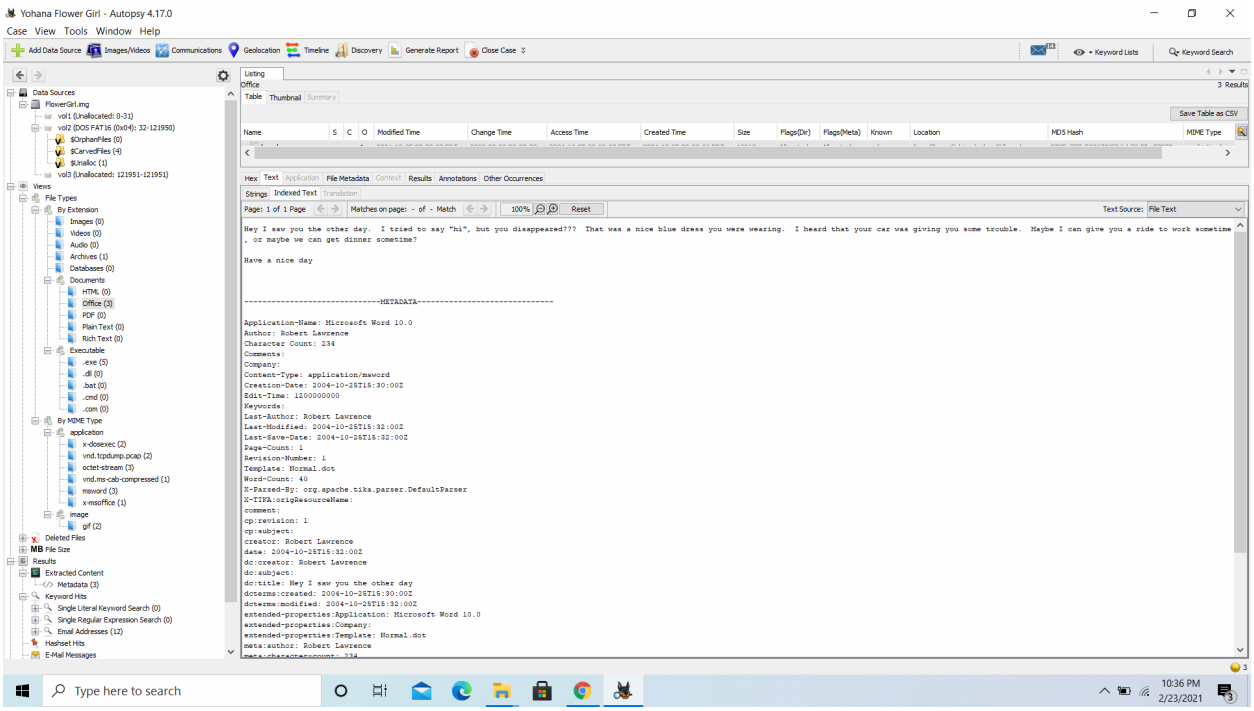
Examiner: Yohana Haileab

The Flower Girl

This is an evidence of a case study about a female employee, sales representative. She has alleged that another employee, Robert also a sales representative has harassed her. To analyze this evidence, First I used the FTK Imager , but I couldn't extract all the evidence. However, I used the FTK Imager to compare the MD5 hash value which is 338ecf17b7fc85bbb2d5ae2bbc729dd5 and got the same got same result. Then I used Autopsy and found all the data's I want. During my investigation using autopsy I used both the image file and MD5 hash value as creating the case. From the flash drive, I have found the three word documents that was sent to her, different types of files: executable files, Documents, a gif image, deleted files, and Email addresses, and meta Data.

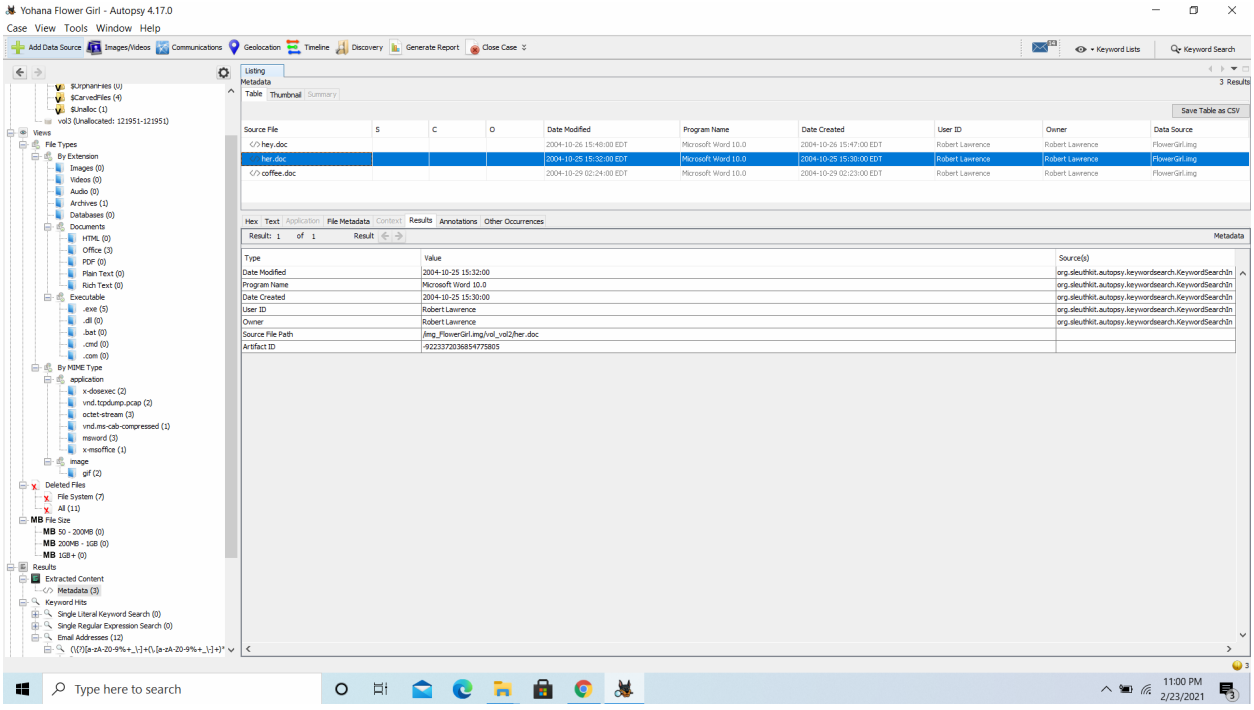
I found all the three documents in office file under views, File types , then by Extension , documents then office.

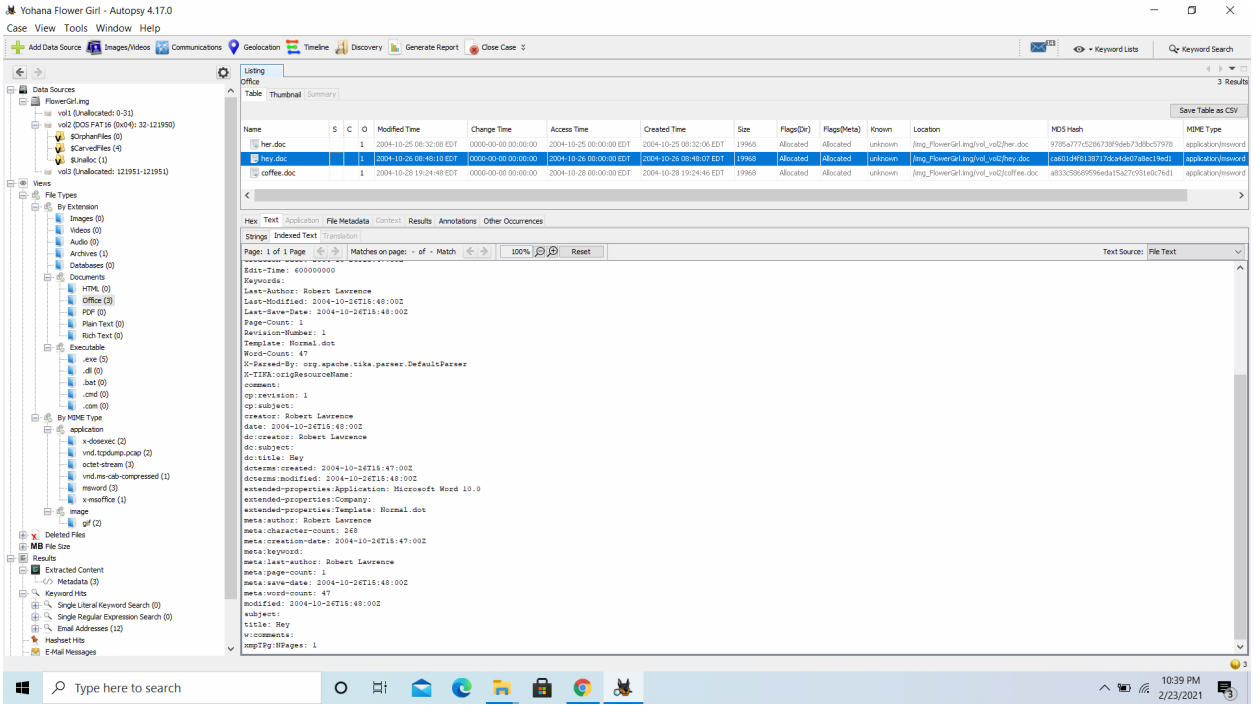


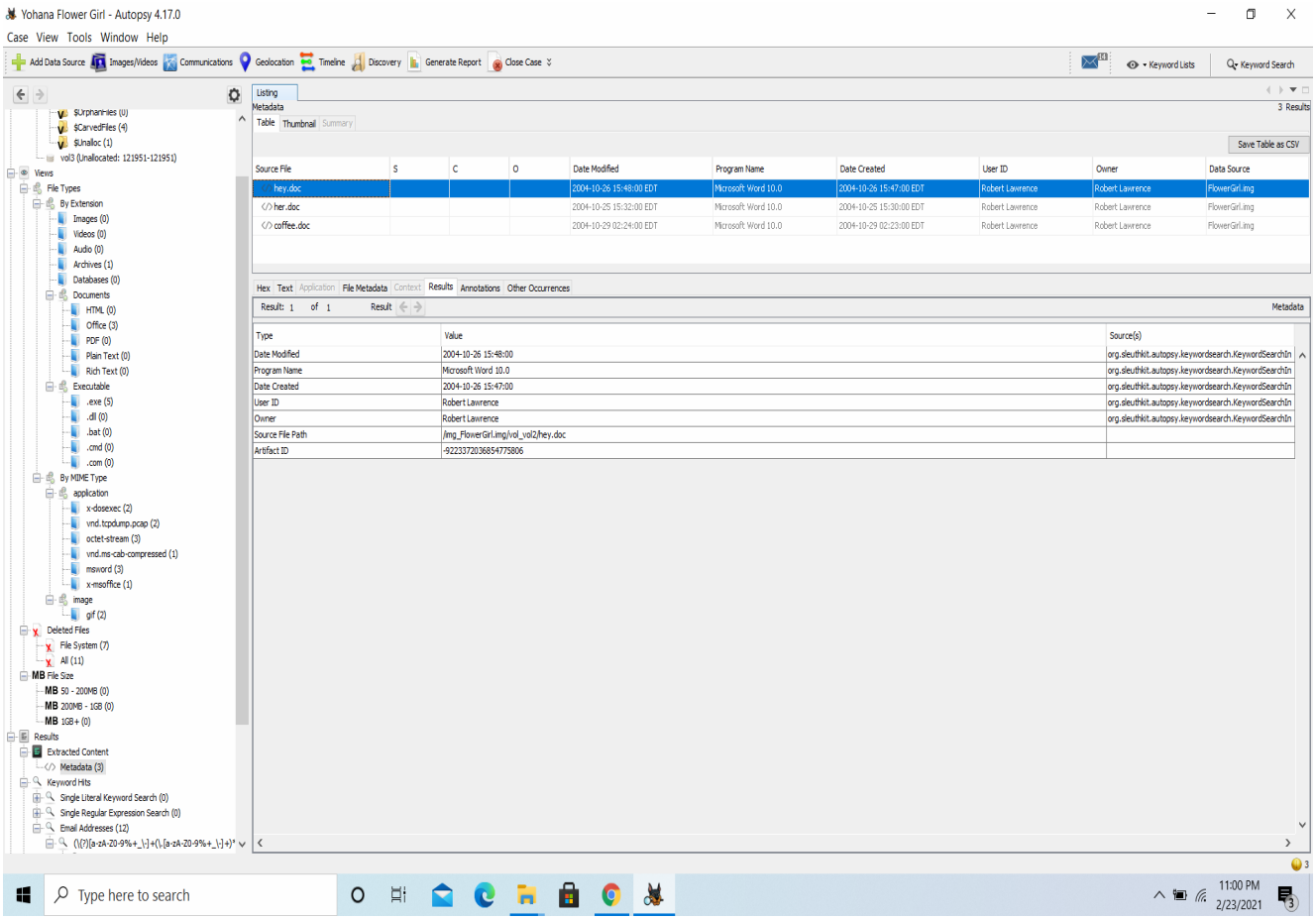
From the above screnshoot document titled her.doc , i found out that the guys name was Robert Lawrence.

He sent her a message. he created the message 2004-10-25 at 15:30:00,

and modified it on 2004-10-25 at 15:32:00. he revised it once.


Yohana Flower Girl - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Metadata
3 Results
Table
Thumbnail
Summary
Save Table as CSV
Source File
S
C
O
Date Modified
Program Name
Date Created
User ID
Owner
Data Source
hey.doc
2004-10-26 15:48:00 EDT
Microsoft Word 10.0
2004-10-26 15:47:00 EDT
Robert Lawrence
FlowerGirl.img
her.doc
2004-10-25 15:32:00 EDT
Microsoft Word 10.0
2004-10-25 15:30:00 EDT
coffee.doc
2004-10-29 02:24:00 EDT
Microsoft Word 10.0
2004-10-29 02:23:00 EDT
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
Result: 1 of 1
Result
Metadata
Type
Value
Source(s)
Date Modified
2004-10-25 15:32:00
org.sleuthkit.autopsy.keywordsearch.KeywordSearchIn
Program Name
Microsoft Word 10.0
Date Created
2004-10-25 15:30:00
User ID
Robert Lawrence
Owner
Source File Path
/img_FlowerGirl.img/vol_vol2/her.doc
Artifact ID
-9223372036854775805
Type here to search
11:00 PM
2/23/2021


Yohana Flower Girl - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Office
3 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
Known
Location
MD5 Hash
MIME Type
her.doc
hey.doc
coffee.doc
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
Strings
Indexed Text
Translation
Page: 1 of 1 Page
Matches on page: - of - Match
100%
Reset
Text Source: File Text
Edit-Time: 600000000
Keywords:
Last-Author: Robert Lawrence
Last-Modified: 2004-10-26T15:48:00Z
Last-Save-Date: 2004-10-26T15:48:00Z
Page-Count: 1
Revision-Number: 1
Template: Normal.dot
Word-Count: 47
X-Parsed-By: org.apache.tika.parser.DefaultParser
X-TIKA:origResourceName:
comment:
cp:revision: 1
cp:subject:
creator: Robert Lawrence
date: 2004-10-26T15:48:00Z
dc:creator: Robert Lawrence
dc:subject:
dc:title: Hey
dcterms:created: 2004-10-26T15:47:00Z
dcterms:modified: 2004-10-26T15:48:00Z
extended-properties:Application: Microsoft Word 10.0
extended-properties:Company:
extended-properties:Template: Normal.dot
meta:author: Robert Lawrence
meta:character-count: 268
meta:creation-date: 2004-10-26T15:47:00Z
meta:keyword:
meta:last-author: Robert Lawrence
meta:page-count: 1
meta:save-date: 2004-10-26T15:48:00Z
meta:word-count: 47
modified: 2004-10-26T15:48:00Z
subject:
title: Hey
w:comments:
xmpTPg:NPages: 1
Type here to search
10:39 PM
2/23/2021



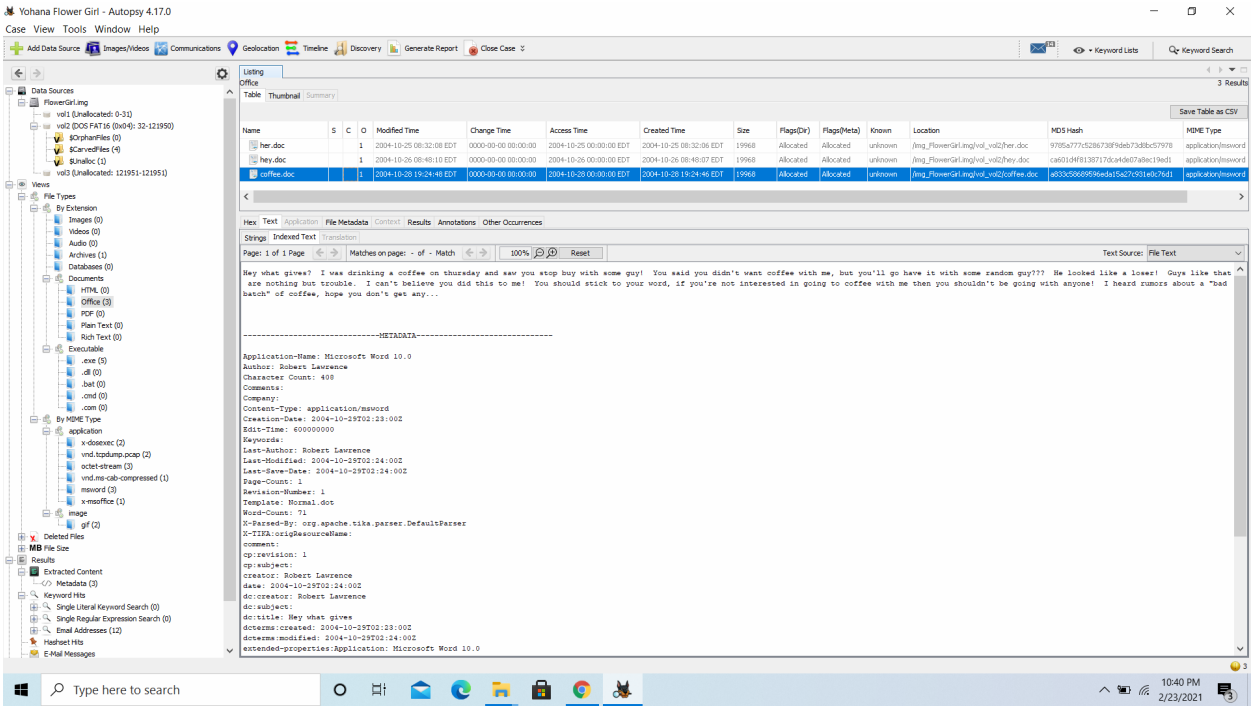
And from the hey.doc ,

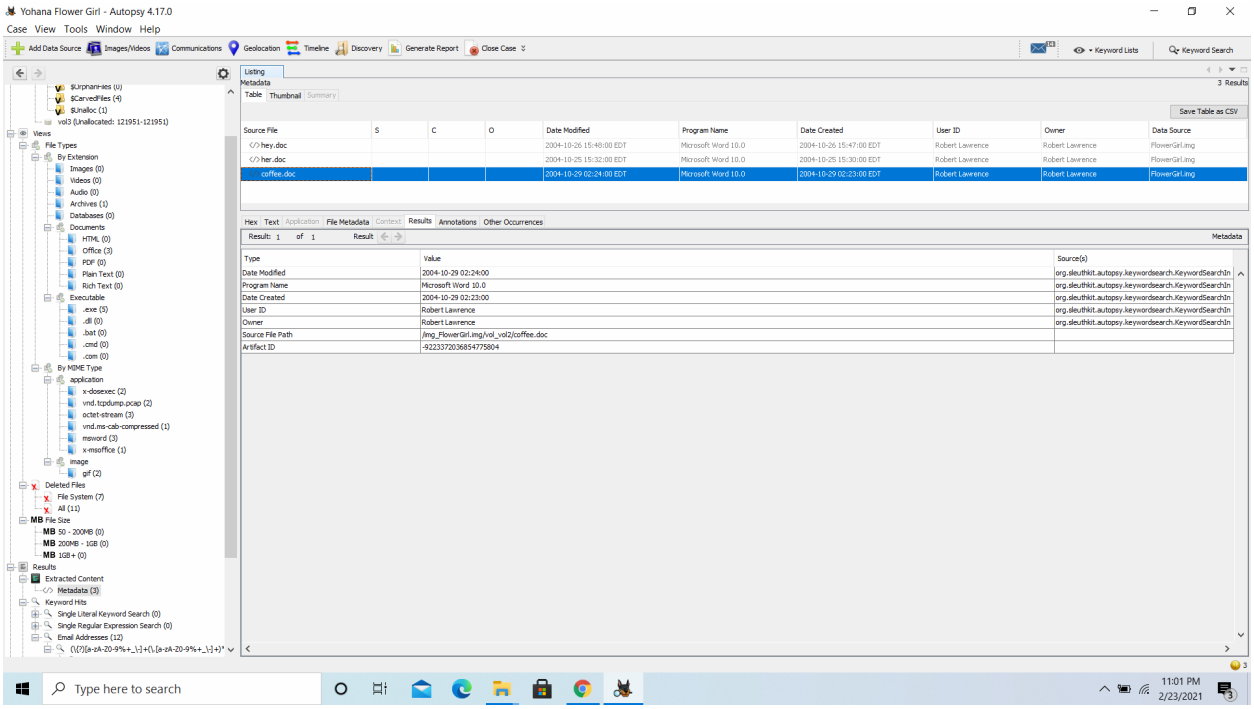
He wrote her a 268 charactered text

He created it on 2004-10-26 at15:47:00

And then he modified it in 2004-10-26 at 15:48:00

And the last save was the same day as he modified it. And the creator was Robbert again.





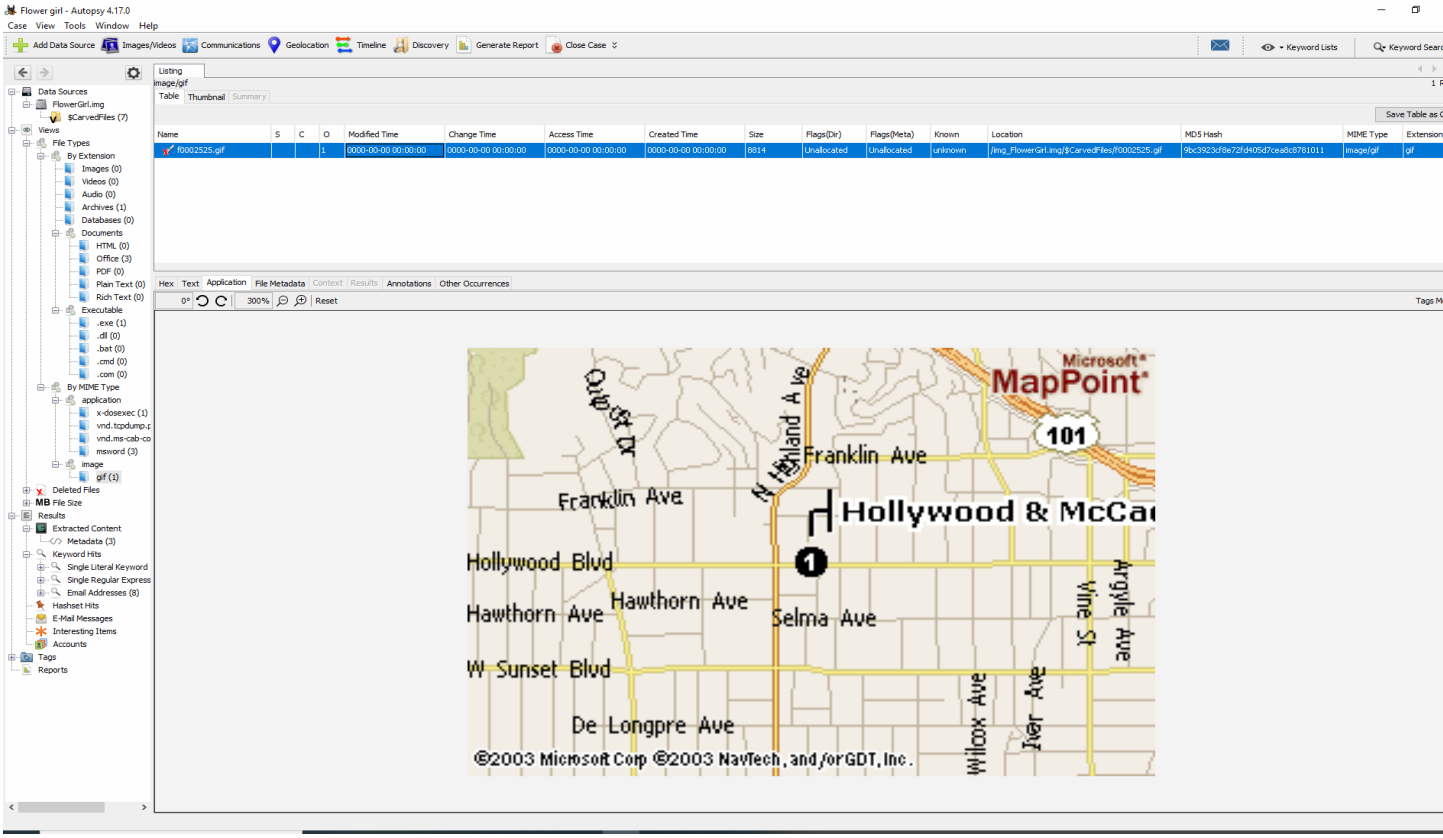
the third document titled Coffee.doc ,

was created 2004-10-29 at 02:23:00

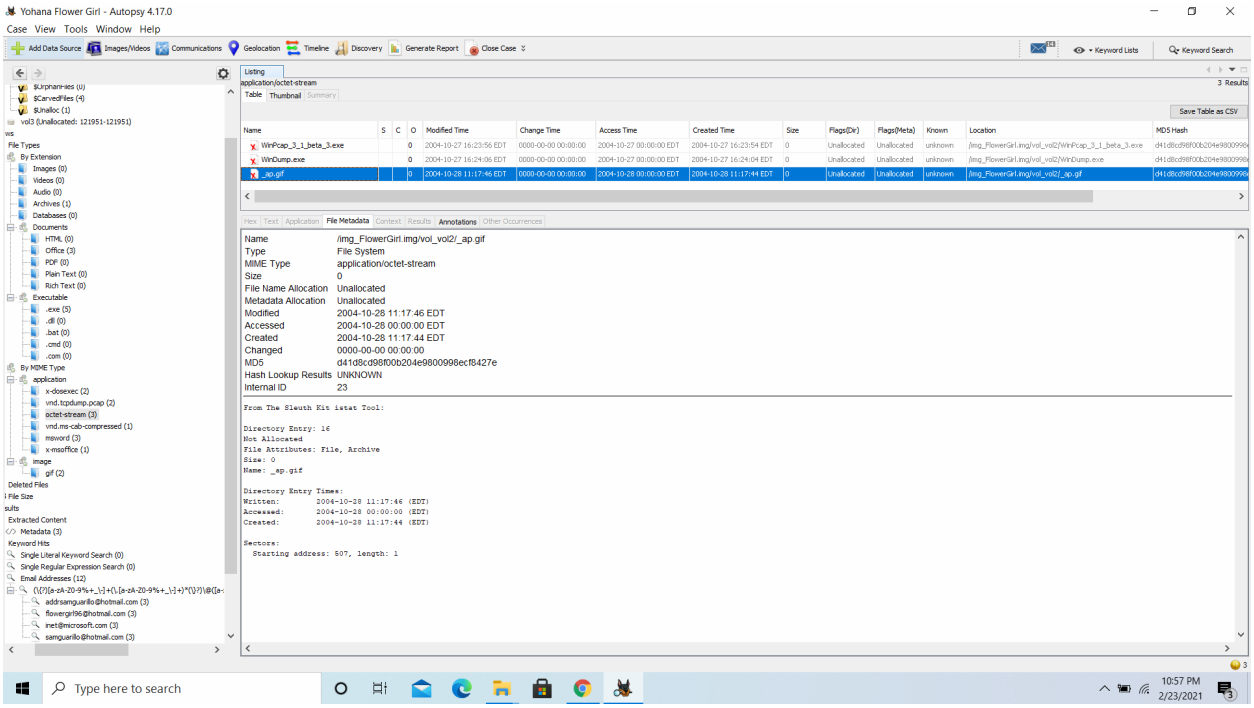
Last modified 2004-10-29 at 02:24:00

Last save date 2004-10-29 at 02:24:00Z and The creator was the same guy Robert.

Moreover , I found a gif image under file under views, File types , then by MIME Type, then image then gif. This pic is taken at the Hollywood & McCaddn, the place where Robert and Laila meet.



Created: 2004-10-28 at 11:17:44 EDT and Modified: 2004-10-28 at 11:17:46. EDT



In addition I have found four email addresses.

addrsamguarillo@hotmail.com Robert's email

flowergirl96@hotmail.com This was Laila's email address

inet@microsoft.com

samguarillo@hotmail.com This was Robert's email address

and while analyzing those emails I have found the message she sent him (samguarillo@hotmail.com) after she receive the two doc messages (hey.doc which was received in October 26 and her.doc which was received in October 25) .

The body of the email was : A coffee

It was created on Thu ,28 Oct 2004 at 19:10:54

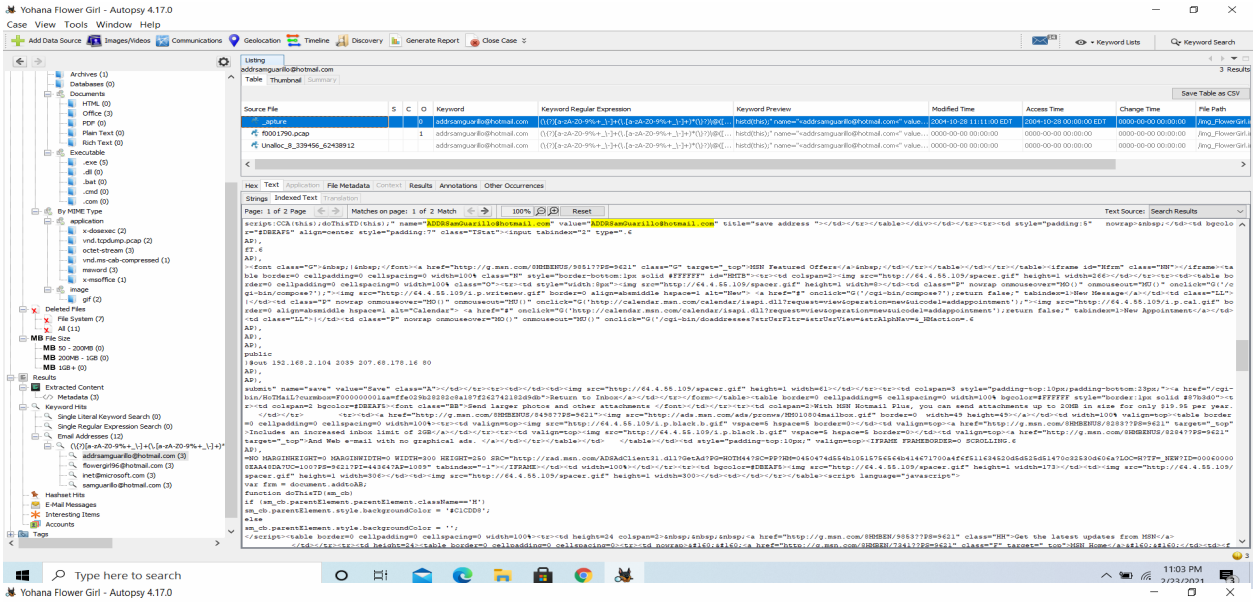
Login = flowergirl 96

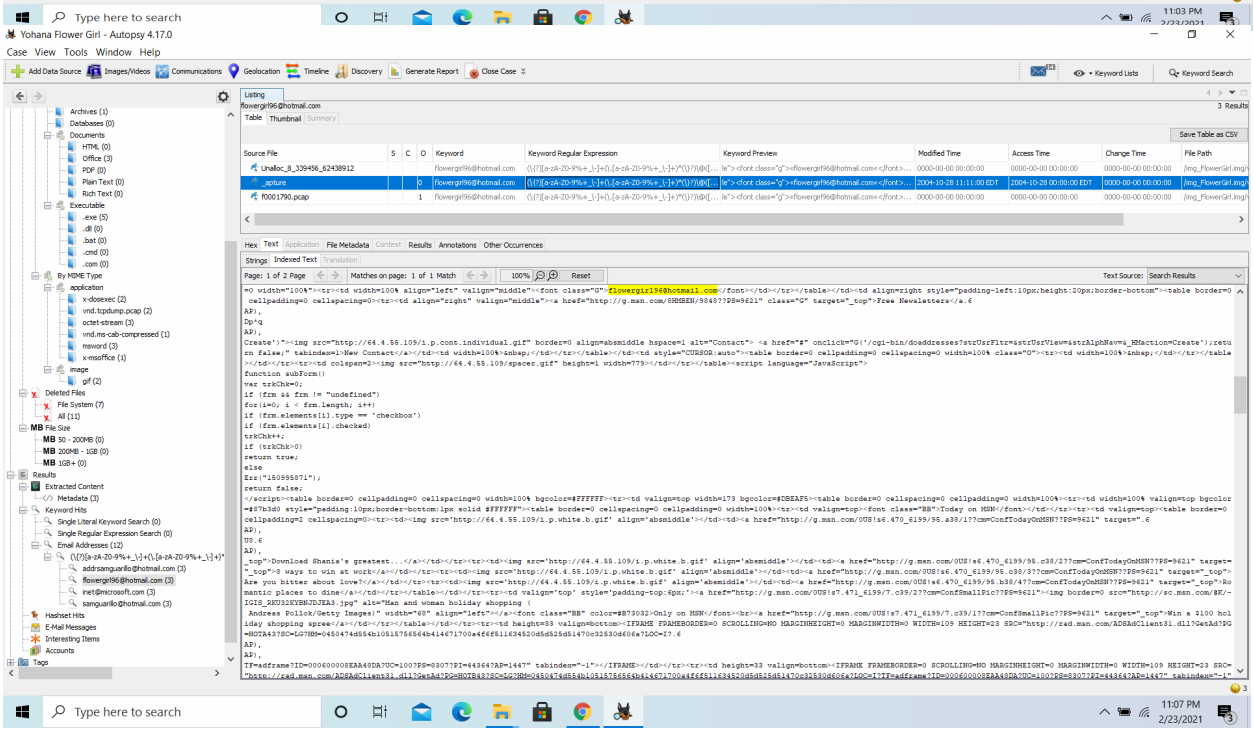
She said "Sure coffee sounds great lets meet at the coffee shop on the corner Hollywood and McCaddn. It's the nice out of the way spot. See you at 7 p.m Leila."

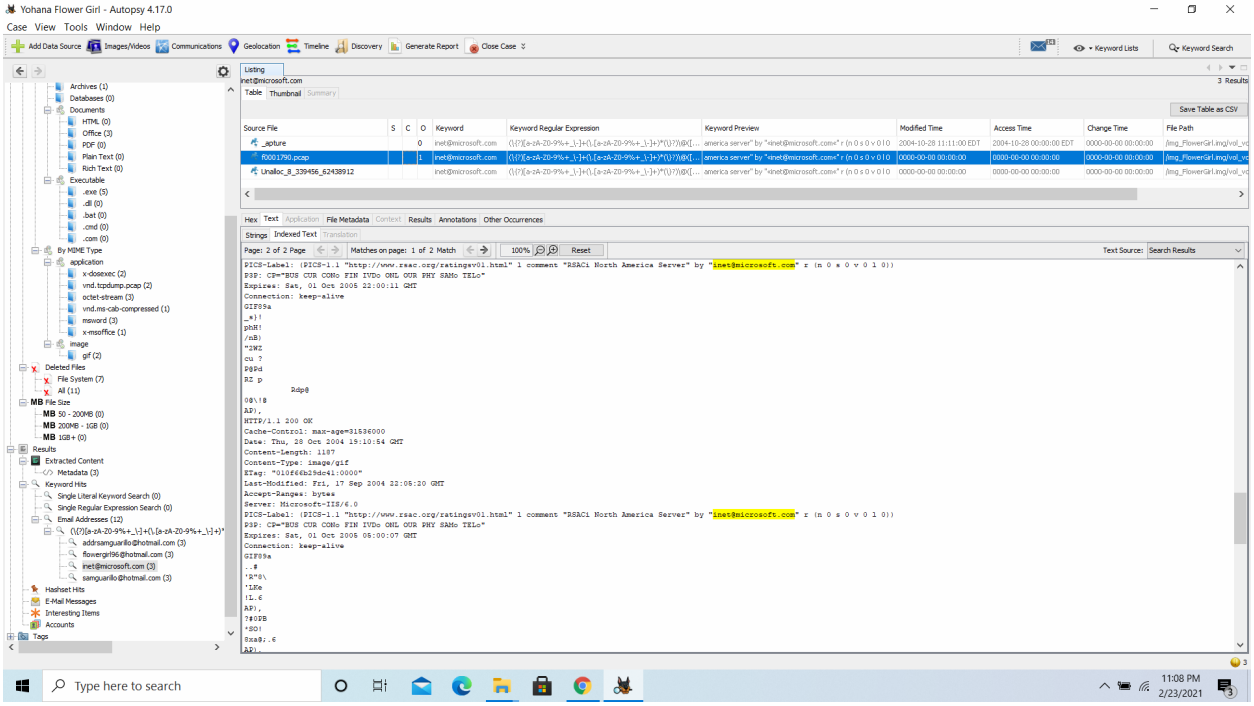
So, from this email I can tell they have agreed to meet at Hollywood & McCaddn. (the map is tagged above).

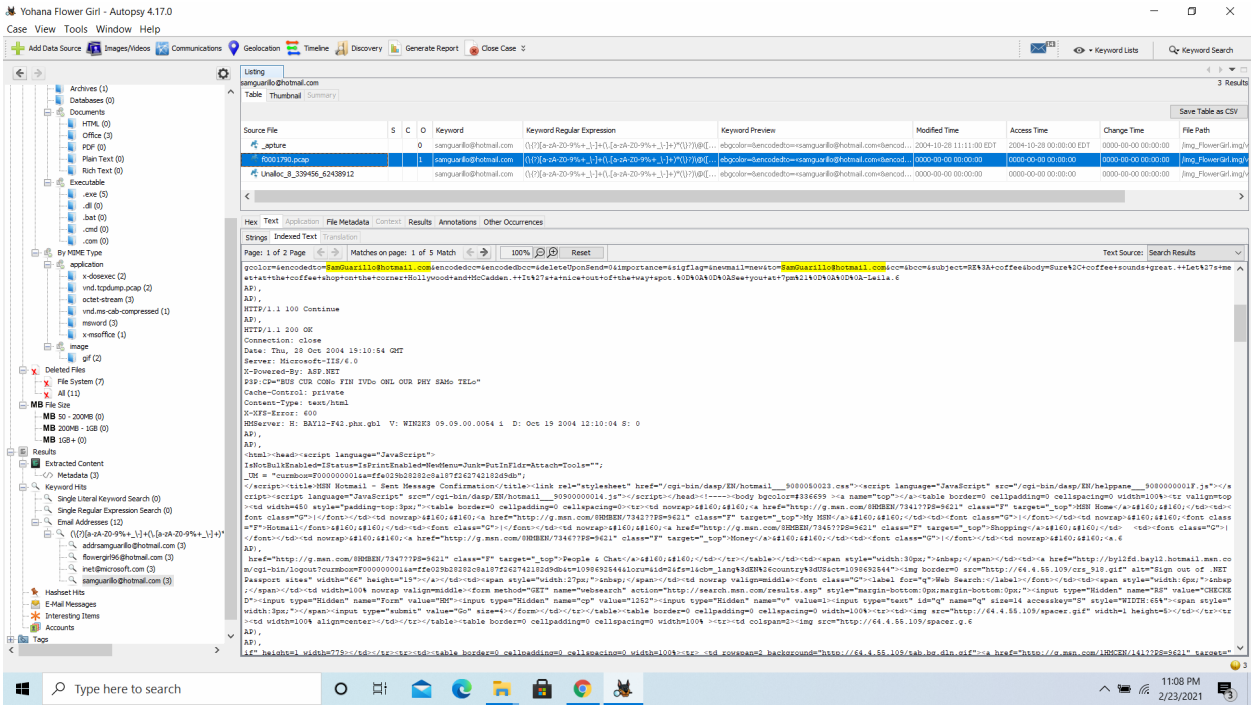
From the above analysis her login information was, Login = flowergirl 96

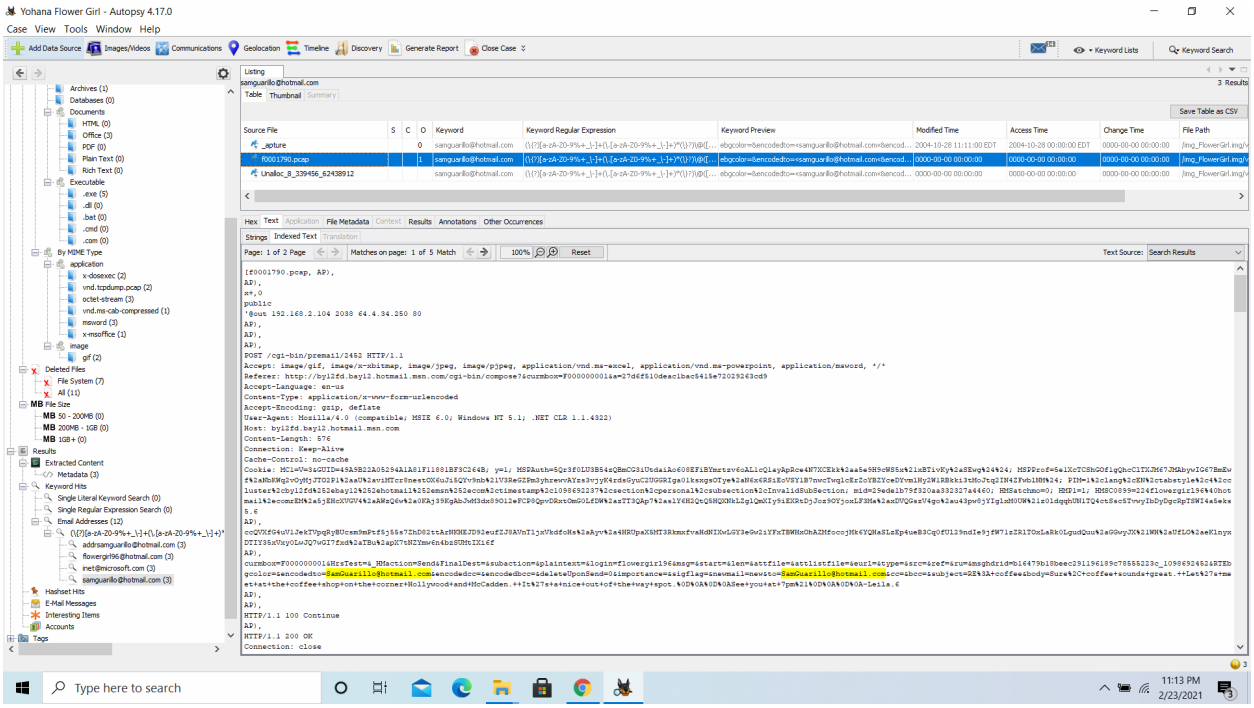
They call her flower girl ,because I think it is her nick name .That's why she used it for her login information.


Yohana Flower Girl - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
addrsamguarillo@hotmail.com
3 Results
Table
Thumbnail
Summary
Save Table as CSV
Source File
Keyword
Keyword Regular Expression
Keyword Preview
Modified Time
Access Time
Change Time
File Path
_apture
f0001790.pcap
Unalloc_8_339456_62438912
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
Strings
Indexed Text
Translation
Page: 1 of 2 Page
Matches on page: 1 of 2 Match
Reset
Text Source:
Search Results
Archives (1)
Databases (0)
Documents
HTML (0)
Office (3)
PDF (0)
Plain Text (0)
Rich Text (0)
Executable
.exe (5)
.dll (0)
.bat (0)
.cmd (0)
.com (0)
By MIME Type
application
x-dosexec (2)
vnd.tcpdump.pcap (2)
octet-stream (3)
vnd.ms-cab-compressed (1)
msword (3)
x-msoffice (1)
image
gif (2)
Deleted Files
File System (7)
All (11)
MB File Size
MB 50 - 200MB (0)
MB 200MB - 1GB (0)
MB 1GB+ (0)
Results
Extracted Content
Metadata (3)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (12)
addrsamguarillo@hotmail.com (3)
flowergirl96@hotmail.com (3)
inet@microsoft.com (3)
samguarillo@hotmail.com (3)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Type here to search
11:03 PM
2/23/2021


Yohana Flower Girl - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
flowergirl96@hotmail.com
3 Results
Table
Thumbnail
Summary
Save Table as CSV
Source File
Keyword
Keyword Regular Expression
Keyword Preview
Modified Time
Access Time
Change Time
File Path
Unalloc_8_339456_62438912
_apture
f0001790.pcap
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
Strings
Indexed Text
Translation
Page: 1 of 2 Page
Matches on page: 1 of 1 Match
Reset
Text Source:
Search Results
Archives (1)
Databases (0)
Documents
HTML (0)
Office (3)
PDF (0)
Plain Text (0)
Rich Text (0)
Executable
.exe (5)
.dll (0)
.bat (0)
.cmd (0)
.com (0)
By MIME Type
application
x-dosexec (2)
vnd.tcpdump.pcap (2)
octet-stream (3)
vnd.ms-cab-compressed (1)
msword (3)
x-msoffice (1)
image
gif (2)
Deleted Files
File System (7)
All (11)
MB File Size
MB 50 - 200MB (0)
MB 200MB - 1GB (0)
MB 1GB+ (0)
Results
Extracted Content
Metadata (3)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (12)
addrsamguarillo@hotmail.com (3)
flowergirl96@hotmail.com (3)
inet@microsoft.com (3)
samguarillo@hotmail.com (3)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Type here to search
11:07 PM
2/23/2021

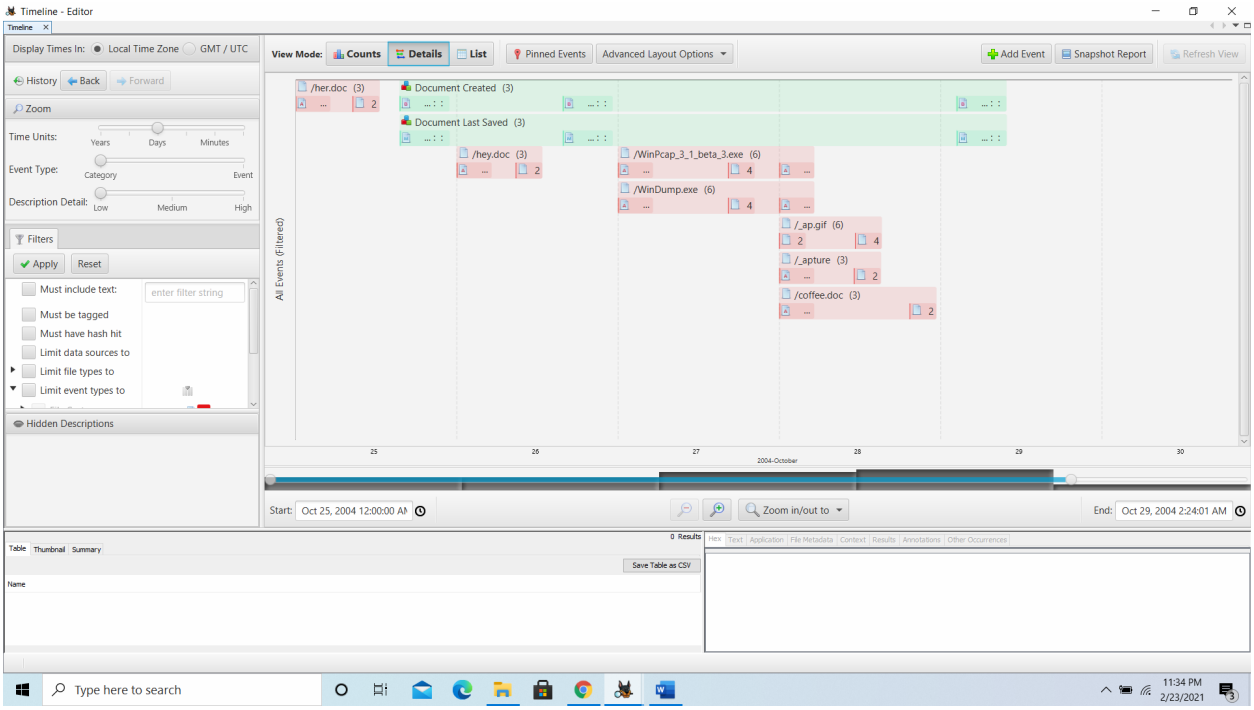

Yohana Flower Girl - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
inet@microsoft.com
3 Results
Table
Thumbnail
Summary
Save Table as CSV
Source File
Keyword
Keyword Regular Expression
Keyword Preview
Modified Time
Access Time
Change Time
File Path
_apture
f0001790.pcap
Unalloc_8_339456_62438912
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
Strings
Indexed Text
Translation
Page: 2 of 2 Page
Matches on page: 1 of 2 Match
100%
Reset
Text Source:
Search Results
Archives (1)
Databases (0)
Documents
HTML (0)
Office (3)
PDF (0)
Plain Text (0)
Rich Text (0)
Executable
.exe (5)
.dll (0)
.bat (0)
.cmd (0)
.com (0)
By MIME Type
application
x-dosexec (2)
vnd.tcpdump.pcap (2)
octet-stream (3)
vnd.ms-cab-compressed (1)
msword (3)
x-msoffice (1)
image
gif (2)
Deleted Files
File System (7)
All (11)
MB File Size
MB 50 - 200MB (0)
MB 200MB - 1GB (0)
MB 1GB+ (0)
Results
Extracted Content
Metadata (3)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (12)
addrsamguarillo@hotmail.com (3)
flowergirl96@hotmail.com (3)
inet@microsoft.com (3)
samguarillo@hotmail.com (3)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Type here to search
11:08 PM
2/23/2021


Yohana Flower Girl - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
samguarillo@hotmail.com
3 Results
Table
Thumbnail
Summary
Save Table as CSV
Source File
Keyword
Keyword Regular Expression
Keyword Preview
Modified Time
Access Time
Change Time
File Path
_apture
f0001790.pcap
Unalloc_8_339456_62438912
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
Strings
Indexed Text
Translation
Page: 1 of 2 Page
Matches on page: 1 of 5 Match
100%
Reset
Text Source:
Search Results
Archives (1)
Databases (0)
Documents
HTML (0)
Office (3)
PDF (0)
Plain Text (0)
Rich Text (0)
Executable
.exe (5)
.dll (0)
.bat (0)
.cmd (0)
.com (0)
By MIME Type
application
x-dosexec (2)
vnd.tcpdump.pcap (2)
octet-stream (3)
vnd.ms-cab-compressed (1)
msword (3)
x-msoffice (1)
image
gif (2)
Deleted Files
File System (7)
All (11)
MB File Size
MB 50 - 200MB (0)
MB 200MB - 1GB (0)
MB 1GB+ (0)
Results
Extracted Content
Metadata (3)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (12)
addrsamguarillo@hotmail.com (3)
flowergirl96@hotmail.com (3)
inet@microsoft.com (3)
samguarillo@hotmail.com (3)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Type here to search
11:08 PM
2/23/2021



- I also found all the files he sent to her under the Deleted files.
  Her.doc , Hey.doc ,Coffee.doc , f0000833.cab and f0001541.exe .

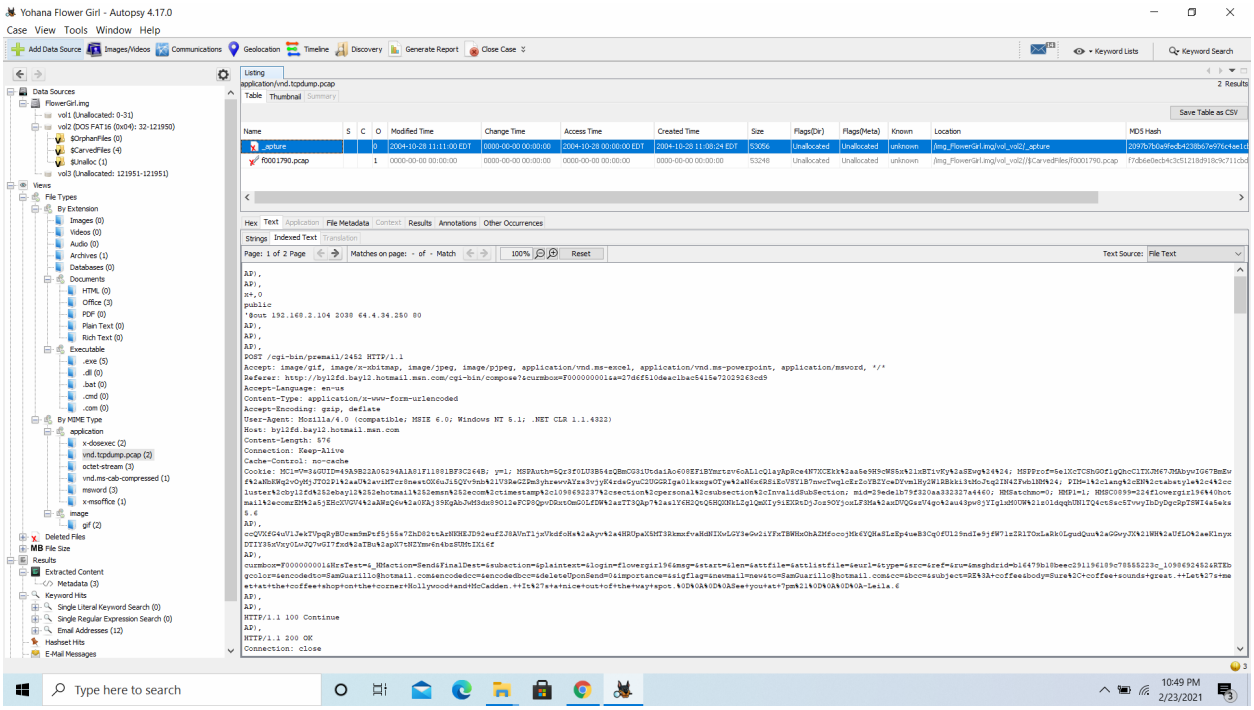
And below is the details timeline of each and every activity.



I also found some applications by MIME type :

vnd.tcpdump.pcap ,

from that file I found the login information of Leila. Which is flowergirl 96 .



Finally, I would like to conclude my investigation by pointing out who is guilty. First Robert was texting nicely admiring her and offering her a coffee. She even agreed and go out with him for a coffee. But the day after that, He started sending her obnoxious emails. According to law of privacy Robert is guilty because he was following her. This crime is called Stalking, or harassment and it's a criminal offense.