

# **LAPORAN PRAKTIKUM**

## **FTK IMAGER**



Oleh:

Nama : L Hafidl Alkhair  
Nim : 2023903430060  
Kelas : TRKJ 2C  
Jurusan : Teknologi Informasi dan Komputer  
Progam Studi : Teknologi Rekayasa Komputer dan Jaringan  
Dosem Pengampu : Umri Erdiansyah, S.Kom., M.Kom

**PROGRAM STUDI TEKNOLOGI REKAYASA KOMPUTER JARINGAN**  
**JURUSAN TEKNOLOGI INFORMASI DAN KOMPUTER**  
**POLITEKNIK NEGERI LHOKSEUMAWE**

**2025**

## LEMBAR PENGESAHAN

No. Praktikum : 01 /TIK/TRKJ-2C/ Analis Forensik Pertahanan Cyber  
Judul : Laporan Praktikum FTK Imager  
Nama : L Hafidl Alkhair  
Nim : 2023903430060  
Kelas : TRKJ 2C  
Jurusan : Teknologi Informasi Dann Komputer  
Program Studi : Teknologi Rekayasa Komputer Jaringan  
Tanggal Praktikum : 20 Maret 2025  
Tanggal Penyerahan : 11 April 2025

Buketrata, 10 April 2025

Dosen Pembimbing,

**Umri Erdiansyah, S.Kom., M.Kom**

NIP. 199010132022031003

## DAFTAR ISI

LEMBAR PENGESAHAN .....	i
DAFTAR ISI.....	ii
BAB I.....	1
A.    Tujuan Praktikum .....	1
B.    Dasar teori .....	1
C.    Alat yang Diperlukan .....	1
BAB II.....	2
A.    Kegiatan Praktikum .....	2
BAB III .....	15
A.    Kesimpulan .....	15

# **BAB I**

## **PENDAHULUAN**

### **A. Tujuan Praktikum**

Diharapkan setelah praktikum ini mahasiswa dapat:

1. Mengetahui cara menggunakan FTK Imager untuk akuisisi data digital.
2. Memahami proses membuat image file dari media penyimpanan sebagai bukti digital.
3. Mempelajari teknik verifikasi dan dokumentasi hasil akuisisi data menggunakan FTK Imager.

### **B. Dasar teori**

Digital forensik adalah ilmu forensik yang fokus pada pengumpulan dan analisis data dari perangkat digital. Proses ini harus dilakukan dengan hati-hati agar data asli tetap utuh dan bisa digunakan sebagai bukti sah kalau dibutuhkan dalam proses hukum.

FTK Imager adalah sebuah tool yang digunakan untuk meng-akuisisi atau melakukan imaging suatu file, direktori, partisi atau physical disk untuk keperluan forensik. Dengan menggunakan FTK Imager, data yang diakuisisi akan terjamin keasliannya.

### **C. Alat yang Diperlukan**

Peralatan yang diperlukan adalah:

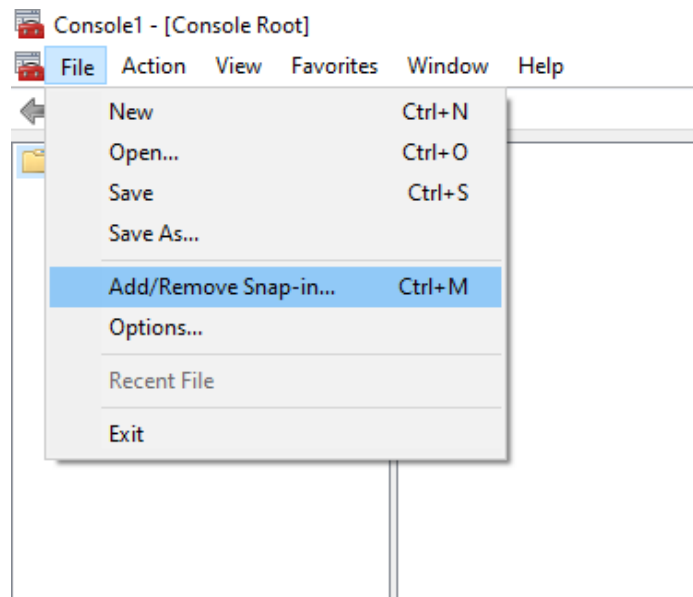
- Laptop/PC
- Flashdisk
- FTK Imager

## BAB II

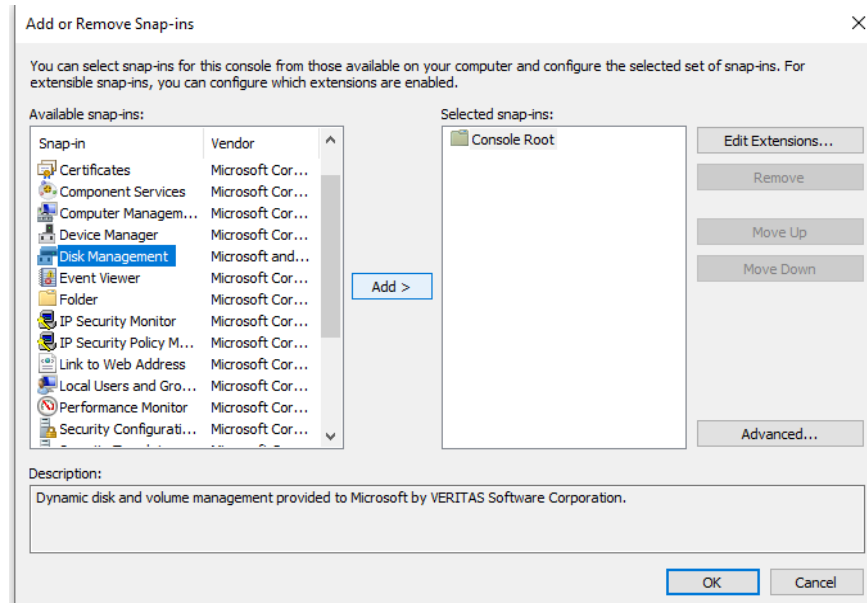
### PEMBAHASAN

#### A. Kegiatan Praktikum

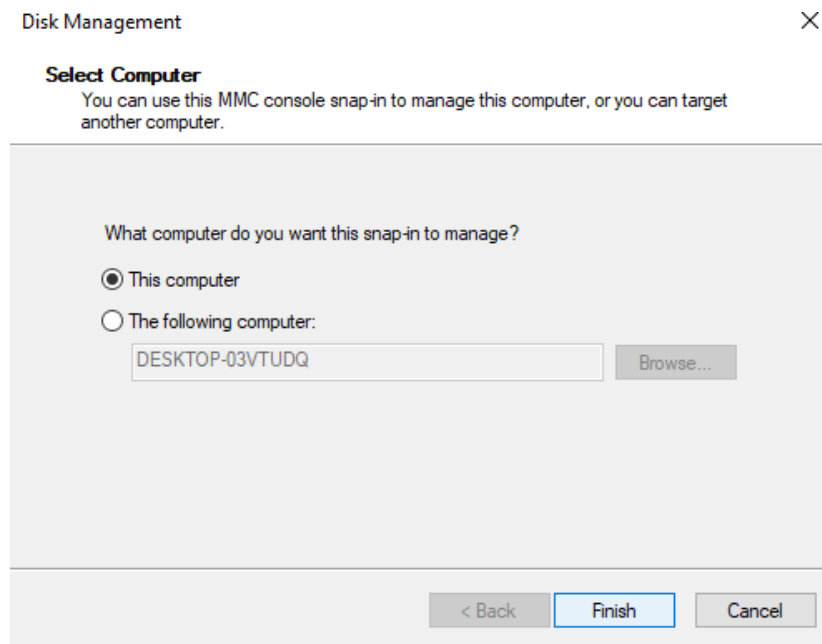
1. Pertama-tama, sambungkan flashdisk ke laptop.
2. Kemudian, klik tombol Start di pojok kiri bawah, ketik mmc pada kolom pencarian, lalu tekan Enter. MMC (Microsoft Management Console) berfungsi untuk memeriksa apakah flashdisk dikenali oleh sistem.
3. Setelah jendela MMC terbuka, klik menu File, lalu pilih opsi Add/Remove Snap-in.



4. Pada panel sebelah kiri, temukan dan pilih **Disk Management**, lalu tekan tombol **Add** yang berada di tengah layar.

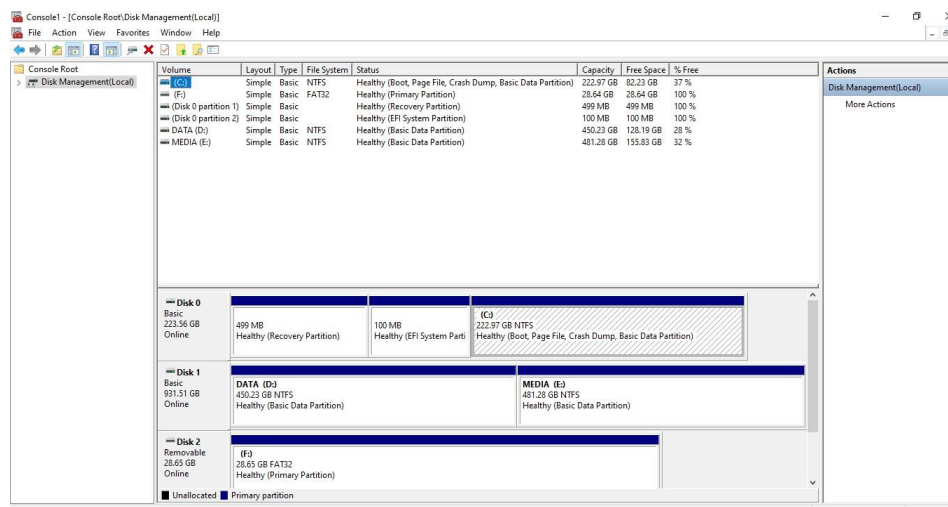


5. Setelah menekan tombol Add, akan muncul jendela baru. Pilih opsi This Computer karena kita ingin menampilkan isi disk pada komputer yang sedang digunakan. Selanjutnya, klik Finish, lalu tekan OK.



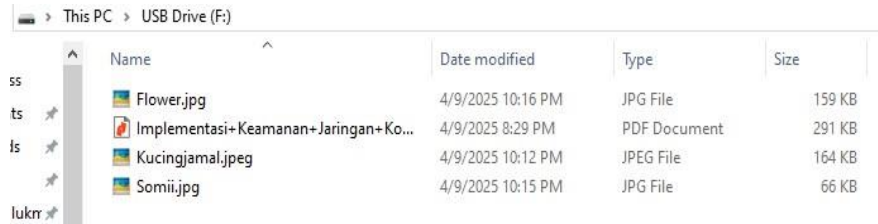
6. Berikutnya, kita akan melihat tampilan Disk Management yang menampilkan beberapa informasi, seperti:

- Disk yang sedang terhubung (misalnya Disk 0, Disk 1, dan sebagainya).
- Partisi yang tersedia, seperti drive C: (lokasi instalasi Windows), D:, atau bahkan flashdisk.
- Detail mengenai ukuran, status, serta nama dari masing-masing partisi.



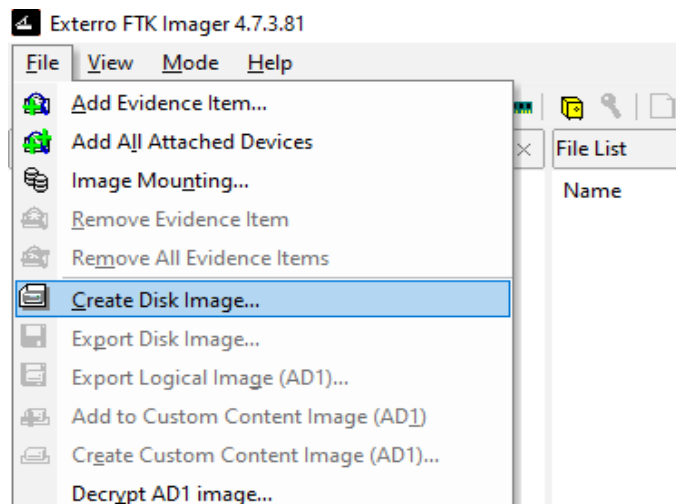
7. Langkah ini bertujuan untuk memastikan bahwa flashdisk telah terdeteksi dengan baik oleh sistem. Ini merupakan tahap pemeriksaan awal sebelum memulai proses imaging menggunakan FTK Imager.

8. Periksa isi flashdisk terlebih dahulu untuk memastikan bahwa file yang akan dianalisis secara forensik memang ada di dalamnya.



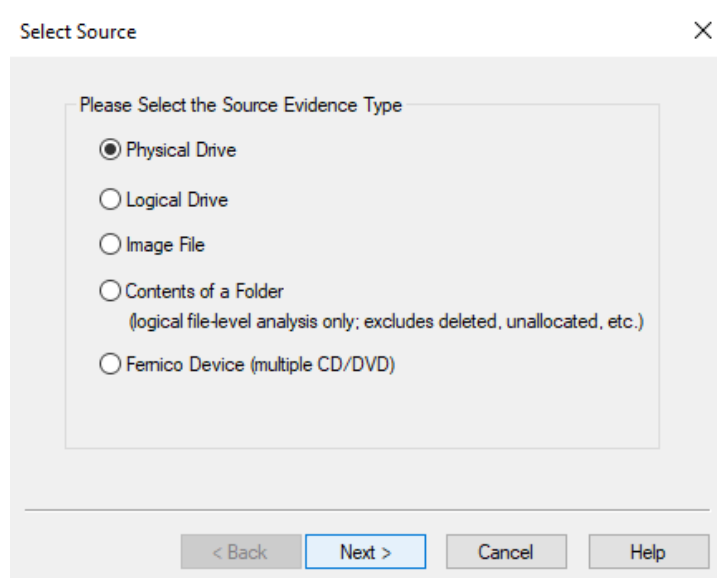
Name	Date modified	Type	Size
Flower.jpg	4/9/2025 10:16 PM	JPG File	159 KB
Implementasi+Keamanan+Jaringan+Ko...	4/9/2025 8:29 PM	PDF Document	291 KB
Kucingjamal.jpeg	4/9/2025 10:12 PM	JPEG File	164 KB
Sonii.jpg	4/9/2025 10:15 PM	JPG File	66 KB

9. Buka aplikasi FTK Imager, kemudian klik File > Create Disk Image. Langkah ini digunakan untuk membuat salinan (image) dari media penyimpanan seperti flashdisk.



10. Pilih jenis data yang akan di-image. Karena ingin menyalin seluruh isi flashdisk, pilih opsi **Physical Drive**, lalu klik **Next**.

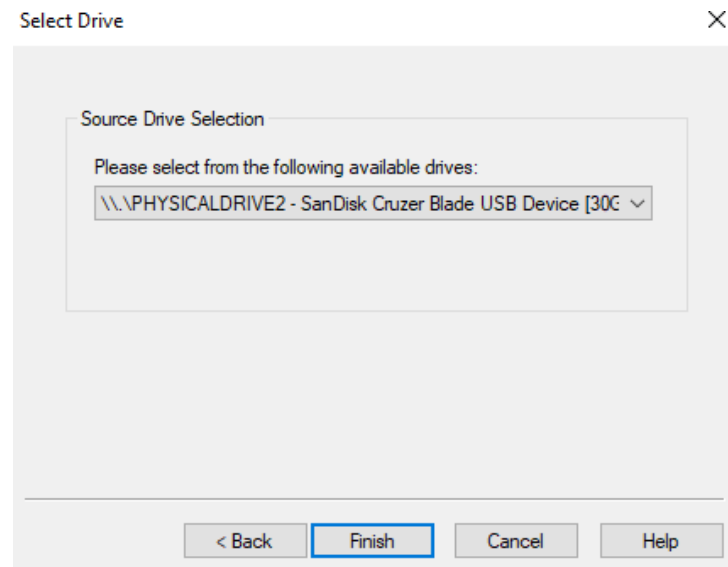




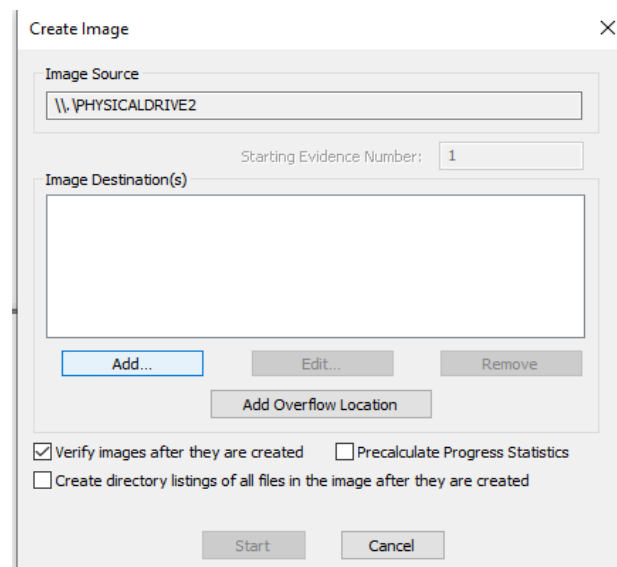
Penjelasan jenis opsi image:

- **Physical Drive:** Menyalin seluruh data dari perangkat, termasuk ruang kosong dan file tersembunyi.
- **Logical Drive:** Hanya menyalin partisi yang terlihat (seperti di File Explorer).
- **Image File:** Digunakan bila sudah memiliki image sebelumnya dan ingin menyalin ulang.
- **Content of a Folder:** Menyalin hanya isi dari satu folder.
- **Femico Device:** Untuk media CD/DVD.

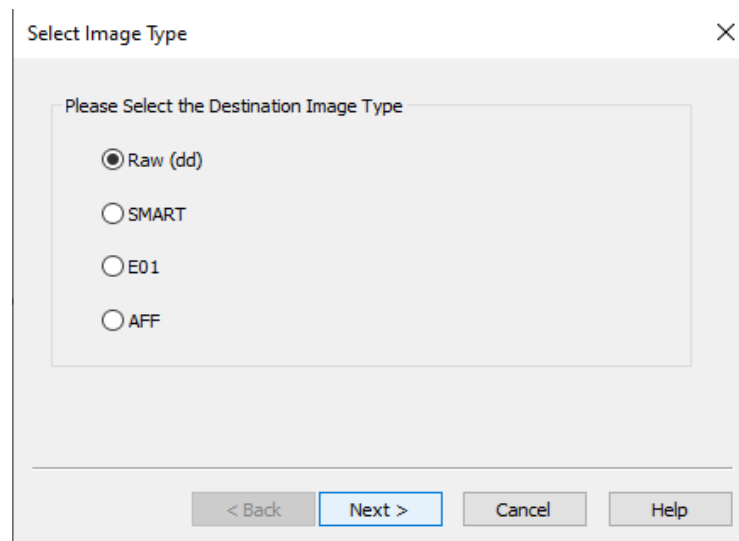
11. Setelah itu, FTK Imager akan menampilkan daftar seluruh perangkat penyimpanan yang terhubung ke komputer. Pilih flashdisk yang dimaksud, lalu klik Finish.



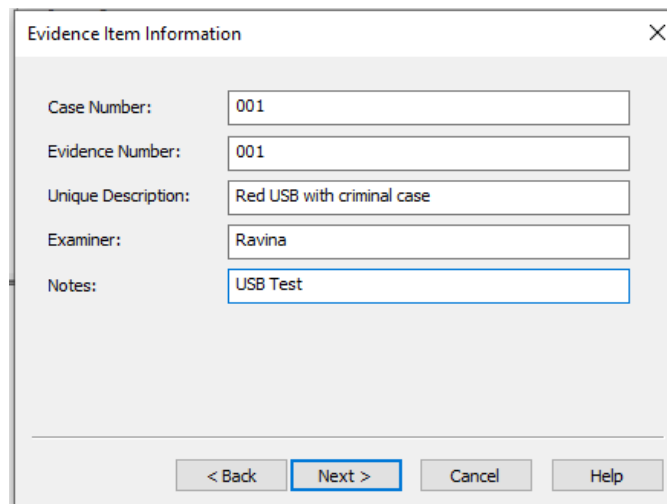
12. Pada jendela Create Image, klik tombol Add untuk menentukan lokasi penyimpanan file hasil image.



13. Isi informasi kasus pada bagian berikutnya. Ini penting untuk dokumentasi dan pelacakan yang akurat serta profesional. Setelah mengisi semua detail, lanjutkan dengan klik Next.

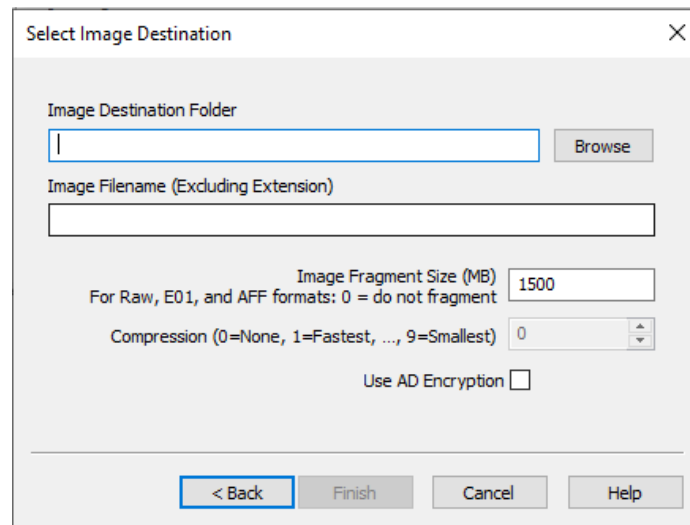


A dialog box titled "Select Image Type" with a close button (X) in the top right corner. The main area contains the text "Please Select the Destination Image Type" followed by four radio button options: "Raw (dd)" (selected), "SMART", "E01", and "AFF". At the bottom, there are four buttons: "< Back", "Next >" (highlighted with a blue border), "Cancel", and "Help".

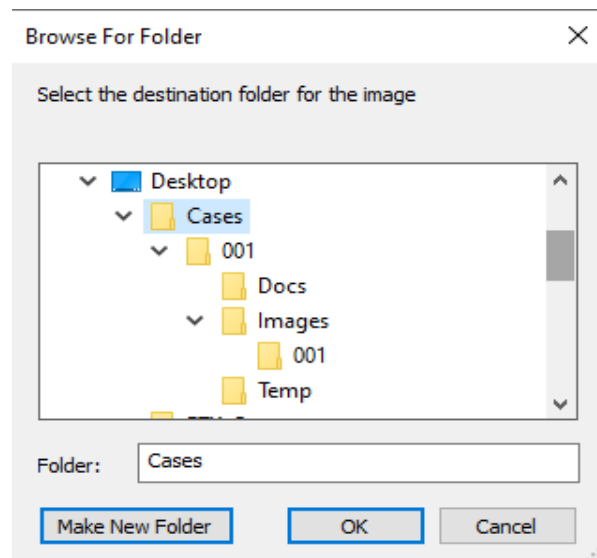


A dialog box titled "Evidence Item Information" with a close button (X) in the top right corner. It contains five text input fields with labels to their left: "Case Number:" (value: 001), "Evidence Number:" (value: 001), "Unique Description:" (value: Red USB with criminal case), "Examiner:" (value: Ravina), and "Notes:" (value: USB Test). At the bottom, there are four buttons: "< Back", "Next >" (highlighted with a blue border), "Cancel", and "Help".

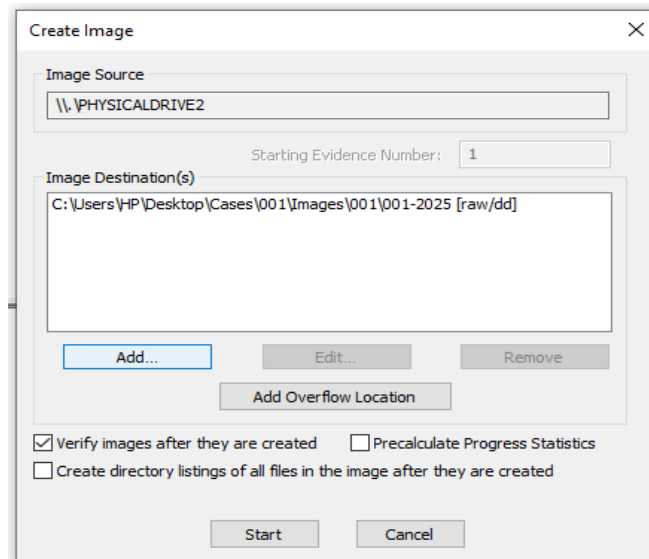
14. Klik tombol Browse untuk memilih direktori penyimpanan file image.



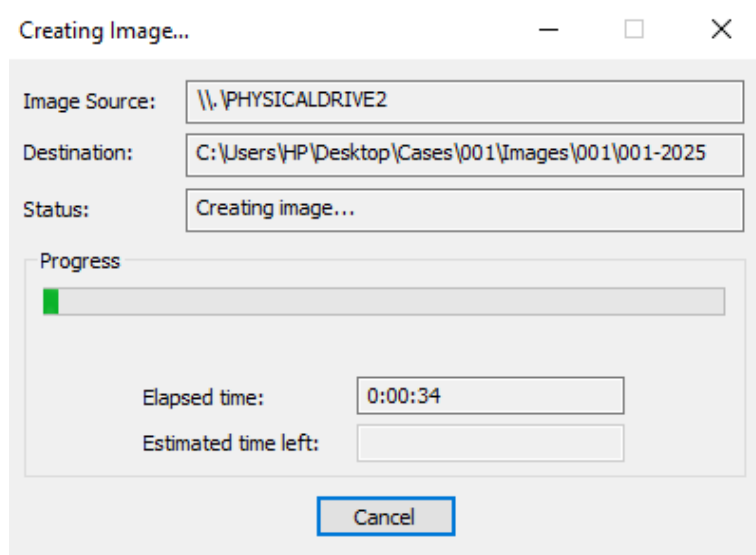
15. Tentukan lokasi penyimpanan file. Dalam contoh ini: Desktop > cases > 001 > docs (untuk dokumentasi) > images (untuk file image) > temporary working space. Pilih folder 001 di dalam folder images, lalu klik OK.



16. Pada kolom Image Filename (Excluding Extension), masukkan nama file image. Misalnya: 001-2025, lalu klik Finish.
17. Setelah klik Finish, kamu akan kembali ke halaman awal Create Image, dan tujuan penyimpanan file akan muncul di bagian bawah (Image Destination). Klik Start untuk memulai proses.

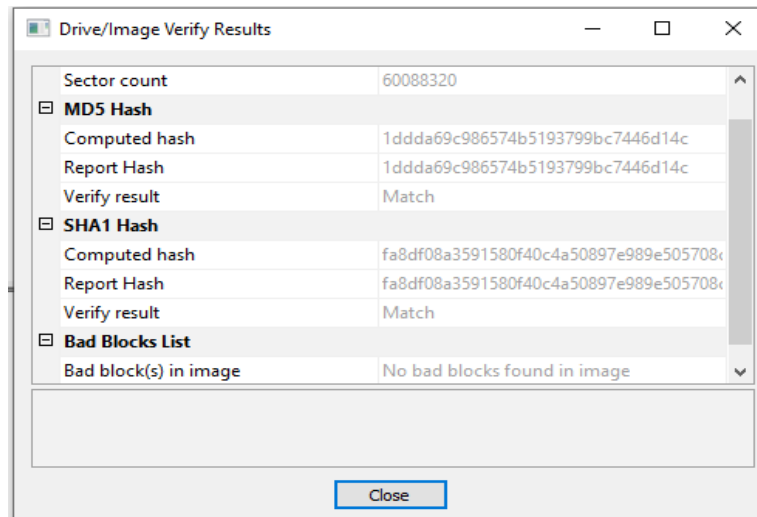


18. Proses penyalinan data dari flashdisk ke file image dimulai. Semua data akan disalin untuk dianalisis nantinya.























19. Setelah selesai, FTK Imager secara otomatis melakukan verifikasi terhadap file image menggunakan proses hashing.

Pada gambar diatas, ada dua jenis hash yang ditampilkan:



- MD5 dan SHA1 hash digunakan untuk memastikan data yang diambil identik dengan aslinya.
- Jika Computed Hash = Report Hash dan statusnya Match, maka data dipastikan tidak mengalami perubahan.
- Informasi tambahan seperti No bad blocks found menunjukkan bahwa tidak ada kerusakan sektor pada flashdisk saat proses penyalinan.
- File image seperti 001-2025.001, 001-2025.002, 001-2025.003 merupakan segmented image, yaitu hasil image yang dibagi ke beberapa bagian agar lebih mudah disimpan atau dipindahkan jika ukurannya besar.
- Tersedia juga file 001-2025.001.txt yang berisi log lengkap proses akuisisi.
- Banyaknya file tergantung dari ukuran USB, dalam contoh ini sekitar 29GB.

20. Isi File Log (.txt) dari FTK Imager dibuat otomatis setelah proses akuisisi, berisi detail seperti:

 001-2025.001	4/10/2025 2:57 AM	WinRAR archive	1,536,000 KB
 001-2025.001.txt	4/10/2025 3:21 AM	Text Document	3 KB
 001-2025.002	4/10/2025 2:59 AM	002 File	1,536,000 KB
 001-2025.003	4/10/2025 3:00 AM	003 File	1,536,000 KB
 001-2025.004	4/10/2025 3:01 AM	004 File	1,536,000 KB
 001-2025.005	4/10/2025 3:02 AM	005 File	1,536,000 KB
 001-2025.006	4/10/2025 3:03 AM	006 File	1,536,000 KB
 001-2025.007	4/10/2025 3:05 AM	007 File	1,536,000 KB
 001-2025.008	4/10/2025 3:06 AM	008 File	1,536,000 KB
 001-2025.009	4/10/2025 3:07 AM	009 File	1,536,000 KB
 001-2025.010	4/10/2025 3:08 AM	010 File	1,536,000 KB
 001-2025.011	4/10/2025 3:09 AM	011 File	1,536,000 KB
 001-2025.012	4/10/2025 3:10 AM	012 File	1,536,000 KB
 001-2025.013	4/10/2025 3:11 AM	013 File	1,536,000 KB
 001-2025.014	4/10/2025 3:13 AM	014 File	1,536,000 KB
 001-2025.015	4/10/2025 3:14 AM	015 File	1,536,000 KB
 001-2025.016	4/10/2025 3:15 AM	016 File	1,536,000 KB
 001-2025.017	4/10/2025 3:16 AM	017 File	1,536,000 KB
 001-2025.018	4/10/2025 3:17 AM	018 File	1,536,000 KB
 001-2025.019	4/10/2025 3:18 AM	019 File	1,536,000 KB

001-2024.001.txt - Notepad  
File Edit Format View Help  
Created By AccessData® FTK® Imager 3.1.2.0

Case Information:  
Acquired using: ADI3.1.2.0  
Case Number: 001  
Evidence Number: 001  
Unique description: Gold USB with black case and red LED  
Examiner: Hafidl  
Notes: Test

-----

Information for C:\Users\HP\Documents\Case\001\images\001-2024:

Physical Evidentiary Item (Source) Information:  
[Device Info]  
Source Type: Physical  
[Drive Geometry]  
Cylinders: 972  
Tracks per Cylinder: 255  
Sectors per Track: 63  
Bytes per Sector: 512  
Sector Count: 15,630,336  
[Physical Drive Information]  
Drive Model: SanDisk Cruzer Blade USB Device  
Drive Serial Number: 03020022031921210234  
Drive Interface Type: USB  
Removable drive: True  
Source data size: 7632 MB  
Sector count: 15630336  
[Computed Hashes]  
MD5 checksum: 227ec9bcd6351de7dcbeb131273d2582  
SHA1 checksum: 68a007b0490ec0e1ef30f99185355985848f931e

Image Information:  
Acquisition started: Fri Apr 11 17:18:36 2025  
<

- Informasi kasus dan barang bukti:
  - Case Number: 001
  - Evidence Number: 001
  - Deskripsi: Red USB with criminal case
  - Diperiksa oleh: Hafidl
- Detail teknis perangkat USB:
  - Model: Sandisk Cruzer Blade



- Kapasitas:  $\pm 29.3$  GB
- Tipe: Removable USB
- Serial Number: Unik untuk tiap perangkat
- Hashing:
  - Hash MD5 dan SHA1 digunakan untuk menjamin keaslian data
  - Akan diverifikasi ulang saat proses analisis untuk memastikan integritas data

### **BAB III**

#### **PENUTUP**

##### **A. Kesimpulan**

Dari praktikum ini dapat disimpulkan bahwa proses menyalin data dari flashdisk menggunakan FTK Imager berjalan dengan baik dan sukses. Seluruh data yang ada di flashdisk berhasil disalin tanpa mengalami perubahan apa pun, yang dibuktikan dengan hasil verifikasi hash yang menunjukkan kecocokan. Melalui praktikum ini, saya memperoleh pemahaman yang lebih mendalam tentang bagaimana proses akuisisi data digital dilakukan secara aman, terstruktur, dan dapat dipertanggungjawabkan. Tahapan ini sangat krusial karena merupakan fondasi awal sebelum data dianalisis lebih lanjut.