

Forensics Report CA1

Note: this is a sample template and can be amended as needed. Please review the samples on Brightspace for more information



TU856

BSc in Computer Science

**Philip Herweling**

**C18470774**

School of Computer Science

TU Dublin – City Campus

**20/03/2022**

**Table of Contents**

*1.* *Case Introduction* 5

*2.* *Summary of the information* 5

*3.* *Forensic Tools and Techniques Used* 5

*4.* *Forensic Examination* 6

*5.* *Findings* 6

*6.* *Recommendations* 6

Declaration

I hereby declare that the work described in this dissertation is, except where otherwise stated, entirely my own work and has not been submitted as an exercise for a degree at this or any other university.

Signed:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Philip Herweling

20/03/2022

**Case Information**

**Case Number:** 3241

**Offense:** Suspected Insider Trading

**Submitting Officer:** (Name/ID#)

**Victim:** N/A

**Suspect:** Diana Prince

**Date/Time Seized:** 17th February 2022 @ 17:33

**Location of Seizure:** 123 fake Street, Dublin (Level 2, office 2-12)

|  |  |  |
| --- | --- | --- |
| **Description of Evidence** | | |
| **Item #** | **Quantity** | **Description of Item** (Model, Serial #, Condition, Marks, Scratches) |
| **2341-1** | 1 | TDK 16GB USB Flash Drive – TF10 USB 2.0 Flash Drive  Asset Tag:  Good condition, no external marks present.  Hardware Asset tag: 45378 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# *Case Introduction*

Description of the case and the forensic analysis we were asked to complete.

On Thursday the 17th of February 2022 at 17:33 Diana Prince was caught leaving Superfake inc where she worked with a thumb drive during a routine search. The nature of Superfake inc’s research and general safe servicing and repair is confidential and subject to several government contract worldwide. Employees are not permitted under any circumstances to bring computer hardware or equipment in or out of the building. That’s why employees must go through a scanner which detects metal and computer components and sounds an alarm if such items are detected. When Diana went through the scanner the Alarm sounded to let the security team know that she had some sort of metal on her person. Diana was then asked if she had any metal or computer components on her person and if she was also asked if she wants to remove anything from her pockets and go through the scanner again. Diana said “no” to both questions, so the security team accompanied her into a search room. The Security team proceed to search Diana and found a USB key which they placed into a secure storage container. Following this the manager of the security team proceed to make a chain of custody document.

The USB was then released to the systems manager Miles Dyson who made a forensics image of the USB Key. This image was then passed on to me (Philip Herweling) to complete the forensic examination.

# *Summary of the information*

I am working with an image of a drive found Dianas person. I am tasked with examining this drive and finding any items which are belonging to superfake and are private and not allowed leave the premises. Any items of this nature I am required to report back to superfake and give my recommendations on how they should proceed.

# *Forensic Tools and Techniques Used*

## 3.1 Handling of the USB drive and drive information:

Throughout the handling of this investigation industry standard tools and techniques were used. I received the USB via Superfake Inc through AN Post in a sealed envelope where I had the option to make my own forensic image of the drive and I was also given a copy of the forensic image their Systems Manager Miles Dyson made through a secure web application called Brightspace.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device Make/ Model | Device Serial Number | Description | Device Serial Number | Capacity |
| TF10 USB 2.0 Flash Drive | 2341-1 | Good condition, no external marks present. | 45378 | 16GB |

## 3.2 Tools That Were Used to carry out this Investigation:

|  |  |  |
| --- | --- | --- |
| Tool Name | Version Number | Description |
| FTK Imager | 4.2.1 | FTK Imager is used to create an image of a drive in this case it was a physical drive (USB drive) |
| Autopsy | 4.19.3 | Autopsy is a software which makes it simpler to deploy many of the open-source programs and plugins used in the Sleuth Kit. The GUI make sit easier to flag pertinent sections of data. |
| HxD | 2.5.0.0 (x84-64) | HxD is a software that allowed me to manually carve some files from the disk image created. It allows one to search for files using file signatures. |

## 3.3 FTK Imager:

FTK or Forensic ToolKit is a computer forensics software made by AccessData. Its used to scan hard drives and create a forensic disk image of that drive. These disk images can then be tested on using forensic tool kits and tool such as autopsy etc. FTK imager can recover files that are on the drive but also deleted and corrupted files on a system. In section 4 of this report I explain step by step how Miles used this tool to create a forensic image of the USB drive that was found on Dianas person.

## 3.4 Autopsy:

Autopsy is a digital forensics platform and graphical interface to the Sleuth Kit and other digital forensic tools. It’s used to investigate what happened on a computer or drive etc. It can be used to recover anything on a drive or image etc. Using the GUI you can see the different drives, deleted files, encrypted files metadata etc. It’s a very useful tool and I used it to carry out the forensic examination for this report. I go into detail on how exactly I used it in the next section of this report.

## 3.5 HxD:

This is an editor software application which can be used to analyse, viewing and running of hexadecimal coded files on a computer. It can be used to find files on disk images or drive or other files by searching for the file header and footer i.e. the files signature. It can also be used to manipulate the fundamental binary data that constitutes a computer file. It’s a very powerful utility which can be downloaded for free. In the following section I detail how I use this tool in order to manually carve out files from the forensics disk image.

## 3.6 My System Where I used the tools:

I used Autopsy and HxD on my Razer blade 15 laptop. This is a powerful laptop which has high enough specs to carry out a forensic examination of large drives. It has a core i7 9th generation processor, half a terabit SSD storage, 16Gb of Ram and runs the windows 11 operating system.

# *Forensic Examination*

## 4.1 How FTK imager was used to create an image of the drive:

1. Firstly the FTK Imager software was opened on Miles Dyson machine.
2. After Miles opened the software, he was greeted with the home page where he had to choose the drive type, in this case Miles choose a physical drive.
3. After selecting the drive type Miles had to choose a safe location to save the image to.
4. After choosing the location for the image Miles was then prompted to enter case information such as the case number, evidence number, unique description, examiner and notes.
5. After entering all the case details then selected the folder where he wants to store the image, set the name of the image and then set the image fragment.
6. The Next step for Miles was to press create to create the image.
7. The image is then created and also a log file is created in the same folder.
8. The last step that Miles had to do was Generate the MD5 checksum of the newly created image file and compared it to the MD5 checksum from the FTK Imager log report. These were the same letting Miles know he made an identical copy of the USB drive.

## How I used the HxD editor to do a manual carve

After Miles created the image of the drive and sent it to me securely I was able to start my forensic examination of the image. I decided that the first thing I wanted to do was try and manually carve a few different type of files from the drive to see if there was anything of not I could find.

So the first thing I done was load of the HxD Editor and opened up my disk image:

Graphical user interface, application, Word

Description automatically generated

After I opened the file I decided the first file I would try to find was a jpg file so I searched first for the header of a jpg file which is FF D8 FF:

Graphical user interface, text, table

Description automatically generated

When I searched for the header I found one on line 001E4000. I took note of this line and proceeded to search for a jpg footer which is FF D9:

Graphical user interface, text, application, table

Description automatically generated

After searching for the footer I found one on line 00258DA0. I then proceed to highlight from the header tag I found to the footer tag and paste it in a new file which I saved as carved\_v8.jpg which I then tried to open and see if I had actually found an image. This is the image I found :

A seagull on a beach

Description automatically generated with low confidence

This was a dead end but gave me confidence that id be able to find files that may prove that Diana was breaking company guidelines.

I followed the same steps to try and manually carve out a png file from the forensics image.

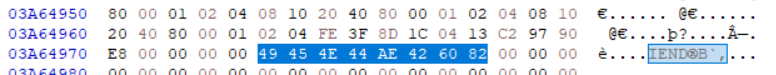
For the png file I searched for a potential header (89 50 4E 47 0D 0A 1A 0A) and footer (49 45 4E 44 AE 42 60 82)

Header for a png:

Icon

Description automatically generated with medium confidence

Footer for a png:



What the png file Shows:

Text, letter

Description automatically generated

## How I used Autopsy

After doing a manual carve, I then decided to use the Autopsy tool in order to inspect the image in further detail. The first thing I had to do was create a new case:

Graphical user interface, text, application, email

Description automatically generated

Then I entered the case details:

Graphical user interface, text, application, email

Description automatically generated

Step 1:

Graphical user interface, text, application

Description automatically generated

Step 2:

Graphical user interface, text, application

Description automatically generated

Step 3:

Graphical user interface, text, application, email

Description automatically generated

Step 4:

Graphical user interface, application

Description automatically generated

Step 5:

Graphical user interface, text, application, email

Description automatically generated

After going through all the steps and loading my image into the new autopsy case I made I am brought to the home screen of autopsy where I can see the file system that was on the USB , deleted files and I can then recover them by exporting them.

Graphical user interface, text

Description automatically generated

# *Findings*

Presentation of findings / results etc….

* What meaningful data was found?
* Was there any hidden or encrypted drives / data?
* Anything suspect or out of the ordinary?
* Etc…

## 5.1 The drive’s structure and files recovered

Text

Description automatically generated

1. Carved Files directory:

There were 21 files in this directory which were all original files. A mix of pictures and .apple files:

Graphical user interface, application, website

Description automatically generated

I took note of some of the pictures which appeared to be pictures of safe blueprints and how the locking mechanism worked. I also read an email which was addressed to a Bruce and also a screenshot of a monitor where the user logged in was a Mr Bruce Wayne.

1. Unalloc File Directory:

There is only one file in this directory which is an original file but doesn’t display anything.

1. Cracking Programs:

There are 11 files in this which is a mix between normal executable files and mac OS executable files. They were all created around the same time leading me to believe they were downloaded from a different computer.

Graphical user interface, application

Description automatically generated with medium confidence

1. .hexEditor

This directory looks like it’s just a hex editor program. After clicking into the files in this directory and reading the meta data I found that this hex editor is part of the Sleuth kit istat tool. I found it suspicious that this tool was found on the USB and suspect that it was used to change the signature of a file so it would be harder to find. I kept this in mind and decided to look out for suspicious files that aren’t loading properly.

1. Holiday Pictures

This directory has 21 files which are all jpg files. A lot of the files in this directory are only partially recovered and don’t display anything. Then there also seems to be genuine pictures of holiday locations, pictures of beaches, seashells etc but after further investigation I found that there are also a lot of pictures of what seem to be safes and safe blueprints, in particular blueprints of the safes lock mechanisms. I also noticed that there are pictures of Bruce Wayne’s screen appear again, these screens also seem to have safe details on them.

A screenshot of a computer

Description automatically generated with medium confidenceA screenshot of a computer

Description automatically generated with medium confidenceA computer screen capture

Description automatically generated with low confidenceGraphical user interface, website

Description automatically generated

As this is the second time I have seen Bruce Wayens name coming up in this investigation I have gotten very suspicious of his involvement In this case.

1. New product spec sheets

This is an empty directory, but I thought it was interesting as this might be a clue as to what information Diana was trying to get her hands on next.

1. Personal

This directory has 7 files in it and seems to be emails that seem to just be pictures and pdf’s of emails that were exchanged between a man called Jon who was sending these emails to Bruce who I suspect is Bruce Wayne who’s name came up already in this investigation.

The emails I was able to open up normally were all the same:

Graphical user interface, text, application

Description automatically generated

1. Research

This directory has 14 files which are mixture of jpg and png files. Any of the files that were fully recovered and I was able to open look to pictures of multiple different types which all have different locking mechanisms and the same email I discovered in the directory before this one.

Graphical user interface, application

Description automatically generated

1. System volume information

This directory has 4 files in it but I wasn’t able to get much information from these files that seemed important to this case, the meta data didn’t show much either when I researched these files.

## Meaningful Data Found

Throughout this investigation I was able to uncover what I believe is meaningful data and, in this section, I will go through and display the files I believe are meaningful.

|  |  |  |
| --- | --- | --- |
| File Name | File Directory | Description |
| F0000032.jpg | Carved Files | This file is a screenshot of Bruce Waynes screen which shows a site called intranet portal which is a super fake ltd portal which contains sensitive information. Note the laptop being used is a mac OS system. |
| F0013896.jpg | Carved Files | This a blueprint of a safes lock mechanism. I couldn’t figure out what model the safe was, I checked the file meta-data but that didn’t reveal much. |
| F0020160.jpg | Carved Files | This is another blueprint which I think is also a safe mechanism but can’t clearly tell which component of the safe it is. |
| F0029664.jpg | Carved Files | This is the same image as the last one except it’s a picture of Bruce Waynes laptop with that image open on it. |
| F0042872.jpg | Carved Files | This is another picture of Bruce Waynes laptop showing an image which is sensitive information and superfake. Doesn’t want brought out of the company. |
| F0057200.jpg | Carved Files | This again is the same image as the first one I showed except its again on Bruce Waynes laptop and not just the image file. |
| F0069288.jpg | Carved Files | This image is another screenshot off Bruce Waynes computer and shows the same image as F0042872.jpg. |
| F0083152.jpg | Carved Files | This is a picture of Bruce Waynes computer and shows some of the blueprints mentioned above but it also shows the projects that Superfake are currently working on. The project they are currently working on are a s follows: Model T800, Model T1000, ModelXR2001, ModelXR3001. |
| F0096216.jpg | Carved Files | This is an email written to Bruce telling him he has access to the T1000 project folder on the Intranet portal that superfake have. It also ask him if he is still available to demo the T800 model on that upcoming Friday. |
| All Files in this  Directory. | .Cracking Programs | All these files I think are meaningful as they seem like files which override the safes locking mechanism. I can’t be sure if they would work but definitely think they are important to note. |
| Safe\_1.jpg | Research | Picture of a safe presumably one which is developed by Superfake. Might be a safe that there is a cracking program for. |
| Safe\_2.jpg | Research | Picture of a safe presumably one which is developed by Superfake. Might be a safe that there is a cracking program for. |
| Safe\_3.jpg | Research | Picture of a safe presumably one which is developed by Superfake. Might be a safe that there is a cracking program for. |
| Safe\_4.jpg | Research | Picture of a safe presumably one which is developed by Superfake. Might be a safe that there is a cracking program for. |
| Safe\_5.png | Research | Picture of a safe presumably one which is developed by Superfake. Might be a safe that there is a cracking program for. |
| Safe\_6.jpg | Research | Picture of a safe presumably one which is developed by Superfake. Might be a safe that there is a cracking program for. |
| Safe\_7.jpg | Research | Picture of a safe presumably one which is developed by Superfake. Might be a safe that there is a cracking program for. |
| Error.mov | Deleted Files | This is a partially recovered file which doesn’t play. I tried a few things to try get something to play such as a manual carve, tried to restore the video by using this site, <https://repairit.wondershare.com/download-repairit-windows.html> and i also tried to download different player on my machine and change the file extension to no avail but I do believe this file could be hiding something of importance to this case. |
| Safe\_cracking\_instructions.pdf | Deleted Files | This file sparked interest right after I read the title so I decided to try and open it using all my browsers with no success so I had to download an application on my laptop to see If that worked which it did. The application is called. Draw board pdf. The reason I choose this app is because I could see an image of the pdf before I tried to open it so I figured this app would open that image which it did. See the pdf below |

Graphical user interface, text

Description automatically generated

|  |  |  |
| --- | --- | --- |
| AddressBook.xlsx | Encryption Detected | This is file is encrypted, I tried to decrypt it but wasn’t successful, I think it could be an interesting file as it could be an address book with a list of address to companies who have a Superfake safe. |
| Blueprints.docx | Encryption Detected | This is file is encrypted, I tried to decrypt it but wasn’t successful. This is also an interesting file as it probably contains more safe blueprints. |

# *Recommendations*

My recommendations for how this case should proceed and what Superfake should do are as follows:

1. Dianas workplace should be checked and any electronics and emails should be gathered up to further investigate what her intentions were and see if any private information has actually been leaked to the wrong people.
2. Bruce Wayne should be investigated to see how he is involved in this case and his work laptop and other work-related items should be seized for investigation.
3. The files which are encrypted should be given to an expert to see if they can decrypt them and find out the contents.