

FTK IMAGER Report

Disusun oleh :

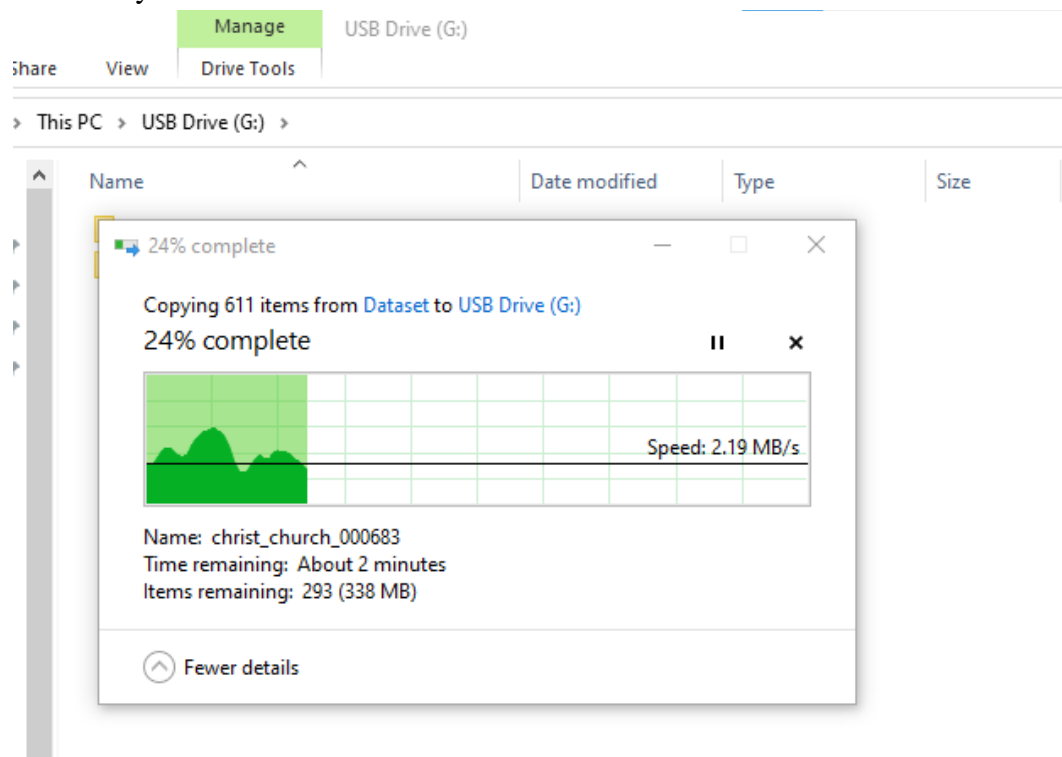
Deny Ahmad Sofyan (1301194274)
Mohamad Rizki Nugraha (1301194092)
Zahid Athallah Shabir (1301194074)

A. Keterangan

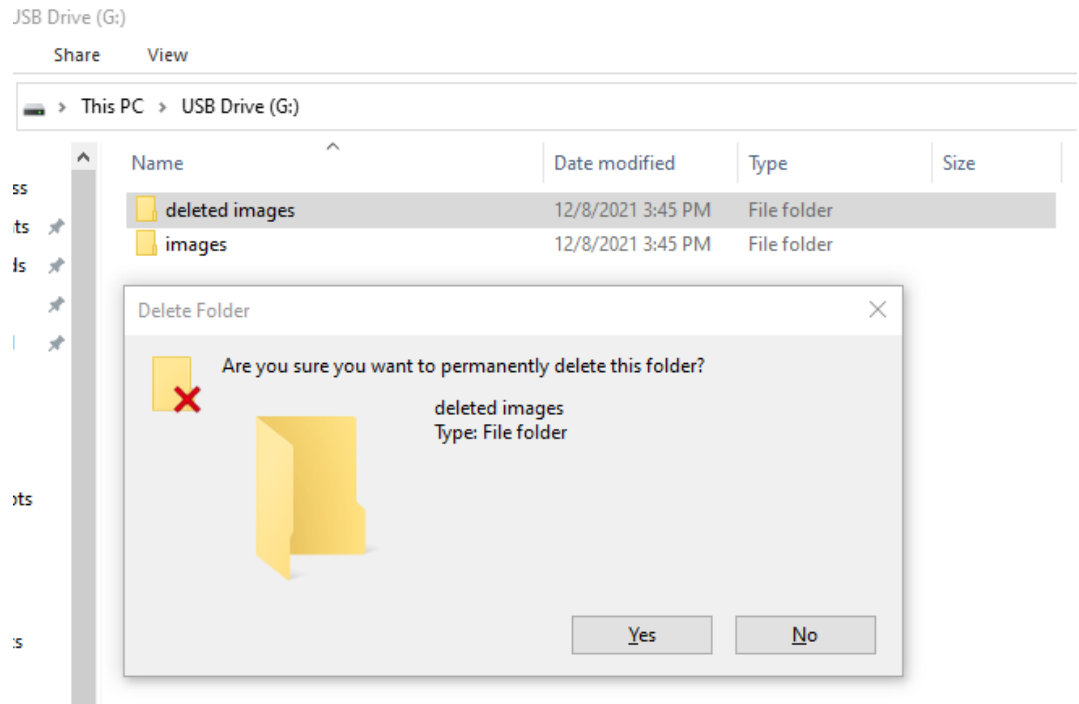
Kelompok kami menggunakan media *Flashdisk* berukuran 4GB sebagai sarana untuk menyimpan dataset yang telah di siapkan sebelumnya. Lalu pada saat persiapan uji coba imaging, kami memilih Destination Image dengan tipe SMART.

B. Langkah Pengerjaan

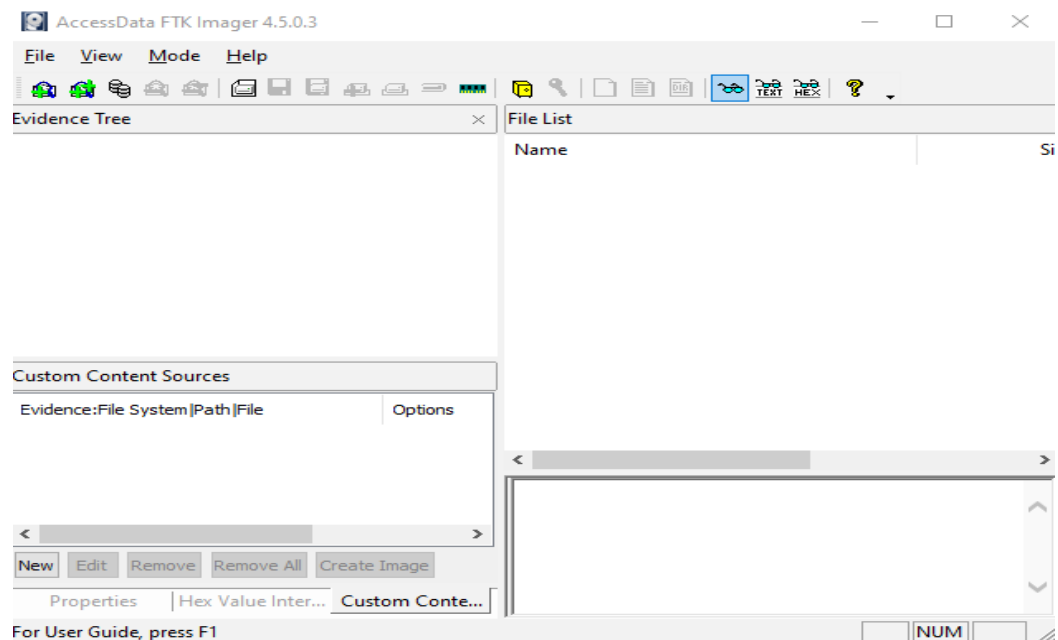
1. Pertama kelompok kami mengunduh dataset dari link google drive pada tautan <https://drive.google.com/drive/folders/1dqsLEOOhEhesHHOIWATc1ohdD-Cm5NW?usp=sharing>.
2. Kedua kelompok kami mensalin dataset ke dalam *Flashdisk* yang telah di siapkan sebelumnya



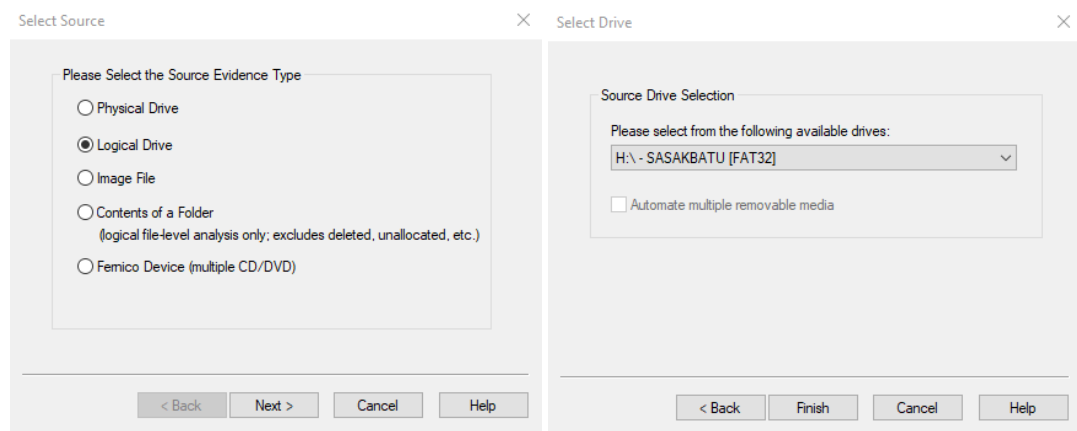
3. Lalu kelompok kami menghapus folder 'Deleted Images' pada dataset yang telah di salin ke *Flashdisk* sebelumnya.



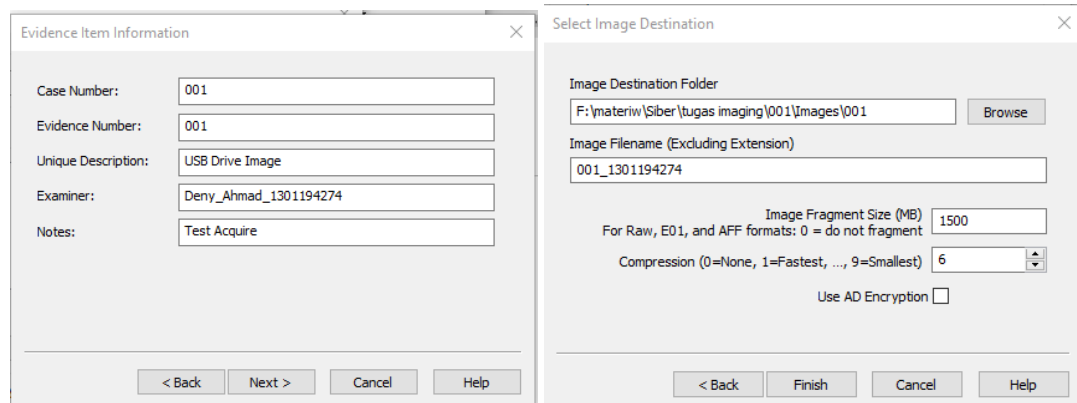
4. Setelah menghapus folder 'Deleted Images' kami menyiapkan tools yang telah di siapkan sebelumnya, yaitu *FTK Imager*



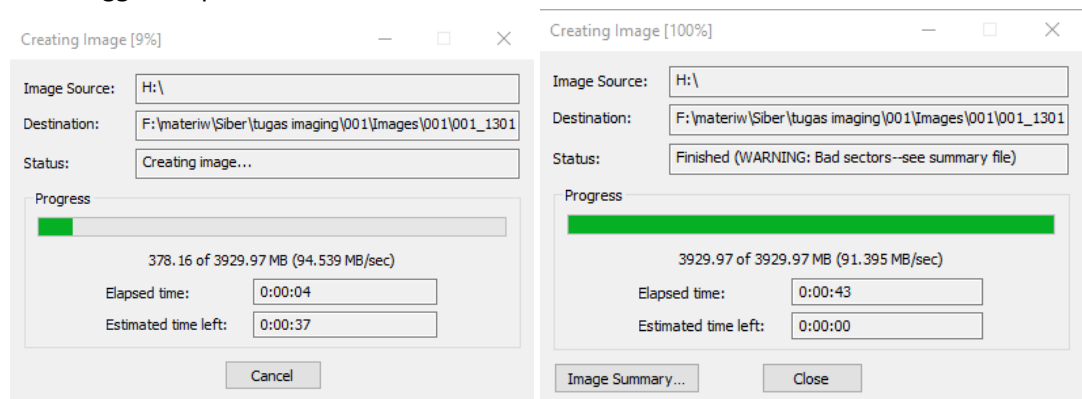
5. Lalu buka pada bagian tab File > Create Disk Image > Logical Drive > Nama *Flashdisk* > Finish



6. Lalu pilih pada bagian selanjutnya 'add' lalu isi sesuai dengan instruksi pada soal lalu setelah semua terisi maka klik 'Finish'



7. Setelah tahap – tahap di atas sudah di lakukan maka klik 'start' untuk memulai program dan tunggu sampai selesai



- Setelah program selesai maka kita lihat pada folder tujuan, apabila sudah ada file maka sukses

are View

This PC > Data (F:) > materiw > Siber > tugas imaging > 001 > Images > 001

Name	Date modified	Type	Size
001_1301194274	12/10/2021 10:47 PM	SMART Format	107,995 KB
001_1301194274.s01	12/10/2021 10:47 PM	CSV File	101 KB
001_1301194274.s01	12/10/2021 10:47 PM	Text Document	2 KB

C. Report / Hasil Uji Coba

- Open and explain the content of 001 folder

are View

This PC > Data (F:) > materiw > Siber > tugas imaging > 001 > Images > 001

Name	Date modified	Type	Size
001_1301194274	12/10/2021 10:47 PM	SMART Format	107,995 KB
001_1301194274.s01	12/10/2021 10:47 PM	CSV File	101 KB
001_1301194274.s01	12/10/2021 10:47 PM	Text Document	2 KB

- Open and explain the content of the text document

001_1301194274.s01 - Notepad

File Edit Format View Help

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 001
Evidence Number: 001
Unique description: USB Drive Image
Examiner: Deny_Sofyan_1301194274
Notes: Test Acquire

Information for F:\materi\w\Siber\tugas imaging\001\Images\001\001_1301194274:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Logical
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 8,048,565
[Physical Drive Information]
Removable drive: False
Source data size: 3929 MB
Sector count: 8048565

Isi dari text document adalah berisi info umum seperti di atas

Dan informasi berupa hasil hashing seperti di bawah

Image Information:

Acquisition started: Fri Dec 10 23:09:45 2021

Acquisition finished: Fri Dec 10 23:15:10 2021

Segment list:

F:\materiw\Siber\tugas imaging\001\Images\001\001_1301194274.s01

Image Verification Results:

Verification started: Fri Dec 10 23:15:10 2021

Verification finished: Fri Dec 10 23:15:35 2021

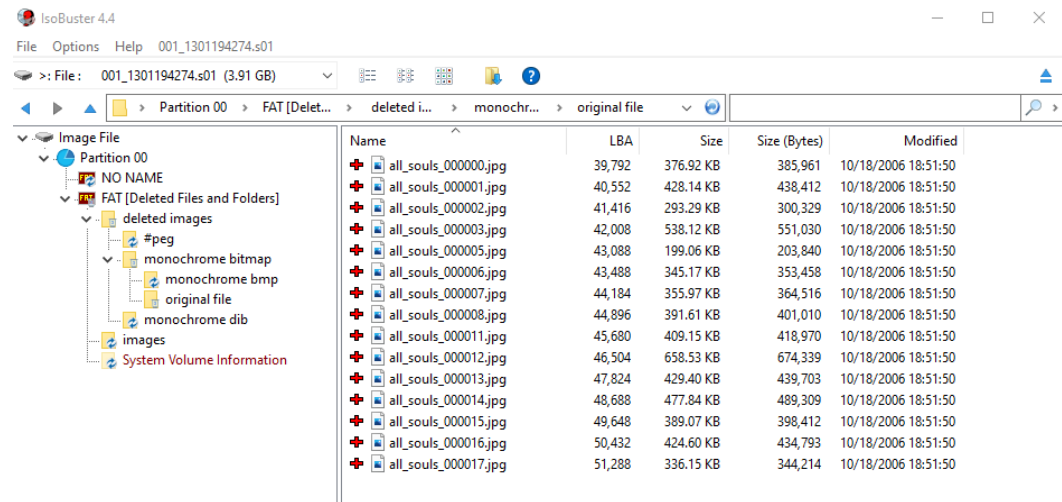
MD5 checksum: fed0b4e8979912e9bde7d0b3e01fd6de : verified

SHA1 checksum: 37d6ed73449fe5e3038f616e3b8b2038e82d688f : verified

Didalamnya tertulis bahwa program men cek checksum megggunakan metode MD5 dan SHA1 dan keduanya verified artinya tidak ada file yang terlewati atau berbeda

3. Can FTK Imager recover all files in the deleted folder?

Bisa, Hal ini dibuktikan dengan kita membuka file disk image bertipe smart dari FTK lalu kita cek di dalamnya apakah ada file yang tadinya di hapus muncul kembali apa tidak, dan di pecobaan kali ini FTK dapat merecovery file yang telah di hapus sebelumnya



4. Write your findings in your report document

Yang kelompok kami temukan pada kegiatan imaging ini adalah bagaimana sebuah file yang telah di hapus terutama gambar dapat di recovery / dikembalikan, dan hal tersebut sesuai dengan materi pada kuliah kami yakni Cyber Security pada bagian Forensik pada kejahatan dan para pelaku kejahatan tidak akan bisa menghapus data apapun pada device mereka, karena nyatanya file juga masih ada 'sampah' nya dan tidak akan hilang kecuali di 'burn'