**Jefferson Nedir?**

**Jefferson**, NTFS dosya sistemindeki **Alternate Data Stream (ADS)** yapısını analiz etmek için kullanılan açık kaynaklı, Python tabanlı bir **adli bilişim aracıdır**. ADS, Windows dosya sisteminde bir dosyaya görünmeyen veriler eklenmesine olanak tanır. Bu özellik saldırganlar tarafından **zararlı yazılımları veya verileri gizlemek** amacıyla kullanılabilir.

Jefferson, disk imajları veya raw (ham) NTFS bölümlerinden **ADS verilerini çıkarma**, **analiz etme** ve **listeme** işlemleri gerçekleştirir.

**🔍 Ne İşe Yarar?**

* 📁 NTFS dosya sisteminde ADS içeren dosyaları tespit eder
* 🔐 ADS verilerini çıkarır ve okunabilir hale getirir
* 🧪 Siber güvenlik ve dijital adli bilişim analizlerinde kullanılır
* 💀 Zararlı yazılım saklama tekniklerini ortaya çıkarır

**🚀 Temel Özellikler**

* Python 3 uyumludur
* Dosya/dizin ADS tespiti ve çıkarımı yapar
* Disk imajı (.dd, .img) veya doğrudan raw NTFS bölümü ile çalışabilir
* CLI (komut satırı) tabanlıdır
* Minimal bağımlılıklara sahiptir

**Kuruluma Geçelim :**

**metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

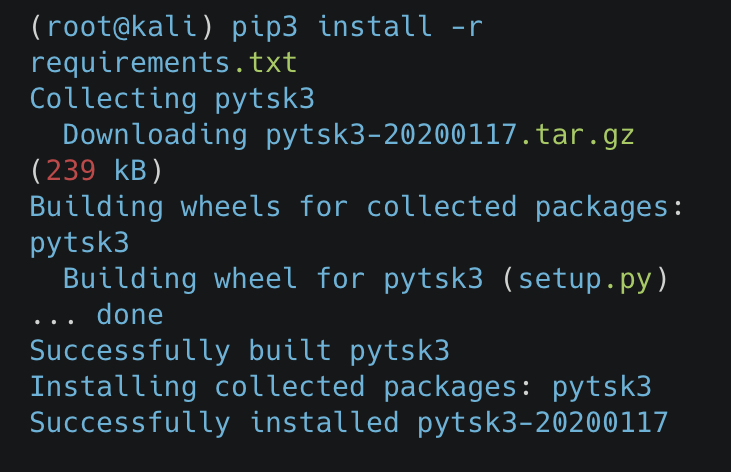
**metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

**yazı tipi, grafik, ekran görüntüsü, tipografi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

**cd Jefferson komutu ile o dizine geçiş yapıyoruz.**



**Kurulumu bitirdik, örnek bir işlem yapalım.**

metin, yazı tipi, ekran görüntüsü içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Bu komut, verdiğin NTFS disk imajı veya bölümünde (örneğin ntfs\_image.dd) bulunan tüm dosyaların **Alternate Data Stream (ADS)** yapılarını tarar ve ekli ADS dosyalarını listeler.

**✅ Avantajları**

* ✅ NTFS ADS'leri hızlı ve doğru biçimde analiz eder
* ✅ Kullanımı kolay CLI tabanlıdır
* ✅ Hafif ve bağımsız çalışır
* ✅ Adli bilişim uzmanları için idealdir
* ✅ Açık kaynaklıdır (denetlenebilir, geliştirilebilir)

**⚠️ Sınırlamaları / Dezavantajları**

* ❌ Sadece NTFS dosya sisteminde çalışır (FAT32, exFAT desteklenmez)
* ❌ Grafik arayüzü yoktur (sadece terminalden kullanılır)
* ❌ Derinlemesine disk analiz araçları kadar kapsamlı değildir (örneğin Autopsy, Sleuth Kit gibi)

**👨‍💼 Kimler Kullanmalı?**

* Adli bilişim analistleri
* Siber güvenlik araştırmacıları
* Zararlı yazılım analistleri
* Red Team / Blue Team ekipleri
* Tehdit avcıları

**📌 Özet**

| **Özellik** | **Açıklama** |
| --- | --- |
| **Araç Adı** | Jefferson |
| **Kullanım Alanı** | NTFS Alternate Data Streams analizi |
| **Desteklenen FS** | NTFS |
| **Kod Dili** | Python 3 |
| **Kurulum** | Git + pip |
| **Avantajı** | ADS’leri otomatik tespit edip çıkarır |
| **Dezavantajı** | Sadece NTFS desteği, GUI yok |