

[illegible]

| | |
|-------------|---|
| 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

```
Aircrack-ng 1.2 rc4

[00:00:00] 364/488132 keys tested (1007.29 k/s)

Time left: 8 minutes, 4 seconds                                0.07%

KEY FOUND! [ 123456789 ]

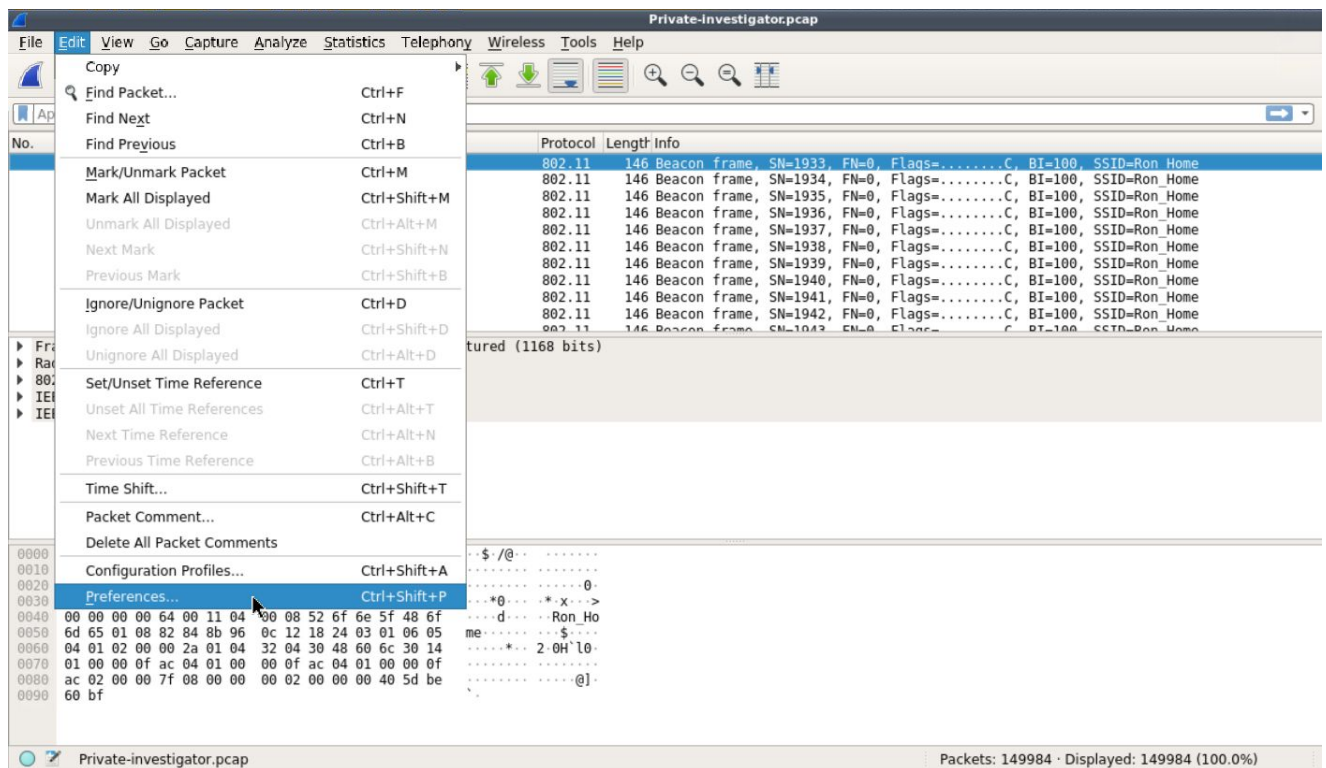
Master Key      : DC A2 6D 78 84 24 D4 CE 4E A8 0A 87 3A A7 CF E1
                  95 0D 67 DD 21 FD 85 AA BE 85 41 11 B3 1C 67 60

Transient Key   : D2 F9 E0 76 5A 89 9A 53 60 86 D3 49 91 D2 AD 61
                  F8 84 69 F8 EA 69 1D E1 92 06 70 F1 A0 92 2C F2
                  84 9D 80 DC 1D CC A3 7F 19 8E D2 4C D5 A2 B3 A4
                  55 1F BB B9 14 0A BD A9 60 50 E4 9C 04 FF D8 C1

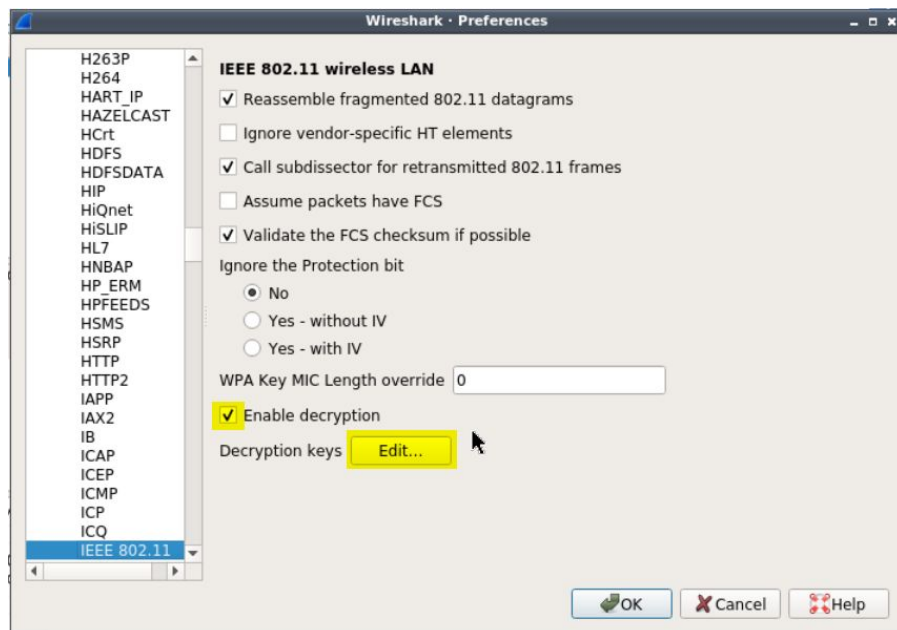
EAPOL HMAC     : 92 18 FE 51 57 E3 D2 54 F5 BA B6 A0 D5 53 A4 9B
student@attackdefense:~/Desktop$
```

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

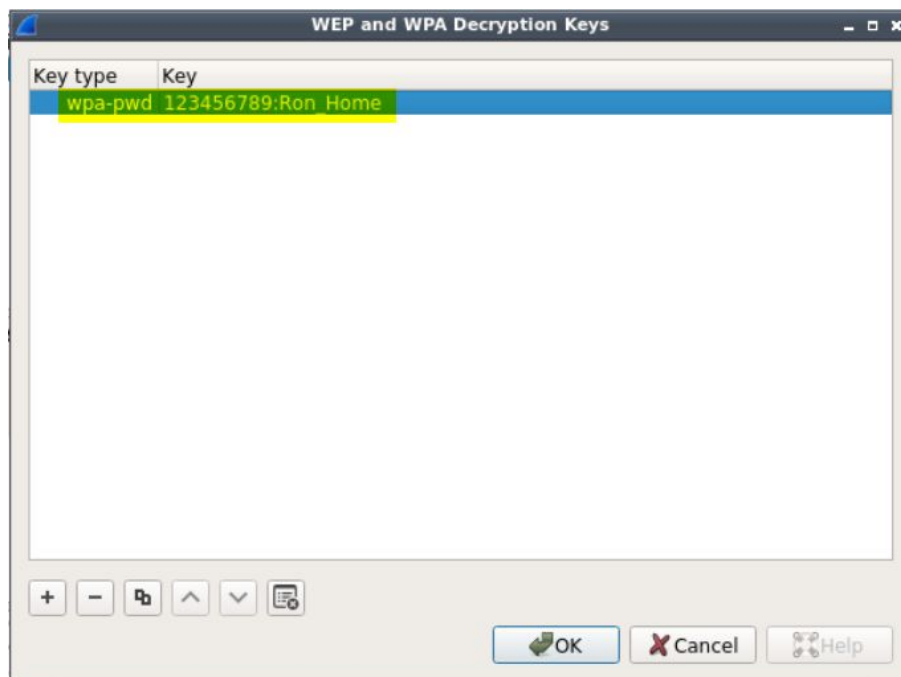
Open Edit > Preferences



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



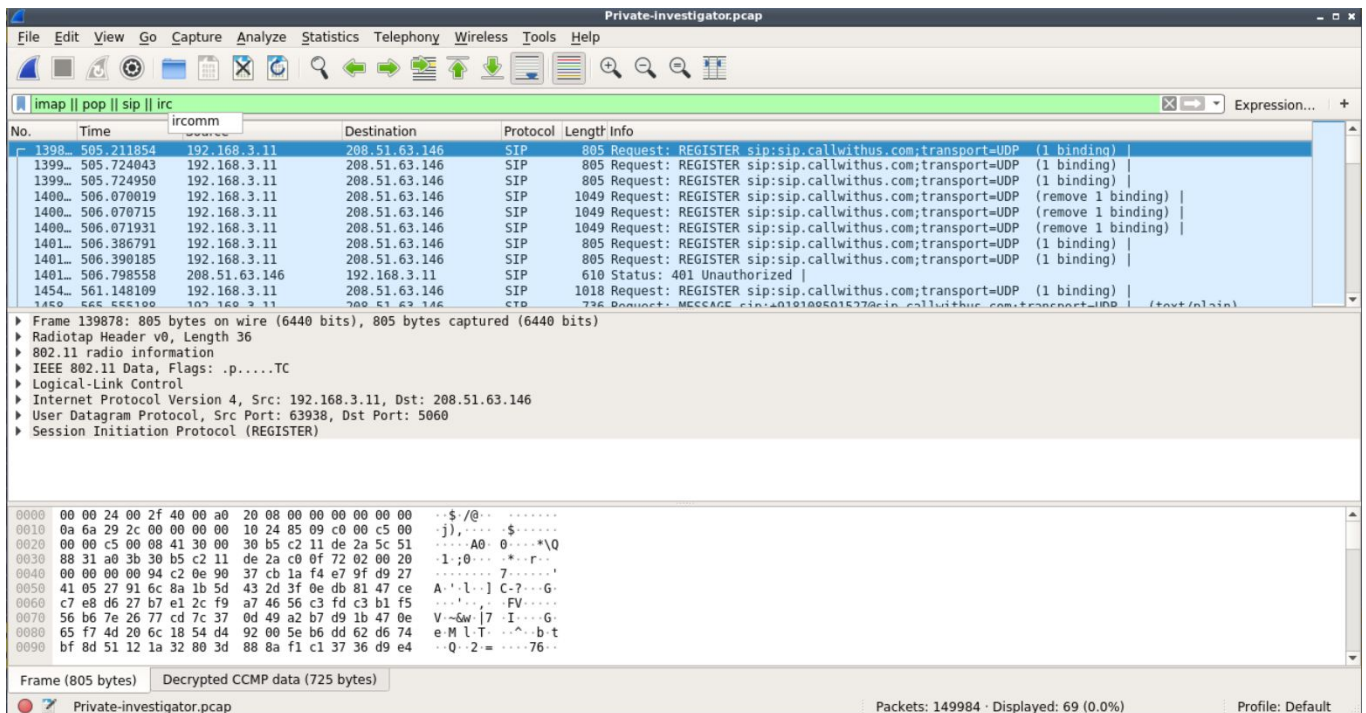
The record is added in the following format <Shared_secret>:<SSID_name>. WPA-PWD denotes WPA secret passphrase.



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.



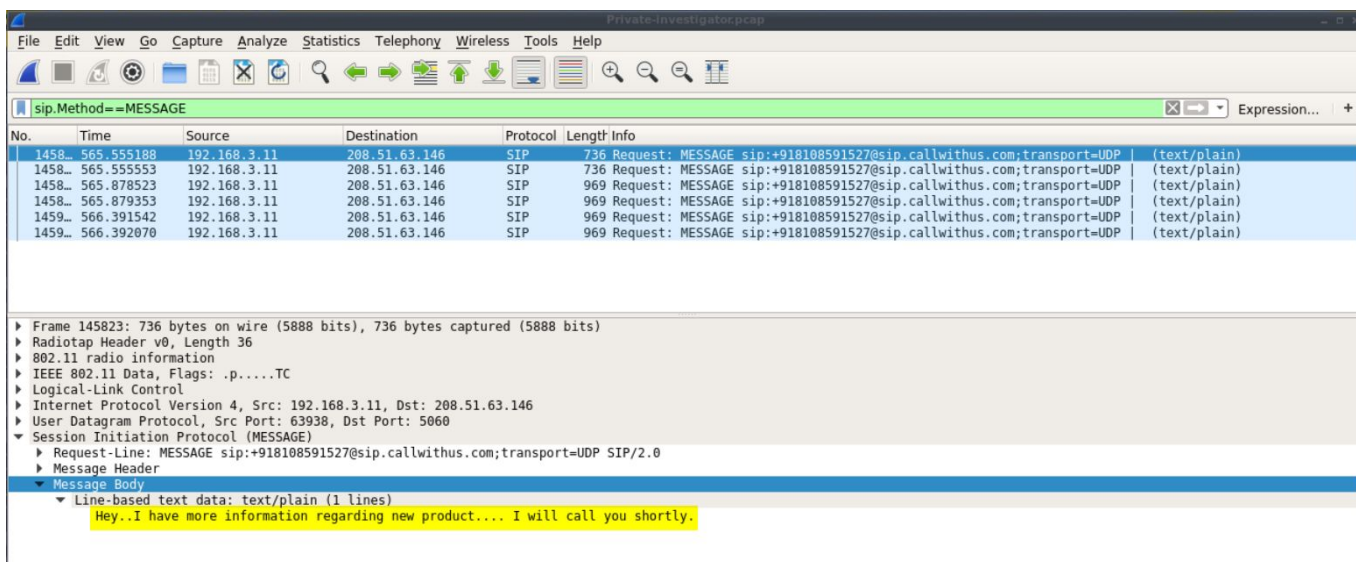
Answer: He is sending SMS (and tried to call) using VoIP service using his home WiFi.

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.

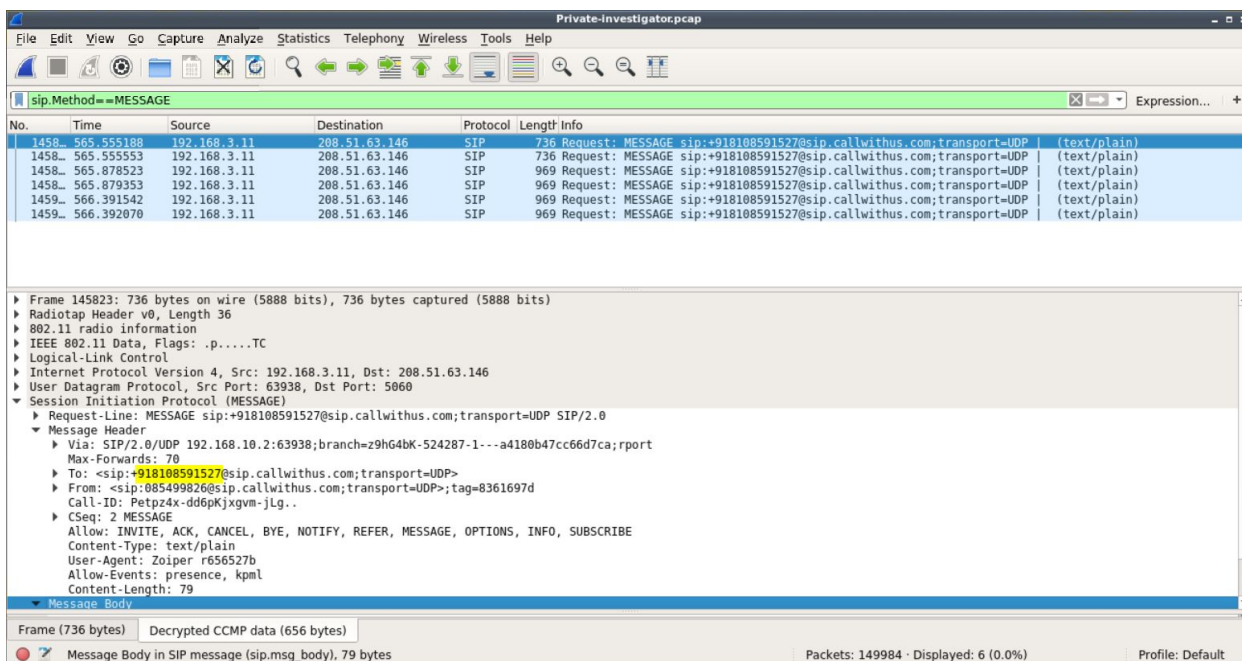
"Hey..I have more information regarding new productI will call you shortly."

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

Private-Investigator.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method==GET

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|--------------|-----------------|----------|--------|---|
| 1013 | 353.811558 | 192.168.3.12 | 192.200.175.27 | HTTP | 485 | [TCP ACKed unseen segment] GET /content/images/blog-box.png HTTP/1.1 |
| 1014 | 354.007007 | 192.168.3.12 | 107.6.77.98 | HTTP | 493 | GET /match?excid=42&cjs=0 HTTP/1.1 |
| 1016 | 354.090293 | 192.168.3.12 | 151.101.8.249 | HTTP | 569 | GET /js/chartbeat.js HTTP/1.1 |
| 1017 | 354.207547 | 192.168.3.12 | 104.66.29.71 | HTTP | 571 | [TCP ACKed unseen segment] GET /libtrc/impl.217-RELEASE.js HTTP/1.1 |
| 1018 | 354.260712 | 192.168.3.12 | 52.5.11.212 | HTTP | 627 | GET /pong/v1/events?assetId=86916538&eventType=pageView&referral=https%3A%2F%2Fwww.google.co... |
| 1021 | 354.439314 | 192.168.3.12 | 151.101.100.211 | HTTP | 529 | [TCP ACKed unseen segment] GET /server1600/f99e5/product_images/uploaded_images/acc-wifi1.jp... |
| 1025 | 354.790524 | 192.168.3.12 | 151.101.100.211 | HTTP | 552 | [TCP ACKed unseen segment] [TCP Previous segment not captured] GET /server1600/f99e5/produ... |
| 1025 | 355.012087 | 192.168.3.12 | 52.84.108.82 | HTTP | 501 | GET /code/ptrack-engagedslots-v10.js HTTP/1.1 |
| 1037 | 356.893969 | 192.168.3.12 | 72.34.250.75 | HTTP | 601 | GET /us.gif?mw=cn6nuId=-8098499140829459202 HTTP/1.1 |
| 1037 | 356.894590 | 192.168.3.12 | 72.34.250.75 | HTTP | 604 | GET /us.gif?mw=appnex&nuId=5692232096449824047 HTTP/1.1 |

Frame 101354: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits)

Radiotap Header v0, Length 36

802.11 radio information

IEEE 802.11 Data, Flags: .p..R..TC

Logical-Link Control

Internet Protocol Version 4, Src: 192.168.3.12, Dst: 192.200.175.27

Transmission Control Protocol, Src Port: 49810, Dst Port: 80, Seq: 2272, Ack: 32891, Len: 357

Hypertext Transfer Protocol

GET /content/images/blog-box.png HTTP/1.1\r\n

Host: www.spygeargadgets.com\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:48.0) Gecko/20100101 Firefox/48.0\r\n

Accept: */*\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Referer: http://www.spygeargadgets.com/mini-spy-cameras/\r\n

Connection: keep-alive\r\n

Pragma: no-cache\r\n

Cache-Control: no-cache\r\n

\r\n

[Full request URI: http://www.spygeargadgets.com/content/images/blog-box.png]

[HTTP request 5/5]

[Prev request in frame: 100499]

Frame (485 bytes) Decrypted CCMP data (405 bytes)

Private-Investigator.pcap Packets: 149984 · Displayed: 579 (0.4%) Profile: Default

Private-Investigator.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method==GET

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|------------|--------------|-----------------|----------|--------|--|
| 97957 | 351.433453 | 192.168.3.12 | 151.101.100.211 | HTTP | 554 | [TCP ACKed unseen segment] GET /server1600/f99e5/products/836/images/4388/spygeargadgets-hc... |
| 97959 | 351.433456 | 192.168.3.12 | 151.101.100.211 | HTTP | 549 | [TCP ACKed unseen segment] GET /server1600/f99e5/product_images/uploaded_images/acc-expanda... |
| 98069 | 351.663729 | 192.168.3.12 | 151.101.100.211 | HTTP | 565 | [TCP ACKed unseen segment] GET /server1600/f99e5/products/595/images/2410/playback_view_ce... |
| 98531 | 352.042400 | 192.168.3.12 | 23.211.213.232 | HTTP | 480 | [TCP ACKed unseen segment] GET /Web/SeaVuln.aspx?CBP=bs R.11 HTTP/1.1 |
| 98537 | 352.043834 | 192.168.3.12 | 151.101.100.211 | HTTP | 535 | [TCP ACKed unseen segment] GET /server1600/f99e5/product_images/uploaded_images/acc-video-i... |
| 98539 | 352.044416 | 192.168.3.12 | 151.101.100.211 | HTTP | 536 | [TCP ACKed unseen segment] GET /server1600/f99e5/product_images/uploaded_images/acc-tv-play... |
| 98689 | 352.101590 | 192.168.3.12 | 23.212.50.83 | HTTP | 394 | GET /cx.js HTTP/1.1 |
| 98952 | 352.308605 | 192.168.3.12 | 151.101.100.211 | HTTP | 574 | [TCP ACKed unseen segment] GET /server1600/f99e5/products/817/images/4214/hc250_usb_adapter... |
| 98954 | 352.308701 | 192.168.3.12 | 151.101.100.211 | HTTP | 549 | [TCP ACKed unseen segment] GET /server1600/f99e5/products/817/images/4023/adatper_camera le... |
| 99108 | 352.370718 | 192.168.3.12 | 151.101.100.211 | HTTP | 553 | GET /server1600/f99e5/products/817/images/4318/micro_sd_card_recording_41089.1458362060.50... |

Frame 97957: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits)

Radiotap Header v0, Length 36

802.11 radio information

IEEE 802.11 Data, Flags: .p.....TC

Logical-Link Control

Internet Protocol Version 4, Src: 192.168.3.12, Dst: 151.101.100.211

Transmission Control Protocol, Src Port: 49735, Dst Port: 80, Seq: 3008, Ack: 300191, Len: 426

Hypertext Transfer Protocol

GET /server1600/f99e5/products/836/images/4388/spygeargadgets-hc400-box_72389.1467925635.50.50.jpg?c=2 HTTP/1.1\r\n

Host: cdn2.bigcommerce.com\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:48.0) Gecko/20100101 Firefox/48.0\r\n

Accept: */*\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Referer: http://www.spygeargadgets.com/mini-spy-cameras/\r\n

Connection: keep-alive\r\n

Pragma: no-cache\r\n

Cache-Control: no-cache\r\n

\r\n

[Full request URI: http://cdn2.bigcommerce.com/server1600/f99e5/products/836/images/4388/spygeargadgets-hc400-box_72389.1467925635.50.50.jpg?c=2]

[HTTP request 5/7]

[Prev request in frame: 95738]

Frame (554 bytes) Decrypted CCMP data (474 bytes)

Private-Investigator.pcap Packets: 149984 · Displayed: 579 (0.4%) Profile: Default

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.