**Plaso (log2timeline) Nedir?**

Plaso, sistem üzerinde gerçekleşmiş olayları zaman sırasına göre analiz etmeye yarayan açık kaynaklı bir adli bilişim aracıdır. Özellikle bir cihazda neler olmuş, ne zaman olmuş sorularını cevaplamak için kullanılır.

Bu işlemi yaparken çeşitli log (kayıt) dosyalarını, tarayıcı geçmişini, USB kullanım bilgilerini, sistem saatlerini ve daha fazlasını analiz eder. Böylece bize bir zaman çizelgesi (timeline) sunar.

Plaso, dijital olayları zaman sırasına göre sıralayan ve araştırmayı kolaylaştıran bir analiz aracıdır.

**Plaso Nasıl Kurulur?**

Plaso, Python ile yazılmıştır. Kali Linux gibi siber güvenlik dağıtımlarında genellikle ön yüklü gelir.

Debian/Ubuntu Tabanlı Linux Kurulumu:

***sudo apt-get update***

***sudo apt-get install plaso***

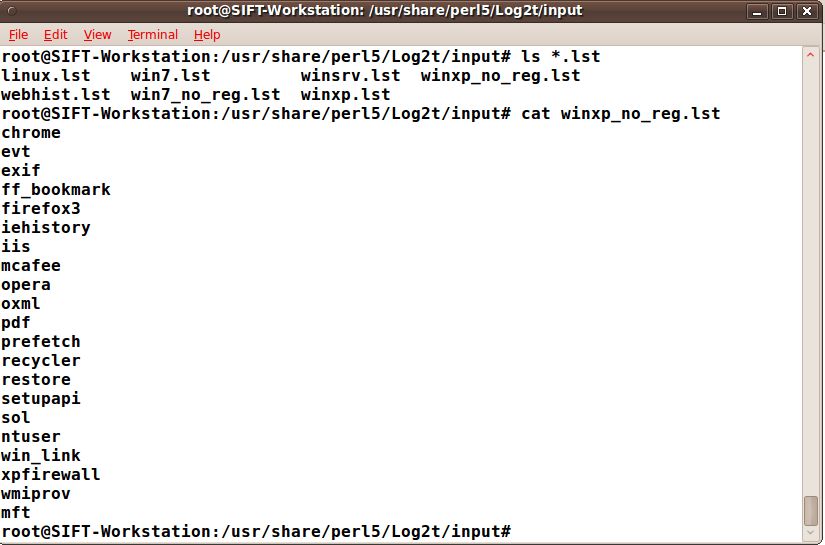
Plaso, log2timeline.py ve psort.py adında iki ana komutla çalışır. Birincisi zaman çizelgesi oluşturur, ikincisi bu çizelgeyi okunabilir hale getirir.

**Plaso ile Neler Yapılabilir?**

Plaso sayesinde aşağıdaki dijital izler analiz edilebilir:

* Tarayıcı geçmişleri (Chrome, Firefox)
* Sistem olay günlükleri (event logs)
* USB cihaz takılıp çıkarılma kayıtları
* Dosya erişim, değiştirme ve silme zamanları
* Kullanıcı oturum açma/kapama geçmişi
* NTFS, MFT, $LogFile gibi sistem dosyaları

Tüm bu veriler kronolojik olarak sıralanır ve geçmişte neler yaşandığı adım adım ortaya çıkar.



Tasks kısmında worker PID’leri, sayı olarak işlenen artefakt sayısı gibi bilgiler yer alıyor.

**Temel Kullanım Komutları**

Zaman çizelgesi dosyasını oluşturma:

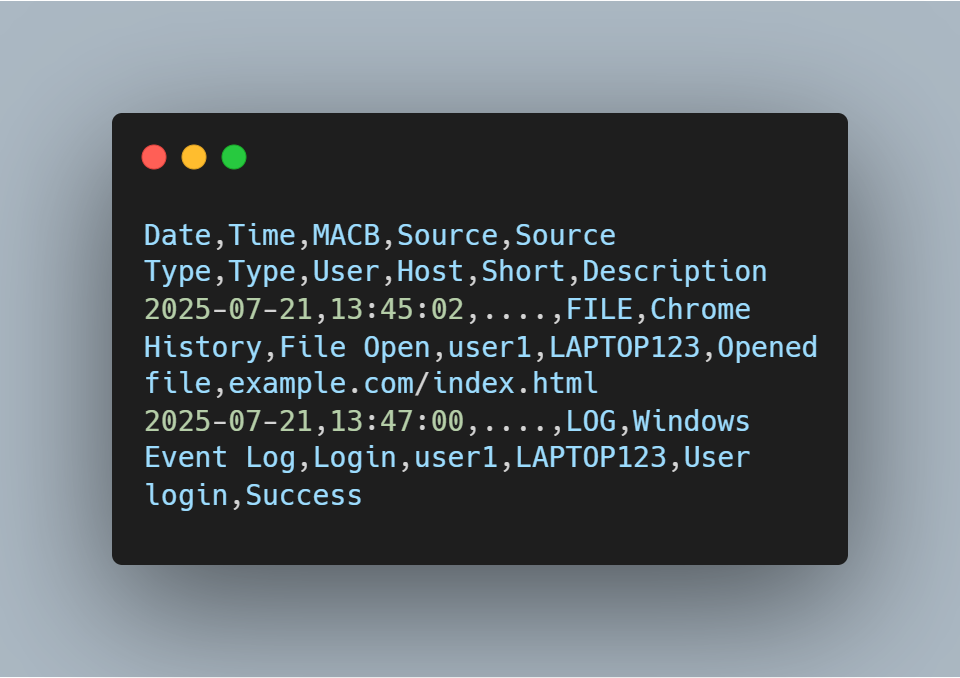
***log2timeline.py olaylar.plaso /mnt/diskimage***

log2timeline.py, disk imajından olayları çıkarır ve .plaso formatında veri oluşturur.

Okunabilir zaman çizelgesi haline getirme:

***psort.py -o l2tcsv olaylar.plaso > olaylar.csv***

psort.py, oluşturulan .plaso dosyasını .csv dosyasına dönüştürür (Excel'de açılabilir).



Bu çıktıda:

* Hangi tarihte ne olmuş?
* Hangi kullanıcı neye erişmiş?
* Hangi dosya açılmış, silinmiş?

gibi sorulara yanıt verir.