İmaj Alma Toolları

DD Tool ile İmaj Alma

- `/dd.exe -list` : Takılı diskleri listeler
- `/dd.exe if=<source_drive> of=<full_copy_name> bs=512` : Disk kopyası almak için
- `/dx.exe if=<full_copy_name> of=<source_drive> bs=512` : HDD'yi yedekten geri yüklemek için kullanılır.

`dd` Ne Yapar?

- Bir disk ya da disk bölgesinin **birebir kopyasını** alır (`bit-level imaging`).
- Verileri **analiz etmez**, sadece **aktarır**.

Seçenekler

- bs=block size
- count=NUM(NUM ile belirtilen sayıda bloğu kopyalar)
- skip=NUM(NUM ile belirtilen sayıda bloğu atla)
- conv=noerror,sync(Okuma hatası olduğunda işlemi sonlandırma,devam et.)

> Örnek: `dd if=\\.\f: of=C:\deneme image\image.001 bs=512 count=700 conv=noerror,sync`

–cryptsum **<hashtype>** (Hash Değeri md5, sha, sha1,sha256)
–verify (Veri Bütünlük doğrulama)
–cryptout **<file>** (hash değerini dosyaya yaz)
–log **<file>** (log kayıtlarını dosyaya yaz)
–localwrt (yerel sürücülere yazmaya izin ver)
–ata_hpa (HPA(Host Protected Area)'yı geçici olarak devre dışı bırak)

Örnek:
dd if=\\.\f: of=C:\Users\vfv\Desktop\deneme image\image.001 bs=512 –cryptsum md5 –verify –cryptout C:\Users\vfv\Desktop\deneme image\hash.txt –localwrt

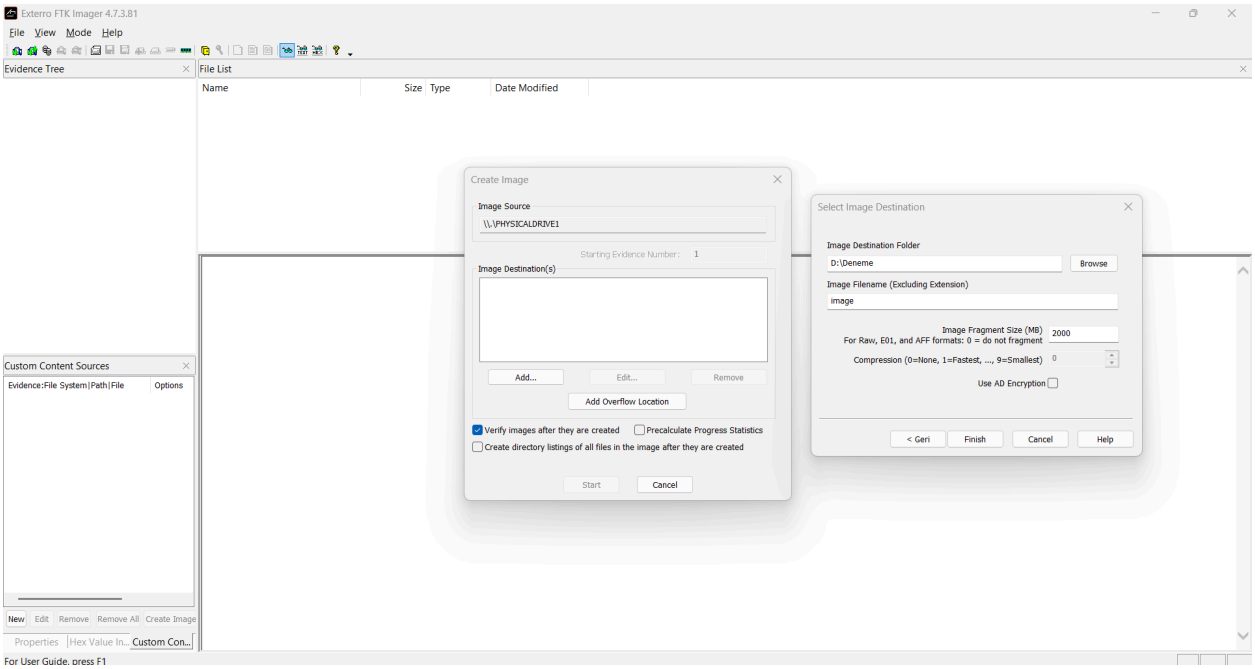
- Örneğin: `/dev/sda1`'i `backup.img` olarak yedekler.
- Disk imajı alıp inceleme yaparken (adli bilişim)
- Sistem taşıma işlemleri (clone) için

FTK Imager

> Resmi siteden program indilir ve kurulur.Ardından ***Program Files→AccessData→FTK Imager*** dosyasını kopyalayıp bir USB belleği yapıştırılması gerekir.

Kullanım Alanı	Açıklama
📦 **Disk imajı alma**	Fiziksel disk, bölüm, USB, CD/DVD gibi aygıtların bit seviyesinde kopyası alınır (E01, RAW, AFF formatlarında).
🔍 **Veri önizleme**	İmaj dosyasını açarak dosya yapısını, silinmiş dosyaları, metadata bilgilerini görebilirsin.
🗂️ **Silinmiş verileri görüntüleme**	NTFS gibi sistemlerde silinmiş ancak üzerine yazılmamış veriler okunabilir.
🧪 **Hash hesaplama**	SHA1, MD5 gibi hash algoritmalarıyla imaj dosyasının bütünlüğü doğrulanabilir.
📝 **Raporlama**	Alınan imajlar, hash değerleri ve veriler hakkında otomatik rapor oluşturabilir.
📸 **RAM görüntüsü alma (belirli sürümlerde)**	Canlı sistemlerden RAM dump alınabilir.

FTK Imager ile İmaj Oluşturma ve Açma



File→Create Image ve usb belleği seçerek image oluşturma

- ***File→Add Evidince Item*** kısmından image dosyasının olduğu dizin seçilerek image eklenebilir.
- Sol menüden örneğin bir disk seçip "**Add Custom Content Image**" butonuna tıklayıp oradan **Wildcard options** kısmında ***** dan sonra gelen kısma örneğin .jpg gibi bir uzantı yazılırsa bu imaj içinde .jpg uzantılı imajları görüntüler.

🖋Ömer Faruk Baysal