Digital Forensics

Cyber Security

Arranged by:

Inacio Campos – 1301183625

School of computing

Telkom University

Bandung

Table of Contents

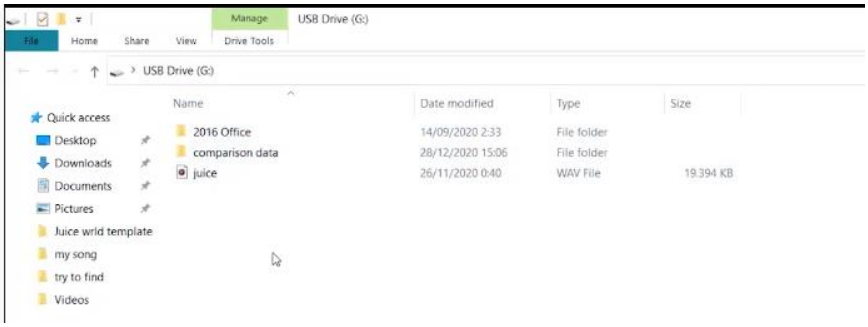
I. Introduction

This report Is about the final project of cyber security which is about Digital forensic. I will collect evidence in digital form and examine it. I have done a scenario of external storage with 3 main contents, a document file, a video and a photo that would be deleted.

The examination will be done by doing the identification, preservation and analysis of the external storage which is a USB of those deleted files. The process of preservation would be done using a tools “access data FTK imager” and then we will analyze the content that displayed after we mounted.

II. The evidence (identification)

The evidence is an external storage (USB) with black and red color brand **SanDisc 4Gb** which included file multimedia and document.



III. The objective of Examination

We are required to identify if there is deleted or formatted file in the USB disk and then I will compare with the original content that I have deleted.

Objective:

1. Check all the content of the USB disk
2. Find formatted of deleted file
3. Identify the missing data
4. Analyze

IV. Examination Procedure (preservation)

1. Process of preparing the data

I have an external storage which SUB disk then I copied a document a video and a photo. After that I saved these three files to analyze. Then I delete these files from The USB disk. Thus, the USB is ready to be examined.

2. Process of Examination

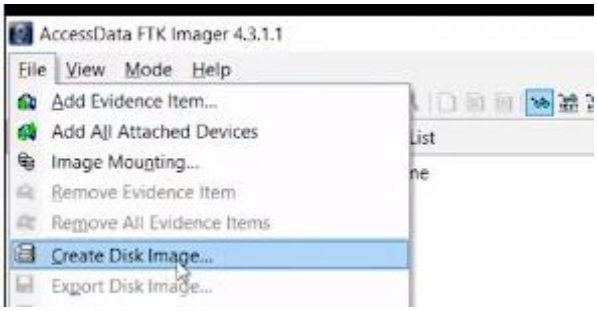
I used Access Data FTK imager version version 4.3.1 as a tool to examine the evidence.

2.1. Process of creating image

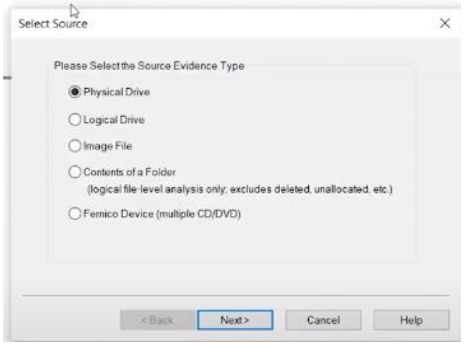
Is the process copying entire data of external storage.

a. The steps to create a disk image

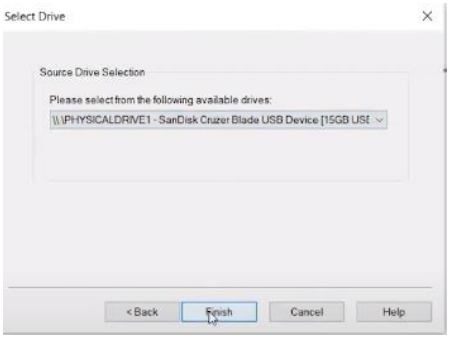
1



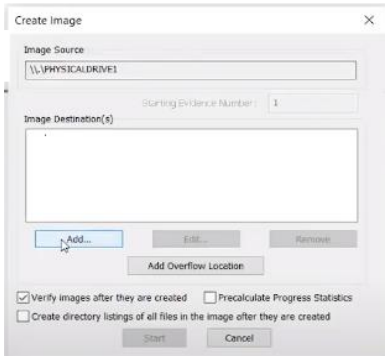
2



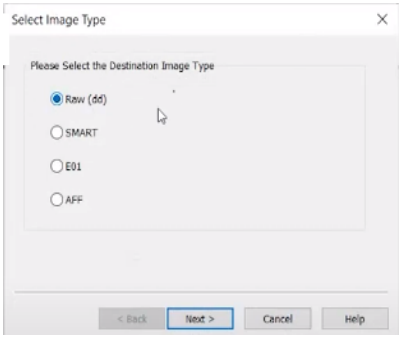
3



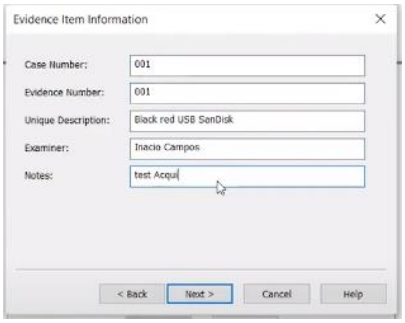
4



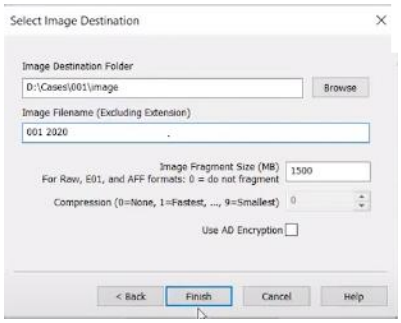
5



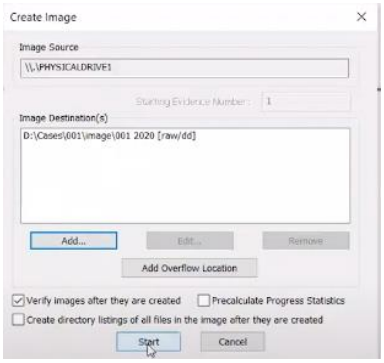
6



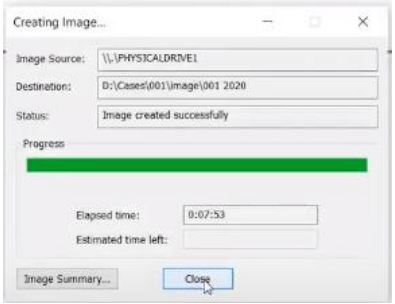
7



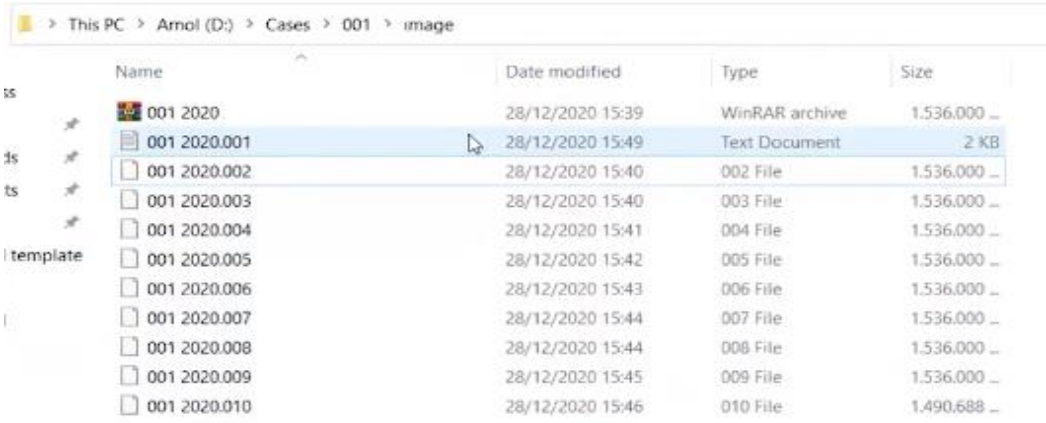
8



9

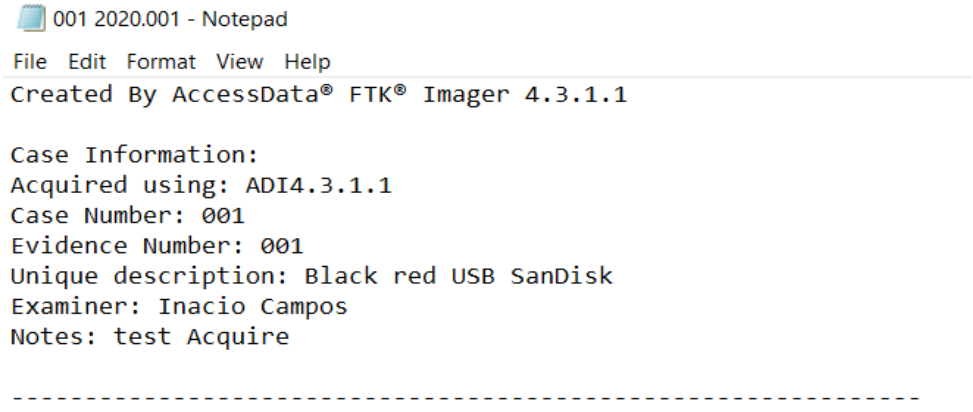


b. Result of Disk Imager



In the text document file consist of interesting information about the image of data that was created:

- **The information about the case including case no, evidence and examiner**



- **The information about the USB disk including the contents. There are 2 hash computation to verify the image that produce is the same with the content of the USB drive.**

```
Information for D:\Cases\001\image\001 2020:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1.906
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 30.629.376
[Physical Drive Information]
 Drive Model: SanDisk Cruzer Blade USB Device
 Drive Serial Number: 4C531001420822105555
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 14955 MB
 Sector count:    30629376
[Computed Hashes]
 MD5 checksum:    06fa6a6b0f50f016c1e1d239aae80f42
 SHA1 checksum:   f6fd7a181830403124ac3b61ae935d3e8540c549
```

- **Information about the image including the date and the destination of the image folder**

```
Image Information:
 Acquisition started:   Mon Dec 28 15:38:30 2020
 Acquisition finished:  Mon Dec 28 15:46:23 2020
 Segment list:
  D:\Cases\001\image\001 2020.001
  D:\Cases\001\image\001 2020.002
  D:\Cases\001\image\001 2020.003
  D:\Cases\001\image\001 2020.004
  D:\Cases\001\image\001 2020.005
  D:\Cases\001\image\001 2020.006
  D:\Cases\001\image\001 2020.007
  D:\Cases\001\image\001 2020.008
  D:\Cases\001\image\001 2020.009
  D:\Cases\001\image\001 2020.010
```

‘’’

- **The verification of the image content and the content Of the USB disk. FTK imager verified that the contents of the disk image are the same with USB disk.**

```
Image Verification Results:
 Verification started:  Mon Dec 28 15:46:32 2020
 Verification finished: Mon Dec 28 15:49:44 2020
 MD5 checksum:    06fa6a6b0f50f016c1e1d239aae80f42 : verified
 SHA1 checksum:   f6fd7a181830403124ac3b61ae935d3e8540c549 : verified
```

V. Analyze the content (analysis)

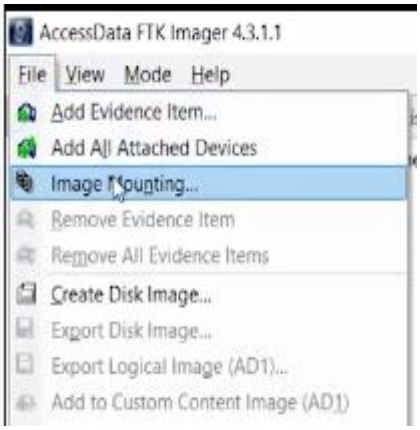
Determine significance, reconstruct fragments of data and draw conclusion based on evidence found.

1. Process of Mounting

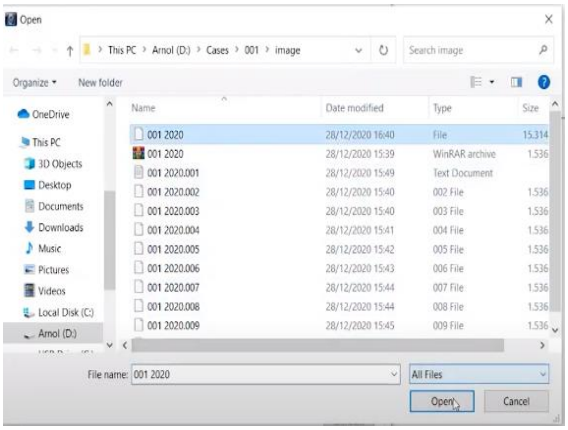
is a **process** by which the operating system makes files and directories on a storage device (disk image that we created) available for users to access via the computer's file system.

a. The step of Mounting

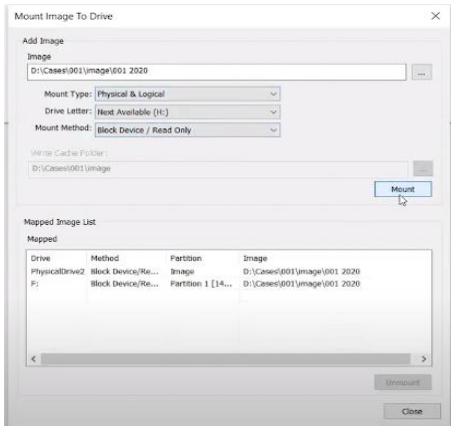
1



2

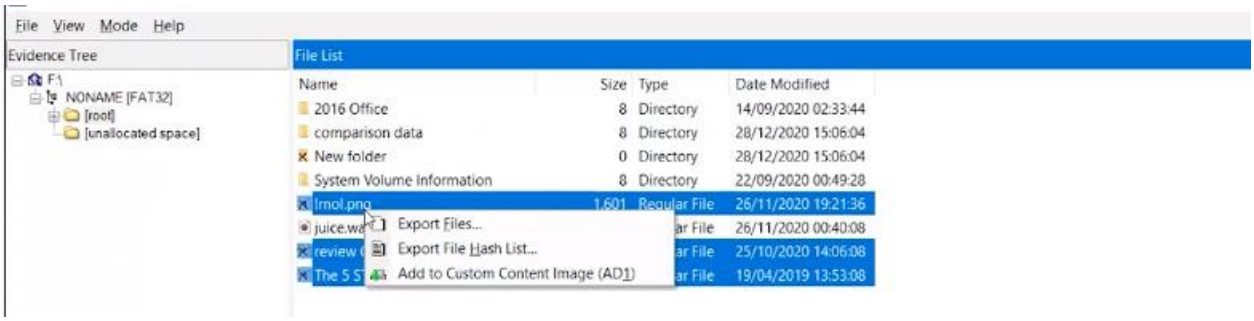


3



b. The result of mounting

- **The result after mounting we can see there are 5 deleted files which is including our 3 deleted file. furthermore, we are going to export this files and analyze the content of the file.**

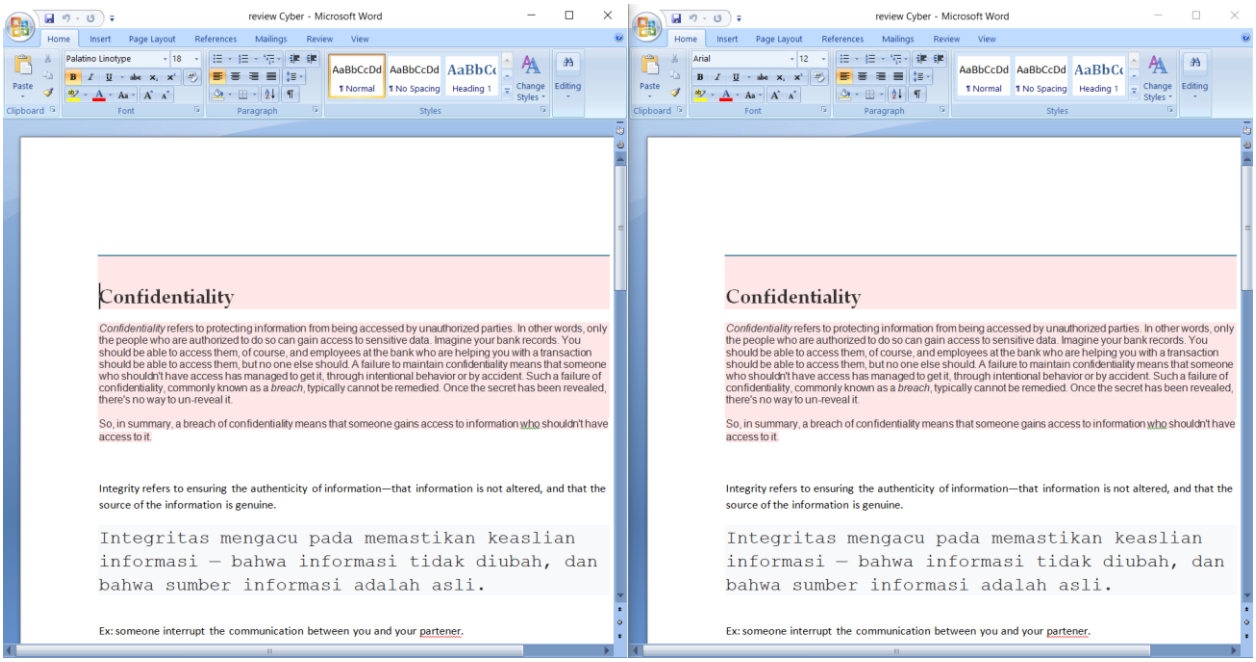


c. Comparison

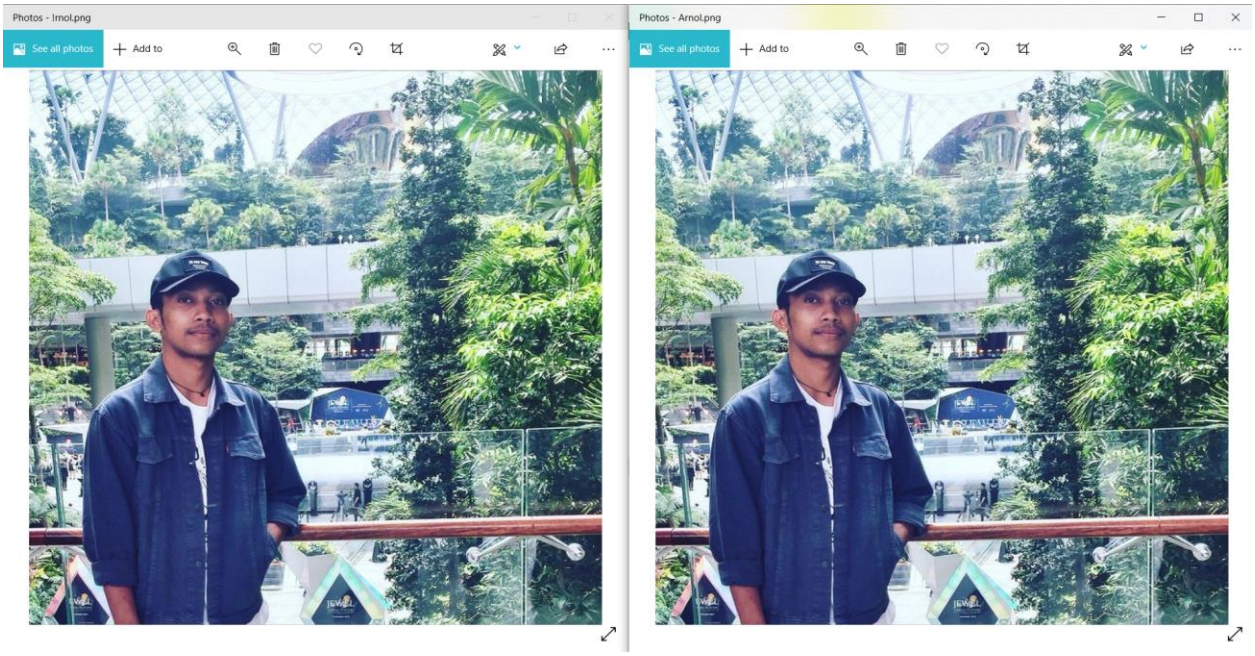
The Comparison between the mounted files contents and the original file contents.

- **Document file**

  As we can see the contents are exactly the same.

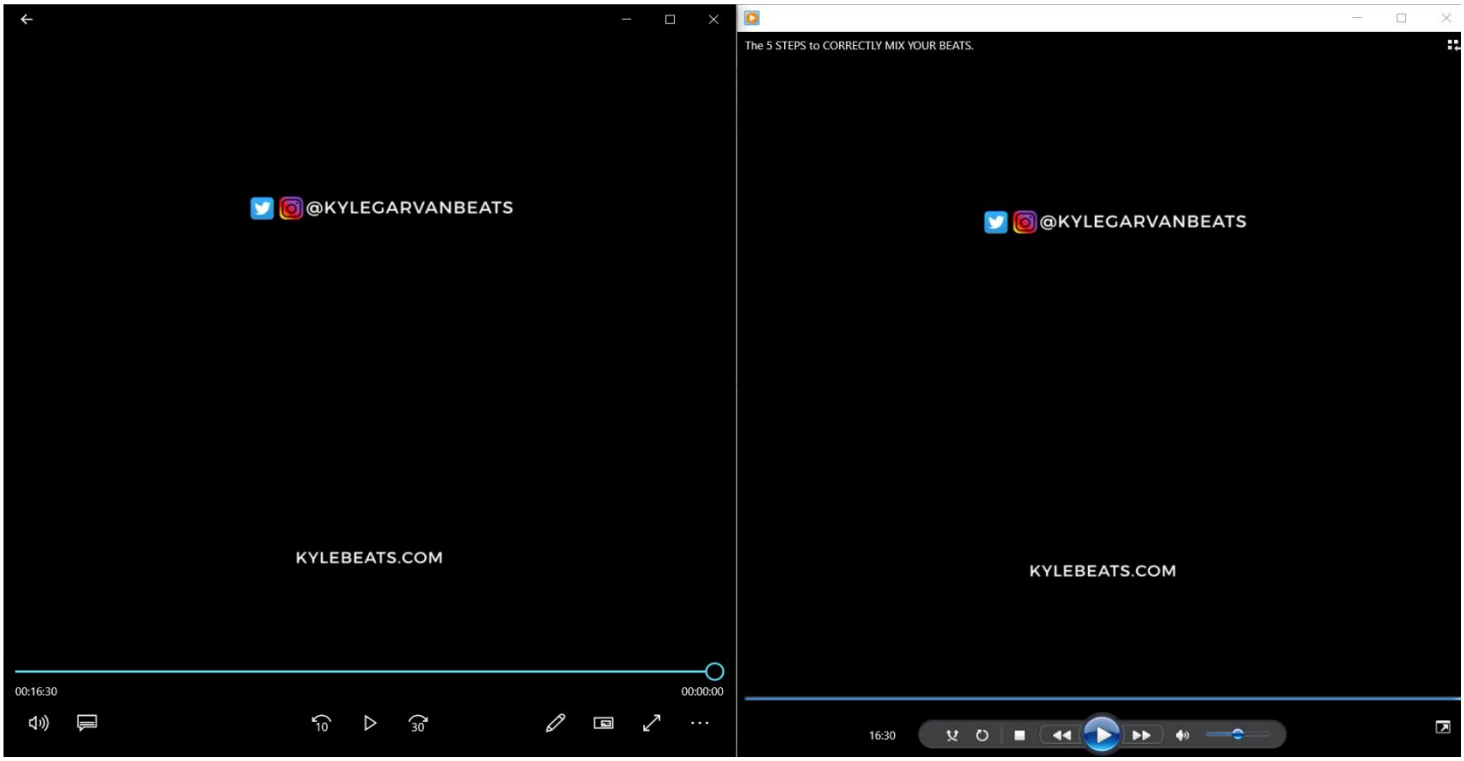


- **photo**



- **Video**

  The duration of the mounted and original video both are 16:30.

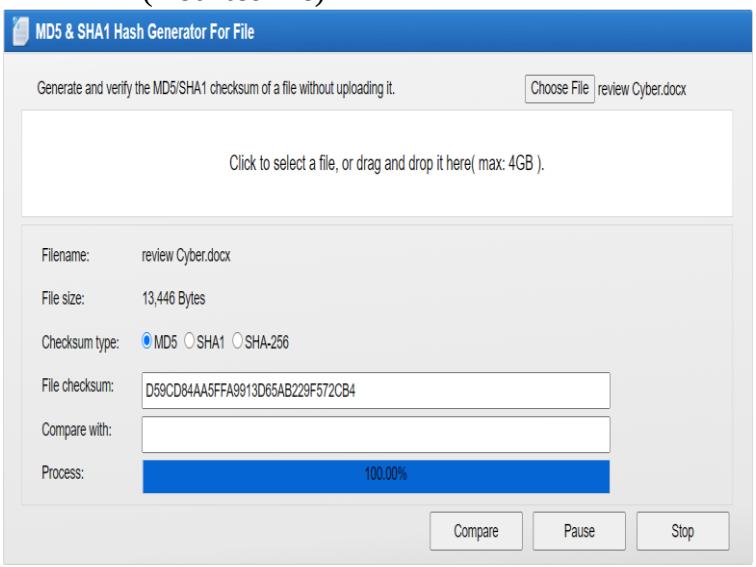


d. Comparison with has value

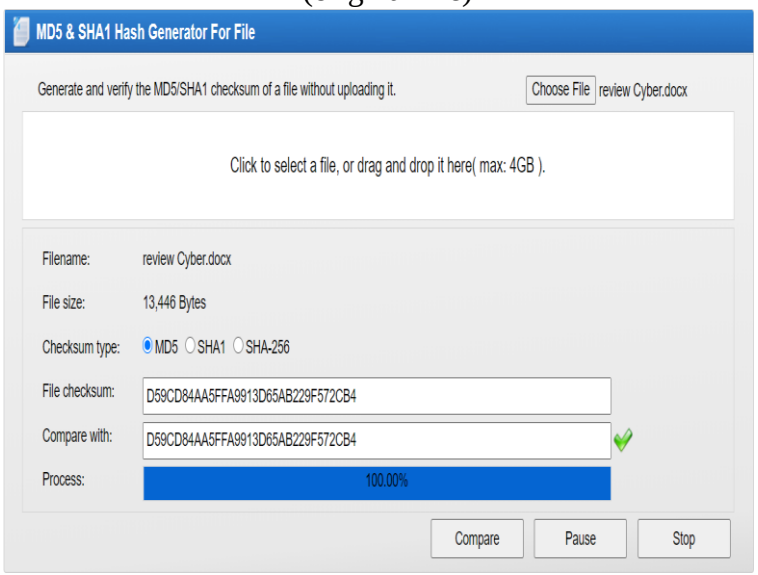
We will compare the hash value of the mounted files content to the has value of the original content see if the content are exactly the same

- **Document**

(mounted file)

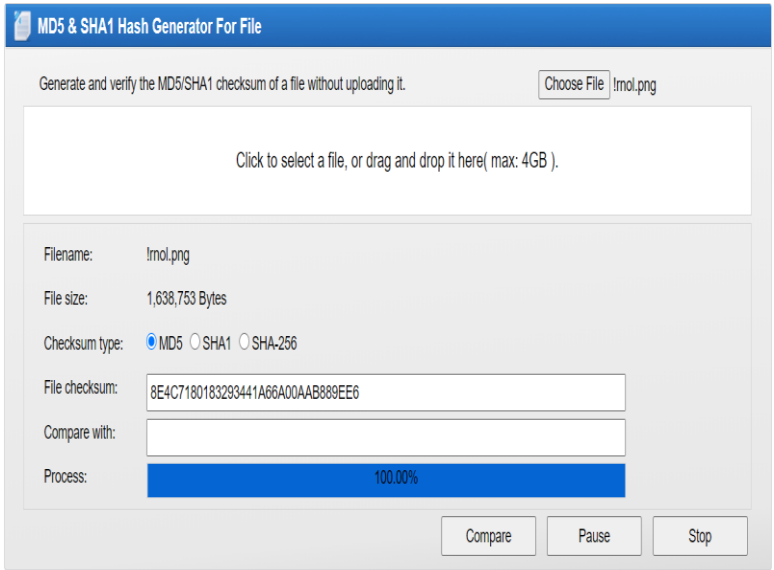


(original file)

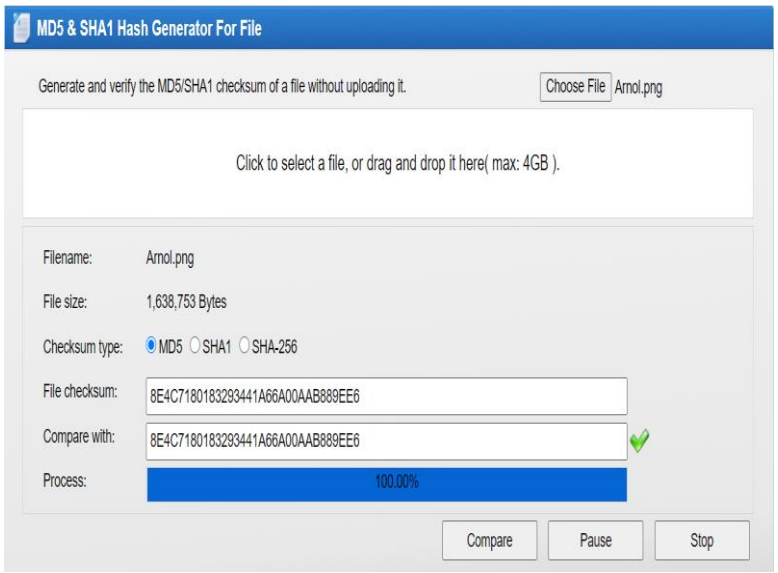


- **Photo**

(mounted file)

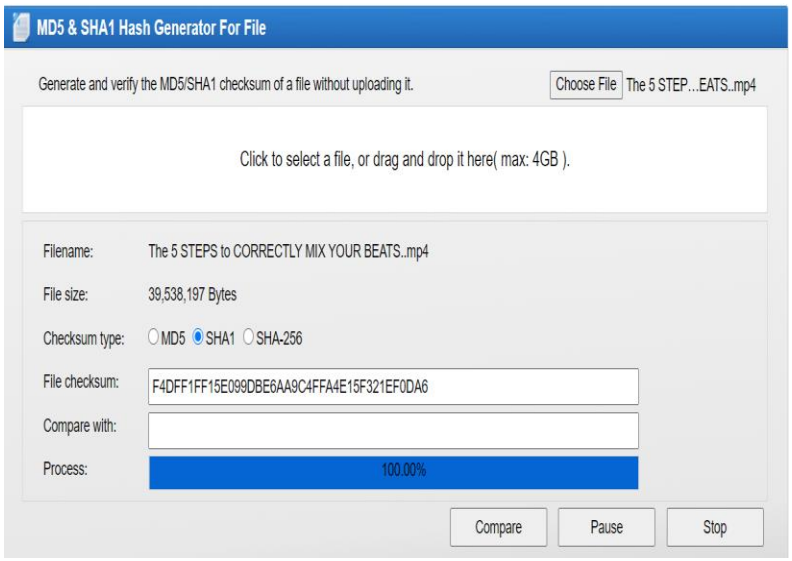


(original file)

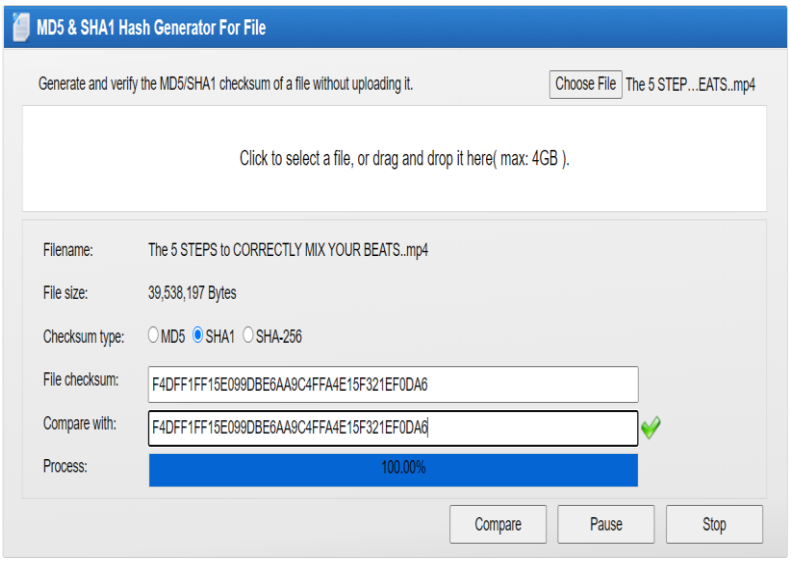


- **Video**

(mounted file)



(original file)



VI. Conclusion

After we did the process of creating disk imager, we mounted the image and compared the contents in the disk image with the original contents we conclude that the contents are exactly the same.

REFERENCE

Slide Digital Inverstigation cyber security Telkom university.

Lecturer video Ms. Farah Aphie:
https://drive.google.com/file/d/1U6QBUy6UK5DSoX_fubdHb-8zr_n0FUb0/view

Check the video of process creating disk image and mounting here:

https://www.youtube.com/watch?v=o5UKAdW82ys&list=PLQysy_rxXo9cEQ7M1TG8stZx-DyGsiaJs&index=14