İmaj Alma Toolları ve Autopsy

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.

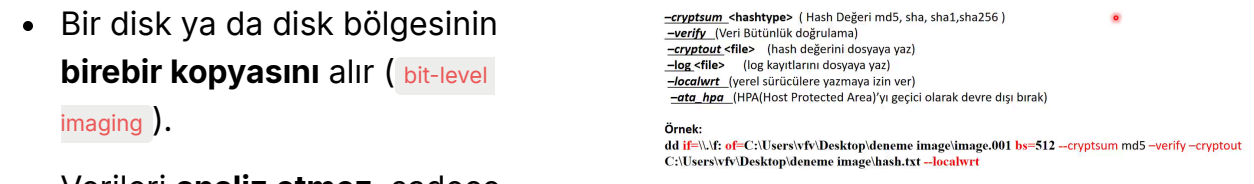
`dd` Ne Yapar?

- 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`



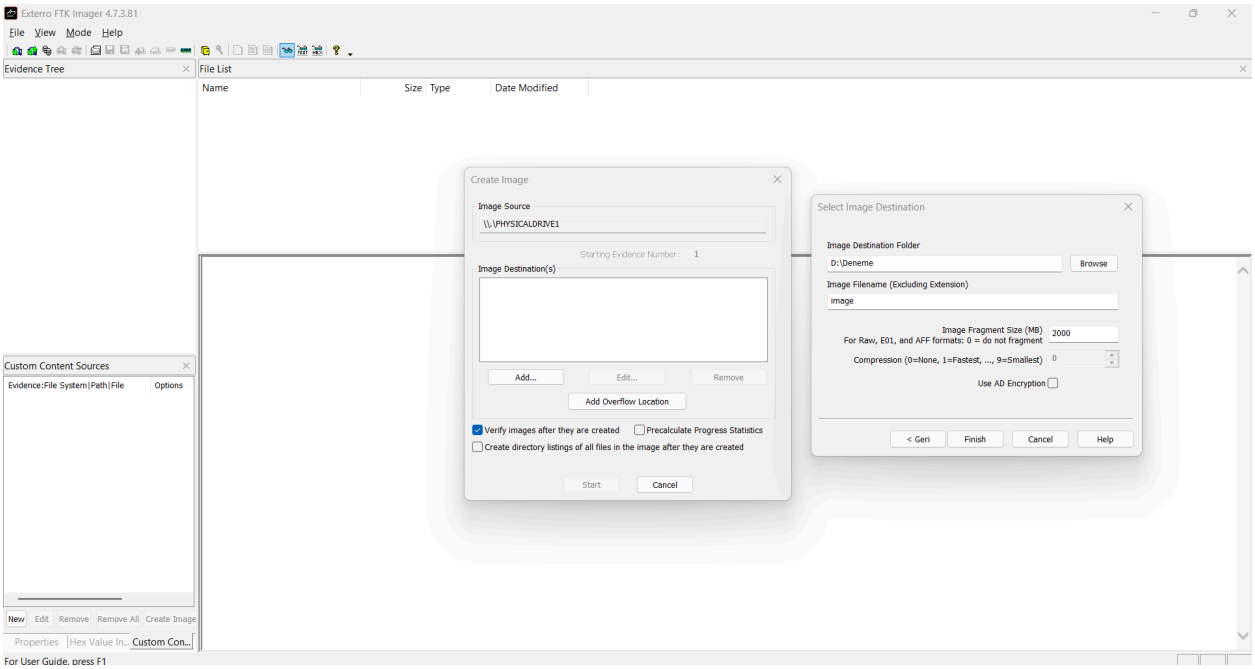
- Örneğin: `/dev/sda1`'i `backup.img` olarak yedekler.
- Disk imajı alıp inceleme yaparken (adli bilişim)
- Sistem taşıma işlemleri (clone) için

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.

Autopsy

> Autopsy, dijital delillerin toplanması, analizi ve raporlanması için kullanılan kapsamlı bir dijital adli analiz (forensic analysis) yazılımıdır.

🔍 Ne tür analizler yapar?

- Disk imajlarını analiz eder.
- Silinmiş dosyaları kurtarır.
- E-posta, tarayıcı geçmişi, çerezler gibi kullanıcı verilerini inceler.

- Zaman damgalarını (MAC times) okur.
- Chat uygulamaları, belge içerikleri, metadata'lar gibi verileri analiz eder.
- Hash eşleştirmeleriyle kötü amaçlı yazılımları veya bilinen dosyaları tanır.
- Anahtar kelime araması yapar.
- Görsel analiz ve EXIF verisi okuma sağlar.

Başlıca Invegst Modelleri

🔍 Dosya Tipi Tanımlama (File Type Identification)

- Dosyaların içeriklerine göre türünü (örneğin .jpg, .exe) belirler. Yanıltıcı dosya uzantılarını tespit etmeye yardımcı olur.

📂 Gömülü Dosyaları Ayıkla (Extract Embedded Files)

- ZIP, DOCX gibi içinde başka dosya barındıran dosyaları açar ve içeriğini çıkarır.

🧬 EXIF Metadata Parser

- Fotoğraflar gibi medya dosyalarının içindeki EXIF verilerini (konum, cihaz, tarih vb.) analiz eder.

💾 Dosya Sistemi Analizi (File System Analysis)

- Silinmiş dosyaları, zaman damgalarını, erişim izinlerini ve diğer dosya sistemi meta verilerini inceler.

🧠 Anahtar Kelime Arama (Keyword Search)

- Belirli kelimeler ya da ifadeler için otomatik metin araması yapar (örneğin "password", "confidential" gibi).

📧 E-Posta Ayıklama (Email Parser)

- E-posta istemcilerine ait dosyalardan (PST, MBOX vb.) e-postaları, ekleri ve ilgili meta verileri çıkarır.

🌐 Web Artıkları Analizi (Web Artifacts)

- Tarayıcı geçmişi, çerezler, kayıtlı şifreler gibi verileri analiz eder (özellikle Chrome, Firefox gibi tarayıcılardan).

🗃️ Hash Analizi (Hash Lookup)

- Dosya hash'lerini veritabanındaki (örneğin NSRL) bilinen iyi/kötü dosyalarla karşılaştırır.

💬 Chat / Mesajlaşma Uygulamaları Analizi

- Skype, WhatsApp gibi mesajlaşma uygulamalarının veri tabanlarını analiz eder (Autopsy eklenti ile desteklenebilir).

🔧 Dosya Ayıklama / Modül Çalıştırma (Embedded File Extractor)

- İç içe geçmiş (örneğin bir belge içindeki resim) dosyaları çıkarır ve ayrı analiz yapılmasını sağlar.

📄 Text Extraction / String Extractor

- Belgelerden ve dosyalardan metin veya metin benzeri veri parçalarını çeker (özellikle analiz için).

🕵️ Recent Activity

- Kullanıcının yakın dönemdeki etkinliklerini (açılan dosyalar, ziyaret edilen siteler vb.) raporlar.

🖋️Ömer Faruk Baysal