

Digital Forensics

Cyber Security



Arranged by:

Inacio Campos – 1301183625

School of computing

Telkom University

Bandung

Table of Contents

I.	Introduction	3
II.	The evidence (identification).....	3
III.	The objective of Examination.....	3
IV.	Examination Procedure (preservation).....	3
1.	Process of preparing the data.....	3
2.	Process of Examination.....	4
2.1.	Process of creating image	4
a.	The steps to create a disk image.....	4
b.	Result of Disk Imager	5
V.	Analyze the content (analysis).....	6
1.	Process of Mounting	6
a.	The step of Mounting	6
b.	The result of mounting	7
c.	Comparison.....	7
d.	Comparison with has value.....	9
VI.	Conclusion.....	10
	REFERENCE.....	11

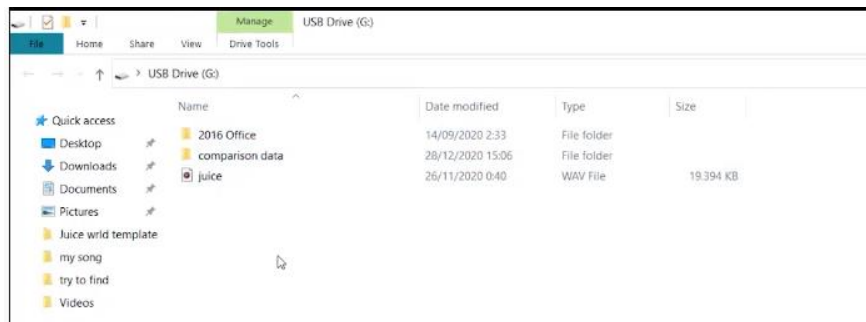
I. Introduction

This report is about the final project of cyber security which is about Digital forensics. 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 tool "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 **SanDisk 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 or 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 is a USB 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.

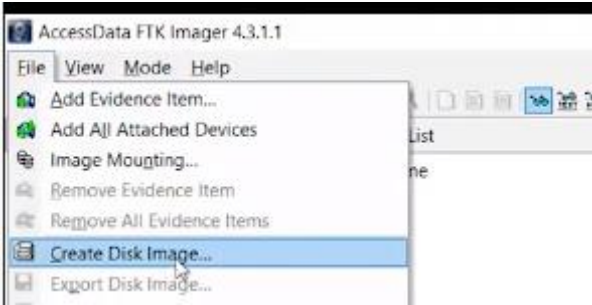

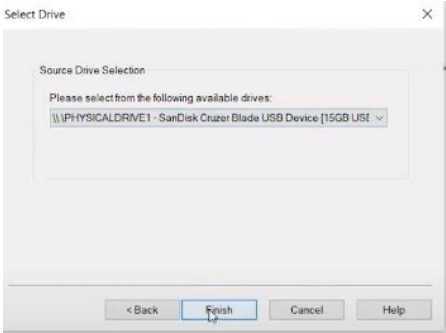
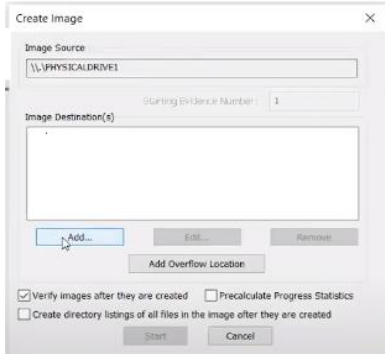
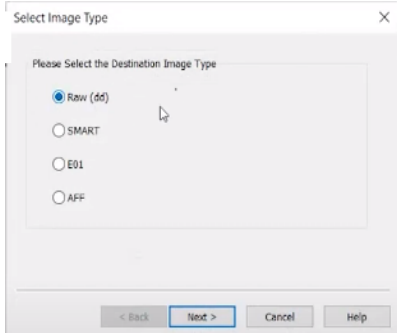
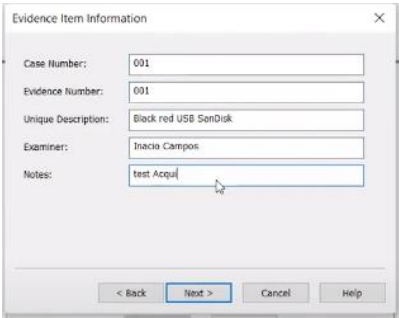
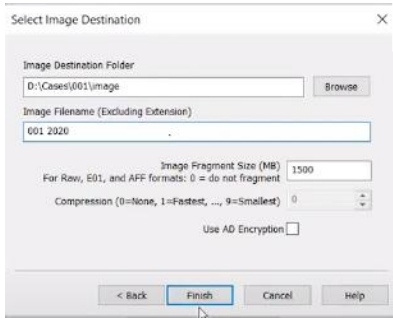
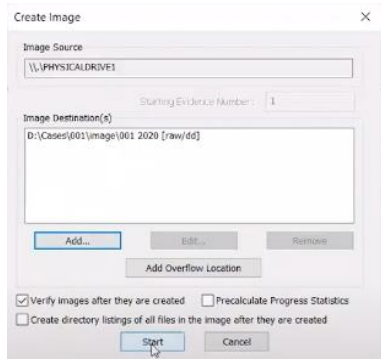
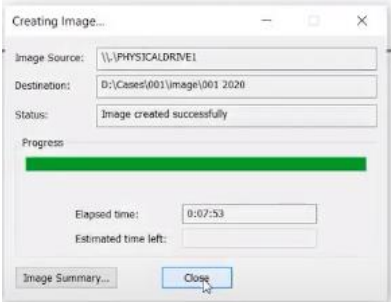
2. Process of Examination

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

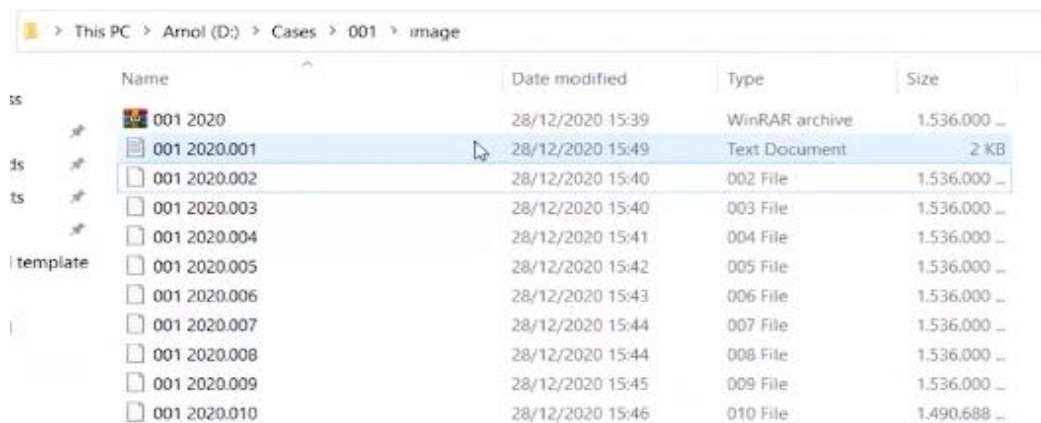
2.1. Process of creating image

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



The screenshot shows a Windows File Explorer window with the address bar displaying the path: > This PC > Arnol (D:) > Cases > 001 > image. The main area contains a table of files and folders. The files are listed with their names, dates modified, types, and sizes. The file '001 2020.001' is highlighted.

Name	Date modified	Type	Size
001 2020.	28/12/2020 15:39	WinRAR archive	1.536.000 ...
001 2020.001	28/12/2020 15:49	Text Document	2 KB
001 2020.002	28/12/2020 15:40	002 File	1.536.000 ...
001 2020.003	28/12/2020 15:40	003 File	1.536.000 ...
001 2020.004	28/12/2020 15:41	004 File	1.536.000 ...
001 2020.005	28/12/2020 15:42	005 File	1.536.000 ...
001 2020.006	28/12/2020 15:43	006 File	1.536.000 ...
001 2020.007	28/12/2020 15:44	007 File	1.536.000 ...
001 2020.008	28/12/2020 15:44	008 File	1.536.000 ...
001 2020.009	28/12/2020 15:45	009 File	1.536.000 ...
001 2020.010	28/12/2020 15:46	010 File	1.490.688 ...

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**

001 2020.001 - Notepad

File Edit Format View Help

Created By AccessData® FTK® Imager 4.3.1.1

Case Information:

Acquired using: ADI4.3.1.1

Case Number: 001

Evidence Number: 001

Unique description: Black red USB SanDisk

Examiner: Inacio Campos

Notes: test Acquire

- **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

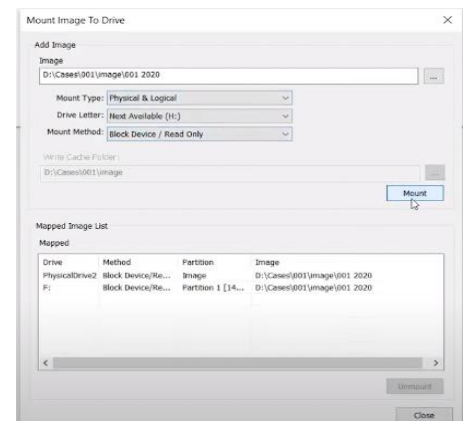
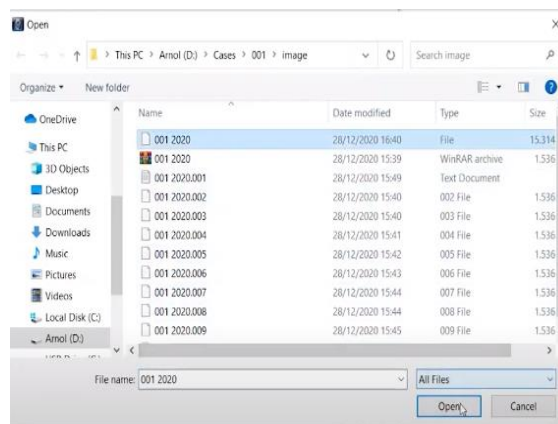
is a **process** by which the operating system makes files and directories on a storage device (disk image that we created) available for users to access via the computer's file system.

a. The step of Mounting

1

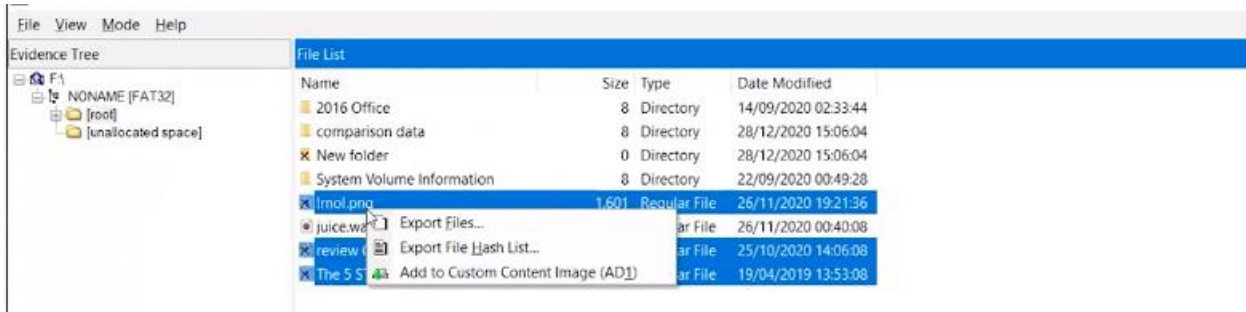
2

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.

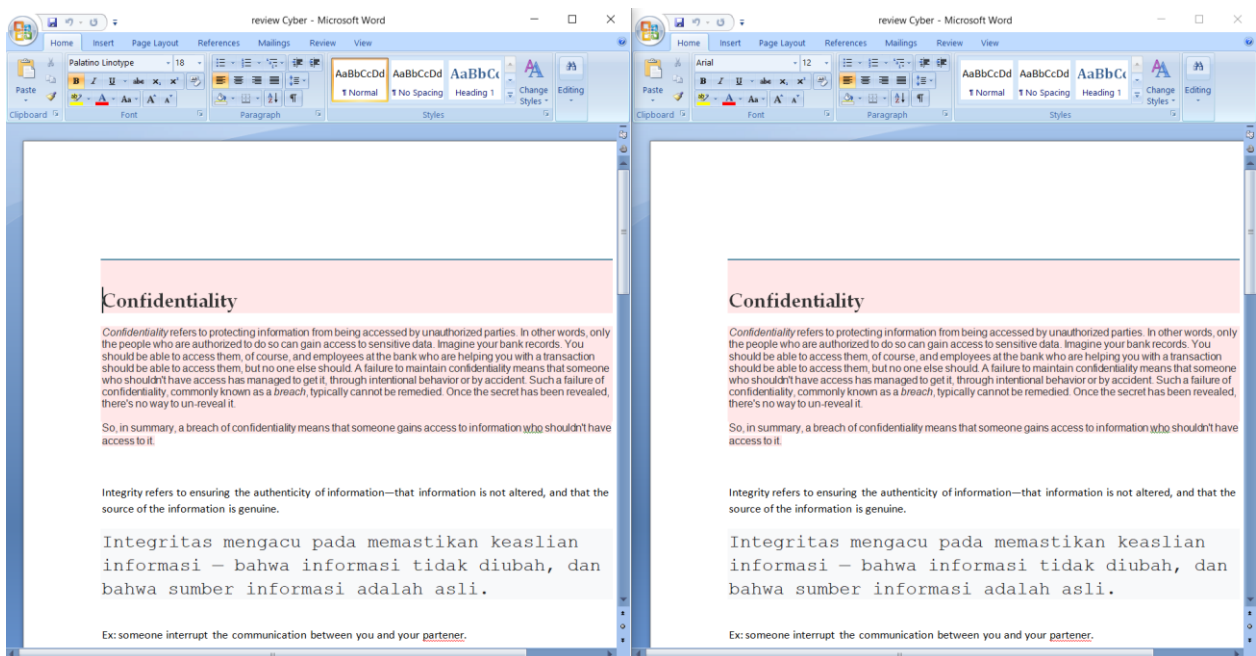


c. Comparison

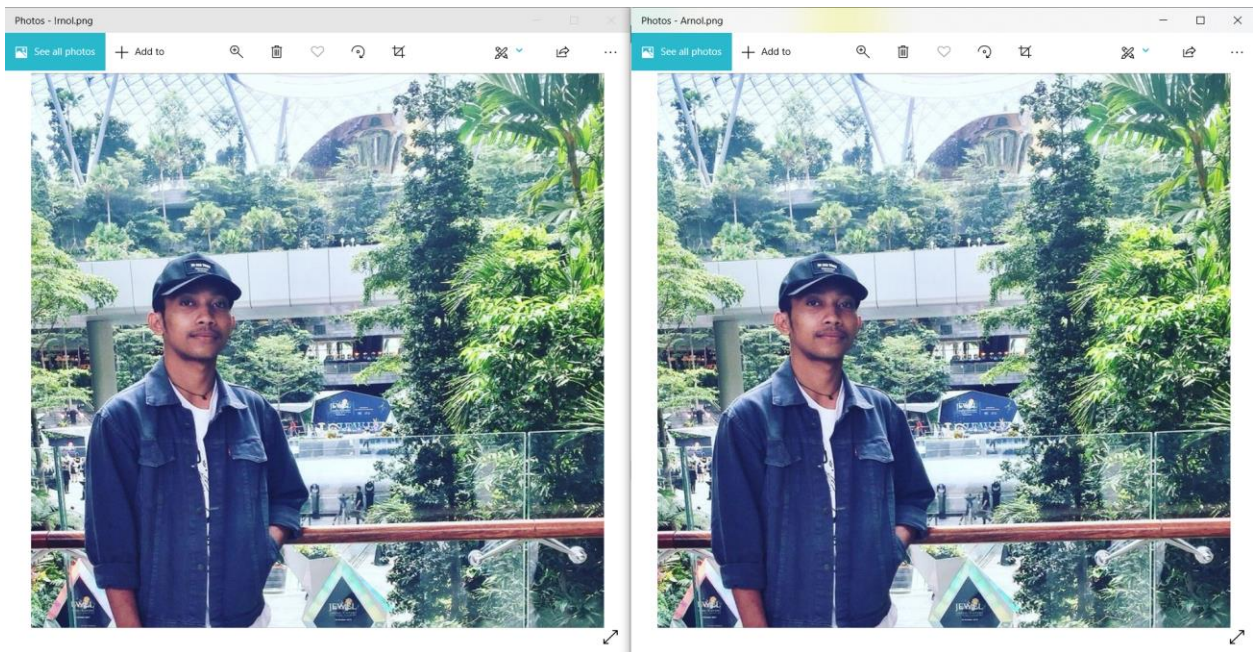
The Comparison between the mounted files contents and the original file contents.

- **Document file**

As we can see the contents are exactly the same.

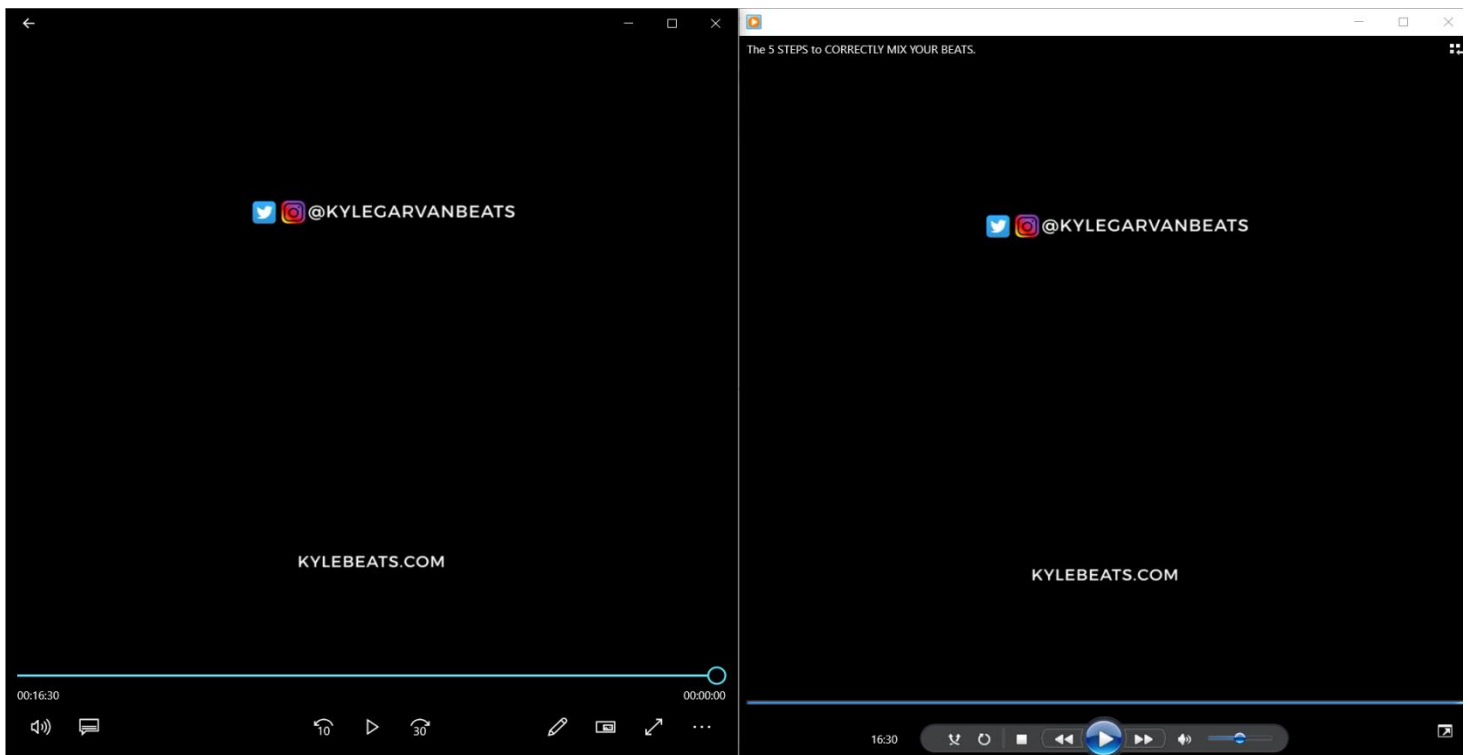


- **photo**



- **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)

The screenshot shows the 'MD5 & SHA1 Hash Generator For File' web application. The interface includes a header with the application name, a sub-header 'Generate and verify the MD5/SHA1 checksum of a file without uploading it.', and a 'Choose File' button. Below this is a large white box with the text 'Click to select a file, or drag and drop it here(max: 4GB).'. The main form area contains the following fields: 'Filename:' with the value 'review Cyber.docx', 'File size:' with '13,446 Bytes', 'Checksum type:' with radio buttons for MD5 (selected), SHA1, and SHA-256, 'File checksum:' with the value 'D59CD84AA5FFA9913D65AB229F572CB4', 'Compare with:' with an empty text box, and 'Process:' with a blue progress bar at 100.00%. At the bottom are three buttons: 'Compare', 'Pause', and 'Stop'.

(original file)

This screenshot is identical to the one for the mounted file, but the 'Compare with:' field contains the same hash value 'D59CD84AA5FFA9913D65AB229F572CB4' as the 'File checksum' field. A green checkmark is visible to the right of the 'Compare with:' input box, indicating a successful comparison. The 'Process:' bar remains at 100.00%.

- **Photo**

(mounted file)

The screenshot shows the 'MD5 & SHA1 Hash Generator For File' web application. The interface includes a header with the application name, a sub-header 'Generate and verify the MD5/SHA1 checksum of a file without uploading it.', and a 'Choose File' button. Below this is a large white box with the text 'Click to select a file, or drag and drop it here(max: 4GB).'. The main form area contains the following fields: 'Filename:' with the value 'Imol.png', 'File size:' with '1,638,753 Bytes', 'Checksum type:' with radio buttons for MD5 (selected), SHA1, and SHA-256, 'File checksum:' with the value '8E4C7180183293441A66A00AAB889EE6', 'Compare with:' with an empty text box, and 'Process:' with a blue progress bar at 100.00%. At the bottom are three buttons: 'Compare', 'Pause', and 'Stop'.

(original file)

This screenshot is identical to the one for the mounted photo file, but the 'Compare with:' field contains the same hash value '8E4C7180183293441A66A00AAB889EE6' as the 'File checksum' field. A green checkmark is visible to the right of the 'Compare with:' input box, indicating a successful comparison. The 'Process:' bar remains at 100.00%.

- **Video**

(mounted file)

MD5 & SHA1 Hash Generator For File

Generate and verify the MD5/SHA1 checksum of a file without uploading it. Choose File The 5 STEP...EATS..mp4

Click to select a file, or drag and drop it here(max: 4GB).

Filename: The 5 STEPS to CORRECTLY MIX YOUR BEATS..mp4

File size: 39,538,197 Bytes

Checksum type: ☐ MD5 ☒ SHA1 ☐ SHA-256

File checksum: F4DFF1FF15E099DBE6AA9C4FFA4E15F321EF0DA6

Compare with:

Process: 100.00%

Compare Pause Stop

(original file)

MD5 & SHA1 Hash Generator For File

Generate and verify the MD5/SHA1 checksum of a file without uploading it. Choose File The 5 STEP...EATS..mp4

Click to select a file, or drag and drop it here(max: 4GB).

Filename: The 5 STEPS to CORRECTLY MIX YOUR BEATS..mp4

File size: 39,538,197 Bytes

Checksum type: ☐ MD5 ☒ SHA1 ☐ SHA-256

File checksum: F4DFF1FF15E099DBE6AA9C4FFA4E15F321EF0DA6

Compare with: F4DFF1FF15E099DBE6AA9C4FFA4E15F321EF0DA6

Process: 100.00%

Compare Pause Stop

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