**Bulk Extractor Nedir?**

Bulk Extractor, disk imajları (örneğin .dd, .img uzantılı dosyalar) veya herhangi bir dosya üzerinde hızlı ve derinlemesine dijital adli analiz yapmaya yarayan açık kaynaklı bir araçtır. Bu araç sayesinde, sistemdeki e-posta adresleri, şifrelenmemiş kredi kartı bilgileri, URL'ler, telefon numaraları gibi önemli dijital izler otomatik olarak çıkarılabilir.

Bulk Extractor, bir dosya ya da disk imajı içinde gizli, dağınık veya silinmiş verileri bulur ve listeler. Özellikle adli bilişim uzmanları tarafından kullanılır.

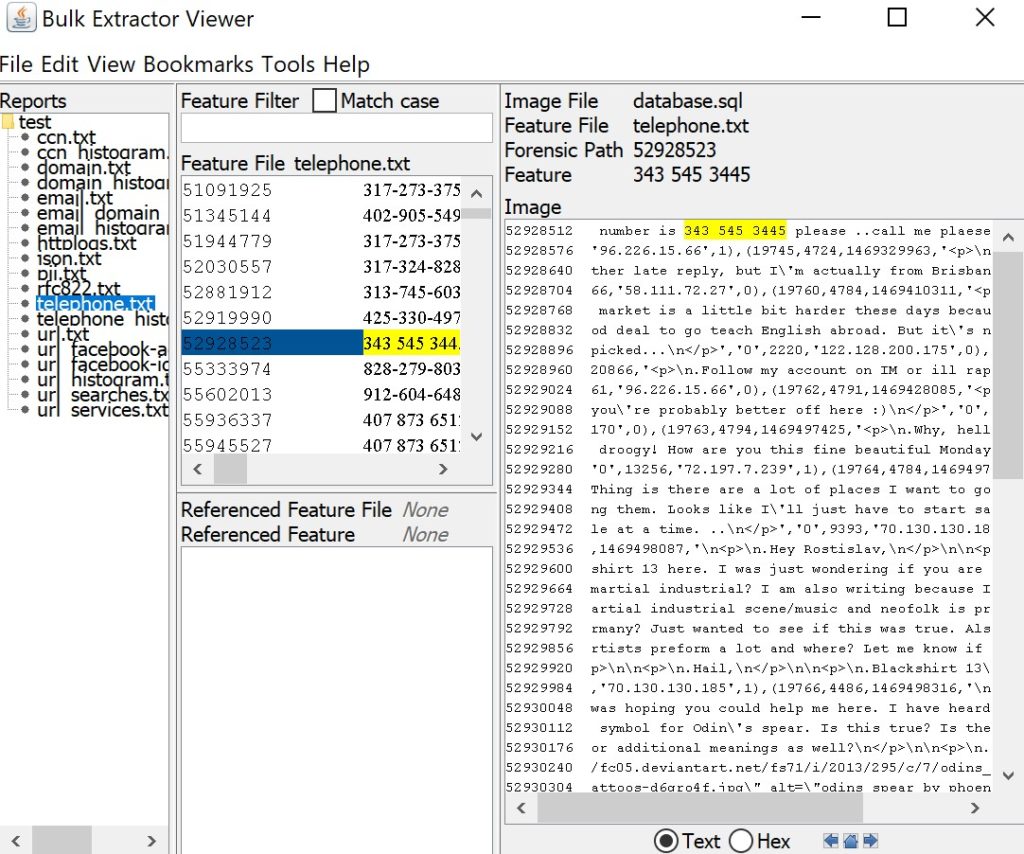
**Bulk Extractor Nasıl Yüklenir?**

Linux Kurulumu (Debian tabanlı sistemler):

***sudo apt-get update***

***sudo apt-get install bulk-extractor***

macOS için: ***brew install bulk-extractor***

******Sol tarafta feature listesi (örneğin e‑posta adresleri, IP’ler, tel. numaraları) yer alıyor, sağ panelde ise seçili özellik detaylıca görüntüleniyor.

Liste paneli, histrogram verileri içeren “email\_histogram.txt” gibi çıktı dosyalarını da gösteriyor; bu, Bulk Extractor’ın elde edilen verileri analiz ve filtreleme için hızlıca kullanmasını sağlıyor.

**Bulk Extractor ile Neler Yapılabilir?**

Bulk Extractor, herhangi bir disk imajı ya da dosya üzerinde aşağıdaki bilgileri otomatik olarak bulabilir:

* E-posta adresleri
* URL’ler
* Telefon numaraları
* Kredi kartı numaraları
* ZIP dosyaları, Base64 encoded veriler
* Silinmiş veya artık veriler (residual data)

Bunları tek tek aramaya gerek kalmaz. Bulk Extractor hepsini aynı anda, paralel şekilde tarar.

**Temel Kullanım Komutları**

Basit tarama: ***bulk\_extractor -o cikti\_klsr -R hedef\_klasor***

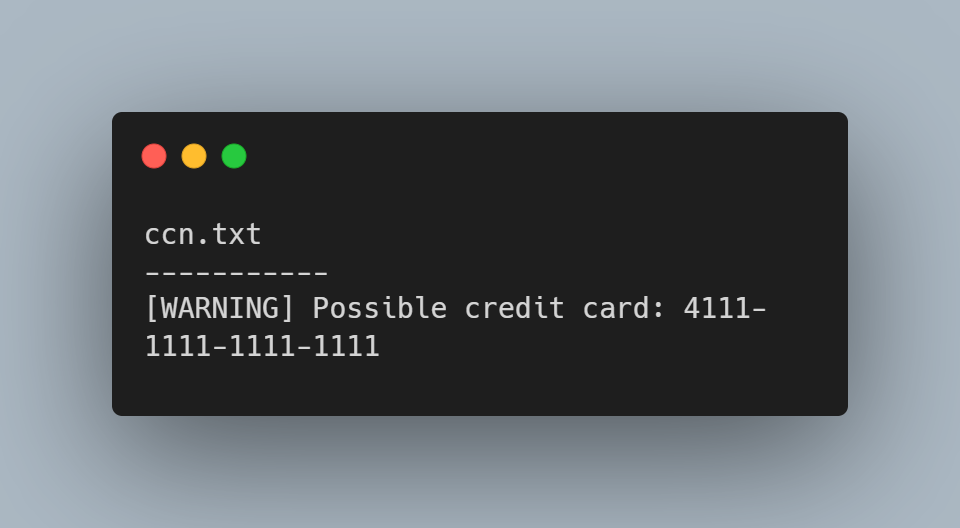
Bu komut, hedef klasör içindeki tüm dosyaları tarar ve cikti\_klsr isimli klasöre analiz sonuçlarını kaydeder.

Disk imajı üzerinde tarama: ***bulk\_extractor -o output/ disk.img***

disk.img adlı disk imajı analiz edilir. Sonuçlar output/ klasöründe oluşur.

Belirli veri türlerini bulma (örnek: e-postalar): ***cat output/email.txt***

**Örnek çıktılar:**

Her tür veri, ayrı ayrı .txt dosyaları içinde listelenir. Öğrenciler için okunması ve analiz edilmesi kolaydır.

Bulk Extractor, veri kurtarma ve analiz amacıyla geliştirilmiş bir araçtır. Sadece size ait ya da üzerinde yasal analiz izni olan disk görüntülerinde kullanılmalıdır.

Bulk Extractor, karmaşık disk veya dosya analizini kolaylaştıran güçlü bir araçtır. Hedefi, insan gözüyle tespit edilmesi zor olan bilgileri otomatik olarak ortaya çıkarmaktır. Özellikle adli bilişim, siber güvenlik ve veri kurtarma alanlarında çokça kullanılır.