



**National University**  
of computer and emerging sciences

## Lab 07

CYL2002 Digital Forensics - Lab

Name : Mirza Humayun Masood(i22-1749)

Section : CY-A

*Submitted to: Sir Ubaid Ullah*

Department of Cyber Security BS(CY)

FAST-NUCES Islamabad

---

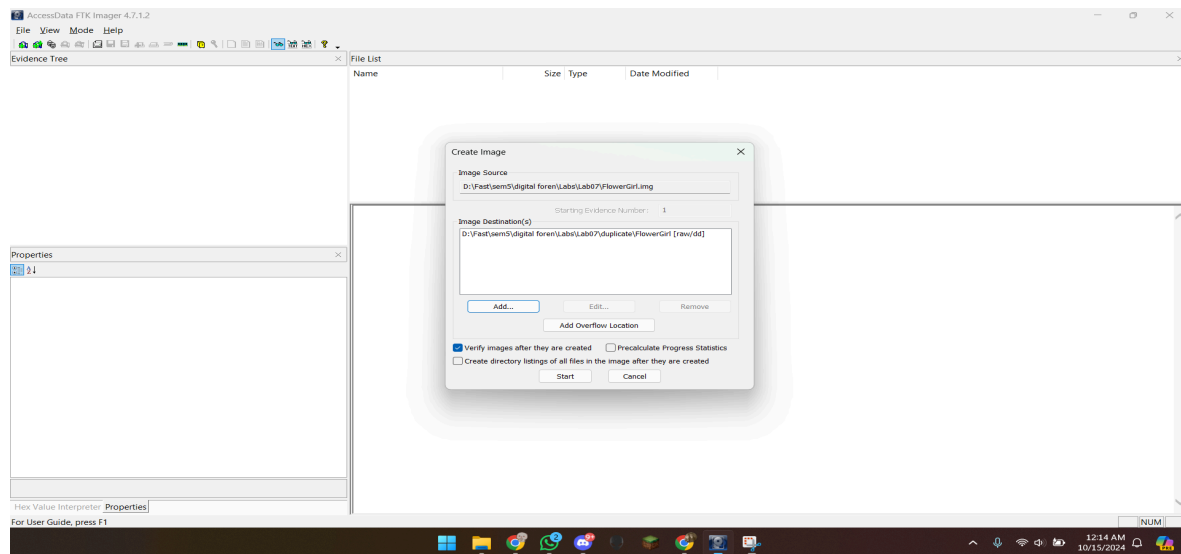
## Case Background:

In this harassment case, a female sales representative has accused her colleague, Robert, of harassing her by sending three emails to her private email address, which she has submitted to HR as evidence. She also reported that Robert appeared at a coffee shop where she was having coffee with a friend.

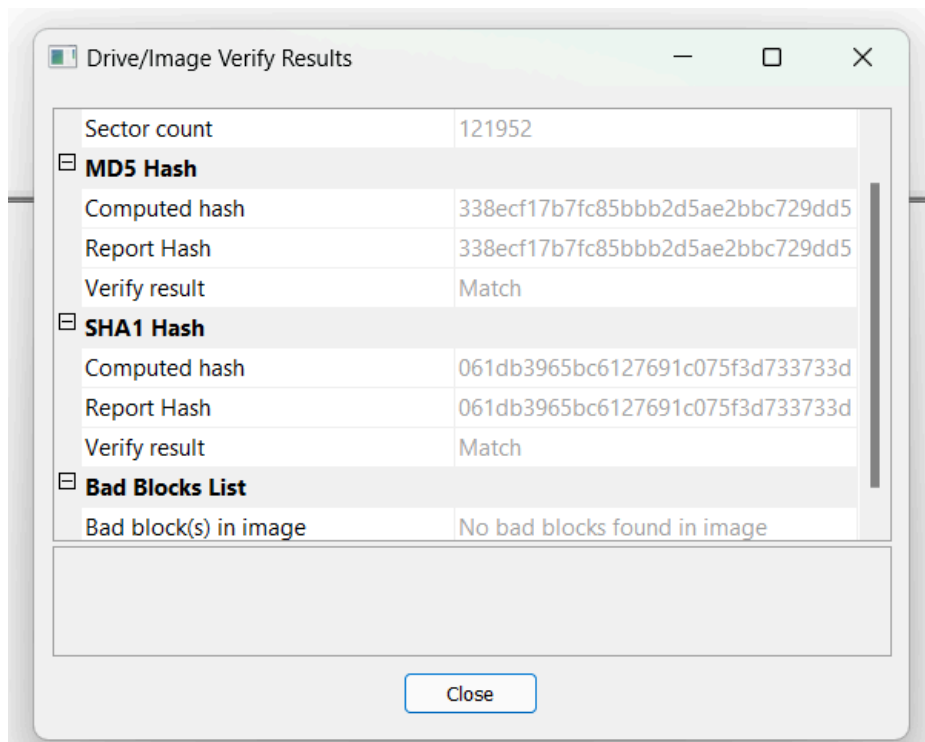
## Tools Used:

1. FTK Imager
2. Autopsy
3. Wireshark

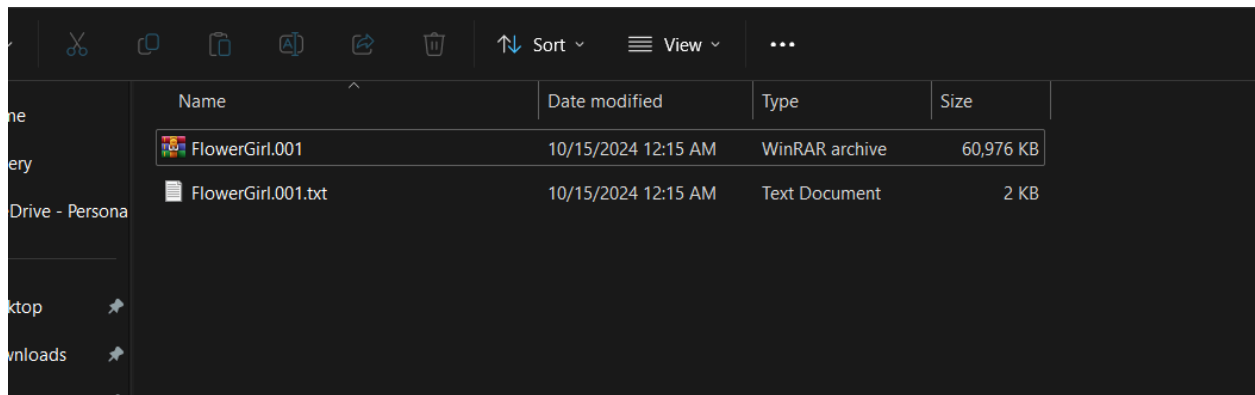
## File Duplication Process:



## Authentication:



So the Image is matched.



## Analysis:

### Deleted Files :

FileName	WinPcap_3_1_beta_3.exe
Owner	
Last Modified	2004-10-27 17:23:50 EDT
MD5	4cbac34b99000f1b0d8b2b3d729684f4

FileName	WinDump.exe
Owner	
Last Modified	2004-10-27 17:24:02 EDT
MD5	79375b77975aa53a1b0507496107bff7

FileName	f0000910.exe
Owner	
Last Modified	0000-00-00 00:00:00
MD5	79375b77975aa53a1b0507496107bff7

FileName	f0000202.cab
Owner	
Last Modified	0000-00-00 00:00:00
MD5	5d198a5b20dd0e8cc8f2ebd6745ededa

FileName	f0001790.pcap
Owner	
Last Modified	0000-00-00 00:00:00
MD5	f7db6e0ecb4c3c51218d918c9c711cbd

FileName	_apture
Owner	
Last Modified	2004-10-28 12:11:00 EDT
MD5	2097b7b0a9fedb4238b67e976c4ae1cb














FileName	_ap.gif
Owner	
Last Modified	2004-10-28 12:17:46 EDT
MD5	9bc3923cf8e72fd405d7cea8c8781011

FileName	f0001894.gif
Owner	
Last Modified	0000-00-00 00:00:00
MD5	9bc3923cf8e72fd405d7cea8c8781011

FileName	WinPcap_3_1_beta_3.exe
Owner	
Last Modified	2004-10-27 17:23:56 EDT
MD5	d41d8cd98f00b204e9800998ecf8427e

FileName	WinDump.exe
Owner	
Last Modified	2004-10-27 17:24:06 EDT
MD5	d41d8cd98f00b204e9800998ecf8427e

FileName	_ap.gif
Owner	
Last Modified	2004-10-28 12:17:46 EDT
MD5	d41d8cd98f00b204e9800998ecf8427e




Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
 WinPcap_3_1_beta_3.exe				2004-10-27 17:23:50 EDT	0000-00-00 00:00:00	2004-10-28 01:00:00 EDT	2004-10-27 17:23:54 EDT	485810	Unallocated	Unallocated
 WinDump.exe				2004-10-27 17:24:02 EDT	0000-00-00 00:00:00	2004-10-28 01:00:00 EDT	2004-10-27 17:24:04 EDT	450560	Unallocated	Unallocated
 f0000910.exe			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	450560	Unallocated	Unallocated
 f0000202.cab			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	361872	Unallocated	Unallocated
 f0001790.pcap			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	53248	Unallocated	Unallocated
 _apture				2004-10-28 12:11:00 EDT	0000-00-00 00:00:00	2004-10-28 01:00:00 EDT	2004-10-28 12:08:24 EDT	53056	Unallocated	Unallocated
 _ap.gif				2004-10-28 12:17:46 EDT	0000-00-00 00:00:00	2004-10-28 01:00:00 EDT	2004-10-28 12:17:44 EDT	8814	Unallocated	Unallocated
 f0001894.gif			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8814	Unallocated	Unallocated
 WinPcap_3_1_beta_3.exe				2004-10-27 17:23:56 EDT	0000-00-00 00:00:00	2004-10-27 01:00:00 EDT	2004-10-27 17:23:54 EDT	0	Unallocated	Unallocated
 WinDump.exe				2004-10-27 17:24:06 EDT	0000-00-00 00:00:00	2004-10-27 01:00:00 EDT	2004-10-27 17:24:04 EDT	0	Unallocated	Unallocated
 _ap.gif				2004-10-28 12:17:46 EDT	0000-00-00 00:00:00	2004-10-28 01:00:00 EDT	2004-10-28 12:17:44 EDT	0	Unallocated	Unallocated

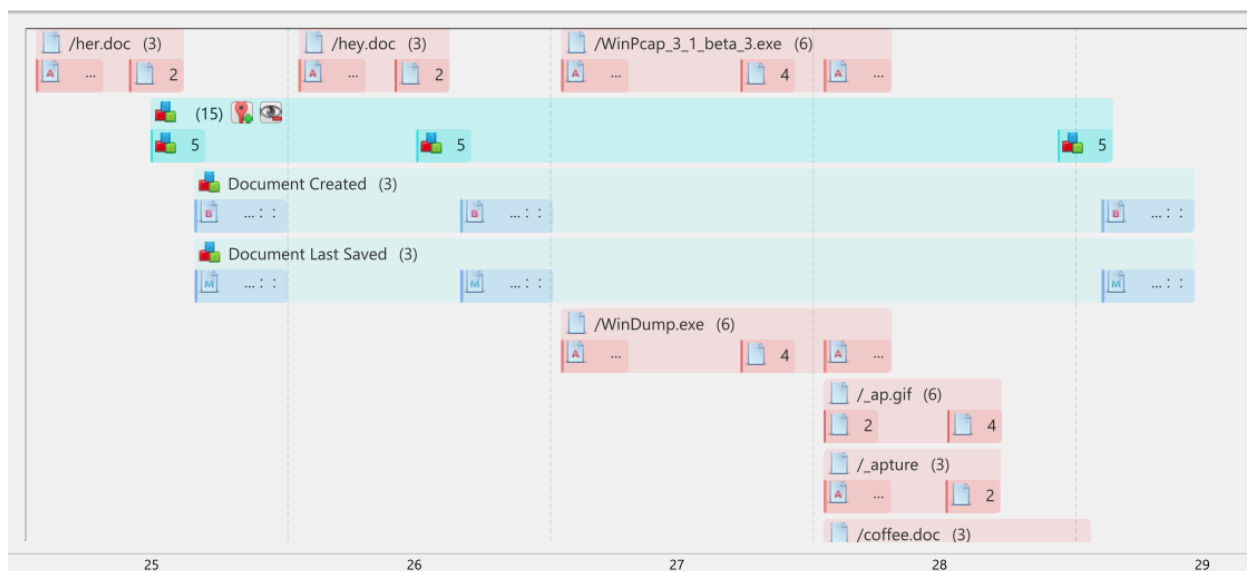
## Not Deleted Files :

FileName	coffee.doc
Owner	Robert Lawrence
Last Modified	2004-10-28 20:24:48 EDT
MD5	a833c58689596eda15a27c931e0c76d1

FileName	her.doc
Owner	Robert Lawrence
Last Modified	2004-10-25 09:32:08 EDT
MD5	9785a777c5286738f9deb73d8bc57978

FileName	hey.doc
Owner	Robert Lawrence
Last Modified	2004-10-26 09:48:10 EDT
MD5	ca601d4f8138717dca4de07a8ec19ed1

 coffee.doc		0	2004-10-28 20:24:48 EDT	0000-00-00 00:00:00	2004-10-28 01:00:00 EDT	2004-10-28 20:24:46 EDT	19968	Allocated	Allocated
 her.doc		0	2004-10-25 09:32:08 EDT	0000-00-00 00:00:00	2004-10-25 01:00:00 EDT	2004-10-25 09:32:06 EDT	19968	Allocated	Allocated
 hey.doc		0	2004-10-26 09:48:10 EDT	0000-00-00 00:00:00	2004-10-26 01:00:00 EDT	2004-10-26 09:48:07 EDT	19968	Allocated	Allocated



Now to analyze the data in the files, we have to view the files in a timeline order, so First file is her.doc.

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

2nd file is hey.doc

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?

3rd File is Coffee.doc

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...



The \_ap.gif had the location of The Coffee Shop.



This image was created in the filesystem one day before coffee.doc was created.

tcp.stream eq 0

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
3	0.024273	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 segment of a reassembled PDU]
6	0.024472	192.168.2.104	64.4.34.250	TCP	338	2038 → 80 [PSH, ACK] Seq=1461 Ack=1 Win=17520 Len=276 [TCP segment of a reassembled PDU]
8	0.054777	64.4.34.250	192.168.2.104	TCP	60	80 → 2038 [ACK] Seq=1 Ack=1737 Win=17520 Len=0
9	0.086289	64.4.34.250	192.168.2.104	HTTP	79	HTTP/1.1 100 Continue
10	0.135817	64.4.34.250	192.168.2.104	TCP	389	80 → 2038 [PSH, ACK] Seq=26 Ack=2313 Win=16944 Len=335 [TCP segment of a reassembled PDU]
11	0.135872	192.168.2.104	64.4.34.250	TCP	54	2038 → 80 [ACK] Seq=2313 Ack=361 Win=17160 Len=0

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: "ru" = ""  
Form item: "msghrid" = "b10479b18bec291196189c78555223c\_1098692452"  
Form item: "RTBgcolor" = ""  
Form item: "encodedto" = "SamGuarillo@hotmail.com"  
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  
Key: body  
Value: Sure, coffee sounds great. Let's meet at the coffee shop on the corner Hollywood and McCadden. It's a nice out of  
Value (urlencoded-form.value), 182 bytes  
Packets: 125 · Displayed: 34 (27.2%)  
Profile: Default

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

In this case, the victim appears to be a female sales representative named Flowergirl. Another individual, Sam Guarillo, was also involved, as he received an email from Flowergirl inviting him to meet at the coffee shop at 7 pm, where Robert also showed up. Following this incident, a document titled "coffee.doc" was

created, in which Robert mentioned the coffee shop and noted that the victim was with another man.

So that means he sniffed the mails, and got to know the location of the coffee shop, and time as well.

As Robert's PC had wincap and WinDump, that shows he sniffed the packets.

### **Reason for the Name:**

The reason was to hide the identity of the Victim, and also her email address was Flowergirl96, so that's why this case was named FlowerGirl.

### **Personal verdict:**

My personal verdict is that Robert is guilty, as he possesses three documents on the USB drive containing threatening messages. Additionally, he has a network capture file that includes the email Flowergirl sent to Sam, which also specifies the location of the shop where Flowergirl and Sam were supposed to meet.