# F20FO Coursework 2

Digital Forensics Investigation

Chandrashekhar Ramaprasad (cr2007)
BSc. Computer Science (Hons.)
H00356126

## Contents



---

# Introduction

In the role of a Digital Forensics Analyst assigned to this case, the task was to manage a piece of evidence retrieved from a suspect. This involved creating two forensically sound images of the seized digital evidence and conducting a forensic analysis using two designated tools.

This report documents the imaging process, establishes the chain of custody, and outlines the analysis performed on the provided digital evidence.

---

# Forensic Imaging Process

For the initial first task of the assignment, the objective was to create a verifiable forensic image of the seized digital evidence media. This was achieved using two forensic tools: FTK Imager and dd for windows. The forensic image produced with FTK Imager was in EnCase Image (`.E01`) format, whereas the image created with dd for windows was in Raw Image (`.img`) format.

## FTK Imager

In generating the initial forensic image, FTK Imager was employed to create the first forensic image of the VMWare virtual disk files. FTK Imager streamlines the process by automatically gathering the accompanying disk files within the designated directory when the base Virtual Disk file is chosen as the source path, simplifying the procedure.

The steps for creating a verifiable forensic image of the evidence media using FTK Imager are as follows:

1. Open FTK Imager
2. Navigate to File > Create Disk Image
3. Choose 'Image File' as the option
4. Specify the Source Path for the Evidence Media
5. Add a destination for the image using the Add Button, selecting the E01 type
6. Provide necessary information for the Evidence Item
7. Select the Image Destination folder and specify the file name
8. Set the Image Fragment Size to 0 to prevent fragmentation
9. Click on '**Start**' to initiate the process

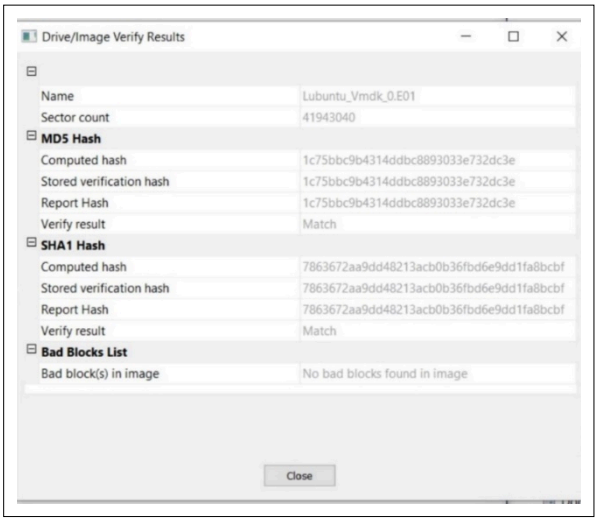


Figure 1: The results page in FTK Imager containing the Hash values after the imaging process.

This process resulted in the creation of an EnCase Image (`.E01`) file, serving as a forensic image of the evidence disk, with associated Hash values stored for verification.

The imaging process was completed within approximately 15 minutes.

## dd for windows

For the second forensic image, dd for windows, a free, open-source tool developed by Chrysocome and Newbigin (2010) was utilized for flexible file conversion and copying in a win32 environment. Unlike FTK Imager, dd for windows does not automatically gather and combine supporting virtual disk files in the Evidence folder. To address this, additional steps were undertaken before creating a forensic image using dd for windows.

### VMware-VDiskManager

The initial task involved merging the split-up vmdk files into a single file using the `vmware-diskmanager` command in VMware. This command is accessible in VMWare Fusion and VMWare Workstation. For VMWare Player, a separate utility can be obtained from the VMware website. The process, outlined by Ahmed (2014) , proceeded as follows:

1. Navigate to the directory where the VMware application is installed (typically, `C:\Program Files (x86)\VMware\VMware Workstation` on Windows)
2. Make a note of the file path where the VM disk files are located
3. Open Command Prompt and navigate to the directory containing the VM disk files
4. To merge the files into a single .vmdk file, execute the following command in the terminal:

```shell
"C:\Program Files (x86)\VMware\VMware Workstation\vmware-diskmanager.exe" `
-r "Path/to/File.vmdk" `
-t 0 MyNewImage.vmdk
```

5. The new file will be created.


Figure 2: A screenshot of the VDiskManager command to merge the vmdk files.

### Forensic Imaging

Once the combined VM Disk Image was generated, it was utilized to create the forensic image using dd for windows. The process involved:

1. Downloading and extracting the Binary ZIP package of the dd tool from the Chrysocome website
2. Open Command Prompt in the directory containing the 'dd.exe' file
3. Executing the following command in the Command Prompt window:

```shell
.\dd.exe if="file/path/of/evidence.vmdk" of="output/file/path/file.img"
```

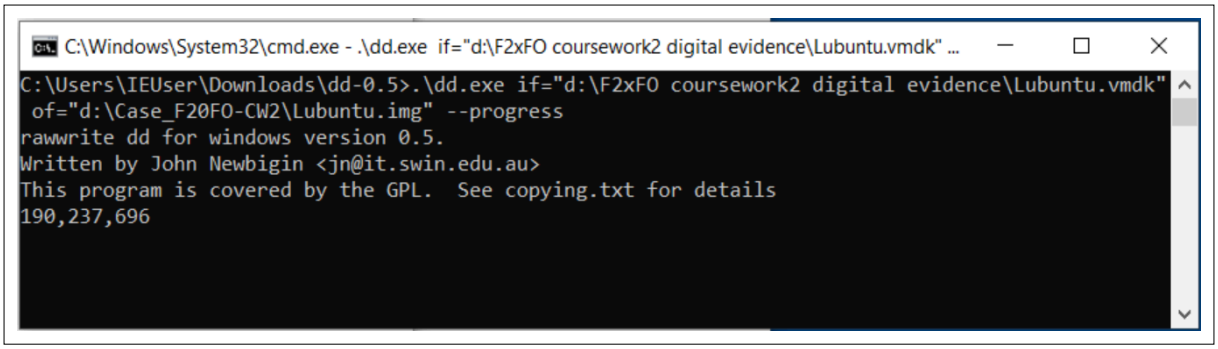


Figure 3: A screenshot of the dd tool being used in progress to create a forensic image of a disk image.

The imaging process using **dd for windows** took approximately 2 hours to complete.

---

## Forensic Analysis

In the Forensic Analysis phase, the forensic tools Autopsy, and OSForensics were used to analyse the forensic images of the digital evidence.

Upon initial inspection, it was determined that the system is a Linux machine running the Lubuntu operating system. Six users were identified by examining the 'home' directory:

1. f21fo-cw2
2. student1
3. student2
4. tutor1
5. user_one
6. user_ten

The primary user, "**f21fo-cw2**", was found to be responsible for all activity on the machine, while the other users retained only their configurations.

### Password-Protected Word Documents

There were 3 password-protected documents in the machine.

The passwords for the encrypted files were using John the Ripper, a free and open-source password cracking tool, and Python 2.7 for extracting the passwords for the files.

The following steps, outlined by LeCain (2023), were followed to crack the passwords and examine the documents:

1. Installed Python 2.7.18, the last release of Python 2, as of April 2020
2. Installed and extracted John the Ripper
3. Copied the `office2john.py` script from John the Ripper to the Python 2.7 directory.
4. Executed the script against the password-protected file:

```
1  .\python.exe office2john.py <file>.doc                    Shell
```

```
C:\Python27>.\python.exe .\office2john.py "Evidence_F20FO/9464-Albert Einstein.doc"
9464-Albert Einstein.doc:$oldoffice$1*867d6947deca0b62fe61323eecceef1d*ed7f90d4f425227d38d7e2d191877b0c*0b4acde8f1
edf21481f0e4daaf1435be::::Evidence_F20FO/9464-Albert Einstein.doc

C:\Python27>.\python.exe .\office2john.py "Evidence_F20FO/9472-Nicolaus Copernicus.doc"
9472-Nicolaus Copernicus.doc:$oldoffice$1*a6d5398bf51dc3a28ab48cfcd1dcf910*285f3c933fcdc9a7ea49a6993ee56e04*33f7c4
d8ed0967bb7cc24fc7830ceecd::::Evidence_F20FO/9472-Nicolaus Copernicus.doc
```

5. Recorded the hash values extracted from the Python script
6. Stored the hash value in a text file within the 'john' directory (the location of the John the Ripper program)
7. Downloaded the Rockyou.txt wordlist (~133MB) and stored it inside the 'john' directory
8. Ran the John the Ripper program using the Rockyou.txt wordlist to crack the hash values present in the text file (the MS Office hashes)

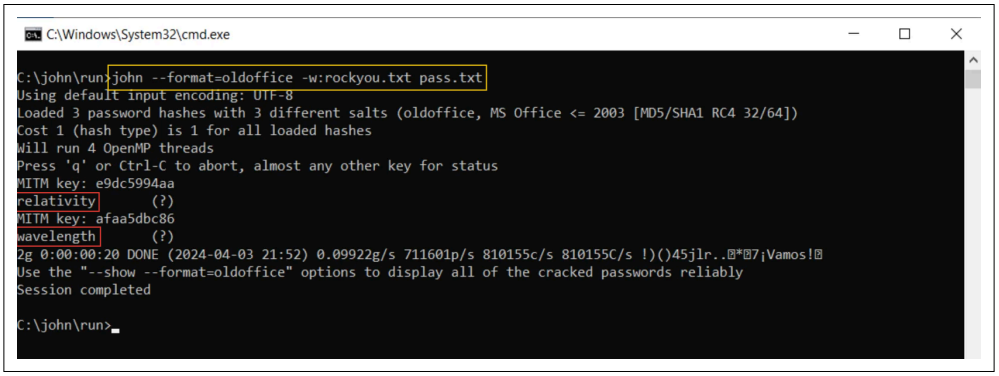


Figure 4: Command Prompt output of the John the Ripper program

Analysis of the cracked passwords revealed that they corresponded to specific individuals' contributions to the scientific community. For instance, passwords referenced Einstein's theory of relativity and Copernicus' foundational work in astronomy, which often involves the analysis of light across various wavelengths to study celestial objects.

## EXIF Images

Further analysis revealed a diverse range of devices used for capturing the images, with most device specifics readily available either through the file names or within the file metadata.

The brands and models identified in the images are as follows:

| Brand | Models |
|---|---|
| Agfa | DC-504, DC-733s, DC-830i, Sensor505-x, Sensor 530s |
| Canon | Ixus55, Ixus70, EX-Z150 |
| Fujifilm | FinePixJ50 |
| Kodak | M1063 |
| Nikon | CoolPix S170, D200, D70, D70s |
| Olympus | MJU |
| Panasonic | DMC-FZ50 |
| Pentax | Optio A40, Optio W60 |
| Praktica | DCZ5.9 |
| Ricoh | GX100 |
| Rollei | RCP-7325XS |
| Samsung | Galaxy S2, VLUU NV15, VLUU L74 |
| Sony | DSC-H50, DSC-T77, DSC-W170 |
| ZTE | Orange San Francisco |

The images primarily consisted of outdoor scenery, a cup full of candy, and a teacup, captured from various perspectives. Additionally, numerous random images of books, roads, and outdoor scenes were observed.

---

## Bash History

Upon further examination of the forensic image using OSForensics, attention was drawn to the '**.bash_history**' file, housing the command history for the Bash shell, generated for each user within their respective '**home**' directory.

An observation was made regarding the user's attempts to install the Wine library, enabling Windows applications to run on Linux systems.

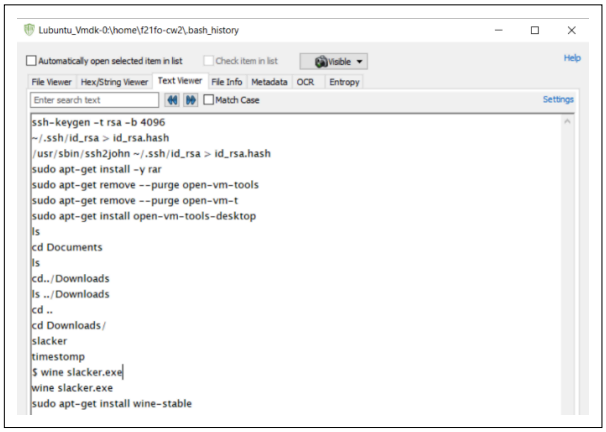


Figure 5: A screenshot of the contents of the '**.bash_history**' file.

Subsequently, the user attempted to execute the Wine tool on 'slacker.exe' and then utilize the 'timestomp' tool. A quick online search revealed that 'slacker.exe' is a tool for concealing secret data in stack space (mhibert, 2018), while Timestomp is a technique for altering file timestamps (Dumont and ESET, 2020).

An unusual aspect was noted wherein the user initially attempted to run the '`wine`' command before installing the '`wine-stable`' package. The first line in the file denotes the first command successfully executed in the system, followed by subsequent commands.

Additionally, it was observed that the user generated an **RSA key pair** with a key length of 4096 bits. They then attempted to decipher the contents of the RSA key using John the Ripper, specifically via the '**ssh2john**' Python script, with the output redirected to the '**id_rsa.hash**' file.

---

### Issues Faced

During the forensic analysis, encountering issues with OSForensics was very common. Certain sections or functionalities of the application would always trigger errors, leading to the generation of debug reports and automatic closure of the app, as illustrated by the screenshot.

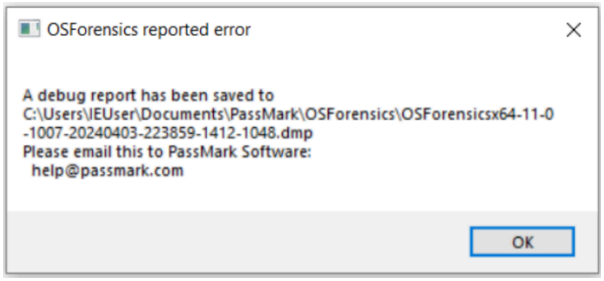


Figure 6: Screenshot of the error message displayed by the OSForensics tool

---

## Conclusion

In conclusion, this report outlines the tasks undertaken in a case involving digital evidence retrieved from a suspect. The assignment involved creating forensically sound images of the evidence and conducting a thorough forensic analysis. The findings reveal significant insight into the user's activities, including attempts to conceal the data and modify timestamps using specialized tools. Additionally, the discovery of password-protected documents and the cracking of their passwords provides further context to the case.

The thorough examination of the Bash history file uncovered the user's efforts to leverage the Wine library to execute Windows applications on the Linux system, as well as the generation of an RSA key pair and subsequent attempts to decipher its contents. These observations suggest the suspect's familiarity with various forensic tools and techniques, potentially indicating an advanced understanding of digital forensics.

Overall, the comprehensive forensic analysis of the evidence provides valuable information that can aid in the ongoing investigation. The detailed documentation of the imaging process and the comprehensive chain of custody contribute to the forensic integrity of the evidence, ensuring its admissibility in any legal proceedings. The insights gained from this analysis will undoubtedly prove instrumental in the progression of the case.

---

# Appendix

## Chain of custody

| Date | Time | Action |
|---|---|---|
| March 19, 2024 | 17:44 | Acquired Digital Evidence from Line Manager (Course Leader) |
| March 21, 2024 | 19:18 | Created Forensic Image 1 using 'FTK Imager' |
| March 28, 2024 | 00:22 | Created Forensic Image 2 using 'dd for windows' |
| March 30, 2024 | 17:50 | Created Autopsy case using the Forensic Image |
| March 31, 2024 | 03:52 | Autopsy case setup (Ingest) completed |
| April 2, 2024 | 08:45 | Setup New Case in OSForensics |

---

# References

Ahmed, S. (2014) *HOW TO MERGE MULTIPLE VMDK'S INTO SINGLE VMDK*. WordPress.com. Available at: https://vmexpo.wordpress.com/2014/04/15/how-to-merge-multiple-vmdks-into-single-vmdk/.

Chrysocome and Newbigin, J. (2010) *dd for windows*. Chrysocome. Available at: http://www.chrysocome.net/dd.

Dumont, R. and ESET (2020) *Indicator Removal: Timestomp*. The MITRE Corporation. Available at: https://attack.mitre.org/techniques/T1070/006/.

LeCain, L. (2023) *Cracking Encrypted Microsoft Office Files*. YouTube Inc.. Available at: https://youtu.be/PsFFSrtLXYY.

mhibert (2018) *Slacker.exe and Timestomp.exe*. Forensic Focus. Available at: https://www.forensicfocus.com/forums/general/slacker-exe-and-timestomp-exe/.