FTK Imager দিয়ে Image নেওয়ার পূর্ণ প্রসেস

🧱 ১. Full Physical Disk Imaging (পূর্ণ হার্ডডিস্ক ইমেজিং)

👉 **উদ্দেশ্য:** সম্পূর্ণ হার্ডডিস্কের প্রতিটি বিট/সেক্টর কপি করে একটি ফোরেনসিক ইমেজ তৈরি করা।

☑ ধাপসমূহ:

1. **FTK Imager চালু করুন।**
2. উপরে থেকে ➕ `File > Create Disk Image` এ ক্লিক করুন।
3. **Select Source Type:**
   - `Physical Drive` নির্বাচন করুন এবং `Next` চাপুন।
4. **Drive নির্বাচন:**
   - আপনার হার্ডডিস্ক (যেমন 0 - \.\PHYSICALDRIVE0) নির্বাচন করুন।
5. `Finish` চাপুন।
6. এবার **Destination image type** নির্বাচন করুন:
   - `Raw (dd)` / `E01` / `SMART` (সাধারণত `E01` নিরাপদ ও compress করা হয়)
7. **Evidence Item Information** পূরণ করতে বলবে – চাইলে Skip করুন বা Name, Case Number দিন।
8. **Destination Path** সেট করুন (কোথায় ইমেজ ফাইলটি সেভ করবেন):
   - Location দিন (যেমন: D:\FTK_Images\disk_image.E01)
   - Fragment size (Default রাখুন বা 1500 MB দিতে পারেন)
9. `Finish` চাপুন।
10. ইমেজিং শুরু হবে এবং Status দেখাবে।

💿 ২. Logical Drive Imaging (C:, D:, E:\ - এসব আলাদা ড্রাইভের ইমেজ)

👉 **উদ্দেশ্য:** হার্ডডিস্কের ভিতরের এক বা একাধিক পার্টিশনের ইমেজ তৈরি করা।

☑ ধাপসমূহ:

1. **FTK Imager চালু করুন।**
2. ➕ `File > Create Disk Image` এ ক্লিক করুন।
3. **Select Source Type:**
   - `Logical Drive` নির্বাচন করুন > `Next`
4. আপনি যে Drive/Image নিতে চান (C:, D:, E: ইত্যাদি), সেগুলো টিক চিহ্ন দিন।
   - একাধিক Drive একসাথে নির্বাচন করা যাবে।
5. `Finish` চাপুন।
6. এবার `Add` ক্লিক করে:
   - Image Type: `Raw (dd)` বা `E01` নির্বাচন করুন

- Destination Path দিন (যেমন: D:\FTK_Images\logical_image.E01)

7. `Finish` চাপুন।
8. এবার `Start` দিলে, সব নির্ধারিত Logical Drive একসাথে Image তৈরি হবে।

⚖️ তুলনামূলক পার্থক্য

বৈশিষ্ট্য	Full Physical Imaging	Logical Drive Imaging
Target	সম্পূর্ণ হার্ডডিস্ক	নির্দিষ্ট Drive (C:, D:)
System Files	Hidden + Deleted files সহ	শুধু দৃশ্যমান drive content
Time & Size	বেশি সময় ও স্পেস প্রয়োজন	তুলনামূলক কম
Forensics Level	Highest integrity for evidence	শুধু কার্যকর ডেটা বিশ্লেষণের জন্য

🔍 Live vs Dead Imaging

কনসেপ্ট	Live Imaging	Dead Imaging
অবস্থান	চলমান System থেকে Image নেওয়া	সিস্টেম Shutdown করে Image নেওয়া
সম্ভাবনা	Memory Capture সম্ভব (RAM Dump সহ)	Memory capture সম্ভব না
ঝুঁকি	পরিবর্তনের সম্ভাবনা থাকে (Logs, Temp)	খুব নিরাপদ ও নির্ভরযোগ্য
ব্যবহার	Incident Response সময়	ফরেনসিক তদন্তে বেশি ব্যবহৃত