**Kayıp Dosyaların İzinde: Adli Bilişim Aracı Scalpel Rehberi**

Dijital dünyada veri kaybı, hepimizin korkulu rüyasıdır. Yanlışlıkla silinen bir fotoğraf albümü, formatlanmış bir hafıza kartı veya bozulmuş bir hard disk... Bu gibi durumlarda verilerin sonsuza dek kaybolduğunu düşünebilirsiniz. Ancak adli bilişim dünyasında, bu dijital enkazın içinden değerli bilgileri kurtarabilen güçlü araçlar vardır. İşte bu araçların en bilinen ve en etkililerinden biri **Scalpel**'dir.

Bu yazıda, Scalpel'ın ne olduğunu, dijital bir "neşter" gibi çalışarak verileri nasıl kurtardığını, nasıl kurulup kullanılacağını ve gerçek dünya senaryolarında nasıl harikalar yaratabildiğini adım adım inceleyeceğiz.

**1. Scalpel Aracı Nedir?**

**Scalpel**, dosya sisteminden bağımsız olarak çalışan, yüksek performanslı bir "dosya oyma" (file carving) aracıdır. Bu, onun en temel ve en güçlü özelliğidir.

Peki, "dosya oyma" ne anlama gelir? Bunu bir analoji ile açıklayalım:  
Parçalanmış bir kitap düşünün. Sayfalar tamamen dağılmış ve kitabın içindekiler kısmı (yani dosya sistemi) yok olmuş. Ancak siz, her sayfanın başında "Bölüm X" gibi bir başlık ve sayfa sonunda bir sayfa numarası olduğunu biliyorsunuz. Bu başlık ve son bilgileri (header ve footer) kullanarak, kağıt yığını içinden tek tek sayfaları bulup yeniden bir araya getirebilirsiniz.

Scalpel tam olarak bunu yapar. Bir diskin veya disk imajının içeriğini ham veri (1'ler ve 0'lar) olarak okur. Dosya sistemi (NTFS, FAT32, ext4 vb.) bozulmuş veya hiç var olmasa bile, aradığı dosya türlerine ait benzersiz başlangıç (**header**) ve bitiş (**footer**) "imzalarını" (magic numbers) arar. Bu imzaları bulduğunda, aradaki tüm veriyi yeni bir dosya olarak "oyar" ve kurtarır.

Scalpel, popüler adli bilişim aracı olan **Foremost**'un daha hızlı ve daha verimli bir versiyonu olarak geliştirilmiştir.

**2. Neden Kullanılır?**

Scalpel, birkaç kritik senaryoda hayati bir rol oynar:

* **Adli Bilişim (Digital Forensics):** Bir suç soruşturmasında, şüphelinin bilgisayarından silinmiş kanıtları (resimler, belgeler, e-postalar vb.) kurtarmak için kullanılır. Şüpheli diski formatlamış veya dosyaları silmiş olsa bile, Scalpel bu verilerin izini bulabilir.
* **Veri Kurtarma:** Yanlışlıkla formatlanmış USB bellekler, SD kartlar veya silinmiş disk bölümlerinden kişisel verileri (fotoğraflar, videolar, dokümanlar) geri getirmek için kullanılır.
* **Olay Müdahalesi (Incident Response):** Siber saldırıya uğramış bir sistemin disk veya bellek imajı üzerinde, saldırganın bıraktığı veya sildiği zararlı yazılımları, logları veya diğer araçları bulmak için kullanılır.
* **Performans:** Çoklu çekirdek desteği ve optimize edilmiş arama algoritmaları sayesinde, büyük disk imajlarını Foremost'a göre çok daha hızlı tarayabilir.

**3. Nasıl Kurulum Yapılır?**

Scalpel, çoğu Linux dağıtımının paket yöneticilerinde bulunur. Özellikle Kali Linux gibi adli bilişim ve sızma testi odaklı dağıtımlarda varsayılan olarak yüklü gelir.

**Debian/Ubuntu/Kali Linux Üzerinde Kurulum:**

Kurulum son derece basittir. Bir terminal açın ve aşağıdaki komutu çalıştırın:

Generated bash

sudo apt update

sudo apt install scalpel

**En Önemli Adım: Yapılandırma Dosyasını Düzenlemek**

Scalpel'ı kurduktan sonra hemen kullanamazsınız. Hangi tür dosyaları arayacağını ona söylemeniz gerekir. Bu ayarlar /etc/scalpel/scalpel.conf dosyasında bulunur.

1. Yapılandırma dosyasını bir metin editörü ile açın:

sudo nano /etc/scalpel/scalpel.conf

1. Dosyanın içinde, desteklenen tüm dosya türlerinin (jpg, pdf, docx, mp4 vb.) listelendiğini göreceksiniz. Ancak varsayılan olarak hepsinin başında bir diyez işareti (#) vardır, yani hepsi "yorum satırı" durumundadır ve pasiftir.
2. Kurtarmak istediğiniz dosya türlerinin başındaki # işaretini silerek onları aktif hale getirin. Örneğin, JPG ve PDF dosyalarını kurtarmak istiyorsanız, ilgili satırları şu şekilde düzenleyin:

# uncommenting the line.

#

# (e.g. "jpg y 100000 \xff\xd8\xff\xe0\x00\x10 \xff\xd9")

#

#---------------------------------------------------------------------

# GRAPHICS

#---------------------------------------------------------------------

gif y 5000000 \x47\x49\x46\x38\x37\x61 \x00\x3b

gif y 5000000 \x47\x49\x46\x38\x39\x61 \x00\x3b

# bmp y 3072000 \x42\x4d\x36\xc8\x04\x00 # A 1024x768x24bpp BMP

jpg y 20000000 \xff\xd8\xff\xe0\x00\x10\x4a\x46\x49\x46\x00\x01 \xff\xd9

# png y 300000 \x89\x50\x4e\x47\x0d\x0a\x1a\x0a \x49\x45\x4e\x44\xae\x42\x60\x82

# tif y 20000000 \x49\x49\x2a\x00 # Little-endian

# tif y 20000000 \x4d\x4d\x00\x2a # Big-endian

#...

#--------------------------------------------------------------------

# Office documents

#--------------------------------------------------------------------

# NOTE: These formats are container formats and may contain other files

# inside them.

#

# docx y 100000000 \x50\x4b\x03\x04\x14\x00\x06\x00

# ole y 100000000 \xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1

pdf y 100000000 \x25\x50\x44\x46 \x0d\x25\x25\x45\x4f\x46\x0d

pdf y 100000000 \x25\x50\x44\x46 \x0a\x25\x25\x45\x4f\x46\x0a

pdf y 100000000 \x25\x50\x44\x46 \x0d\x0a\x25\x25\x45\x4f\x46\x0d\x0a

1. Dosyayı kaydedip (CTRL+X, sonra Y ve Enter) çıkın. Artık Scalpel kullanıma hazırdır.

**4. Kullanım Parametreleri Nedir?**

Scalpel'ın temel kullanımı şu şekildedir:  
scalpel [hedef\_disk\_imajı\_veya\_aygıt] -o [çıktı\_dizini]

En sık kullanılan parametreler:

* -o <dizin>: Kurtarılan dosyaların kaydedileceği çıktı dizinini belirtir. **Bu dizin ya boş olmalı ya da hiç var olmamalıdır.** Scalpel güvenlik için dolu bir dizine yazma yapmaz.
* -c <dosya>: Varsayılan /etc/scalpel/scalpel.conf yerine özel bir yapılandırma dosyası kullanmak için.
* -v: Ayrıntılı mod (verbose). Scalpel'ın ne yaptığını adım adım ekranda gösterir.
* -h: Yardım menüsünü gösterir.
* -V: Sürüm bilgisini gösterir.

**5. Bu Aracı Etkili Kullanmanın Örnekleri**

Aşağıda, Scalpel'ın pratik ve etkili kullanımını gösteren senaryolar bulunmaktadır.

**Örnek 1: Formatlanmış SD Karttan Fotoğraf Kurtarma**

* **Senaryo:** Tatil fotoğraflarınızın olduğu bir SD kartı yanlışlıkla formatladınız.
* **Açıklama:** Bu, en yaygın veri kurtarma senaryosudur. Adli bilişimde en iyi pratik, her zaman orijinal aygıtın bir imajını (kopyasını) alıp onun üzerinde çalışmaktır. Bu, orijinal veriyi daha fazla bozma riskini ortadan kaldırır.
* **Adımlar:**
  1. SD kartın imajını alın (örneğin /dev/sdb ise):

sudo dd if=/dev/sdb of=~/sd\_kart\_imaji.dd bs=4M status=progress

* 1. scalpel.conf dosyasında jpg ve png satırlarının başındaki # işaretini kaldırın.
  2. Scalpel'ı çalıştırın:

scalpel ~/sd\_kart\_imaji.dd -o ~/kurtarilan\_fotolar

* **Sonuç:** Scalpel, imaj dosyasını tarayacak ve bulduğu tüm JPG/PNG dosyalarını ~/kurtarilan\_fotolar dizini içindeki jpg-XXX ve png-XXX klasörlerine kaydedecektir.

**Örnek 2: Adli İmajdan Silinmiş Belgeleri Bulma**

* **Senaryo:** Bir şüphelinin hard diskinin imajı (case01.E01) üzerinde çalışıyorsunuz ve silinmiş ofis belgelerini arıyorsunuz.
* **Açıklama:** Bu, tipik bir adli bilişim görevidir. Hedef, kanıt niteliği taşıyabilecek PDF, DOCX, XLSX gibi belgelerdir.
* **Adımlar:**
  1. scalpel.conf dosyasında pdf, docx, xlsx, pptx gibi ilgili ofis formatlarını aktif hale getirin.
  2. Scalpel'ı çalıştırın:

scalpel case01.E01 -o ./bulunan\_belgeler

* **Sonuç:** ./bulunan\_belgeler dizininde, bulunan her dosya türü için ayrı ayrı klasörler oluşturulur ve kurtarılan belgeler bu klasörlerin içine kaydedilir.

**Örnek 3: Sadece Belirli Bir Disk Bölümünü Tarama**

* **Senaryo:** 1 TB'lık bir diskin sadece 50 GB'lık ikinci bölümünden (/dev/sda2) veri kurtarmak istiyorsunuz. Tüm diski tarayarak zaman kaybetmek istemiyorsunuz.
* **Açıklama:** Scalpel, tüm disk aygıtı yerine belirli bir disk bölümü üzerinde de çalışabilir. **Uyarı:** Bu işlemi yapmadan önce, o bölümün sisteme bağlı (mounted) olmadığından emin olun (sudo umount /dev/sda2).
* **Adımlar:**
  1. scalpel.conf dosyasını ihtiyacınıza göre düzenleyin.
  2. Scalpel'ı doğrudan bölüm aygıtı üzerinde çalıştırın:

sudo scalpel /dev/sda2 -o /media/user/harici\_disk/kurtarma

* **Sonuç:** Scalpel, sadece /dev/sda2 bölümünü tarayarak işlemi çok daha hızlı tamamlar.

**Örnek 4: Özel Bir Dosya Türü için Kendi Kuralını Yazma**

* **Senaryo:** Standart olmayan, özel bir log dosyası (.xlog) türünü kurtarmanız gerekiyor ve bu türün dosya başlangıcının STARTLOG, bitişinin ise ENDLOG olduğunu biliyorsunuz.
* **Açıklama:** Scalpel'ın gücü, özel kurallar tanımlayabilmesinden gelir.
* **Adımlar:**
  1. scalpel.conf dosyasını açın.
  2. Dosyanın en altına kendi kuralınızı ekleyin:

xlog y 5000000 STARTLOG ENDLOG

(Burada y büyük/küçük harf duyarlı olmadığını, 5000000 ise maksimum dosya boyutunu byte olarak belirtir.)

* 1. Scalpel'ı normal şekilde çalıştırın.
* **Sonuç:** Scalpel artık standart dosya türlerinin yanı sıra, sizin tanımladığınız STARTLOG ile başlayıp ENDLOG ile biten veri bloklarını da xlog dosyası olarak kurtaracaktır.

**Örnek 5: Bellek (RAM) İmajından Veri Oyma**

* **Senaryo:** Bir siber saldırı sonrası sistemin bellek (RAM) imajını (ram\_dump.raw) aldınız. Saldırganın bellekte çalıştırdığı ama diske hiç yazmadığı bir script veya PE (exe) dosyasını bulmaya çalışıyorsunuz.
* **Açıklama:** Bellek de ham veri içerir ve Scalpel burada da çalışabilir. Bu, "fileless malware" (dosyasız zararlı yazılım) tespiti için çok değerli bir tekniktir.
* **Adımlar:**
  1. scalpel.conf dosyasında exe satırını aktif hale getirin. Gerekirse script dilleri için de kurallar ekleyebilirsiniz.
  2. Scalpel'ı bellek imajı üzerinde çalıştırın:

scalpel ram\_dump.raw -o ./bellekten\_kurtarilanlar

* **Sonuç:** Scalpel, bellek imajı içinde bir .exe dosyasının header ve footer izlerini bulursa, bu dosyayı kurtarabilir. Bu dosya, saldırının analizi için kritik bir kanıt olabilir.

**Sonuç**

Scalpel, basit bir komut satırı aracı gibi görünse de, aslında dijital dünyanın enkazından paha biçilmez verileri kurtarabilen son derece güçlü bir dijital arkeoloji aracıdır. Dosya sistemine bağımlı olmaması, hızı ve esnek yapılandırması, onu hem adli bilişim uzmanları hem de veri kaybı yaşayan son kullanıcılar için vazgeçilmez kılar. Unutmayın ki, bu tür araçlar **yalnızca yasal hakkiniz olan veriler üzerinde ve etik kurallar çerçevesinde kullanılmalıdır.** Doğru kullanıldığında Scalpel, umudun tükendiği yerde dijital hayat kurtarabilir.