Defense Documentation

Ryan Hinson

Advisor: Professor Julie Henderson

Statement of Purpose

The purpose of my project was to create a simulated Cyber Forensics scenario. This was done to not only learn about the artifacts a forensic analyst looks for, but also to learn about the tools they use to extract these artifacts. The simulated Scenario I put together sees a criminal leaving digital artifacts while planning a bank heist. I set it up for the criminal to be the Riddler from Batman, just to add some fun to the project. I then mocked up some police report documents to show that the computer was given to me as a forensic analyst.

Research and Background

I researched the industry standard tools needed to complete this project and what artifacts are commonly extracted during the forensic process. I was able to find that they often look for web searches that can show motive as well as documents or metadata from pictures (Murphy, 2019). Professor Henderson was able to point me in the right direction to find the tools I needed like FTK Imager and Registry Viewer.

Software and Hardware

I used a windows machine to create the artifacts. I then used FTK Imager, Access Data Registry viewer, and Exiftool to extract the artifacts and analyze them. I used FTK imager version 4.5, Registry Viewer 2.0, and Exiftool 12.09.

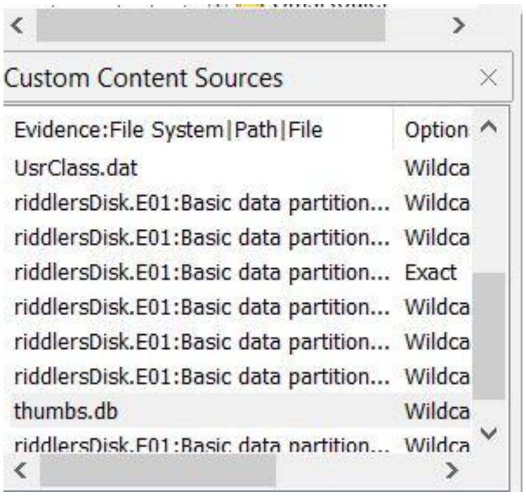
Project Requirements

The requirements were for me to create the artifacts on a machine, and use the proper tools to image the hard drive and extract the artifacts. I created web searches on two different WI-FI networks, downloaded images from the internet included two different security cameras and a bank floorplan. I copied six images from a smartphone connected by a USB, and I created a word document containing plans for the bank robbery. I then used FTK imager to image the hard drive and the RAM. I also created a triage image using FTK imager. I then found the plans document and the pictures using FTK imager. I analyzed these and the lnk files using Exiftool. Once this was done, I used registry viewer to analyze the registry files to see the web searches and the WI-FI connections.

Project Implementation

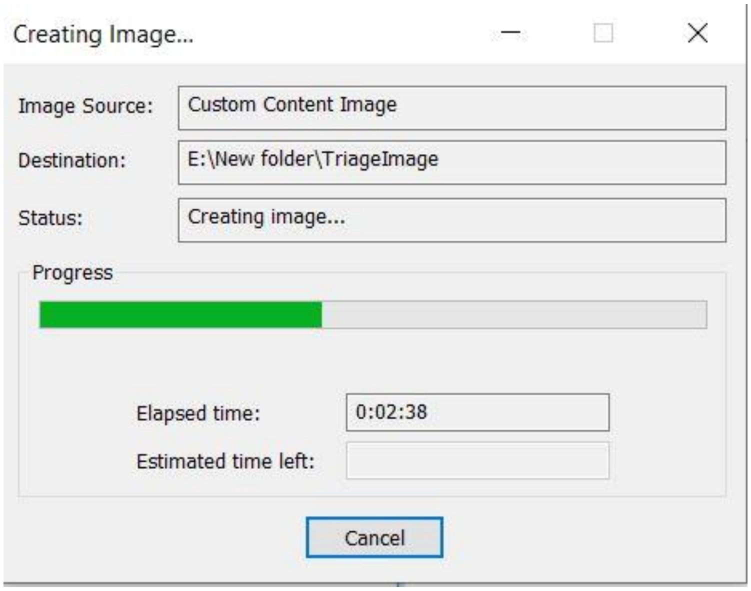
The first step I took was creating the artifacts. This included downloading pictures from the internet and from a connected phone. It also included various web searches as well. All of this is contained in the criminal artifact record document.

Next I made a copy of the hard drive using ftk imager. I also used this to create custom content images of various parts of the hard drive



Custom Content Sources

Evidence:File System|Path|File	Option
UsrClass.dat	Wildca
riddlersDisk.E01:Basic data partition...	Wildca
riddlersDisk.E01:Basic data partition...	Wildca
riddlersDisk.E01:Basic data partition...	Exact
riddlersDisk.E01:Basic data partition...	Wildca
riddlersDisk.E01:Basic data partition...	Wildca
riddlersDisk.E01:Basic data partition...	Wildca
thumbs.db	Wildca
riddlersDisk.E01:Basic data partition...	Wildca



Creating Image...

Image Source: Custom Content Image

Destination: E:\New folder\TriageImage

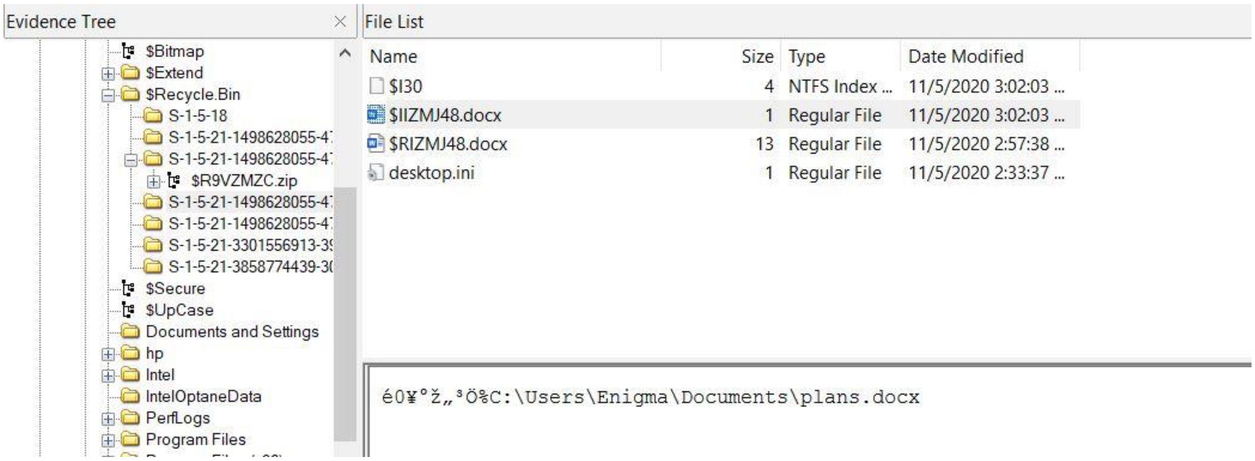
Status: Creating image...

Progress

Elapsed time: 0:02:38

Estimated time left:

After this I used FTK imager to locate the files I needed. I found the plans document and all the pictures first.



Evidence Tree

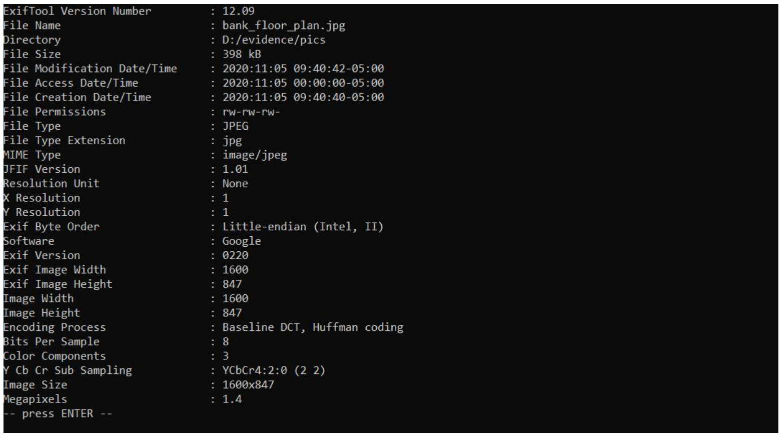
```
$Bitmap
$Extend
$Recycle.Bin
  S-1-5-18
  S-1-5-21-1498628055-4
  S-1-5-21-1498628055-4
    $R9VZMZC.zip
  S-1-5-21-1498628055-4
  S-1-5-21-1498628055-4
  S-1-5-21-3301556913-3
  S-1-5-21-3858774439-3
$Secure
$UpCase
Documents and Settings
hp
Intel
IntelOptaneData
PerfLogs
Program Files
```

File List

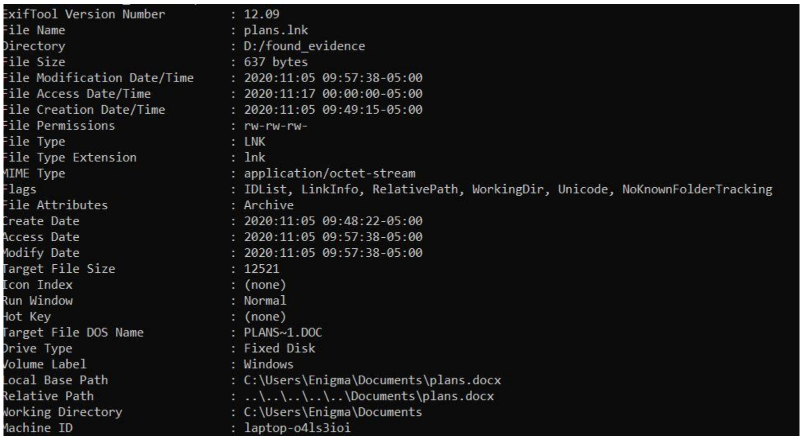
Name	Size	Type	Date Modified
$I30	4	NTFS Index ...	11/5/2020 3:02:03 ...
$IIZMJ48.docx	1	Regular File	11/5/2020 3:02:03 ...
$RIZMJ48.docx	13	Regular File	11/5/2020 2:57:38 ...
desktop.ini	1	Regular File	11/5/2020 2:33:37 ...

```
é0¥°ž„³Ö%C:\Users\Enigma\Documents\plans.docx
```

I then used Exift tool to examine the photos and plans document for metadata.

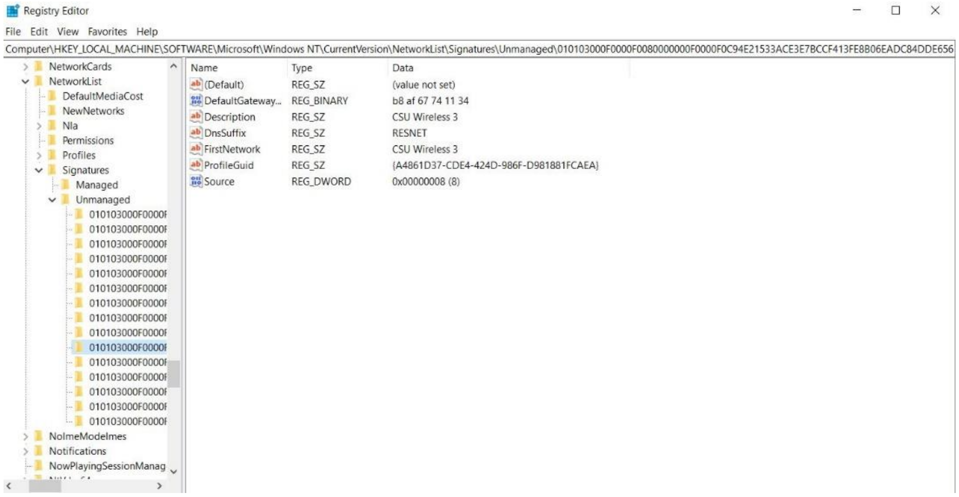


```
ExifTool Version Number         : 12.09
File Name                       : bank_floor_plan.jpg
Directory                       : D:/evidence/pics
File Size                       : 398 kB
File Modification Date/Time     : 2020:11:05 09:40:42-05:00
File Access Date/Time           : 2020:11:05 00:00:00-05:00
File Creation Date/Time         : 2020:11:05 09:40:40-05:00
File Permissions                : rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Exif Byte Order                 : Little-endian (Intel, II)
Software                        : Google
Exif Version                    : 0220
Exif Image Width                : 1600
Exif Image Height               : 847
Image Width                     : 1600
Image Height                    : 847
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1600x847
Megapixels                      : 1.4
-- press ENTER --
```



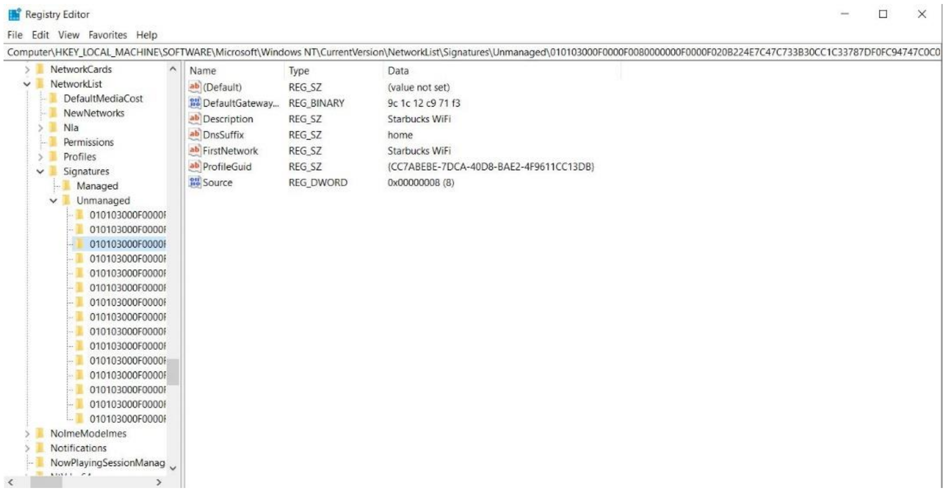
```
ExifTool Version Number         : 12.09
File Name                       : plans.lnk
Directory                       : D:/found_evidence
File Size                       : 637 bytes
File Modification Date/Time     : 2020:11:05 09:57:38-05:00
File Access Date/Time           : 2020:11:17 00:00:00-05:00
File Creation Date/Time         : 2020:11:05 09:49:15-05:00
File Permissions                : rw-rw-rw-
File Type                       : LNK
File Type Extension             : lnk
MIME Type                       : application/octet-stream
Flags                           : IDList, LinkInfo, RelativePath, WorkingDir, Unicode, NoKnownFolderTracking
File Attributes                 : Archive
Create Date                     : 2020:11:05 09:48:22-05:00
Access Date                     : 2020:11:05 09:57:38-05:00
Modify Date                     : 2020:11:05 09:57:38-05:00
Target File Size                : 12521
Icon Index                      : (none)
Run Window                      : Normal
Hot Key                         : (none)
Target File DOS Name            : PLANS~1.DOC
Drive Type                      : Fixed Disk
Volume Label                    : Windows
Local Base Path                 : C:\Users\Enigma\Documents\plans.docx
Relative Path                   : ..\..\..\..\..\Documents\plans.docx
Working Directory               : C:\Users\Enigma\Documents
Machine ID                      : laptop-o4ls3ioi
```

After these files were analyzed, I used registry viewer to analyze the registry files in the custom content image. This allowed me to see wifi connections as well as search history.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged\010103000F0000F0080000000F0000F0C94E21533ACE3E7BCCF413FE8B06EADC84DDE656

Name	Type	Data
(Default)	REG_SZ	(value not set)
DefaultGateway...	REG_BINARY	b8 af 67 74 11 34
Description	REG_SZ	CSU Wireless 3
DnsSuffix	REG_SZ	RESNET
FirstNetwork	REG_SZ	CSU Wireless 3
ProfileGuid	REG_SZ	{A4861D37-CDE4-424D-986F-D981881FCAEA}
Source	REG_DWORD	0x00000008 (8)



Registry Editor

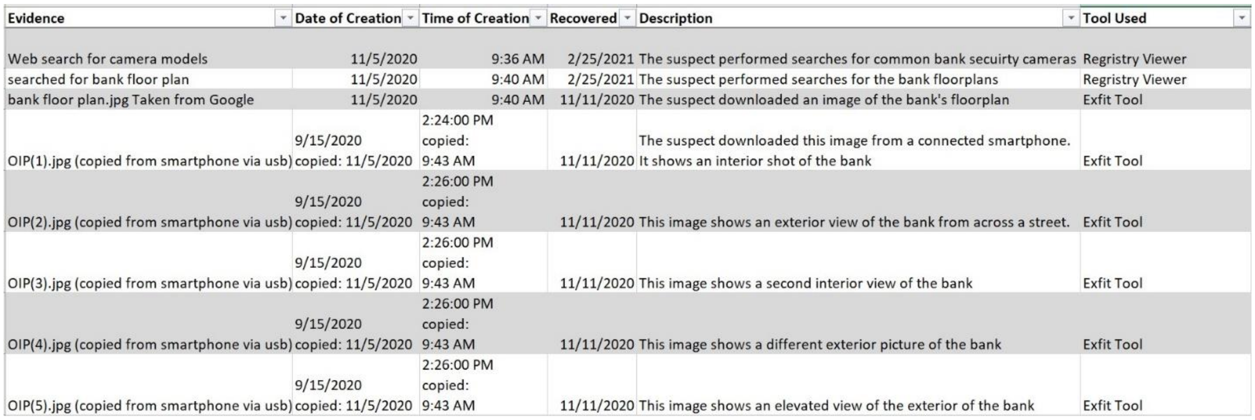
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged\010103000F0000F0080000000F0000F020B224E7C47C733B30CC1C33787DF0FC94747C0C0

```
> NetworkCards
v NetworkList
    DefaultMediaCost
    NewNetworks
  > Nla
    Permissions
  > Profiles
  v Signatures
      Managed
    v Unmanaged
        010103000F0000F
        010103000F0000F
        010103000F0000F
        010103000F0000F
        010103000F0000F
        010103000F0000F
        010103000F0000F
        010103000F0000F
        010103000F0000F
        010103000F0000F
        010103000F0000F
        010103000F0000F
        010103000F0000F
        010103000F0000F
        010103000F0000F
> NoImeModelmes
> Notifications
  NowPlayingSessionManag
```

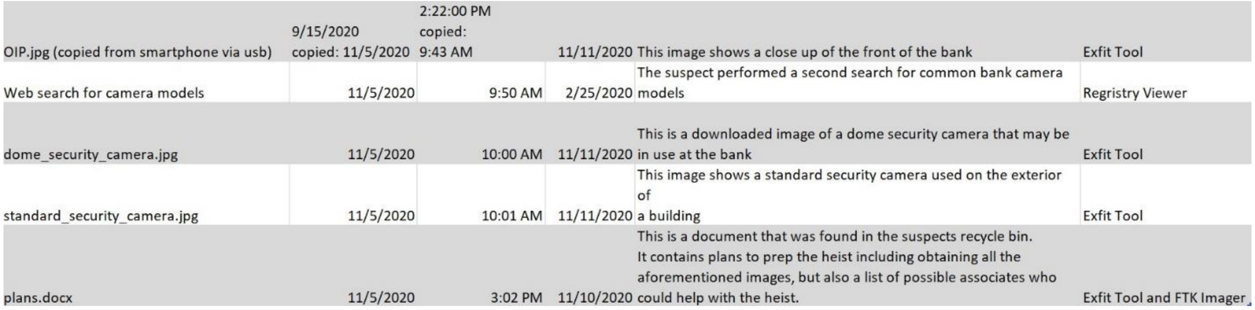
Name	Type	Data
(Default)	REG_SZ	(value not set)
DefaultGateway...	REG_BINARY	9c 1c 12 c9 71 f3
Description	REG_SZ	Starbucks WiFi
DnsSuffix	REG_SZ	home
FirstNetwork	REG_SZ	Starbucks WiFi
ProfileGuid	REG_SZ	{CC7ABEBE-7DCA-40D8-BAE2-4F9611CC13DB}
Source	REG_DWORD	0x00000008 (8)

Lastly, I used all this data to construct a timeline of when all these artifacts were created. This log is contained in the Forensic log spreadsheet. After this, I filled out a supplemental case report form and chain of custody form. Both of these documents would be used in a real life investigative procedure.

Below are two screenshots of my Forensic Log. This shows a complete list of the artifacts I found and what tool I used.



Evidence	Date of Creation	Time of Creation	Recovered	Description	Tool Used
Web search for camera models	11/5/2020	9:36 AM	2/25/2021	The suspect performed searches for common bank secuirty cameras	Regristry Viewer
searched for bank floor plan	11/5/2020	9:40 AM	2/25/2021	The suspect performed searches for the bank floorplans	Regristry Viewer
bank floor plan.jpg Taken from Google	11/5/2020	9:40 AM	11/11/2020	The suspect downloaded an image of the bank's floorplan	Exfit Tool
OIP(1).jpg (copied from smartphone via usb)	9/15/2020 copied: 11/5/2020	2:24:00 PM copied: 9:43 AM	11/11/2020	The suspect downloaded this image from a connected smartphone. It shows an interior shot of the bank	Exfit Tool
OIP(2).jpg (copied from smartphone via usb)	9/15/2020 copied: 11/5/2020	2:26:00 PM copied: 9:43 AM	11/11/2020	This image shows an exterior view of the bank from across a street.	Exfit Tool
OIP(3).jpg (copied from smartphone via usb)	9/15/2020 copied: 11/5/2020	2:26:00 PM copied: 9:43 AM	11/11/2020	This image shows a second interior view of the bank	Exfit Tool
OIP(4).jpg (copied from smartphone via usb)	9/15/2020 copied: 11/5/2020	2:26:00 PM copied: 9:43 AM	11/11/2020	This image shows a different exterior picture of the bank	Exfit Tool
OIP(5).jpg (copied from smartphone via usb)	9/15/2020 copied: 11/5/2020	2:26:00 PM copied: 9:43 AM	11/11/2020	This image shows an elevated view of the exterior of the bank	Exfit Tool



OIP.jpg (copied from smartphone via usb)	9/15/2020 copied: 11/5/2020	2:22:00 PM copied: 9:43 AM	11/11/2020	This image shows a close up of the front of the bank	Exfit Tool
Web search for camera models	11/5/2020	9:50 AM	2/25/2020	The suspect performed a second search for common bank camera models	Regristry Viewer
dome_security_camera.jpg	11/5/2020	10:00 AM	11/11/2020	This is a downloaded image of a dome security camera that may be in use at the bank	Exfit Tool
standard_security_camera.jpg	11/5/2020	10:01 AM	11/11/2020	This image shows a standard security camera used on the exterior of a building	Exfit Tool
plans.docx	11/5/2020	3:02 PM	11/10/2020	This is a document that was found in the suspects recycle bin. It contains plans to prep the heist including obtaining all the aforementioned images, but also a list of possible associates who could help with the heist.	Exfit Tool and FTK Imager

Test Plan

My test plan was to compare the times I found the artifacts to when they were created. Therefore I took down the date and times of creation for the artifacts. The document showing these is included on the Github. I then took my forensic log and compared it to this document to ensure that everything matched.

Test Results

I was able to successfully recover all of the documents and show that they matched. If you compare the forensic log and the criminal artifact record the dates and times match. The included screenshots from Exiftool show how I got the information for the forensic log.

Challenges Overcome

I had a few different issues with my project. My first idea, as indicated in the proposal document, was to use two different virtual machines for the project. However, I was not able to figure out how to copy the Vm's hard drive. This led me to creating a second user on a personal windows machine. The other Issue I had was getting registry viewer to work. I ended up having to remake the image of the hard drive and the custom content images, but was able to get it functional.

Future Improvements

I would like to be able to make this project work using a Virtual machine so that someone recreating the process does not have to copy personal data. I would also like to expand it to work with more tools and artifacts in the future.

References

Murphy, C. (2019). *WHAT ARE FORENSIC ARTIFACTS? – MY FAVORITE ARTIFACTS, PART 0.* Retrieved from Tetra Defense: https://www.tetradefense.com/digital-forensics-services/what-are-forensic-artifacts-my-favorite-artifacts-part-0/#:~:text=Things%20like%20registry%20keys%2C%20files,you%20do%20while%20using%20it.