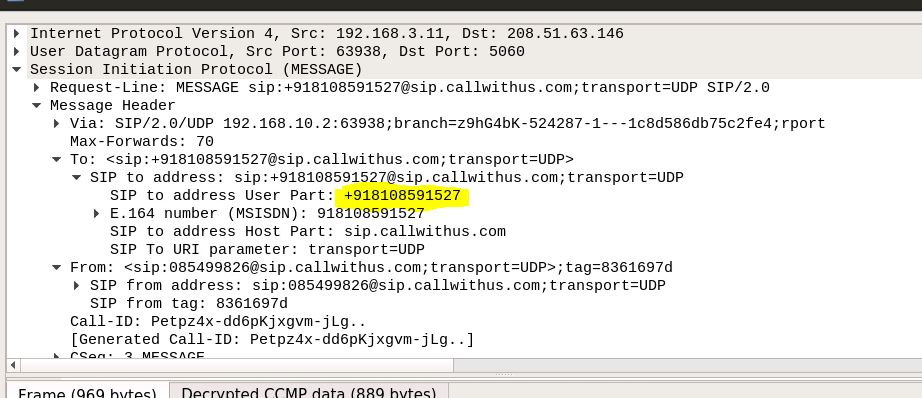
“Hey..I have more information regarding new product ….I will call you shortly.”

**Question 3**: Any contact information of the other party (if any)?

Solution

To check for contact number of the recipient, we further examine the sip traffic by applying the filter: sip.Method==MESSAGE

Which revielled the following

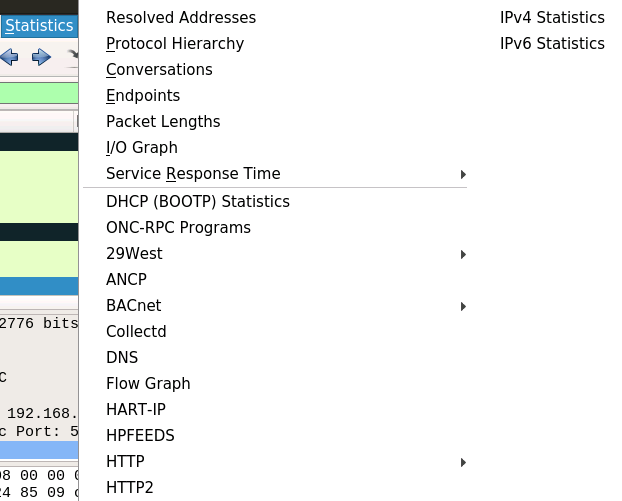


**Answer:** The cell number of other party: +91-8108591527. This number is from India.

**Question 4**: Anything interesting that you observed during the analysis to shed light on his

other motives?

Solution

Check his browsing activity by going to the statistics tab and checking his http GET requests



Answer: He is researching a lot of spy gadgets from the result below. He may be planning to spy on company’s

other employees and steal more information to sell

