



Cyber Forensics Senior Project

RYAN HINSON

Statement of Purpose

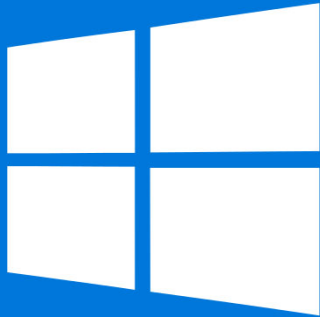
- ▶ The purpose of this project was to simulate a Cyber Forensics Investigation.
- ▶ Cyber Forensics has become a big part of crime scene investigation and many people are still not sure what these analysts do.
- ▶ I wanted to construct a project that gives a basic picture on the tools and the procedure of what Digital Forensics analysts do.

Research and Background

- ▶ Common Artifacts looked for.
- ▶ Industry standard tools
 - ▶ Kali Linux and Sift Workstation
 - ▶ FTK imager and Registry Viewer
 - ▶ ExifTool



Software and Hardware



- ▶ Original Plan for two VMs
 - ▶ Sift workstation and ubuntu
- ▶ Windows Machine with a second user
- ▶ FTK Imager, Registry Viewer, ExifTool
- ▶ Hard drive and flash drive
 - ▶ Write Blocker

Project Requirements

- ▶ Create artifacts on the second user
- ▶ Use FTK Imager to make images of the RAM and Hard Drive
- ▶ Using tools, analyze the images for the created artifacts
- ▶ Use timestamps learned to construct timeline of Criminals Activity

Demonstration

Creating Artifacts

- ▶ Created a Second User on my PC
- ▶ Did web searches, downloaded pictures from the internet
- ▶ Connected a smartphone via USB
 - ▶ Transferred pictures from phone to computer
- ▶ Connected to different Wi-Fi networks
 - ▶ Used these to do more searches and download more images
- ▶ Created a word document and put it in the recycle bin

Artifact record

11/5/20

9:36am started searching

Searched web for cameras

9:40am

Searched for bank floor plan

Downloaded bank floor plan to pictures folder

9:42am

Connected android smartphone via cable

9:43am

Copied smartphone pictures of the bank to pictures folder

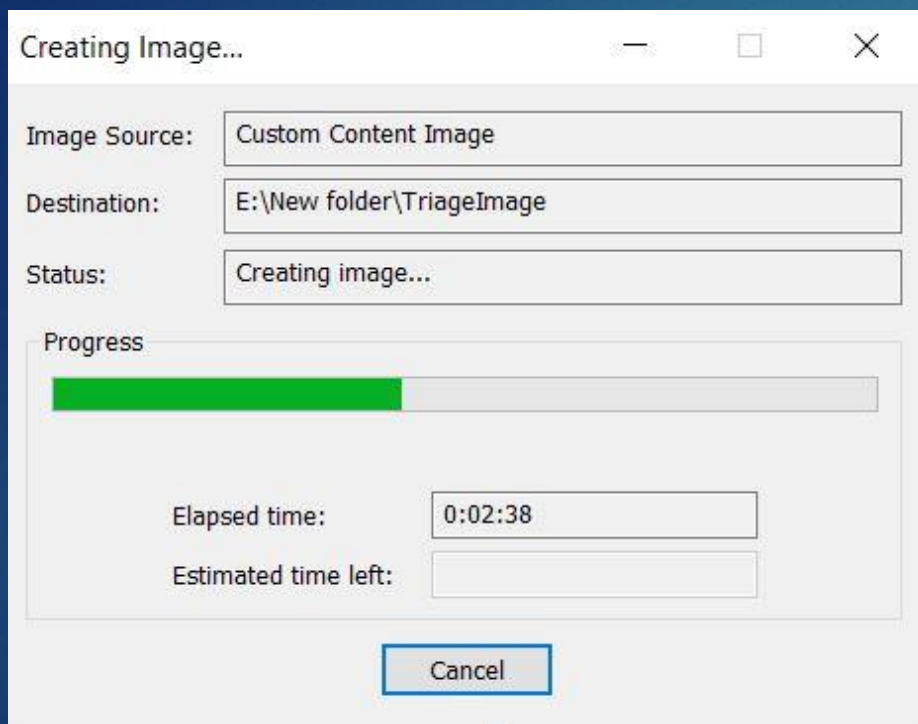
9:48am

Created folder named pics to hold all pictures. It is contained in thispc/pictures

9:48am

Created a word doc in documents called plans

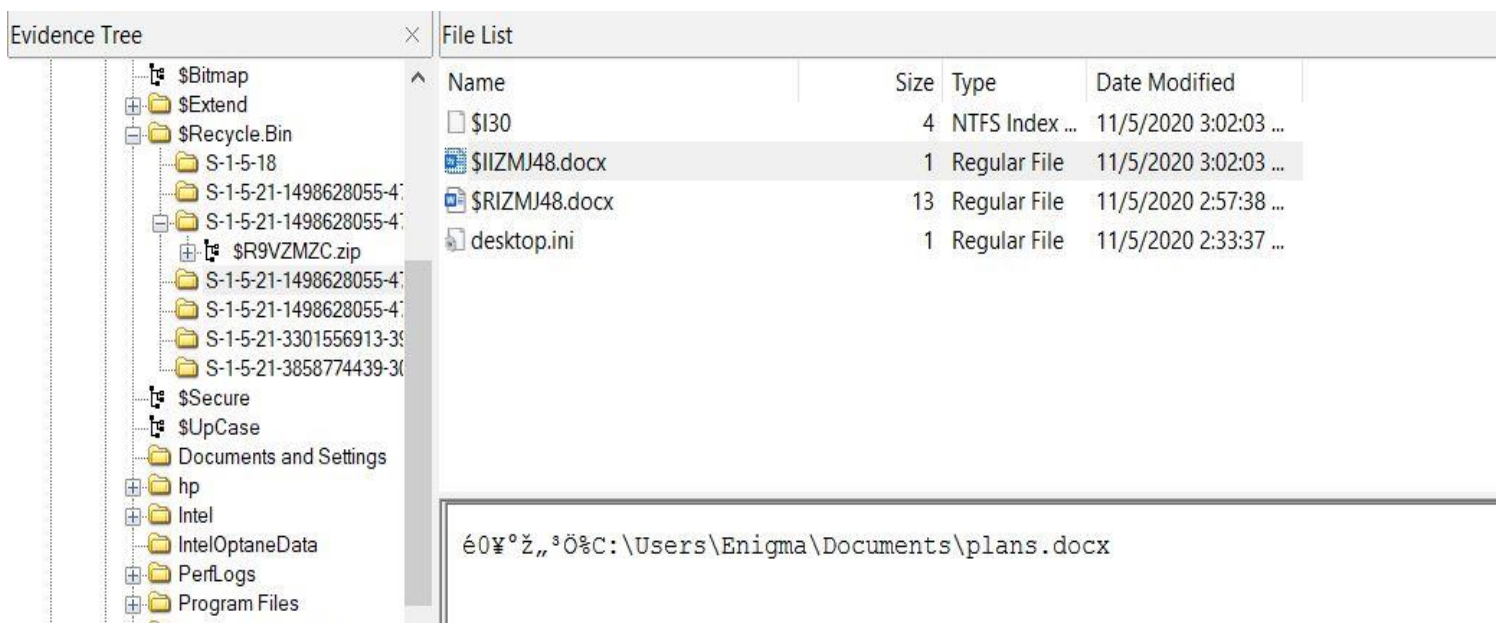
Imaging the Hard drive



- ▶ Put FTK Imager on flash drive
- ▶ Connected to the still running PC
- ▶ Imaged Ram and Hard Drive
- ▶ Created Custom Content images for a triage image

Using FTK Imager

- ▶ Used to not only image the hard drive but to make triage images
- ▶ Can also be used to find files in the image.
- ▶ Gives some basic information on files
- ▶ Industry Standard tool.



The screenshot displays the FTK Imager interface with two main panes: 'Evidence Tree' on the left and 'File List' on the right.

Evidence Tree: Shows a hierarchical view of the image's contents. The root is '\$Bitmap', which contains '\$Extend' and '\$Recycle.Bin'. '\$Recycle.Bin' contains a folder 'S-1-5-18', which in turn contains several subfolders with long alphanumeric names. Other folders visible include '\$Secure', '\$UpCase', 'Documents and Settings', 'hp', 'Intel', 'IntelOptaneData', 'PerfLogs', and 'Program Files'.

File List: A table showing the details of the selected file, '\$IIZMJ48.docx'.

| 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 ... |

At the bottom of the File List pane, the file's path is displayed: `é0¥°ž„³Ö%C:\Users\Enigma\Documents\plans.docx`.

Using Registry Viewer

- ▶ Used to view windows registry files
- ▶ Allows for us to see system configuration
 - ▶ This includes profiles, Wi-Fi connections, and search history
- ▶ Used in conjunction with FTK Imager



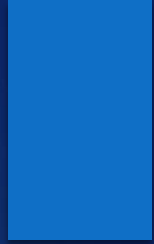
| Name | Type | Data |
|-------------------|------------|--|
| (Default) | REG_SZ | (value not set) |
| DefaultGateway... | REG_BINARY | b8 af 67 74 11 34 |
| Description | REG_SZ | CSU Wireless 3 |
| DnsSuffix | REG_SZ | RESNET |
| FirstNetwork | REG_SZ | CSU Wireless 3 |
| ProfileGuid | REG_SZ | {A4861D37-CDE4-424D-986F-D981881FCAEA}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

Using ExifTool

- ▶ This tool allows for the viewing of metadata and Ink files
- ▶ This can be used to see when files were created and last modified
- ▶ Used to gain a timeline of when things were done by the criminal.

```
EXIFTOOL VERSION Number : 12.03
File Name                 : OIP.jpeg
Directory                 : D:/evidence/pics
File Size                 : 68 kB
File Modification Date/Time : 2020:09:15 14:22:34-04:00
File Access Date/Time     : 2020:11:11 00:00:00-05:00
File Creation Date/Time   : 2020:11:05 09:43:49-05:00
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
Image Width               : 474
Image Height              : 711
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                : 474x711
Megapixels                : 0.337
```

Forensic Log



| 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 security cameras | Registry Viewer |
| searched for bank floor plan | 11/5/2020 | 9:40 AM | 2/25/2021 | The suspect performed searches for the bank floorplans | Registry 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 |

| | | | | | |
|--|--------------------------------|-----------------|------------|---|---------------------------|
| | | 2:22:00 PM | | | |
| OIP.jpg (copied from smartphone via usb) | 9/15/2020 copied: 11/5/2020 | 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 | Registry 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 |

Challenges faces

- ▶ Problems with VMs
- ▶ Problem with first Image
- ▶ Problem with Registry Viewer

Future improvements

- ▶ Using VMs
- ▶ Having access to write blocker
- ▶ Making more artifacts
- ▶ Using more tools



Picture Sources

- ▶ <https://s.softdeluxe.com/icons/png/128/3555/3555359.png>
- ▶ https://storage.googleapis.com/webdesignledger.pub.network/WDL/6f050e39-windows_10_logoblue.svg-copy_windows.jpg
- ▶ https://images-na.ssl-images-amazon.com/images/I/61C6xldizSL.AC_SL1280_.jpg