**🧠 1. Exif Nedir?**

**EXIF (Exchangeable Image File Format)**, özellikle JPEG, TIFF ve bazı RAW dosya formatlarında kullanılan bir **meta veri standardıdır.**

📌 Bir fotoğraf çekildiğinde cihaz tarafından dosyaya şunlar otomatik olarak gömülür:

* Tarih/Saat
* Cihaz marka/model
* GPS koordinatları
* Kullanılan yazılım/sürüm
* ISO, diyafram, enstantane gibi fotoğraf bilgileri

Bu bilgiler saldırganlar veya adli araştırmacılar için **çok değerli ipuçları** olabilir.

**🔍 2. ExifScan Nedir?**

**ExifScan**, dosyaların içindeki EXIF metadata’yı analiz eden açık kaynaklı bir komut satırı aracıdır.  
Python ile yazılmıştır ve özellikle **adli bilişim** ve **OSINT** alanlarında tercih edilir.

📌 Geniş veri formatı desteğiyle EXIF bilgilerini **taranabilir, filtreleyebilir ve çıktılayabilir.**

**🎯 3. Ne İşe Yarar?**

| **İşlev** | **Açıklama** |
| --- | --- |
| 🧾 EXIF bilgilerini gösterme | Dosyanın içinde gömülü tüm meta verileri okur |
| 🌍 GPS koordinatlarını tespit | Fotoğraf nerede çekilmiş? |
| 📷 Cihaz bilgilerini çıkarma | Marka/model bilgisi verir |
| 📆 Tarih bilgisi analizi | İlk oluşturulma, son değiştirilme tarihi |
| 🧪 Çoklu dosya tarama | Klasör içindeki tüm görselleri analiz eder |
| 🔎 Adli iz bulma | OSINT ve forensics için kullanılabilir |

**⚙️ 4. Kurulum (Kali Linux)**

**✅ Gerekli kütüphaneler:**

sudo apt update

sudo apt install python3-pip

pip3 install exifread

✅ ExifScan'i GitHub’dan indir:

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🚀 5. Kullanım Komutları**

**✅ Tek bir dosyada EXIF analizi:**

python3 exifscan.py -i foto.jpg

**✅ Belirli anahtar kelimeleri filtrele:**

python3 exifscan.py -i foto.jpg -k GPS

**✅ Bir klasördeki tüm görselleri tara:**

python3 exifscan.py -d /home/user/fotolar/

**✅ JSON çıktısı almak için:**

python3 exifscan.py -i resim.jpg -j

**📋 6. Örnek Terminal Çıktısı**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🧠 7. EXIF ile Neler Tespit Edilebilir?**

| **Veri Türü** | **Açıklama** |
| --- | --- |
| 📅 Zaman Bilgisi | Çekim, düzenleme, aktarım zamanı |
| 📍 GPS Bilgisi | Konum koordinatları (Google Maps ile eşleştirilebilir) |
| 📱 Cihaz Bilgisi | Marka, model, yazılım sürümü |
| 🧠 Kullanıcı Etkisi | Yazılım adları (örneğin: Photoshop → manipülasyon şüphesi) |
| 📂 Dosya Geçmişi | Oluşturulma/modifiye edilme bilgisi |

**🛡️ 8. Siber Güvenlikte Kullanımı**

* 🕵️‍♂️ OSINT: Fotoğraf paylaşımından kişi/konum tespiti
* 🧪 Adli Bilişim: Şüpheli dosyalardan kimlik/ipucu çıkarımı
* 🎯 Red Team: Sosyal mühendislik öncesi hedef analizi
* 📵 Gizlilik: EXIF verilerini temizlemeyen kullanıcıların izlenmesi

**🎯 9. Öğrenim Kazanımları**

* Görsel dosyalardaki meta verilerin nasıl analiz edildiğini öğrenme
* EXIF üzerinden zaman, cihaz, konum gibi bilgileri çıkarma pratiği
* Adli analizde görsel kanıtların nasıl değerlendirildiğini kavrama
* Python tabanlı bir OSINT aracının terminalde kullanımı