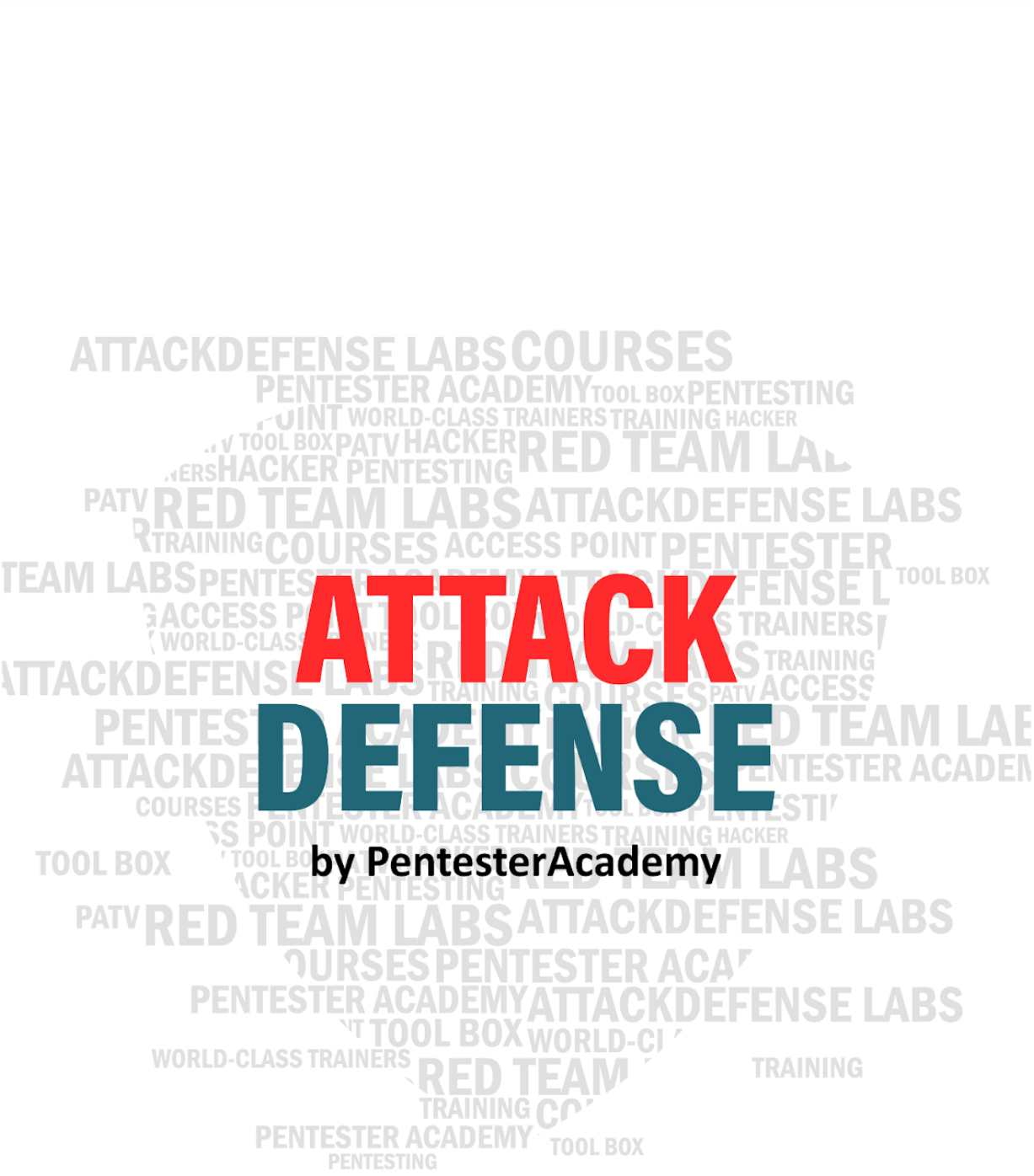

ATTACK
DEFENSE
by PentesterAcademy

Name	Private Investigator
URL	https://www.attackdefense.com/challengedetails?cid=71
Type	Forensics : WiFi

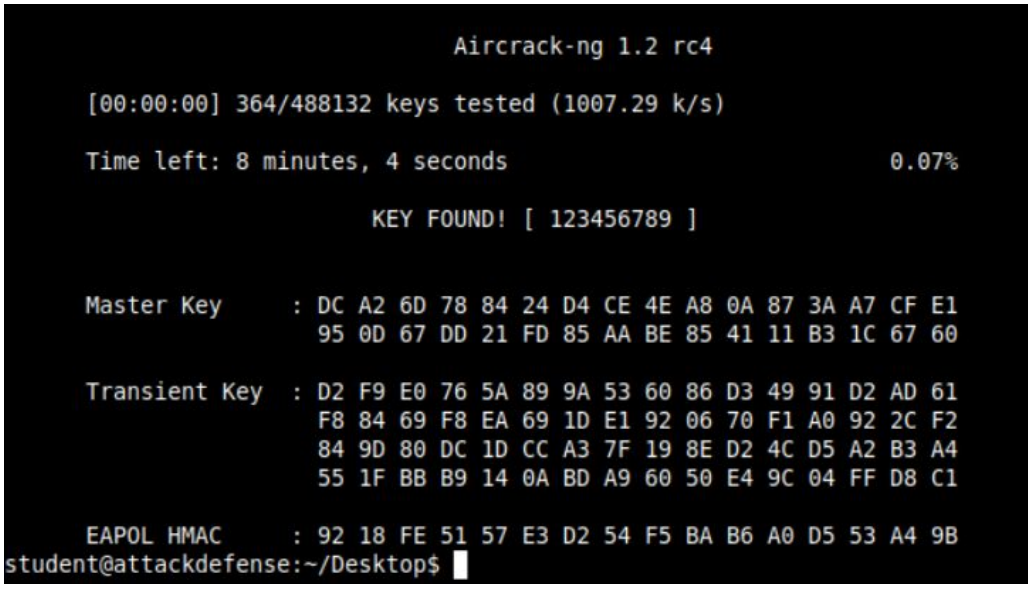
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Question 1: How he is communicating with the other party?

Solution:

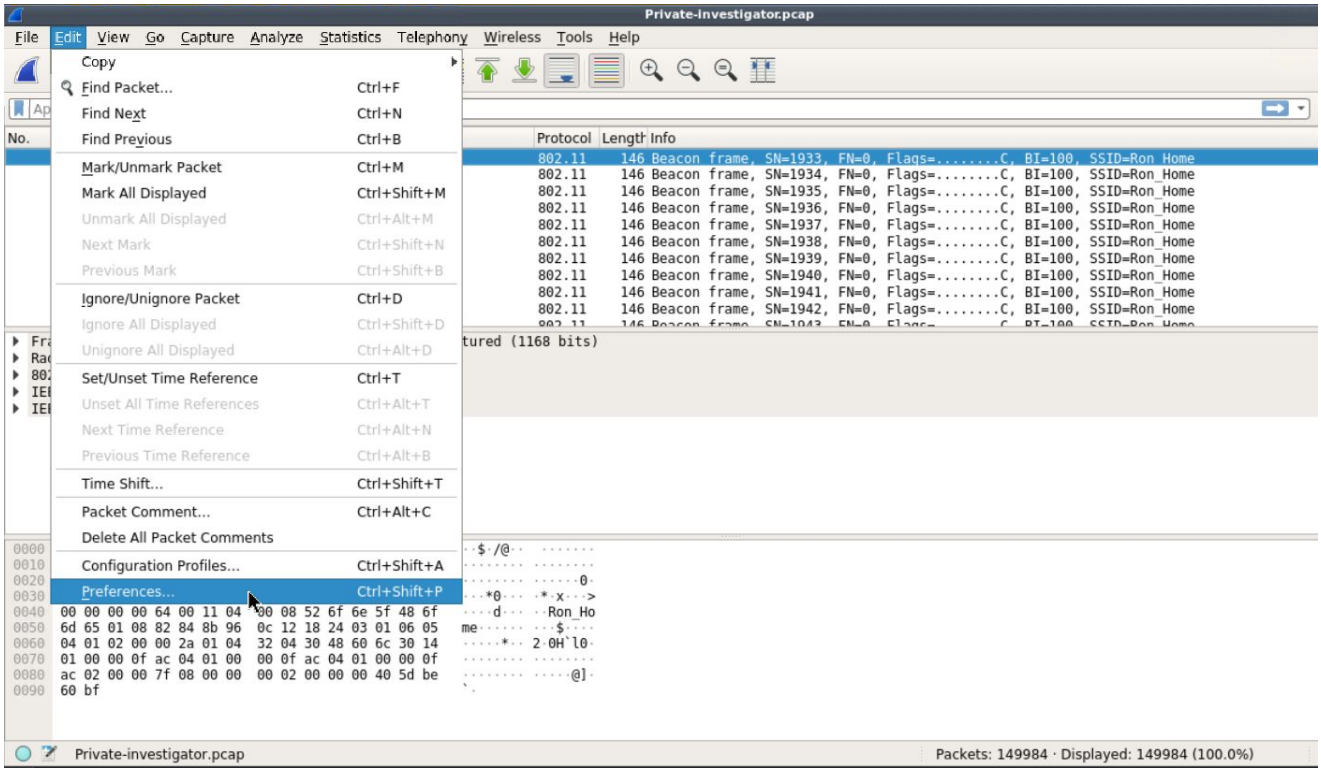
Decrypted WiFi traffic is needed. And, the key is not known, use aircrack-ng to figure out the passphrase using given dictionary.

Command: aircrack-ng -w 1000000-password-seclists.txt -b 30:b5:c2:11:de:2a Private-investigator.pcap

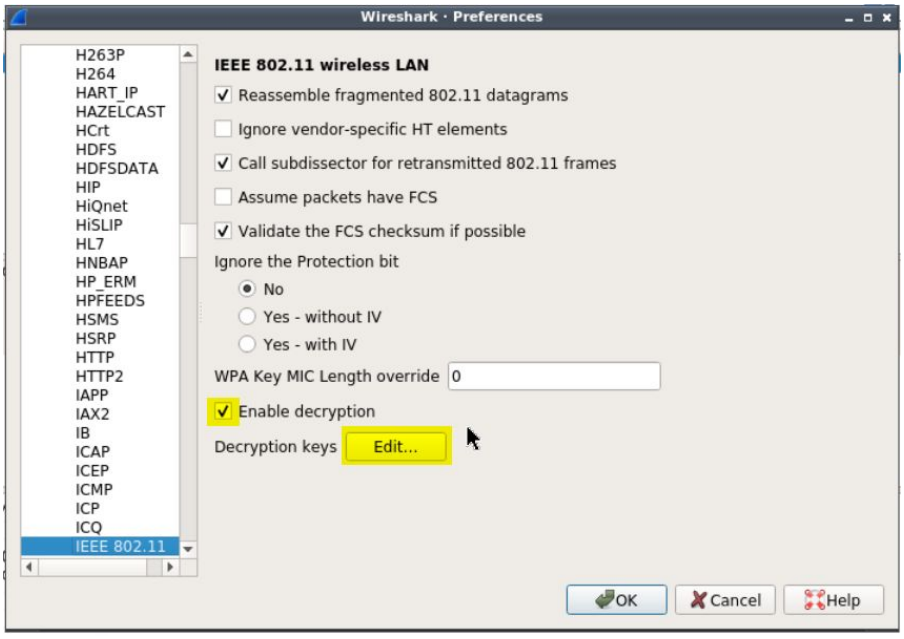


Decrypt the traffic using passphrase. Add the WiFi network details to wireshark as shown below:

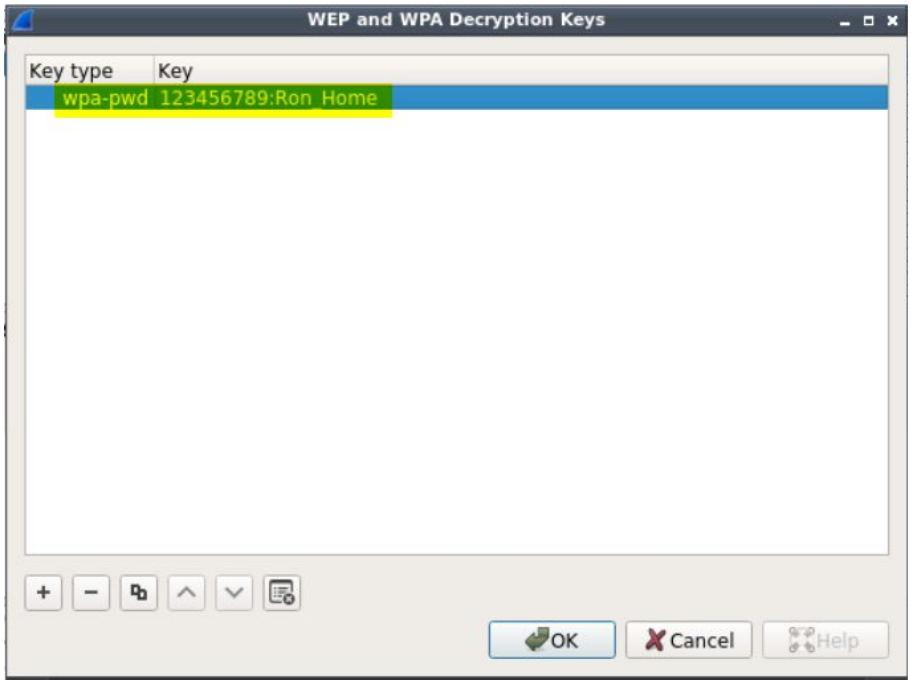
Open Edit > Preferences



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



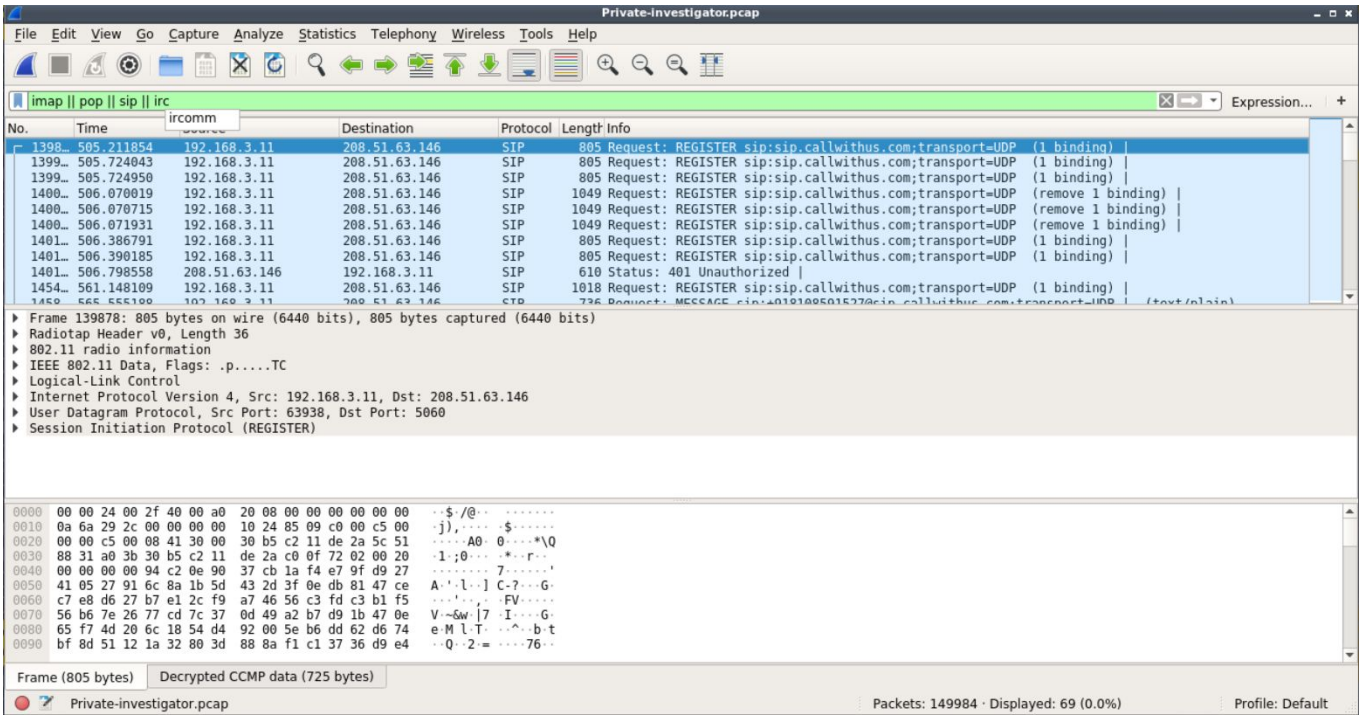
The record is added in the following format <Shared_sercet>:<SSID_name>. WPA-PWD denotes WPA secret passphrase.



On saving the keys and closing the pop up, the traffic will be decrypted. Once the traffic is decrypted, look for commonly used communication protocols e.g. imap, pop, sip, irc

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

SIP traffic is present. Try to understand the activity.



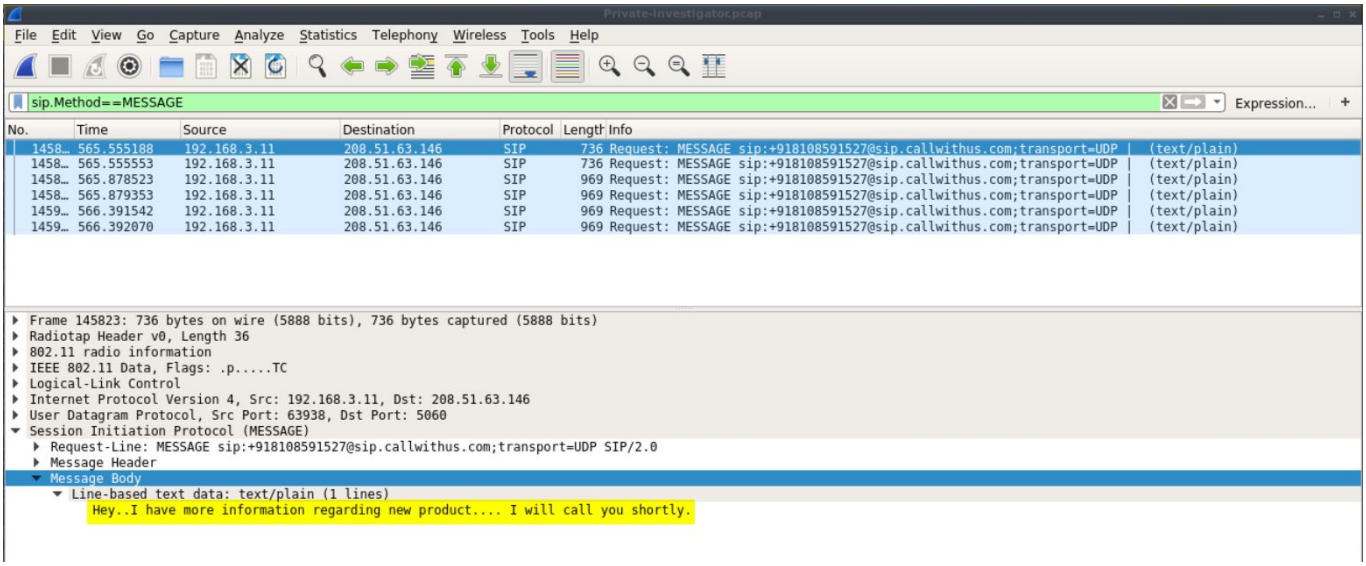
Answer: He is sending SMS (and tried to call) using VoIP service using his home WiFi.

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

Solution

We can extract SIP messages from the traffic.

Filter: sip.Method==MESSAGE



Answer: He sent the following message other party's cell phone.

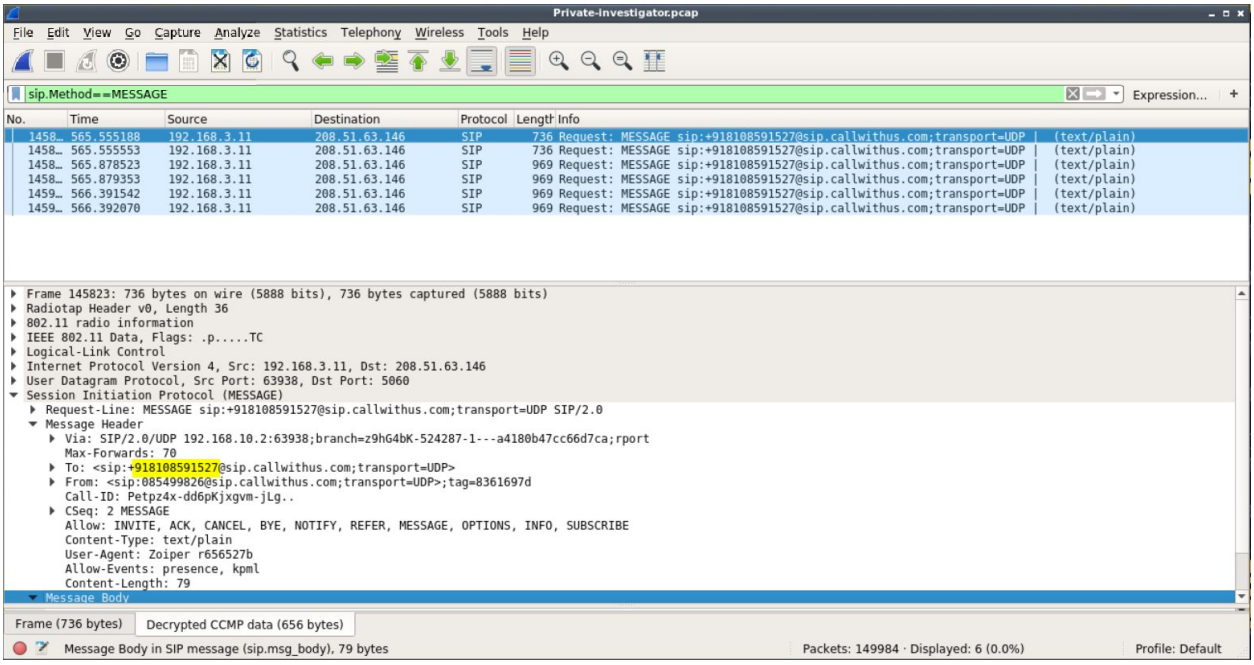
"Hey..I have more information regarding new product ….I will call you shortly."

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

Solution

Check contact number of the recipient

Filter: sip.Method==MESSAGE



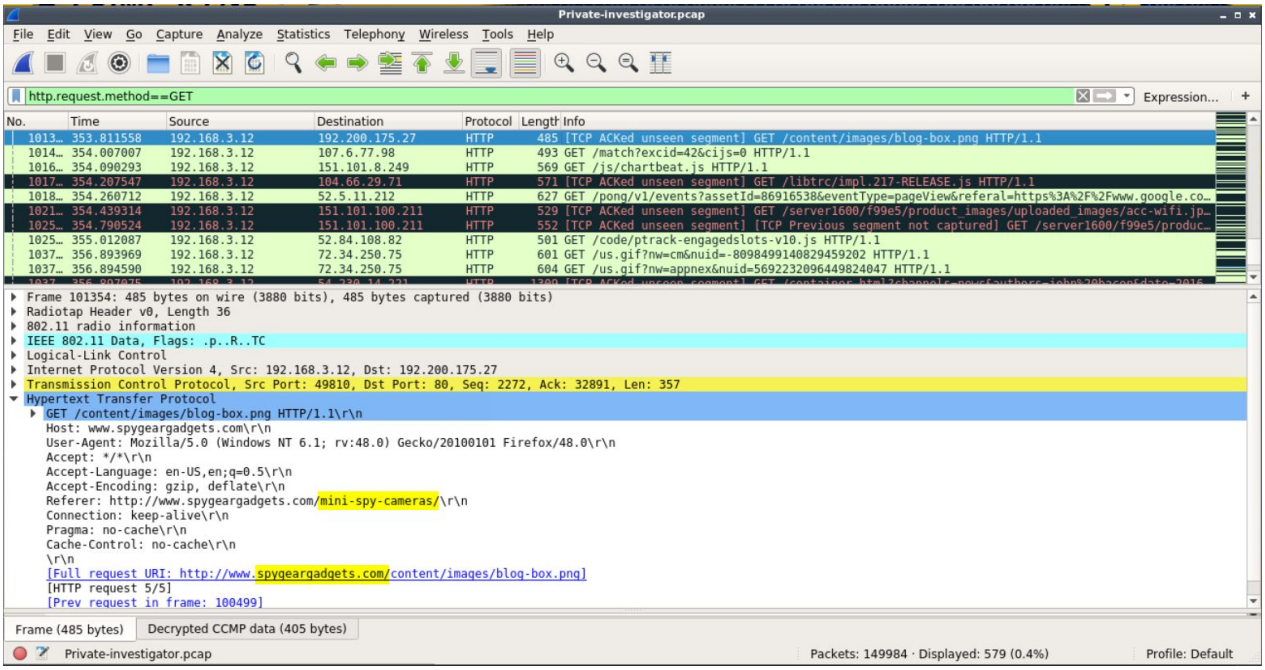
Answer: The cell number of other party: +91-8108591527. This number is from India.

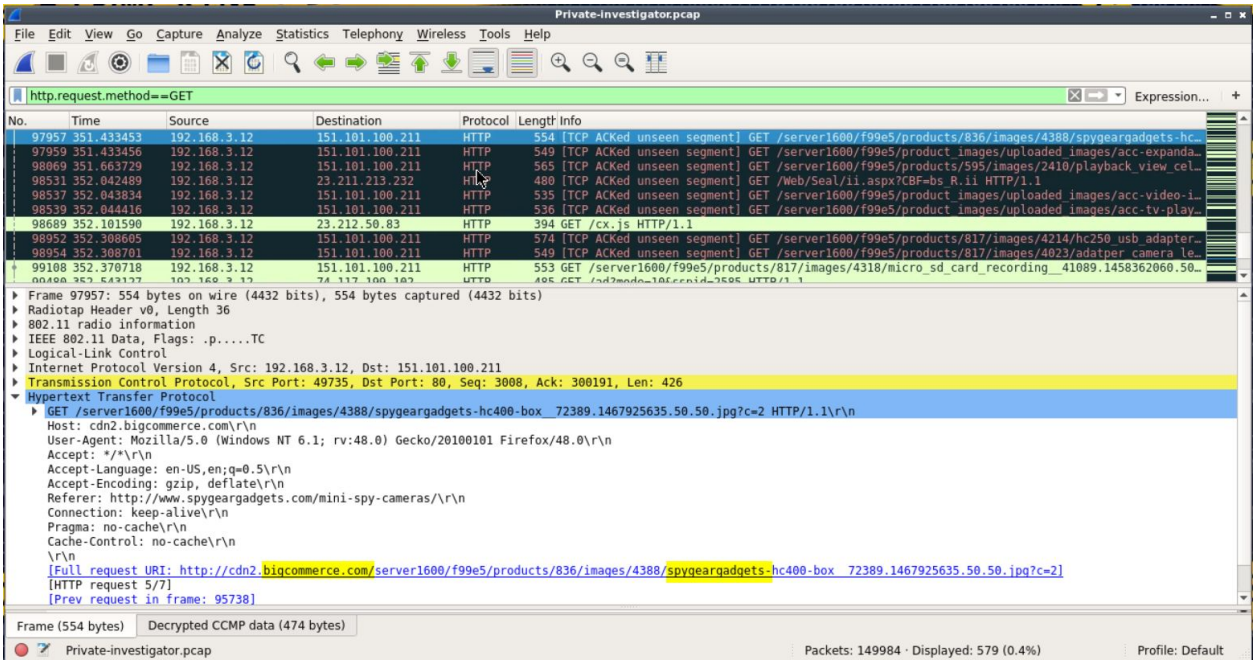
Question 4: Anything interesting that you observed during the analysis to shed light on his other motives?

Solution

Check his browsing activity by dumping the GET request URLs into a file.

Filter: http.request.method==GET





Answer: He is researching a lot of spy gadgets. He may be planning to spy on company's other employees and steal more information to sell.