

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.

The screenshot shows the Autopsy Forensic Browser interface. The left sidebar displays various data sources and analysis modules. The main area shows a search results table for the term 'office'. The table includes columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dr), Flags(Meta), Known, Location, MD5 Hash, and MIME Type. Below the table, a preview pane shows the content of a Microsoft Word document named 'her.doc'. The document contains the text: '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?' Below the text is a 'METADATA' section with the following details:

Application-Name: Microsoft Word 10.0
Author: Robert Lawrence
Character-Count: 234
Comments:
Company:
Content-Type: application/msword
Creation-Date: 2004-10-25T15:30:00Z
Editor-Time: 1200000000
Keywords:
Last-Authored: Robert Lawrence
Last-Modified: 2004-10-25T15:32:00Z
Last-Saved: 2004-10-25T15:32:00Z
Page-Count: 1
Revision-Number: 1
Template: Normal.dot
Type: Microsoft Word Document
X-TIKA:origFilesourceName:
comment:
op:revision: 1
op:subject:
creator: Robert Lawrence
date: 2004-10-25T15:30:00Z
editor: Robert Lawrence
dc:subject:
dttitle: Hey I saw you the other day
document: 2004-10-25T15:30:00Z
dtmodified: 2004-10-25T15:32:00Z
extended-properties: Application: Microsoft Word 10.0
extended-properties: Company:
extended-properties: Template: Normal.dot
meta:author: Robert Lawrence
meta:subject: document

From the above screenshot 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.

The screenshot shows the Yohana Flower Girl - Autopsy 4.17.0 interface. The top navigation bar includes Case, View, Tools, Window, Help, Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, and Close Case. A Keyword Lists section is also present.

The main workspace displays a search results table for 'her.doc'. The table has columns: Source File, S, C, O, Date Modified, Program Name, Date Created, User ID, Owner, and Data Source. The table shows three rows: 'her.doc' (modified 2004-10-25 15:32:00 EDT, Microsoft Word 10.0, created 2004-10-25 15:30:00 EDT, Robert Lawrence, Robert Lawrence, PowerGrL.Img), 'hey.doc' (modified 2004-10-26 15:46:00 EDT, Microsoft Word 10.0, created 2004-10-26 15:47:00 EDT, Robert Lawrence, Robert Lawrence, PowerGrL.Img), and 'coffee.doc' (modified 2004-10-29 02:24:00 EDT, Microsoft Word 10.0, created 2004-10-29 02:23:00 EDT, Robert Lawrence, Robert Lawrence, PowerGrL.Img).

The left sidebar contains a tree view of the investigation, including sections like File Type, By Extension, Plain Text, Rich Text, Executables, DLLs, BATs, CMDs, COMs, Applications, and Deleted Files. A Results section lists artifacts such as MB 50 > 200KB (0), MB 200KB - 1MB (0), and MB 1MB+ (0). A Keyword section includes Single Literal Keyword Search (0) and Single Regular Expression Search (0).

The bottom taskbar includes icons for File Explorer, Mail, Task View, Edge, File Explorer, and Task Manager, along with a search bar and system status indicators.

The screenshot shows the Yohana Flower Girl - Autopsy 4.17.0 interface. The top menu bar includes Case, View, Tools, Window, Help, and several icons for adding data sources, images/videos, communications, geolocation, timeline, discovery, generating reports, and closing cases. A search bar at the top right contains the text "Keyword Lists" and "Keyword Search".

The left sidebar displays a tree view of data sources and files. Under "Data Sources", there is a folder named "PowerGrl.lmg" containing several sub-folders and files, including "vol1 (Unallocated: 0-31)", "vol2 (DOS FAT 6 (0x0) 32-121950)", "vol3 (DOS FAT 6 (0x0) 32-121950)", "vol4 (Unallocated: 0)", "vol5 (Unallocated: 0)", "vol6 (Unallocated: 0)", and "vol7 (Unallocated: 121951-121951)". Under "File Types", categories like "By Extension" (e.g., Text, Images, Audio, Video, Archives, Databases), "Documents" (HTML, PDF, RTF, Plain Text, Rich Text), "Executable" (exe, dll, bat, cmd, com), and "By MIME Type" (application, image, text) are listed. "application" includes sub-categories like "x-dosexec", "vnd.ms-word", "vnd.ms-powerpoint", "vnd.ms-cab-compressed", and "x-msmetafile". "image" includes "gif". "text" includes "MB-Text Files" and "MB-File Size". "Results" includes "Extracted Content" (Metadata, Keyword), "Single Literal Keyword Search", "Regular Expression Search", "Email Addresses", "Hotfile Hits", and "E-Mail Messages".

The main workspace is titled "Listing Office" and shows a table of files. The columns are Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flag(Dr), Flag(Meta), Known, Location, and MD5 Hash. The table lists four files: "her.doc" (modified 2004-10-25 00:32:08 EDT, created 2004-10-25 00:00:00 EDT, size 19968, flagged as Allocated, location [img\_FlowerGrl.lmg]\vol\vol2\her.doc, MD5 hash 97957715286738d57978), "hey.doc" (modified 2004-10-26 00:40:10 EDT, created 2004-10-26 00:00:00 EDT, size 19968, flagged as Allocated, location [img\_FlowerGrl.lmg]\vol\vol2\hey.doc, MD5 hash 040134f1387176a4d07d1e19ed), "coffee.doc" (modified 2004-10-28 19:24:46 EDT, created 2004-10-28 00:00:00 EDT, size 19968, flagged as Allocated, location [img\_FlowerGrl.lmg]\vol\vol2\coffee.doc, MD5 hash 48335959596eda15a52c516a76d1), and "her2.doc" (modified 2004-10-26 00:40:10 EDT, created 2004-10-26 00:00:00 EDT, size 19968, flagged as Allocated, location [img\_FlowerGrl.lmg]\vol\vol2\her2.doc, MD5 hash application/x-msword).

The bottom pane shows detailed file metadata for "hey.doc", including fields like String, IndexedText, Text, Application, File Metadata, Context, Results, Annotations, Other Occurrences, and Translation. It also includes a search bar for "String" and "IndexedText" and a "Matches on page: <-- of -->" search field.

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

3 Results

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	Robert Lawrence	FlowerGrl.Img
her.doc				2004-10-25 15:32:00 EDT	Microsoft Word 10.0	2004-10-25 15:30:00 EDT	Robert Lawrence	Robert Lawrence	FlowerGrl.Img
coffee.doc				2004-10-29 02:24:00 EDT	Microsoft Word 10.0	2004-10-29 02:23:00 EDT	Robert Lawrence	Robert Lawrence	FlowerGrl.Img

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 1 of 1 Result

Type Value Source(s)

Date Modified 2004-10-26 15:48:00 org.sleuthkit.autopsy.keywordsearch.KeywordSearch\$in

Program Name Microsoft Word 10.0 org.sleuthkit.autopsy.keywordsearch.KeywordSearch\$in

Date Created 2004-10-26 15:47:00 org.sleuthkit.autopsy.keywordsearch.KeywordSearch\$in

User ID Robert Lawrence org.sleuthkit.autopsy.keywordsearch.KeywordSearch\$in

Owner Robert Lawrence org.sleuthkit.autopsy.keywordsearch.KeywordSearch\$in

Source File Path /img\_FlowerGrl.Img/vol\_vol2/hey.doc org.sleuthkit.autopsy.keywordsearch.KeywordSearch\$in

Artifact ID 9223372036854775806

By NAME 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)
  - (?:(?:(a-zA-Z0-9%\_+.)+|([a-zA-Z0-9%+\_.]+)+)\*^

11:00 PM 2/23/2021

And from the hey.doc ,

He wrote her a 268 character 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 screenshot shows the Yohana Flower Girl - Autopsy 4.17.0 interface. The top navigation bar includes Case, View, Tools, Window, Help, and several icons for Data Sources, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, and Close Case.

The left sidebar contains a tree view of the case structure:

- Data Sources
  - FlowerGirl
  - Windows-File-System (0x00)
  - vfd2 (DOS FAT16 (0x00): 32-121950)
    - 0x00 (0)
    - 0x01 (4)
    - 0x02 (1)
  - uncal (0x00)

Below this are sections for Virus, File Types, By Extension, Documents, Executable, By MIME Type, and MB File Size.

The main workspace displays a listing of files:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag(Dr)	Flag(Meta)	Known	Location	MDS Hash	MIME Type
her.doc	1	2004-10-26 08:32:08 EDT	0000-00-00 00:00:00	2004-10-25 00:00:00 EDT	2004-10-25 00:00:00 EDT	19968	Allocated	Allocated	Unknown	/mg_FlowerGirl/mg/vd_v02/her.doc	79057752d2879f9db73db577b	application/msword		
hey.doc	1	2004-10-26 08:40:10 EDT	0000-00-00 00:00:00	2004-10-25 00:00:00 EDT	2004-10-26 08:40:07 EDT	19968	Allocated	Allocated	Unknown	/mg_FlowerGirl/mg/vd_v02/hey.doc	c4019f819717c9e0de1a6e119e1	application/msword		
coffee.doc	1	2004-10-26 19:24:46 EDT	0000-00-00 00:00:00	2004-10-28 00:00:00 EDT	2004-10-28 19:24:46 EDT	19968	Allocated	Allocated	Unknown	/mg_FlowerGirl/mg/vd_v02/coffee.doc	a03c5868959ed5a5e27c93fe76d1	application/msword		

Below the table are tabs for Hex, Text, Application, File Metadata, Context, Results, Annotations, Other Occurrences, String, Indexed Text, and Tesseract. The Text tab is selected, showing the content of the 'hey.doc' file:

```
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 bottom right shows the Text Source and File Text buttons. The bottom of the screen features a taskbar with various icons and a search bar.

The screenshot shows the Yohana Flower Girl - Autopsy 4.17.0 interface. The main window displays a file analysis session for a file named 'coffee.doc'. The left sidebar shows various file types and their counts, such as PDFs (3), Office documents (3), and Executables (1). The central pane shows a table of file metadata, including Source File, Date Modified, Program Name, Date Created, User ID, Owner, and Data Source. Below the table is a detailed view of the file's properties, including Type, Value, and Source(s). The bottom pane shows a search results list with items like 'Deleted Files' and 'File System (7)'. The taskbar at the bottom includes icons for File Explorer, Task View, Mail, Edge, File History, and Google Chrome.

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	Robert Lawrence	FlowerGirl.ing
her.doc				2004-10-29 15:32:00 EDT	Microsoft Word 10.0	2004-10-25 15:30:00 EDT	Robert Lawrence	Robert Lawrence	FlowerGirl.ing
coffee.doc				2004-10-29 02:24:00 EDT	Microsoft Word 10.0	2004-10-29 02:23:00 EDT	Robert Lawrence	Robert Lawrence	FlowerGirl.ing

Metadata

Type	Value	Source(s)
Date Modified	2004-10-29 02:24:00	org.sleuthkit.autopsy.keywordsearch.KeywordSearch\$1
Program Name	Microsoft Word 10.0	org.sleuthkit.autopsy.keywordsearch.KeywordSearch\$1
Date Created	2004-10-29 02:23:00	org.sleuthkit.autopsy.keywordsearch.KeywordSearch\$1
User ID	Robert Lawrence	org.sleuthkit.autopsy.keywordsearch.KeywordSearch\$1
Owner	Robert Lawrence	org.sleuthkit.autopsy.keywordsearch.KeywordSearch\$1
Source File Path	J:\img_FlowerGirl\img\vol_02\coffee.doc	org.sleuthkit.autopsy.keywordsearch.KeywordSearch\$1
Artifact ID	9223372036854775804	

Results

- Deleted Content (3)
- File System (7)
  - All (11)
- MB (0)
- MB 10+ (0)
  - MB 2000B (0)
  - MB 200B+ (0)
  - MB 1GB+ (0)
- Results
  - Encrypted Content (3)
  - Rehashable (3)
- Keyword Hits
  - Single Literal Keyword Search (0)
  - Single Regular Expression Search (0)
  - Email Addresses (12)
    - ((?)[a-zA-Z0-9%&^\_`<\`[a-zA-Z0-9%&^\_`>]\*`])\*

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.

The screenshot shows the Autopsy 4.17.0 interface. On the left, the file tree displays a folder named 'Flower girl - Autopsy 4.17.0' containing various data sources and files. A file named '6002525.gif' is selected in the 'Views' section under 'File Types' and 'image/gif'. The main pane shows a table of file metadata, with one row highlighted for '6002525.gif'. Below the table is a Microsoft MapPoint map of the Hollywood & McCaddn area, showing streets like Franklin Ave, Hollywood Blvd, and Selma Ave.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash	MIME Type	Extensions
6002525.gif				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	8814	Unallocated	Unallocated	Unknown	/img_FlowerGirl/img/\$CarvedFiles/0002525.gif	9bc3923c9e72fd05d7ea8cd781011	Image/gif	gif

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

This screenshot shows the Autopsy interface with the file '6002525.gif' selected. The left pane shows the file tree with 'Flower girl - Autopsy 4.17.0' selected. The right pane displays detailed file metadata for '6002525.gif'. The file is identified as an application/octet-stream with a size of 0. It was modified on 2004-10-27 16:23:54 EDT and accessed on 2004-10-27 16:23:54 EDT. The file was created on 2004-10-27 16:24:06 EDT and last changed on 2004-10-27 16:24:04 EDT. The MD5 hash is d4108c9800b204e9800998ecf8427e. The file is listed as unallocated. The file name is '6002525.gif' and it is located at '/img\_FlowerGirl/img/vol\_002/\_ap.gif'. The file type is 'File System' and the MIME type is 'application/octet-stream'. The file size is 0. The file has no file name allocation and no media allocation. The file was modified on 2004-10-28 11:17:46 EDT, accessed on 2004-10-28 00:00:00 EDT, created on 2004-10-28 11:17:44 EDT, and last changed on 0000-00-00 00:00:00. The MD5 hash is d4108c9800b204e9800998ecf8427e. The file lookup results show an internal ID of 23. The file was from the Sleuth Kit tool, with a directory entry time of 2004-10-28 11:17:46 (EDT), written on 2004-10-28 11:17:46 (EDT), accessed on 2004-10-28 00:00:00 (EDT), and created on 2004-10-28 11:17:44 (EDT). Sensors report a starting address of 607, length of 0. The file is located at 'C:\Windows\system32\cmd.exe'.

In addition I have found four email addresses.

[addrssamguarillo@hotmail.com](mailto:addrssamguarillo@hotmail.com) Robert's email

[flowergirl96@hotmail.com](mailto:flowergirl96@hotmail.com) This was Laila's email address

[inet@microsoft.com](mailto:inet@microsoft.com)

[samguarillo@hotmail.com](mailto: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](mailto: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.



The screenshot shows the Yohana Flower Girl - Autopsy 4.17.0 interface. The top navigation bar includes Case, View, Tools, Window, Help, and a Keyword Search field. The main workspace displays a file analysis session for 'sanguillo@hotmail.com'. The left sidebar lists various file types and their counts, such as Archives (1), Documents (1), HTML (0), Office (3), PDF (0), Plain Text (0), Rich Text (0), Executable (0), and more. A 'Deleted Files' section is also present. The central area shows a detailed view of a file named '20011760.jpg', with tabs for Listing, Source File, Hex Text, Application, File Metadata, Context, Results, Annotations, and Other Occurrences. The 'Results' tab is active, showing a table with columns: Modified Time, Access Time, Change Time, and File Path. The table contains two rows of data. The bottom of the interface features a search bar, a toolbar with various icons, and a system tray.

- 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.

The screenshot shows the Timeline - Editor application with the following details:

- Timeline View:** The main area displays a horizontal timeline from October 25, 2004, to October 30, 2004. Events are color-coded by source or type.
- Event Details:** A tooltip for an event on October 28, 2004, shows "her.doc (3)" with three sub-events: "Document Created (3)", "Document Last Saved (3)", and "File Deleted (3)".
- Filters:** On the left, there are filters for "Must include text:" (with a search bar), "Must be tagged", "Must have hash hit", "Limit data sources to", "Limit file types to", and "Limit event types to".
- Hidden Descriptions:** A section labeled "Hidden Descriptions" is present.
- Search and Tools:** At the bottom, there are search icons for "Start" (Oct 25, 2004) and "End" (Oct 29, 2004 2:24:01). There are also buttons for "Zoom in/out to" and "Save Table as CSV".
- Bottom Panel:** The bottom panel contains tabs for "Table", "Thumbnail", and "Summary". It also includes a "Results" section with a "Hex" view and other analysis tools.

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 .

The screenshot shows the Yohana Flower Girl - Autopsy 4.17.0 interface. The top navigation bar includes Case, View Tools, Window, Help, and a Keyword Search field. The main workspace displays a file analysis session for a PCAP file named 'f0001790.pcap'. The left sidebar shows a tree view of the file structure, including Data Sources (PowerGirl.jpg, PowerGirl.m4a), File Types (Images, Videos, Audio, Archives, Databases), Documents (HTML, Office, PDF, Plain Text, Text), Executables (exe, dll, bat, cmd, powershell), and By MIME Type (application/x-dosexec, vnd.tzdump.pcap, octet-stream, vnd.ms-compressed, rawdata, x-wmefi). A 'Deleted Files' section is also present. The right side features a detailed table of file contents, search results, and a preview pane. The bottom status bar shows system information like battery level, signal strength, and the date/time.

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.