Case Name: Wk 7 Final Project
Examiner Name: Candace [redacted]

Table of Contents

List of Illustrative Materials

Tables

Figures

Executive Summary

Background

The Utica Police Department has identified two suspects in their investigation of a string of bank robberies that have occurred within Utica City limits for the past three months. Up until this point, however, they have not had enough evidence to definitively tie the suspects to the crimes. During a recent traffic stop of one suspect, officers seized a USB drive. An evidence technician acquired a raw image of the drive as officers were unable to view its contents.

Request

Sergeant Brunson has directed the image to the examiner for analysis. Specifically, the examiner should ascertain whether the drive is relevant to the investigation, and whether it contains any information related to the next planned robbery target. Both allocated and unallocated files should be reviewed.

Summary of Findings

One allocated file was retrieved from the hard drive image, which was unopenable in its original format. By de-nesting the file a jpeg file was ultimately revealed: a picture of freeway traffic taken from the inside of a passenger vehicle. This image did not appear relevant to the investigation and lacked GPS exif data. It did, however, contain the phone model of the suspect. 5 files were carved from unallocated space (see table 1 for offset and header/footer summation): *File1, file2, file3, file4,* and *file5. File1* shows an address: 233 Genesee Street in Utica, New York. *File2* is a picture of the M&T Bank logo. *File3* is a street view of an M&T Bank. Its exif data revealed the coordinates 43°06'01.0"N 75°13'57.0"W. These coordinates were confirmed using Google Maps. These coordinates also refer to the same place as the coordinates in *File1*. *File4* is a picture of cross street signs “Bleecker St” and “Kossuth Ave”, and the superimposed text “MEET HERE AFTER THE JOB”. *File5* is a low-quality image of an image aggregate website that does not appear relevant to the investigation.

File Type	Header	Header Offset	Footer	Footer Offset
Doc	D0 CF 11 E0 A1 B1 1A E1	0x00705000	57 6F 72 64 2E 44 6F 63 75 6D 65 6E 74 2E	0x0070A652
Jpeg/Jfif	FF D8 FF E0	0X004A9000	FF D9	0X004AC1E9
Jpeg	FF D8 FF E1	0x004D9000	FF D9	0x00703AC0
Png	89 50 4E 47 0D 0A 1A 0A	0x004A000	49 45 R3 44 AE 42 60 82	0x004D5DBC
Png	89 50 4E 47 0D 0A 1A 0A	0x06E72F6E	49 45 R3 44 AE 42 60 82	0x06E7D17F

Table 1: Unallocated file locations

Evidence Table

Table 2 outlines the evidence items of this case.

Description	Designation	Filename	MD5 Hash
Evidence Provided	Preservation Copy	FinalProject.001	7f348c4b49091f6b6389dc513f9f380d
Evidence Created	Working Copy	xxFinalProject.001	7f348c4b49091f6b6389dc513f9f380d

Evidence Examined	Working Copy	xxFinalProject.001	7f348c4b49091f6b6389dc513f9f380d
Script log	Supplemental File	week7.txt.zip	b7c5932d3ea2dc4a2407701ad2a28411

Table 2: Case evidence items

Collection and Analysis

Collection

On 12/14/2019, the raw USB image was made known to the examiner for analysis. The examiner created a new *UPDCase* directory within the *Desktop* directory, then retrieved file *FinalProject.001* via Mozilla Firefox from the CYB356 Fall 2019 shared drive folder called Week 7: Final Project, located at https://drive.google.com/drive/u/3/folders/1s7lZrlPojdteN6vDj7nnimmr3hJH6JvP.

According to the txt file located within the Week 7: Final Project folder, the MD5 and SHA1 checksums for *FinalProject.001* are 7f348c4b49091f6b6389dc513f9f380d and d8d8cbfc6ce82f1310bdc6620f3e3197d58b1fd0, respectively. Examiner navigated to *Downloads* directory in Terminal and hashed the downloaded file using command: "hashdeep -c md5,sha1 FinalProject.001". The results, shown in figure 1, indicate the MD5 (highlighted in yellow) and SHA1 (highlighted in green) hash values match - confirming the purity of the downloaded evidence.

```
candace@ubuntu-cyb356:~/Downloads$ hashdeep -c md5,sha1 FinalProject.001
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,filename
## Invoked from: /home/candace/Downloads
## $ hashdeep -c md5,sha1 FinalProject.001
##
1007681536,7f348c4b49091f6b6389dc513f9f380d,d8d8cbfc6ce82f1310bdc6620f3e3197d58b
1fd0,/home/candace/Downloads/FinalProject.001
```

Figure 1: Verification of retrieved evidence

Examiner moved evidence file from *Downloads* directory to *UPDCase* directory using command "mv FinalProject.001 ../Desktop/UPDCase/FinalProject.001", then created a new directory in *UPDCase* called *Working (*"mkdir Working"). A working copy of the retrieved evidence file was made in the *Working* directory by entering command: "cp ./FinalProject.001 ./Working/xxFinalProject.001". To verify the integrity of the working copy, examiner navigated to the *Working* directory and hashed the file using command: "hashdeep -c md5,sha1 xxFinalProject.001". The results, shown in figure 2, indicate that the working copy's MD5 (highlighted in yellow) and SHA1 (highlighted in green) hash values match - confirming the purity of the working copies.

```
candace@ubuntu-cyb356:~/Desktop/UPDCase/Working$ hashdeep -c md5,sha1 xxFinalPro
ject.001
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,filename
## Invoked from: /home/candace/Desktop/UPDCase/Working
## $ hashdeep -c md5,sha1 xxFinalProject.001
##
1007681536,7f348c4b49091f6b6389dc513f9f380d,d8d8cbfc6ce82f1310bdc6620f3e3197d58b
1fd0,/home/candace/Desktop/UPDCase/Working/xxFinalProject.001
```

Figure 2: Verification of working copy

Analysis

In *Working* directory of Terminal, examiner entered command "fdisk -l xxFinalProject.001". The output of this command (figure 3) indicated the file system of the disk image as FAT16 (yellow) with a start sector of 32 (green).

```
candace@ubuntu-cyb356:~/Desktop/UPDCase/Working$ fdisk -l xxFinalProject.001
Disk xxFinalProject.001: 961 MiB, 1007681536 bytes, 1968128 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x011a4e43

Device                Boot Start     End Sectors  Size Id Type
xxFinalProject.001p1 *       32 1968127 1968096  961M  6 FAT16
```

Figure 3: Disk partition information

In Terminal, Examiner entered command “sudo mount -t vfat -o loop,offset=16384 xxFinalProject.001 /mnt/UPDMount” (offset value determined by multiplying start sector 32 by 512). One file was successfully mounted called *BuyWithMyShare.ods.* In *UPDMount* directory of Terminal, examiner copied the file to *Working* directory via command “cp BuyWithMyShare.ods ~/Desktop/UPDCase/Working”. Examiner attempted to open file with LibreOffice, but the file was unreadable (see figure 4).

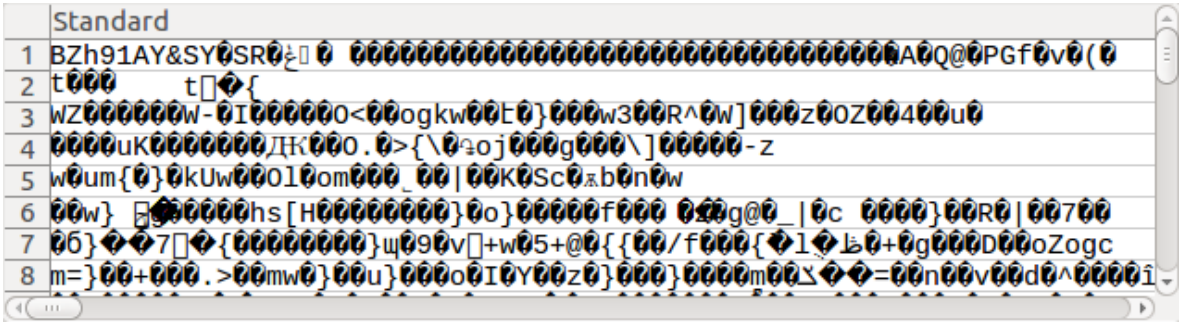

Figure 4: BuyWithMyShare.ods manifestation in LibreOffice

Examiner entered “file BuyWithMyShare.ods” in Terminal, which revealed the .ods suffix to be invalid - the file was actually gzip compressed data. Based on this revelation, a determination was made that the file had been nested. Examiner subsequently followed the procedure detailed in figure 5 to ultimately determine the file as a jpeg. Additional information about the file is also displayed: the phone used to take the picture was a Samsung SM-G920V, and the time stamp of the picture is 2015:06:29 at 11:40:28 (both highlighted in green). Examiner renamed the file with proper extension using command “mv BuyWithMyShare BuyWithMyShare.jpeg”.

```
candace@ubuntu-cyb356:~/Desktop/UPDCase/Working$ file BuyWithMyShare.ods
BuyWithMyShare.ods: gzip compressed data, was "BuyWithMyShare.bz2", last modifie
d: Fri May 19 14:59:48 2017, from Unix
candace@ubuntu-cyb356:~/Desktop/UPDCase/Working$ mv BuyWithMyShare.ods BuyWithMy
Share.gz
candace@ubuntu-cyb356:~/Desktop/UPDCase/Working$ gunzip BuyWithMyShare.gz
candace@ubuntu-cyb356:~/Desktop/UPDCase/Working$ file BuyWithMyShare
BuyWithMyShare: bzip2 compressed data, block size = 900k
candace@ubuntu-cyb356:~/Desktop/UPDCase/Working$ mv BuyWithMyShare BuyWithMyShar
e.bz2
candace@ubuntu-cyb356:~/Desktop/UPDCase/Working$ bunzip2 BuyWithMyShare.bz2
candace@ubuntu-cyb356:~/Desktop/UPDCase/Working$ file BuyWithMyShare
BuyWithMyShare: JPEG image data, Exif standard: [TIFF image data, little-endian,
 direntries=12, height=2988, manufacturer=samsung, model=SM-G920V, orientation=u
pper-left, xresolution=210, yresolution=218, resolutionunit=2, software=G920VVRU
1AOE2, datetime=2015:06:29 11:40:28, width=5312], baseline, precision 8, 5312x29
88, frames 3
```

Figure 5: De-nested allocated file information

Examiner entered command "identify -verbose BuyWithMyShare.jpeg | grep GPS", but no viable GPS information was extracted (see figure 6).

```
candace@ubuntu-cyb356:~/Desktop/UPDCase/Working$ identify -verbose BuyWithMyShar
e.jpeg | grep GPS
candace@ubuntu-cyb356:~/Desktop/UPDCase/Working$
```

Figure 6: No GPS information found in file

Upon visual review (figure 7), examiner found no clearly identifiable information of the suspect except for what appears to be a registration sticker with a date of March 2016.

Figure 7: Close-up of allocated file

xxFinalProject.001 was opened in wxHexEditor. Examiner used the GUI interface to search for common doc file headers and footers. The header (D0 CF 11 E0 A1 B1 1A E1) and footer (57 6F 72 64 2E 44 6F 63 75 6D 65 6E 74 2E) of a doc file were located at offsets 0x00705000 and 0x0070A652, respectively. Examiner highlighted the relevant information, right clicked and pressed **Save As Dump**, and created file

called *file1* in *Working* directory. When opened with LibreOffice, as shown in figure 8, an address was revealed: “233 Genesee Street, Utica, NY 13501”.

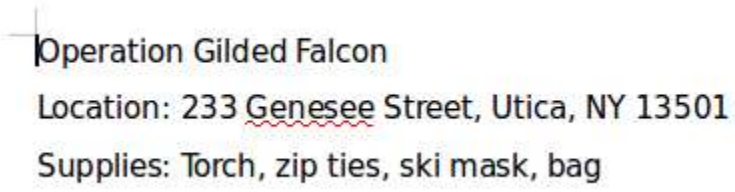

Figure 8: Contents of carved file 1

Examiner then searched for common jpeg file headers and footers. The header (FF D8 FF E0) and footer (FF D9) of a jpeg/jfif file were located at offsets 0x004A9000 and 0x004AC1E9, respectively. Examiner highlighted the relevant information, right clicked and pressed **Save As Dump**, and created *file2* in *Working* directory. When opened with ImageMagick , as shown in figure 9, the logo of M&T Bank was revealed.

Figure 9: Contents of carved file2

Examiner also found the header (FF D8 FF E1) and footer (FF D9) of a jpeg file located at offsets 0x004D9000 and 0x00703AC0, respectively. Examiner highlighted and right clicked the relevant content, clicked **Save As Dump**, and created *file3* in *Working* directory. When opened with ImageMagick , as shown in figure 10, the street view of an M&T Bank location was revealed.

Figure 10: Contents of file3

The specific header of *file3* (FF D8 FF E1) indicates the possibility of exif data. In *Working* directory of Terminal, examiner entered command: “identify -verbose file3 | grep GPS”. Coordinates 43°06'01.0"N 75°13'57.0"W (green box) were discovered, as seen in figure 11.

```
candace@ubuntu-cyb356:~/Desktop/UPDCase/Working$ identify -verbose file3 | grep
GPS
    exif:GPSAltitude: 0/1
    exif:GPSAltitudeRef: 1
    exif:GPSDateStamp: 2016:09:04
    exif:GPSInfo: 810
    exif:GPSLatitude: 43/1, 6/1, 3/1
    exif:GPSLatitudeRef: N
    exif:GPSLongitude: 75/1, 13/1, 57/1
    exif:GPSLongitudeRef: W
    exif:GPSTimeStamp: 17/1, 44/1, 2/1
    exif:GPSVersionID: 2, 2, 0, 0
```

Figure 11: GPS exif data of file3

Examiner searched for aforementioned coordinates using website https://maps.google.com. A screenshot taken in Street View Mode (figure 12) appears to confirm the accuracy of the GPS coordinates because the building matches the building in *file3*.

Figure 12: Street view of coordinates extracted from file3

Examiner then searched for common png file headers and footers. The header (89 50 4E 47 0D 0A 1A 0A) and footer (49 45 R3 44 AE 42 60 82) of a png file were located at offsets 0x004A000 and 0x004D5DBC, respectively. Examiner highlighted and right-clicked relevant content, clicked **Save As Dump**, and created *file4* in *Working* directory. When opened with ImageMagick , as shown in figure 13, a picture of cross street signs -"Bleecker St" and "Kossuth Ave"- and the superimposed text "MEET HERE AFTER THE JOB" was revealed.

Figure 13: Contents of file4

Header (89 50 4E 47 0D 0A 1A 0A) and footer (49 45 R3 44 AE 42 60 82) of another png file were located at offsets 0x06E72F6E and 0x06E7D17F, respectively. Examiner highlighted and right-clicked relevant content, clicked **Save As Dump**, and created *file5* in *Working* directory. When opened with ImageMagick , as shown in figure 14, a low-quality image of an image aggregate website was revealed. It did not appear to be relevant to the bank investigation.

Figure 14: Contents of file5

Conclusion

Sergeant Brunson of the Utica Police Department provided the raw image of a USB drive seized during a traffic stop. It is suspected to belong to the suspects of a string of robbery cases in Utica City limits over the past three months. Sergeant Brunson requested the examiner to retrieve allocated and unallocated files that may indicate the next planned robbery target.

One allocated file was retrieved from the hard drive image: a picture of freeway traffic taken from the inside of a passenger vehicle. 5 files were carved from unallocated space: *File1, file2, file3, file4,* and *file5. File1* shows an address: 233 Genesee Street in Utica, New York. *File2* is a picture of the M&T Bank logo. *File3* is a street view of an M&T Bank. Its exif data revealed the coordinates 43°06'01.0"N 75°13'57.0"W. These coordinates also refer to the same place as the coordinates in *File1. File4* is a picture of cross street signs “Bleecker St” and “Kossuth Ave”, and the superimposed text “MEET HERE AFTER THE JOB”. *File5* is a low-quality image that does not appear relevant to the investigation.

Based on multiple references to (address, gps coordinates, pictures), the M&T bank located at 233 Genesee Street should be focused on as a possible next robbery target.

Appendix A: Examiner Workstation Specifications

- Computer Name:
- Operating System (OS) Name:
- OS Version:
- System Make/Model:
- System Serial Number:
- Processor:
- Installed RAM:
- Time Zone of Examiner Machine: Mountain Standard Time
- System date/time is consistent with the time zone listed above, as verified by: http://nist.time.gov/.

Appendix B: Virtual Machine (VM) Specifications

- Virtual Machine Name: ubuntu-cyb356
- Operating System Name: Ubuntu
- Operating System Version: 16.04.6 LTS (Xenial)
- Virtual Machine Serial Number: 0
- Examiner's Time Zone: Mountain Standard Time
- System date and time are consistent with the time zone listed above, as verified by: http://nist.time.gov/.

Appendix C: Tools Used

- Hashdeep v4.4-2
- Wxhexeditor v0.23+repack
- ImageMagick v6.8.9.9-7u
- LibreOffice v5.1.6.2
- File v5.25
- Mount 2.27.1