2024

Case101: Flower Girl

DEPARTMENT OF INTERNAL INVESTIGATIONS

AHMAD ABDULLAH MUJHAID I221609

Table of Contents

Introduction 3

Acquisition & Tools Used 3

Authentication & Duplication 3

Analysis 5

Files 5

Executive Summary

Introduction

In today's digital age, USB devices are commonly used to store and transfer data. However, they can also be leveraged to carry out malicious activities, such as unauthorized data exfiltration or the spread of malware. This report presents the analysis conducted on a USB image obtained in connection with Mr Robert, a sales representative and key suspect in this investigation who has been accused of harassing one of his colleagues on and off work.

The investigation aims to determine the contents of the USB device, assess its usage, and identify any potential malicious activity. By examining the file system, timestamps, and artefacts on the device, we seek to uncover key evidence that could assist in understanding the events that occurred.

The analysis was conducted in accordance with digital forensic best practices, ensuring data integrity throughout the process. The following sections will outline the methodology used in acquiring and analysing the USB image, as well as the findings and conclusions drawn from the investigation.

Acquisition & Tools Used

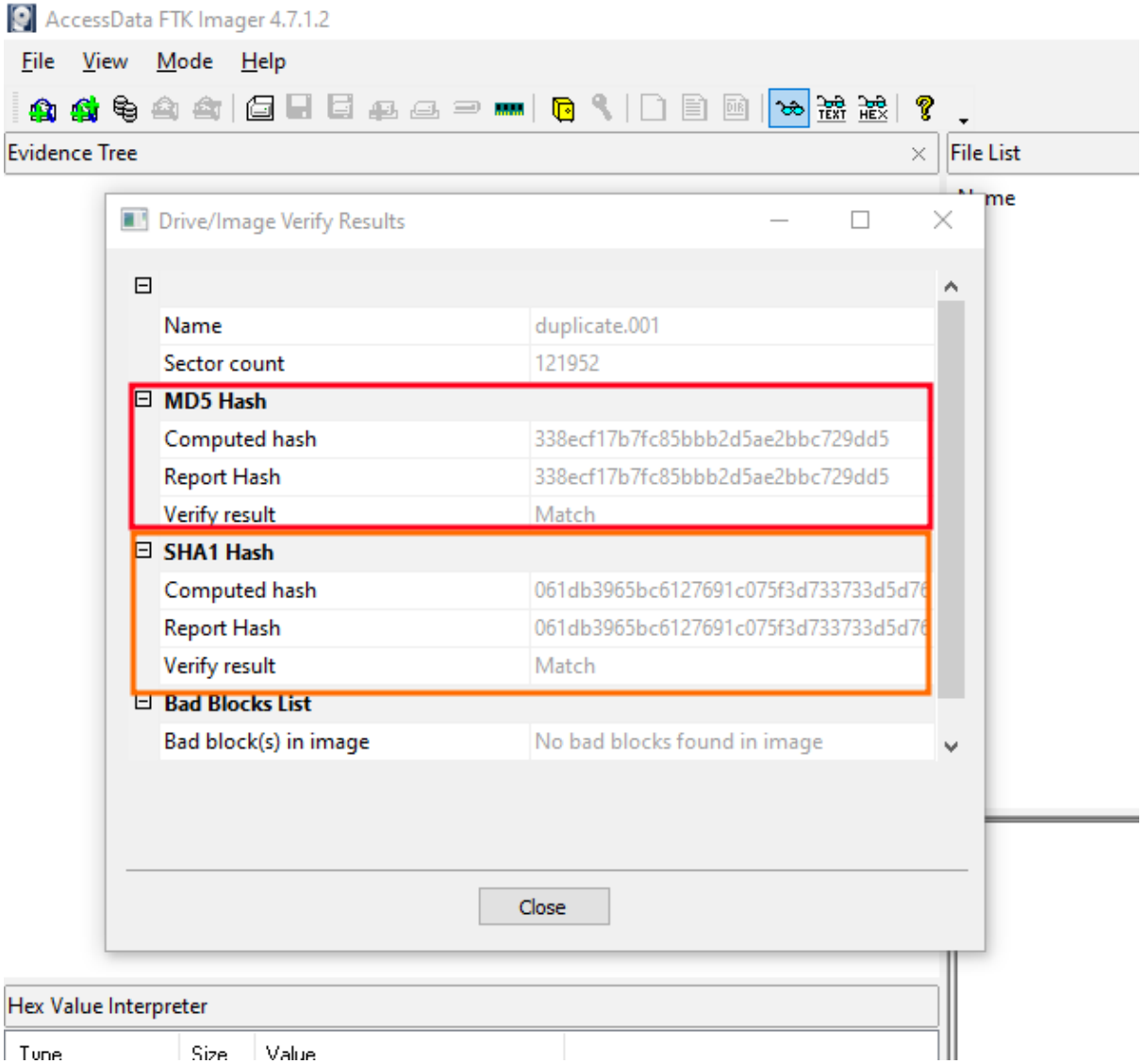
The original image of the USB was acquired from ABC Corp's HR department under the suspicion of finding evidence related to the said act of harassment.

The tools that were used for this investigation are free or open-source and commonly are used to carry out digital investigations.

- **FTK Imager:** Used to make a duplicate image file of the original image to ensure integrity.
- **Autopsy:** Used to do a complete analysis of the image for any evidence.

Authentication & Duplication

The given image of the USB was immediately duplicated using FTK Imager Software, a forensic tool used to acquire and create exact copies (forensic images) of digital media without altering the original data. It also allows users to preview and analyze files, including deleted data, from a variety of devices.The duplicate image is a RAW format image meaning it contains all the data that the original image file ‘FlowerGirl.img’ contains.



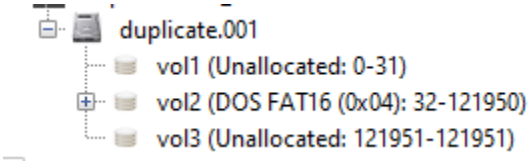
Case101: 1 Picture of duplication of the Image – 02:10 UTC-5

Analysis

Using Autopsy, we started investigating the USB image file to find some evidence of whether the accused did the act or not.

There were three volumes in the USB disk image.

1. **Vol1:** Containing 32 Sectors of unallocated data
2. **Vol2:** The main volume that contains actual data related to the investigation having 121918 sectors ranging from 32-121950
3. **Vol3:** Is a single sector unallocated volume.



- **File System:** The file system used by the main Volume Vol2 is FAT16.

Files

The below table shows the files that were present on the USB disk image. This table contains both deleted and non-deleted files

Name	Modified Time	Change T	Access Time	Created Time	Size
$OrphanFiles	0000-00-00 00:00:00	0000-00-0	0000-00-00 00:00:00	0000-00-00 00:00:00	0
$FAT1	0000-00-00 00:00:00	0000-00-0	0000-00-00 00:00:00	0000-00-00 00:00:00	122368
$FAT2	0000-00-00 00:00:00	0000-00-0	0000-00-00 00:00:00	0000-00-00 00:00:00	122368
$MBR	0000-00-00 00:00:00	0000-00-0	0000-00-00 00:00:00	0000-00-00 00:00:00	512
$CarvedFiles	0000-00-00 00:00:00	0000-00-0	0000-00-00 00:00:00	0000-00-00 00:00:00	0
$Unalloc	0000-00-00 00:00:00	0000-00-0	0000-00-00 00:00:00	0000-00-00 00:00:00	0
_ap.gif	2004-10-28 11:17:46 GMT-04:00	0000-00-0	2004-10-28 00:00:00 GMT-04:00	2004-10-28 11:17:44 GMT-04:00	0
_ap.gif	2004-10-28 11:17:46 GMT-04:00	0000-00-0	2004-10-28 00:00:00 GMT-04:00	2004-10-28 11:17:44 GMT-04:00	8814
_apture	2004-10-28 11:11:00 GMT-04:00	0000-00-0	2004-10-28 00:00:00 GMT-04:00	2004-10-28 11:08:24 GMT-04:00	53056
coffee.doc	2004-10-28 19:24:48 GMT-04:00	0000-00-0	2004-10-28 00:00:00 GMT-04:00	2004-10-28 19:24:46 GMT-04:00	19968
her.doc	2004-10-25 08:32:08 GMT-04:00	0000-00-0	2004-10-25 00:00:00 GMT-04:00	2004-10-25 08:32:06 GMT-04:00	19968
hey.doc	2004-10-26 08:48:10 GMT-04:00	0000-00-0	2004-10-26 00:00:00 GMT-04:00	2004-10-26 08:48:07 GMT-04:00	19968
WinDump.exe	2004-10-27 16:24:06 GMT-04:00	0000-00-0	2004-10-27 00:00:00 GMT-04:00	2004-10-27 16:24:04 GMT-04:00	0
WinDump.exe	2004-10-27 16:24:02 GMT-04:00	0000-00-0	2004-10-28 00:00:00 GMT-04:00	2004-10-27 16:24:04 GMT-04:00	450560
WinPcap_3_1_beta_3.exe	2004-10-27 16:23:56 GMT-04:00	0000-00-0	2004-10-27 00:00:00 GMT-04:00	2004-10-27 16:23:54 GMT-04:00	0
WinPcap_3_1_beta_3.exe	2004-10-27 16:23:50 GMT-04:00	0000-00-0	2004-10-28 00:00:00 GMT-04:00	2004-10-27 16:23:54 GMT-04:00	485810
f0001790.pcap	0000-00-00 00:00:00	0000-00-0	0000-00-00 00:00:00	0000-00-00 00:00:00	53248

Looking at the files we see three ***doc*** files in which the emails were done by Mr Robert to his colleague.

Her.doc

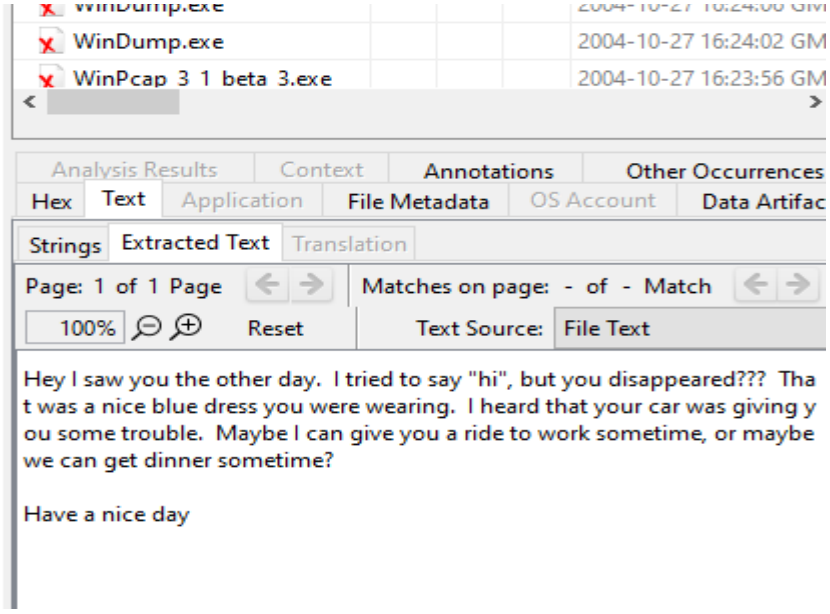
According to the timestamp in the metadata of the emails, this email was done first

- **Application Name**: Microsoft Word 10.0
- **Author**: Robert Lawrence
- **Character Count**: 234
- **Creation Date**: October 25, 2004, at 15:30:00 UTC
- **Last Author**: Robert Lawrence
- **Last Modified Date**: October 25, 2004, at 15:32:00 UTC
- **Last Save Date**: October 25, 2004, at 15:32:00 UTC
- **Page Count**: 1
- **Revision Number**: 1
- **Template**: Normal.dot
- **Word Count**: 40
- **Title**: "Hey I saw you the other day"

The email was as such:

“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?

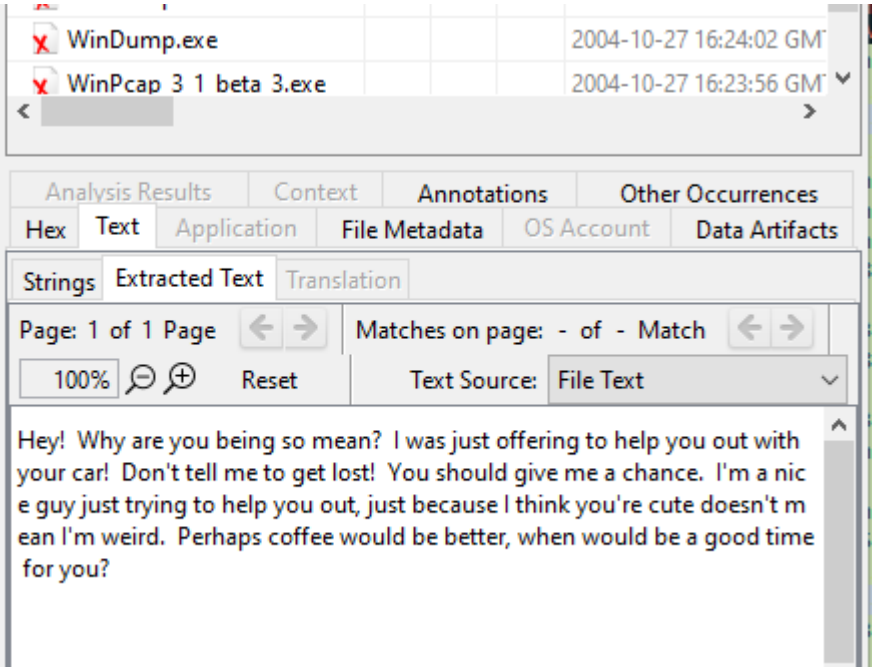
Have a nice day”



Hey.doc

- **Application Name**: Microsoft Word 10.0
- **Author**: Robert Lawrence
- **Creation Date**: October 26, 2004, at 15:47:00 UTC
- **Last Author**: Robert Lawrence
- **Last Modified Date**: October 26, 2004, at 15:48:00 UTC
- **Last Save Date**: October 26, 2004, at 15:48:00 UTC
- **Title**: "Hey"

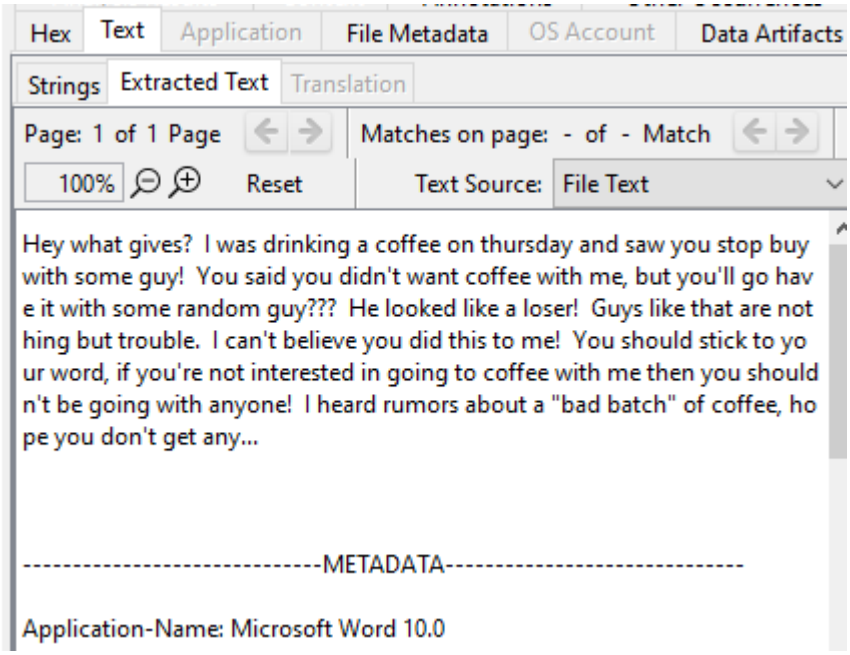
“Hey! Why are you being so mean? I was just offering to help you out with your car! Don't tell me to get lost! You should give me a chance. I'm a nice guy just trying to help you out, just because I think you're cute doesn't mean I'm weird. Perhaps coffee would be better, when would be a good time for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



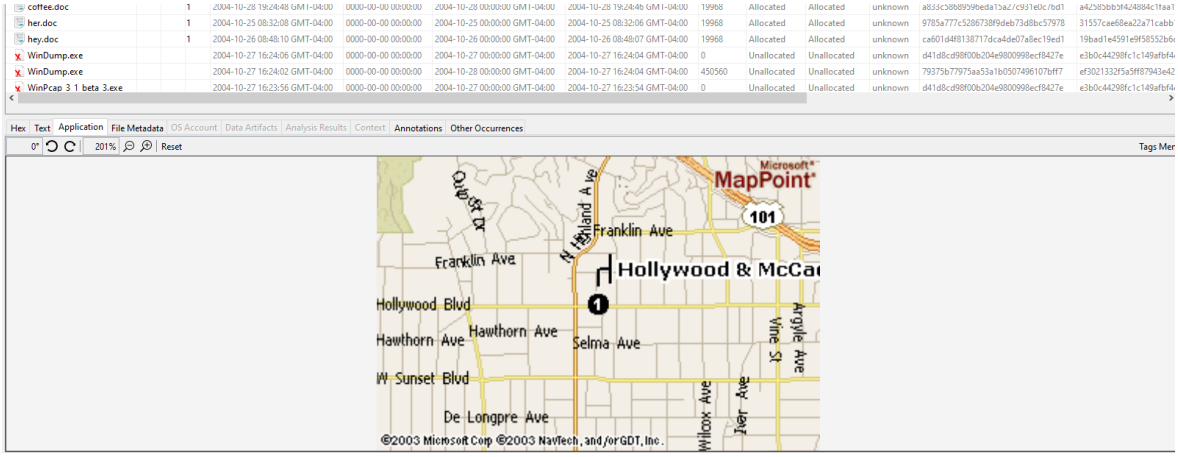
Coffee.doc

- **Author**: Robert Lawrence
- **Creation Date**: October 29, 2004, at 02:23:00 UTC
- **Last Author**: Robert Lawrence
- **Last Modified Date**: October 29, 2004, at 02:24:00 UTC
- **Last Save Date**: October 29, 2004, at 02:24:00 UTC
- **Title**: "Hey what gives"

“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...”



(1)



“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.

See you at 7pm!

-Leila”