Forensics Investigation

Case Name: Flower Girl

Investigator:

Abdul Sami Qasim (22i-1725)
CY-D

To:

Ubaid Ullah

Dated: 7th Oct 2024 (GMT +5)

Case Background:

This is a harassment case in which a female sales representative is accusing another sales representative, Robert, of harassing her by sending her emails on her private email (3 in total) which were provided to HR. She also said that Robert showed up a coffee show where she was drinking coffee with friend.

Tools Used:

1. FTK Imager
2. Autopsy
3. Wireshark

Image Authentication:

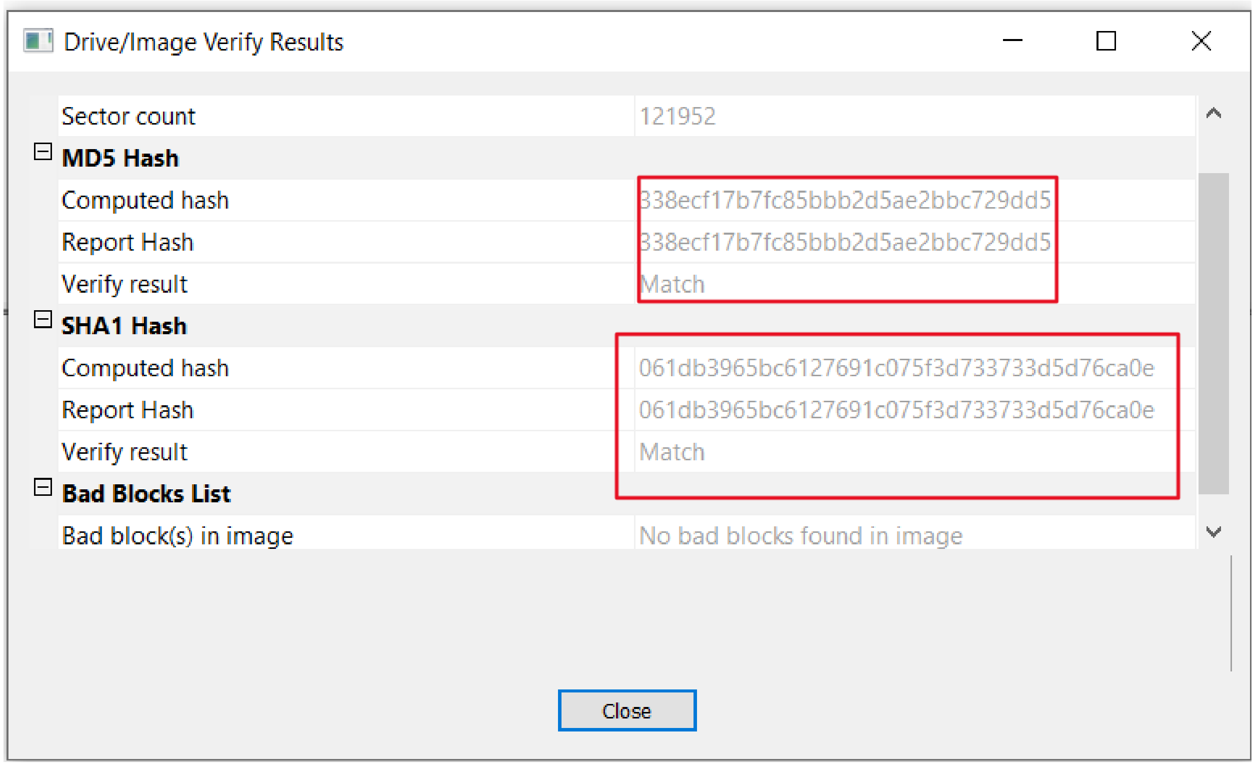
The hash provided to us of the given image file is:

MD5 hash: 338ecf17b7fc85bbb2d5ae2bbc729dd5

Checking the hash again:

MD5 hash: 338ecf17b7fc85bbb2d5ae2bbc729dd5

Image Duplication:



Sector count	121952
MD5 Hash	
Computed hash	338ecf17b7fc85bbb2d5ae2bbc729dd5
Report Hash	338ecf17b7fc85bbb2d5ae2bbc729dd5
Verify result	Match
SHA1 Hash	
Computed hash	061db3965bc6127691c075f3d733733d5d76ca0e
Report Hash	061db3965bc6127691c075f3d733733d5d76ca0e
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

The hashes of both the files have been mentioned above and both hashes match.

Analysis:

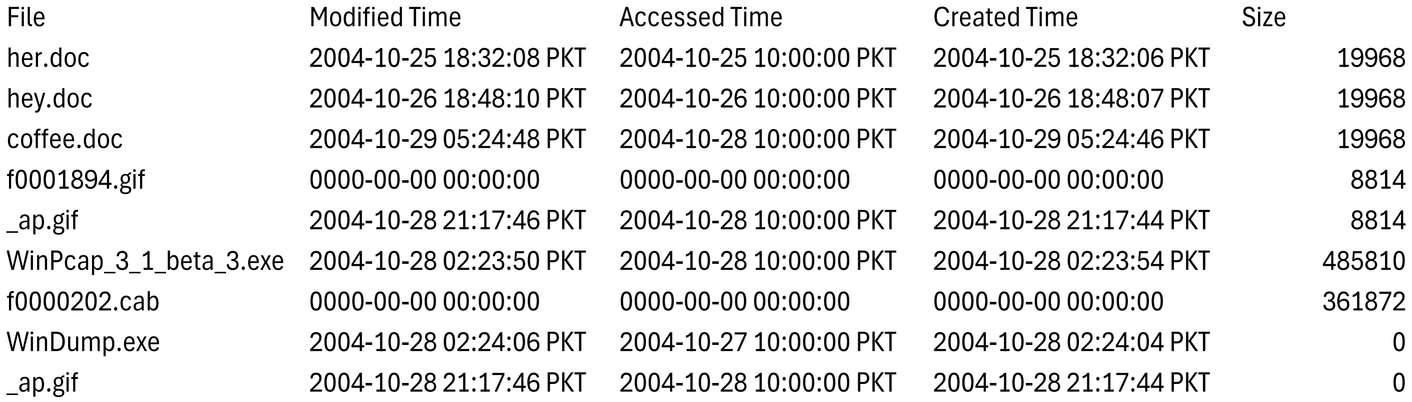
14 files have been found in total, out of which 11 are deleted and 3 are not deleted .doc files.

Deleted Files:

f0001894.gif
_ap.gif
WinPcap_3_1_beta_3.exe
f0000202.cab
WinDump.exe
_ap.gif
WinPcap_3_1_beta_3.exe
_apture
f0001790.pcap
WinDump.exe
f0000910.exe

Not deleted document files:

her.doc
hey.doc
coffee.doc



File	Modified Time	Accessed Time	Created Time	Size
her.doc	2004-10-25 18:32:08 PKT	2004-10-25 10:00:00 PKT	2004-10-25 18:32:06 PKT	19968
hey.doc	2004-10-26 18:48:10 PKT	2004-10-26 10:00:00 PKT	2004-10-26 18:48:07 PKT	19968
coffee.doc	2004-10-29 05:24:48 PKT	2004-10-28 10:00:00 PKT	2004-10-29 05:24:46 PKT	19968
f0001894.gif	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8814
_ap.gif	2004-10-28 21:17:46 PKT	2004-10-28 10:00:00 PKT	2004-10-28 21:17:44 PKT	8814
WinPcap_3_1_beta_3.exe	2004-10-28 02:23:50 PKT	2004-10-28 10:00:00 PKT	2004-10-28 02:23:54 PKT	485810
f0000202.cab	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	361872
WinDump.exe	2004-10-28 02:24:06 PKT	2004-10-27 10:00:00 PKT	2004-10-28 02:24:04 PKT	0
_ap.gif	2004-10-28 21:17:46 PKT	2004-10-28 10:00:00 PKT	2004-10-28 21:17:44 PKT	0

The important files here are:

her.doc, the first created document with the following content:

“Hey I saw you the other day. I tried to say "hi", but you disappeared??? That was a nice blue dress you were wearing. I heard that your car was giving you some trouble. Maybe I can give you a ride to work sometime, or maybe we can get dinner sometime?

Have a nice day”

hey.doc, the second created document with the following content:

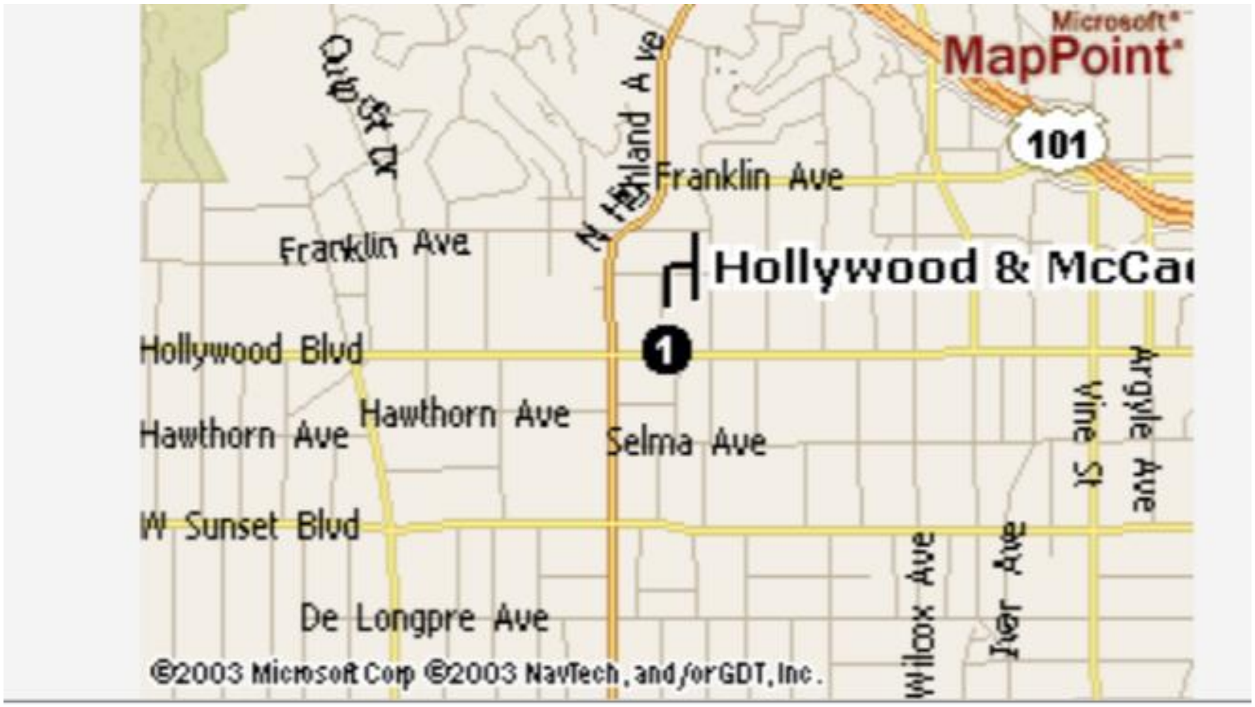
“Hey! Why are you being so mean? I was just offering to help you out with your car! Don't tell me to get lost! You should give me a chance. I'm a nice guy just trying to help you out, just because I think you're cute doesn't mean I'm weird. Perhaps coffee would be better, when would be a good time for you?”

coffee.doc, the third and last document file with the following content:

“Hey what gives? I was drinking a coffee on thursday and saw you stop buy with some guy! You said you didn't want coffee with me, but you'll go have it with some random guy??? He looked like a loser! Guys like that are nothing but trouble. I can't believe you did this to me! You should stick to your word,

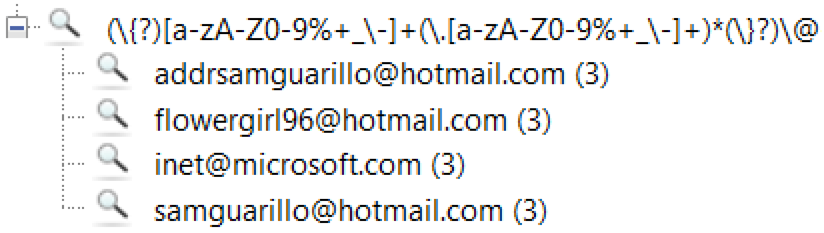
if you're not interested in going to coffee with me then you shouldn't be going with anyone! I heard rumors about a "bad batch" of coffee, hope you don't get any..."

_ap.gif, which is a map image of New York with a pin dropped somewhere on Hollywood Bvd.



This image of the map was located in the filesystem 1 day before the last doc was created (coffee.doc).

f0001790.pcap (creation time: unknown), which is a network capture file located on the usb which has some emails in it, the following are the emails found in this capture file:



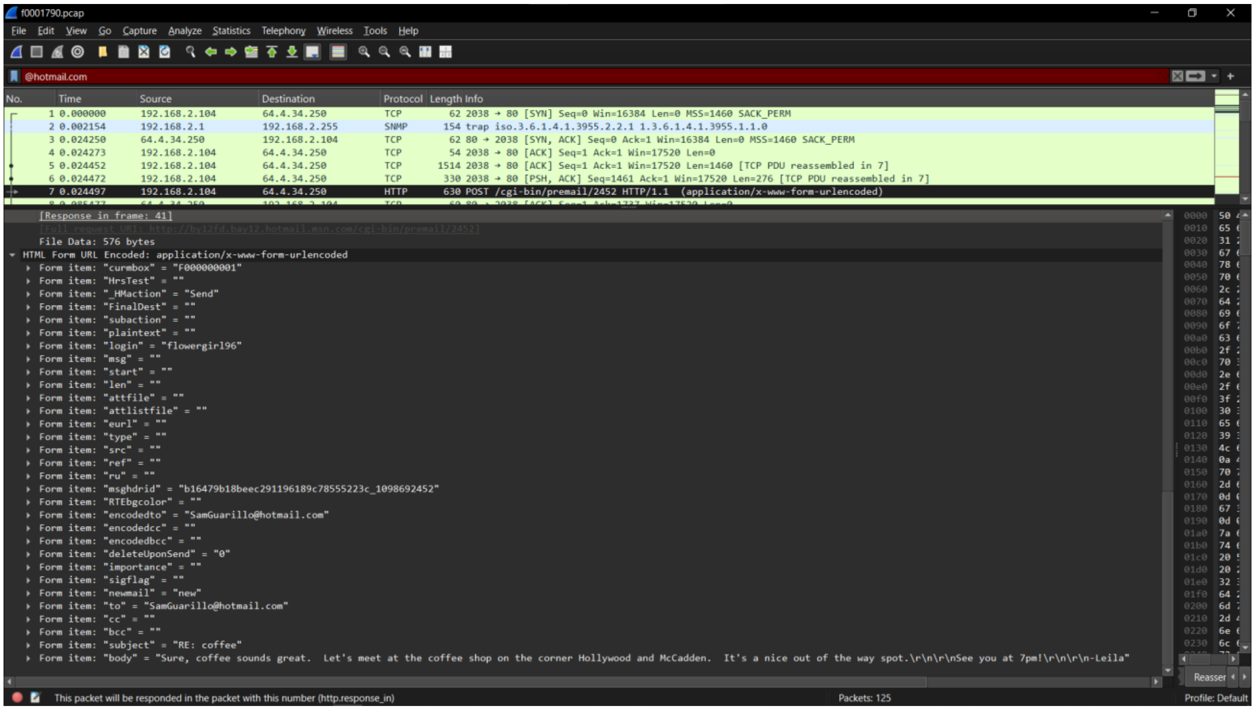
```
⊟ (\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@
    addrsamguarillo@hotmail.com (3)
    flowergirl96@hotmail.com (3)
    inet@microsoft.com (3)
    samguarillo@hotmail.com (3)
```

There's also another file in the system, **_apture (access time: 2004-10-28 10:00:00)** after 7 minutes of this files access, the _ap.gif file which has the map was created. The _apture file has a cutout of some data from the .pcap file, following is the information in this file:

curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=flowergirl96&msg=&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&ref=&ru=&msghdrid=b16479b18beec291196189c78555223c_1098692452&RTEbgcolor=&encodedto=SamGuarillo@hotmail.com&encodedcc=&encodedbcc=&deleteUponSend=0&importance=&sigflag=&newmail=new&to=SamGuarillo@hotmail.com&cc=&bcc=&subject=RE%3A+coffee&body=Sure%2C+coffee+sounds+great.++Let%27s+meet+at+the+coffee+shop+on+the+corner+Hollywood+and+McCadden.++It%27s+a+nice+out+of+the+way+spot.%0D%0A%0D%0ASee+you+at+7pm%21%0D%0A%0D%0A-Leila.6

Mail sent from: flowergirl96
Mail to: SamGuarillo@hotmail.com

It looks like this in wireshark:


f0001790.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
@hotmail.com

```
No.  Time      Source          Destination     Protocol Length Info
  1 0.000000  192.168.2.104   64.4.34.250     TCP        62 2038 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
  2 0.002154  192.168.2.1     192.168.2.255   SNMP      154 trap iso.3.6.1.4.1.3955.2.2.1 1.3.6.1.4.1.3955.1.1.0
  3 0.024250  64.4.34.250     192.168.2.104   TCP        62 80 → 2038 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM
  4 0.024273  192.168.2.104   64.4.34.250     TCP        54 2038 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
  5 0.024452  192.168.2.104   64.4.34.250     TCP      1514 2038 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=1460 [TCP PDU reassembled in 7]
  6 0.024472  192.168.2.104   64.4.34.250     TCP       330 2038 → 80 [PSH, ACK] Seq=1461 Ack=1 Win=17520 Len=276 [TCP PDU reassembled in 7]
  7 0.024497  192.168.2.104   64.4.34.250     HTTP      630 POST /cgi-bin/premail/2452 HTTP/1.1  (application/x-www-form-urlencoded)

    [Response in frame: 41]
    [Full request URI: http://by12fd.bay12.hotmail.msn.com/cgi-bin/premail/2452]
    File Data: 576 bytes
  HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "curmbox" = "F000000001"
    Form item: "HrsTest" = ""
    Form item: "_HMaction" = "Send"
    Form item: "FinalDest" = ""
    Form item: "subaction" = ""
    Form item: "plaintext" = ""
    Form item: "login" = "flowergirl96"
    Form item: "msg" = ""
    Form item: "start" = ""
    Form item: "len" = ""
    Form item: "attfile" = ""
    Form item: "attlistfile" = ""
    Form item: "eurl" = ""
    Form item: "type" = ""
    Form item: "src" = ""
    Form item: "ref" = ""
    Form item: "ru" = ""
    Form item: "msghdrid" = "b16479b18beec291196189c78555223c_1098692452"
    Form item: "RTEbgcolor" = ""
    Form item: "encodedto" = "SamGuarillo@hotmail.com"
    Form item: "encodedcc" = ""
    Form item: "encodedbcc" = ""
    Form item: "deleteUponSend" = "0"
    Form item: "importance" = ""
    Form item: "sigflag" = ""
    Form item: "newmail" = "new"
    Form item: "to" = "SamGuarillo@hotmail.com"
    Form item: "cc" = ""
    Form item: "bcc" = ""
    Form item: "subject" = "RE: coffee"
    Form item: "body" = "Sure, coffee sounds great.  Let's meet at the coffee shop on the corner Hollywood and McCadden.  It's a nice out of the way spot.\r\n\r\nSee you at 7pm!\r\n\r\n-Leila"

This packet will be responded in the packet with this number (http.response_in)    Packets: 125    Profile: Default
```

Flowergirl appears to be the name of the victim in this case, the female sales representative, Sam Guarillo was also involved as he’s the person who got the mail from flowergirl to meet at the coffee shop at 7pm when Robert also showed up. After this, the last coffee.doc was made which had him mentioning a coffee shop and that the victim is with another man.

Reason for case name:

This is the only instance of the use of the name flowergirl, as it appears to be related to the female representative, the case was named as this.

Personal verdict:

My personal verdict is that Robert is guilty as he has 3 doc files in the usb containing the threatening messages, he also has a network capture file containing the email that flowergirl sent to Sam. It also includes the shop location where flowergirl and Sam were to meet.