University of Dhaka

Department of Computer Science and Engineering

CSE-4282: Cryptography and Network Security Lab

Lab09: Network Trace analysis and Attacks: First Part2

Submitted by:

Kamrul Hasan (36)

Suddipta Deb Nath(52)

1. Introduction

In assignment 9, we are given a packet capture file, 4 email attachments and a capture of WPA traffic. Using email attachments and the first pcap file we have to find out detail information about a potential attack that infected a computer. From the screenshot of Microsoft outlook, we assumed that the infected computer operating system is windows. And we have to decrypt the WPA traffic file too.

2. Packet Analysis

We opened email attachments with thunderbird and downloaded the attachments they contain and they are listed below:

1. dawning wall up.zip which contains 460630672421.exe

2. Bill Payment_000010818.xls

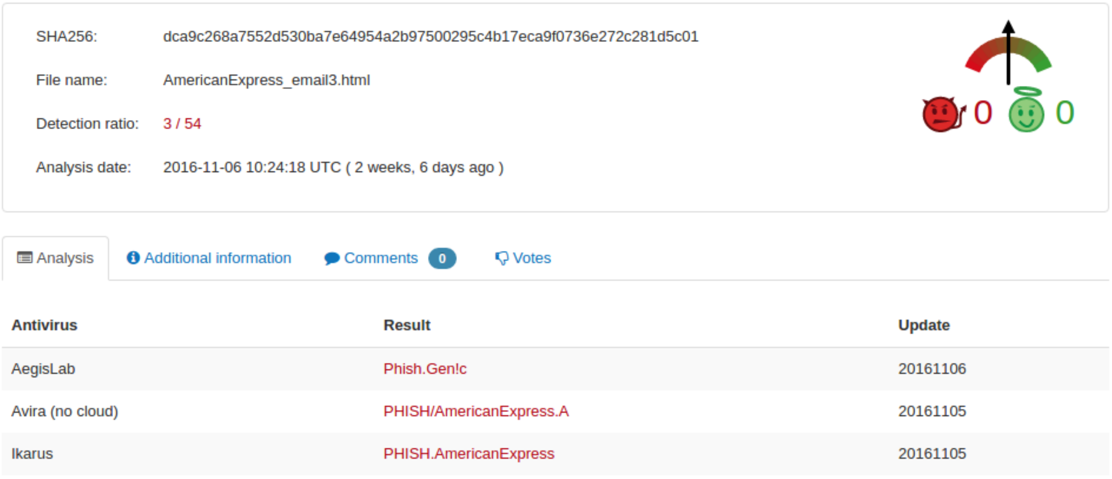
3. AmericanExpress.html

4. fax000497762.zip which contains fax000497762.doc.js

We analyzed all attachments using hybrid-analysis.com and download pcap files to find out which email opened.

3. Finding which email has been opened

First, we open the given pcap file and then we compare downloaded pcap files. We didn’t compare the pcap file that we found from AmericanExpress.html. Because from virus total results we see this mail doesn’t contain any malicious contents that can attack a windows computer. Therefore, third mail is not our desired mail.



SHA256: dca9c268a7552d530ba7e64954a2b97500295c4b17eca9f0736e272c281d5c01

File name: AmericanExpress_email3.html

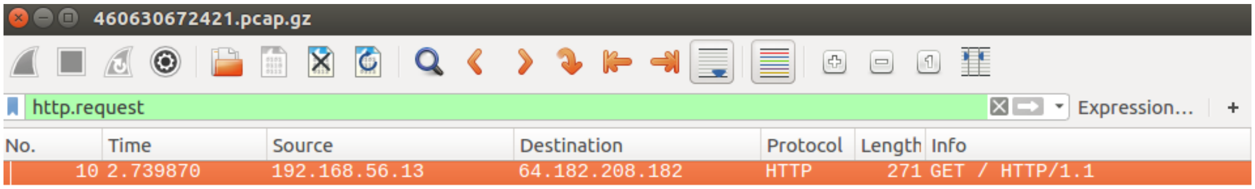
Detection ratio: 3 / 54

Analysis date: 2016-11-06 10:24:18 UTC (2 weeks, 6 days ago)

Antivirus	Result	Update
AegisLab	Phish.Gen!c	20161106
Avira (no cloud)	PHISH/AmericanExpress.A	20161105
Ikarus	PHISH.AmericanExpress	20161105

Figure 1:email

From the first mail virustotal website gave result that it has some malicious content. So we downloaded the pcap file we found this



460630672421.pcap.gz

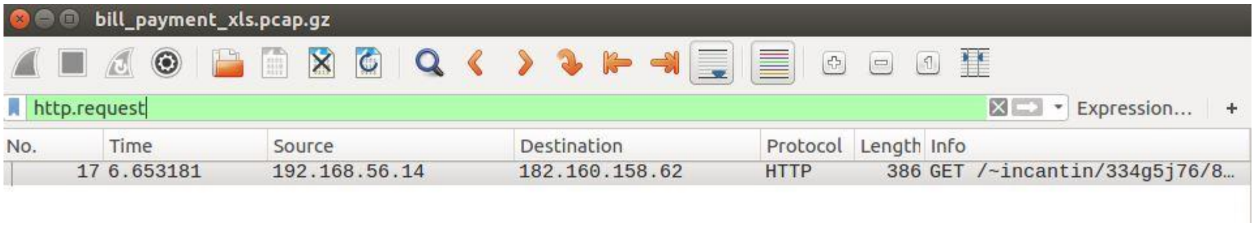
http.request

```
No.    Time        Source           Destination      Protocol  Length  Info
    10 2.739870    192.168.56.13    64.182.208.182   HTTP         271 GET / HTTP/1.1
```

Figure 2

But it did not match with the given file.

For the second mail attachment named Bill Payment_000010818.xls, we downloaded the pcap file and found this



bill_payment_xls.pcap.gz

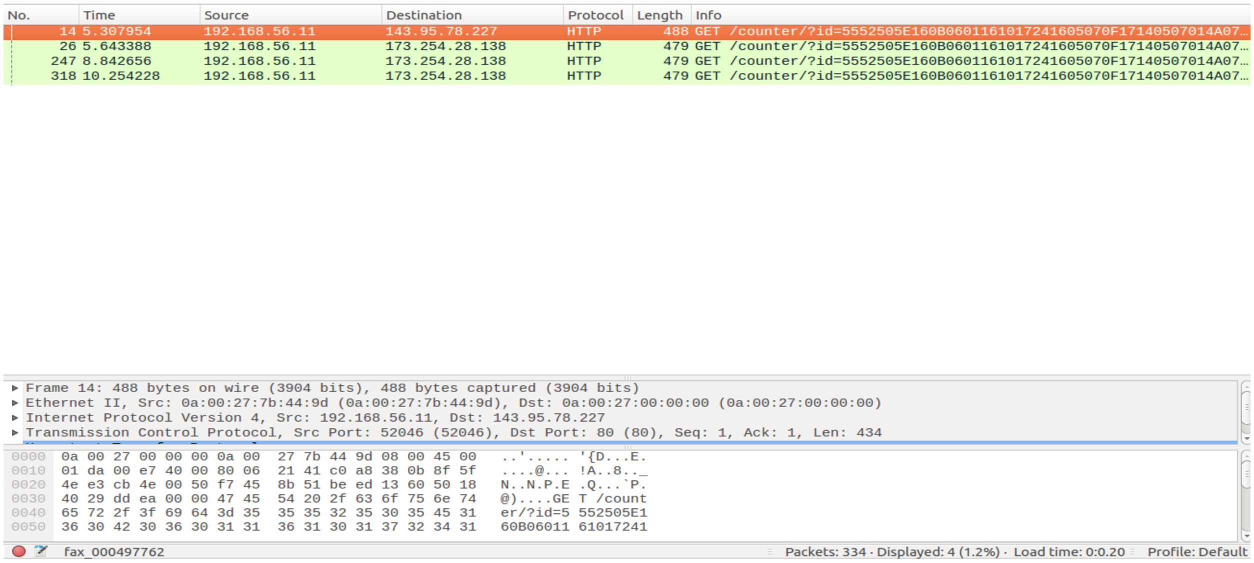
http.request

```
No.    Time        Source           Destination      Protocol  Length  Info
    17 6.653181    192.168.56.14    182.160.158.62   HTTP         386 GET /~incantin/334g5j76/8…
```

Figure 3

But we did not find any match with our original packet capture.

For the fourth mail attachment fax000497762.doc.js we downloaded the pcap file and found this



```
No.   Time       Source          Destination      Protocol Length Info
   14 5.307954   192.168.56.11   143.95.78.227    HTTP       488 GET /counter/?id=5552505E160B0601161017241605070F17140507014A07…
   26 5.643388   192.168.56.11   173.254.28.138   HTTP       479 GET /counter/?id=5552505E160B0601161017241605070F17140507014A07…
  247 8.842656   192.168.56.11   173.254.28.138   HTTP       479 GET /counter/?id=5552505E160B0601161017241605070F17140507014A07…
  318 10.254228  192.168.56.11   173.254.28.138   HTTP       479 GET /counter/?id=5552505E160B0601161017241605070F17140507014A07…
```

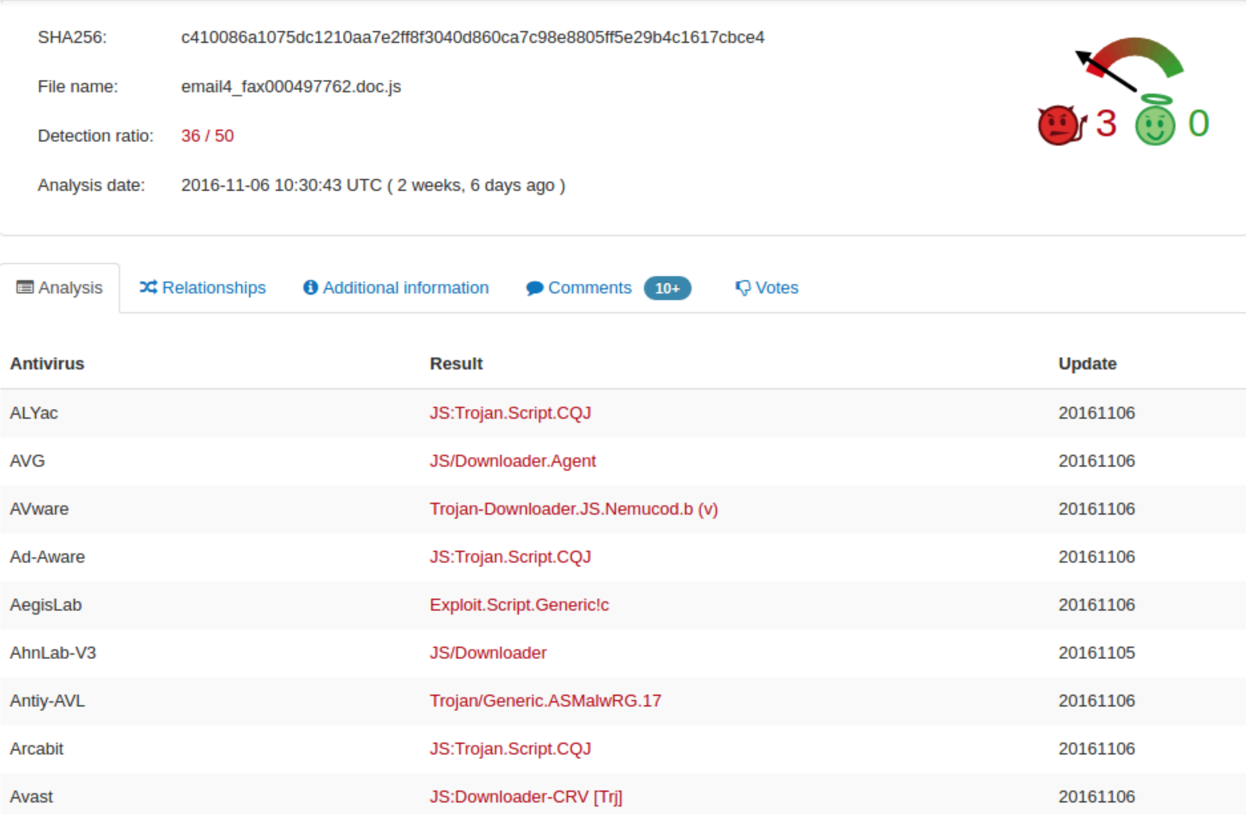
```
▸ Frame 14: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits)
▸ Ethernet II, Src: 0a:00:27:7b:44:9d (0a:00:27:7b:44:9d), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)
▸ Internet Protocol Version 4, Src: 192.168.56.11, Dst: 143.95.78.227
▸ Transmission Control Protocol, Src Port: 52046 (52046), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 434
```

```
0000  0a 00 27 00 00 00 0a 00  27 7b 44 9d 08 00 45 00   ..'..... '{D...E.
0010  01 da 00 e7 40 00 80 06  21 41 c0 a8 38 0b 8f 5f   ....@... !A..8.._
0020  4e e3 cb 4e 00 50 f7 45  8b 51 be ed 13 60 50 18   N..N.P.E .Q...`P.
0030  40 29 dd ea 00 00 47 45  54 20 2f 63 6f 75 6e 74   @)....GE T /count
0040  65 72 2f 3f 69 64 3d 35  35 35 32 35 30 35 45 31   er/?id=5 552505E1
0050  36 30 42 30 36 30 31 31  36 31 30 31 37 32 34 31   60B06011 61017241
```

fax_000497762 — Packets: 334 · Displayed: 4 (1.2%) · Load time: 0:0.20 — Profile: Default

Figure 4

And we found match with our original pcap file. So, we can assume that this mail has been opened and from virustotal.com we see this mail contains lots of potential threat.



SHA256: c410086a1075dc1210aa7e2ff8f3040d860ca7c98e8805ff5e29b4c1617cbce4

File name: email4_fax000497762.doc.js

Detection ratio: 36 / 50

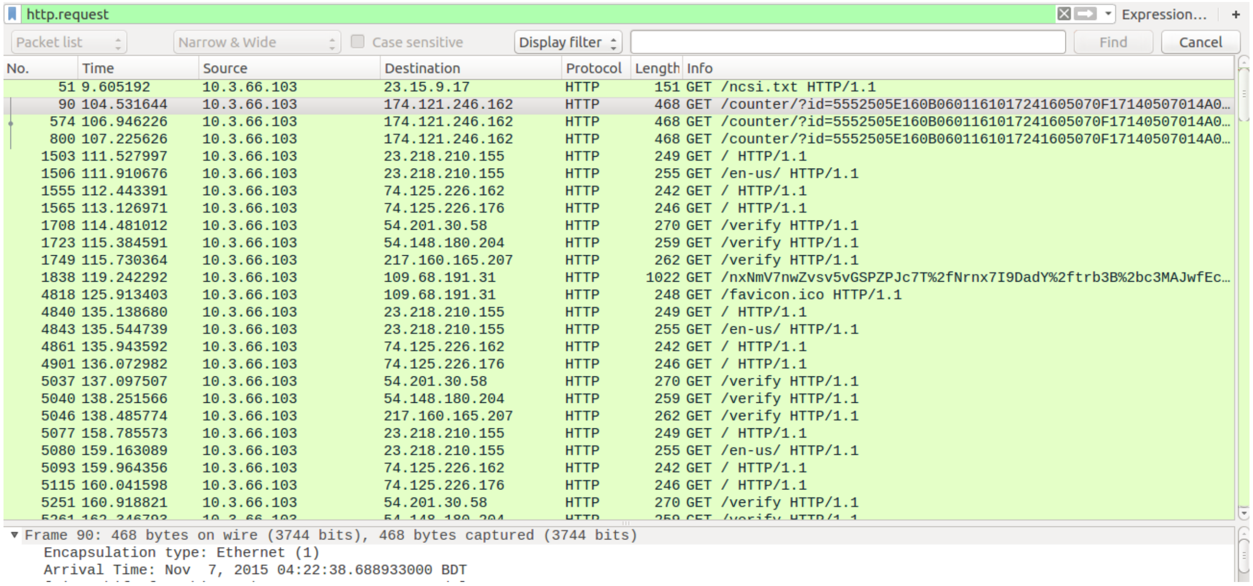
Analysis date: 2016-11-06 10:30:43 UTC (2 weeks, 6 days ago)

Antivirus	Result	Update
ALYac	JS:Trojan.Script.CQJ	20161106
AVG	JS/Downloader.Agent	20161106
AVware	Trojan-Downloader.JS.Nemucod.b (v)	20161106
Ad-Aware	JS:Trojan.Script.CQJ	20161106
AegisLab	Exploit.Script.Generic!c	20161106
AhnLab-V3	JS/Downloader	20161105
Antiy-AVL	Trojan/Generic.ASMalwRG.17	20161106
Arcabit	JS:Trojan.Script.CQJ	20161106
Avast	JS:Downloader-CRV [Trj]	20161106

Figure 5

4. Desired information

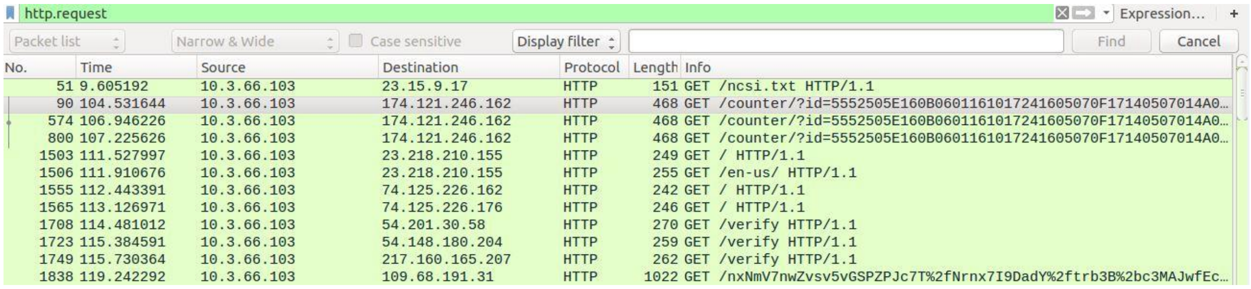
4.1 Date and approximate time of the infection: Nov 7, 2015 , 04:22:30 BDT



```
No.   Time        Source        Destination      Protocol Length Info
   51 9.605192    10.3.66.103   23.15.9.17       HTTP      151 GET /ncsi.txt HTTP/1.1
   90 104.531644  10.3.66.103   174.121.246.162  HTTP      468 GET /counter/?id=5552505E160B0601161017241605070F17140507014A0…
  574 106.946226  10.3.66.103   174.121.246.162  HTTP      468 GET /counter/?id=5552505E160B0601161017241605070F17140507014A0…
  800 107.225626  10.3.66.103   174.121.246.162  HTTP      468 GET /counter/?id=5552505E160B0601161017241605070F17140507014A0…
 1503 111.527997  10.3.66.103   23.218.210.155   HTTP      249 GET / HTTP/1.1
 1506 111.910676  10.3.66.103   23.218.210.155   HTTP      255 GET /en-us/ HTTP/1.1
 1555 112.443391  10.3.66.103   74.125.226.162   HTTP      242 GET / HTTP/1.1
 1565 113.126971  10.3.66.103   74.125.226.176   HTTP      246 GET / HTTP/1.1
 1708 114.481012  10.3.66.103   54.201.30.58     HTTP      270 GET /verify HTTP/1.1
 1723 115.384591  10.3.66.103   54.148.180.204   HTTP      259 GET /verify HTTP/1.1
 1749 115.730364  10.3.66.103   217.160.165.207  HTTP      262 GET /verify HTTP/1.1
 1838 119.242292  10.3.66.103   109.68.191.31    HTTP     1022 GET /nxNmV7nwZvsv5vGSPZPJc7T%2fNrnx7I9DadY%2ftrb3B%2bc3MAJwfEc…
 4818 125.913403  10.3.66.103   109.68.191.31    HTTP      248 GET /favicon.ico HTTP/1.1
 4840 135.138680  10.3.66.103   23.218.210.155   HTTP      249 GET / HTTP/1.1
 4843 135.544739  10.3.66.103   23.218.210.155   HTTP      255 GET /en-us/ HTTP/1.1
 4861 135.943592  10.3.66.103   74.125.226.162   HTTP      242 GET / HTTP/1.1
 4901 136.072982  10.3.66.103   74.125.226.176   HTTP      246 GET / HTTP/1.1
 5037 137.097507  10.3.66.103   54.201.30.58     HTTP      270 GET /verify HTTP/1.1
 5040 138.251566  10.3.66.103   54.148.180.204   HTTP      259 GET /verify HTTP/1.1
 5046 138.485774  10.3.66.103   217.160.165.207  HTTP      262 GET /verify HTTP/1.1
 5077 158.785573  10.3.66.103   23.218.210.155   HTTP      249 GET / HTTP/1.1
 5080 159.163089  10.3.66.103   23.218.210.155   HTTP      255 GET /en-us/ HTTP/1.1
 5093 159.964356  10.3.66.103   74.125.226.162   HTTP      242 GET / HTTP/1.1
 5115 160.041598  10.3.66.103   74.125.226.176   HTTP      246 GET / HTTP/1.1
 5251 160.918821  10.3.66.103   54.201.30.58     HTTP      270 GET /verify HTTP/1.1
 5261 162.346793  10.3.66.103   54.148.180.204   HTTP      259 GET /verify HTTP/1.1
▾ Frame 90: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov  7, 2015 04:22:38.688933000 BDT
```

Figure 6

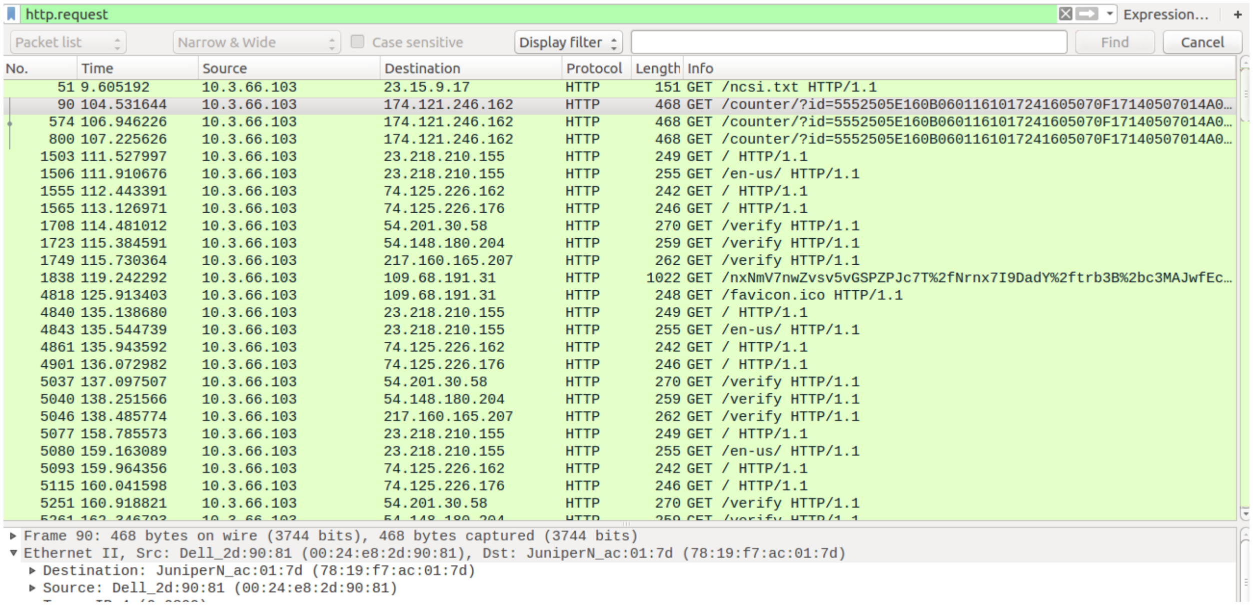
4.2. The infected computer's IP address: 10.3.66.103



```
No.   Time        Source        Destination      Protocol Length Info
   51 9.605192    10.3.66.103   23.15.9.17       HTTP      151 GET /ncsi.txt HTTP/1.1
   90 104.531644  10.3.66.103   174.121.246.162  HTTP      468 GET /counter/?id=5552505E160B0601161017241605070F17140507014A0…
  574 106.946226  10.3.66.103   174.121.246.162  HTTP      468 GET /counter/?id=5552505E160B0601161017241605070F17140507014A0…
  800 107.225626  10.3.66.103   174.121.246.162  HTTP      468 GET /counter/?id=5552505E160B0601161017241605070F17140507014A0…
 1503 111.527997  10.3.66.103   23.218.210.155   HTTP      249 GET / HTTP/1.1
 1506 111.910676  10.3.66.103   23.218.210.155   HTTP      255 GET /en-us/ HTTP/1.1
 1555 112.443391  10.3.66.103   74.125.226.162   HTTP      242 GET / HTTP/1.1
 1565 113.126971  10.3.66.103   74.125.226.176   HTTP      246 GET / HTTP/1.1
 1708 114.481012  10.3.66.103   54.201.30.58     HTTP      270 GET /verify HTTP/1.1
 1723 115.384591  10.3.66.103   54.148.180.204   HTTP      259 GET /verify HTTP/1.1
 1749 115.730364  10.3.66.103   217.160.165.207  HTTP      262 GET /verify HTTP/1.1
 1838 119.242292  10.3.66.103   109.68.191.31    HTTP     1022 GET /nxNmV7nwZvsv5vGSPZPJc7T%2fNrnx7I9DadY%2ftrb3B%2bc3MAJwfEc…
```

Figure 7

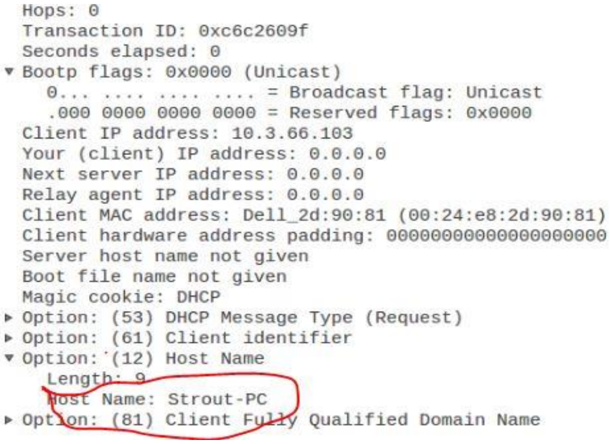
4.3 The infected computer's MAC address: 00:24:e8:2d:90:81



```
No.    Time       Source         Destination      Protocol Length Info
    51 9.605192   10.3.66.103    23.15.9.17       HTTP      151 GET /ncsi.txt HTTP/1.1
    90 104.531644 10.3.66.103    174.121.246.162  HTTP      468 GET /counter/?id=5552505E160B0601161017241605070F17140507014A0…
   574 106.946226 10.3.66.103    174.121.246.162  HTTP      468 GET /counter/?id=5552505E160B0601161017241605070F17140507014A0…
   800 107.225626 10.3.66.103    174.121.246.162  HTTP      468 GET /counter/?id=5552505E160B0601161017241605070F17140507014A0…
  1503 111.527997 10.3.66.103    23.218.210.155   HTTP      249 GET / HTTP/1.1
  1506 111.910676 10.3.66.103    23.218.210.155   HTTP      255 GET /en-us/ HTTP/1.1
  1555 112.443391 10.3.66.103    74.125.226.162   HTTP      242 GET / HTTP/1.1
  1565 113.126971 10.3.66.103    74.125.226.176   HTTP      246 GET / HTTP/1.1
  1708 114.481012 10.3.66.103    54.201.30.58     HTTP      270 GET /verify HTTP/1.1
  1723 115.384591 10.3.66.103    54.148.180.204   HTTP      259 GET /verify HTTP/1.1
  1749 115.730364 10.3.66.103    217.160.165.207  HTTP      262 GET /verify HTTP/1.1
  1838 119.242292 10.3.66.103    109.68.191.31    HTTP     1022 GET /nxNmV7nwZvsv5vGSPZPJc7T%2fNrnx7I9DadY%2ftrb3B%2bc3MAJwfEc…
  4818 125.913403 10.3.66.103    109.68.191.31    HTTP      248 GET /favicon.ico HTTP/1.1
  4840 135.138680 10.3.66.103    23.218.210.155   HTTP      249 GET / HTTP/1.1
  4843 135.544739 10.3.66.103    23.218.210.155   HTTP      255 GET /en-us/ HTTP/1.1
  4861 135.943592 10.3.66.103    74.125.226.162   HTTP      242 GET / HTTP/1.1
  4901 136.072982 10.3.66.103    74.125.226.176   HTTP      246 GET / HTTP/1.1
  5037 137.097507 10.3.66.103    54.201.30.58     HTTP      270 GET /verify HTTP/1.1
  5040 138.251566 10.3.66.103    54.148.180.204   HTTP      259 GET /verify HTTP/1.1
  5046 138.485774 10.3.66.103    217.160.165.207  HTTP      262 GET /verify HTTP/1.1
  5077 158.785573 10.3.66.103    23.218.210.155   HTTP      249 GET / HTTP/1.1
  5080 159.163089 10.3.66.103    23.218.210.155   HTTP      255 GET /en-us/ HTTP/1.1
  5093 159.964356 10.3.66.103    74.125.226.162   HTTP      242 GET / HTTP/1.1
  5115 160.041598 10.3.66.103    74.125.226.176   HTTP      246 GET / HTTP/1.1
  5251 160.918821 10.3.66.103    54.201.30.58     HTTP      270 GET /verify HTTP/1.1
  5261 162.346793 10.3.66.103    54.148.180.204   HTTP      259 GET /verify HTTP/1.1
▶ Frame 90: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits)
▼ Ethernet II, Src: Dell_2d:90:81 (00:24:e8:2d:90:81), Dst: JuniperN_ac:01:7d (78:19:f7:ac:01:7d)
  ▶ Destination: JuniperN_ac:01:7d (78:19:f7:ac:01:7d)
  ▶ Source: Dell_2d:90:81 (00:24:e8:2d:90:81)
```

Figure 8

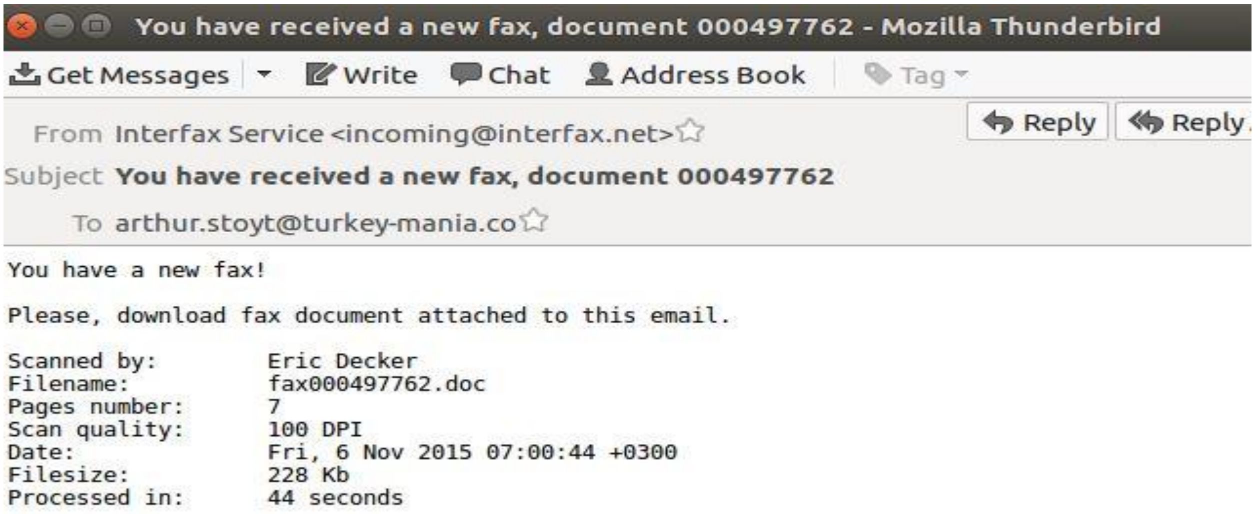
4.4 The infected computer's host name: Strout-PC



```
  Hops: 0
  Transaction ID: 0xc6c2609f
  Seconds elapsed: 0
▼ Bootp flags: 0x0000 (Unicast)
    0... .... .... .... = Broadcast flag: Unicast
    .000 0000 0000 0000 = Reserved flags: 0x0000
  Client IP address: 10.3.66.103
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Dell_2d:90:81 (00:24:e8:2d:90:81)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
▶ Option: (53) DHCP Message Type (Request)
▶ Option: (61) Client identifier
▼ Option: (12) Host Name
    Length: 9
    Host Name: Strout-PC
▶ Option: (81) Client Fully Qualified Domain Name
```

Figure 9

4.5. Which email the employee opened: The fourth email with subject “You have received a new fax, document 000497762”


You have received a new fax, document 000497762 - Mozilla Thunderbird
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply

From Interfax Service <incoming@interfax.net>

Subject You have received a new fax, document 000497762

To arthur.stoyt@turkey-mania.co

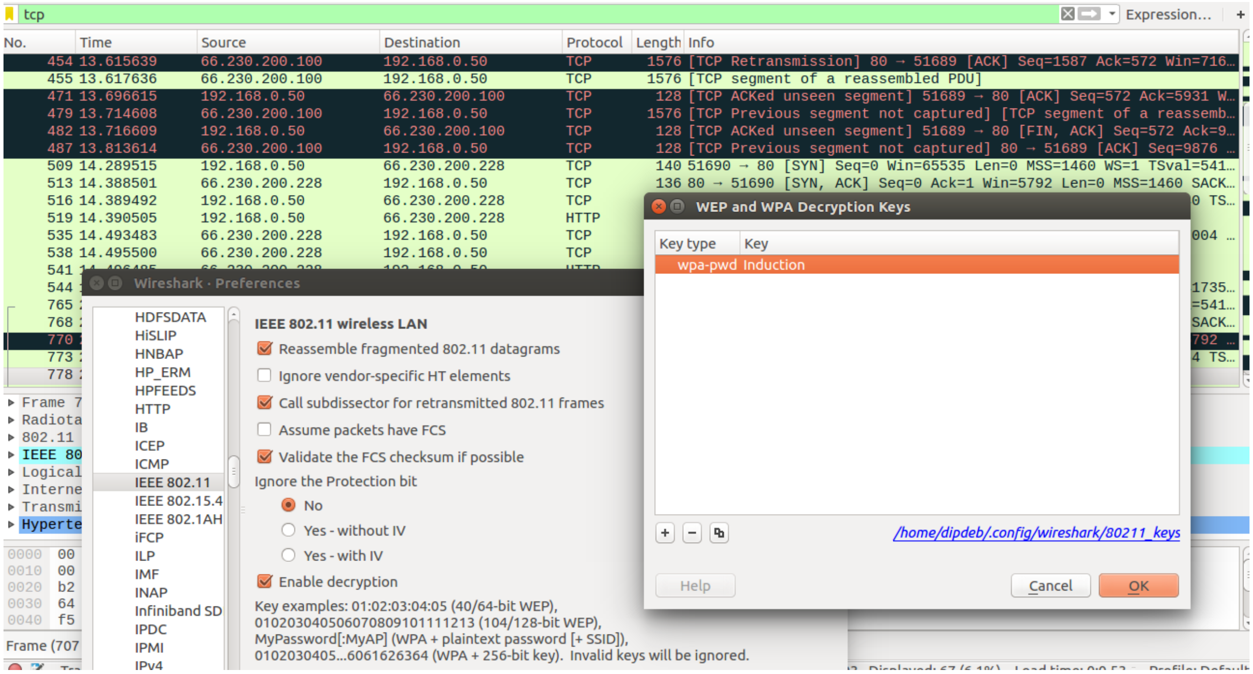
```
You have a new fax!

Please, download fax document attached to this email.

Scanned by:          Eric Decker
Filename:            fax000497762.doc
Pages number:        7
Scan quality:        100 DPI
Date:                Fri, 6 Nov 2015 07:00:44 +0300
Filesize:            228 Kb
Processed in:        44 seconds
```

Figure 10

5. Decrypting Wifi: As the password is given, we can easily decrypt the encrypted wifi file using Wireshark. We have enable decrypt option and give the password just going edit->preference->IEEE802.11.



```
No.  Time       Source          Destination     Protocol Length Info
 454 13.615639  66.230.200.100  192.168.0.50    TCP      1576 [TCP Retransmission] 80 → 51689 [ACK] Seq=1587 Ack=572 Win=716…
 455 13.617636  66.230.200.100  192.168.0.50    TCP      1576 [TCP segment of a reassembled PDU]
 471 13.696615  192.168.0.50    66.230.200.100  TCP       128 [TCP ACKed unseen segment] 51689 → 80 [ACK] Seq=572 Ack=5931 W…
 479 13.714608  66.230.200.100  192.168.0.50    TCP      1576 [TCP Previous segment not captured] [TCP segment of a reassemb…
 482 13.716609  192.168.0.50    66.230.200.100  TCP       128 [TCP ACKed unseen segment] 51689 → 80 [FIN, ACK] Seq=572 Ack=9…
 487 13.813614  66.230.200.100  192.168.0.50    TCP       128 [TCP Previous segment not captured] 80 → 51689 [ACK] Seq=9876 …
 509 14.289515  192.168.0.50    66.230.200.228  TCP       140 51690 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=1 TSval=541…
 513 14.388501  66.230.200.228  192.168.0.50    TCP       136 80 → 51690 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK…
 516 14.389492  192.168.0.50    66.230.200.228  TCP                                                                       0 TS…
 519 14.390505  192.168.0.50    66.230.200.228  HTTP
 535 14.493483  66.230.200.228  192.168.0.50    TCP                                                                     004 …
 538 14.495500  66.230.200.228  192.168.0.50    TCP
 541
 544                                                                                                                   1735…
 765                                                                                                                   =541…
 768                                                                                                                   SACK…
 770                                                                                                                   792 …
 773                                                                                                                   4 TS…
 778

▸ Frame 7
▸ Radiota
▸ 802.11
▸ IEEE 80
▸ Logical
▸ Interne
▸ Transmi
▸ Hyperte

0000  00
0010  00
0020  b2
0030  64
0040  f5

Frame (707
```

IEEE 802.11 wireless LAN

☑ Reassemble fragmented 802.11 datagrams

☐ Ignore vendor-specific HT elements

☑ Call subdissector for retransmitted 802.11 frames

☐ Assume packets have FCS

☑ Validate the FCS checksum if possible

Ignore the Protection bit

● No

○ Yes - without IV

○ Yes - with IV

☑ Enable decryption

Key examples: 01:02:03:04:05 (40/64-bit WEP), 01020304050607080910111213 (104/128-bit WEP), MyPassword[:MyAP] (WPA + plaintext password [+ SSID]), 0102030405…6061626364 (WPA + 256-bit key). Invalid keys will be ignored.

Key type	Key
wpa-pwd	Induction

/home/dipdeb/.config/wireshark/80211_keys

Figure 11

6. **Breaking WiFi:** At first ,airmon-ng start wlan0 to enable monitor mod.

The airdump-ng wlan0mon to get the list of the networks in our area and a lot of information about them .

Then, We use airdump-ng –c [channel] –bssid[BSSID of target network] –w [path] wlan0mon

Now we will see the client of the target network .

Now, we use aireplay-ng -0 2 –a [BSSID of the network] –c [client bssid] wlan0mon

-0 is a shortcut for the deauth mod and the 2 is the number of deauth packets to sen

-a indicates the access point/router's BSSID , replace [router bssid] with the BSSID of the target network

-c indicates the client's BSSID , the device we are typing to deauth

Now, after entering this command in another new window, We get "handsake message" to the airdump window, it means handshake has been captured. And we get pcap file on that network .

Now, aircrack-ng –a2 –b [router bssid] –w [path to wordlist] [path of the pcap file]

-a is the method aircrack will use to crack the handshake ,2 = WPA method,

-b stands for bssid, replace [router bssid] with the BSSID of the target router

-w stands for wordlist

Aircrack-ng will now launch into the process of cracking the password. However, it will only crack it if the password happens to be in the wordlist that you've selected. Sometimes, it's not. If this is the case, you can try other wordlists. If you simply cannot find the password no matter how many wordlists you try, then it appears your penetration test has failed, and the network is at least safe from basic brute-force attacks.

Cracking the password might take a long time depending on the size of the wordlist