Arkime (Moloch) - Eğitim Materyali

# 🕵️‍♂️ Arkime (Eski adıyla Moloch) Nedir?

Arkime, yüksek hızlı, büyük ölçekli ağ trafiği yakalama ve indeksleme sistemidir. Özellikle siber olay incelemesi (forensics) ve ağ trafiği analizinde kullanılır.  
ElasticSearch, Zeek gibi araçlarla entegre çalışarak paket analizini görsel hale getirir.

# 🚀 Özellikleri

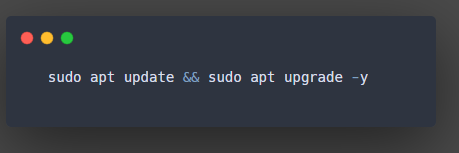
- Tam paket yakalama (full packet capture)  
- Elasticsearch tabanlı hızlı arama ve indeksleme  
- Web arayüzü ile görsel trafik inceleme  
- Zeek, Suricata gibi araçlarla entegrasyon  
- PCAP dışa aktarma ve oturum izleme

# 📌 Kullanım Alanları

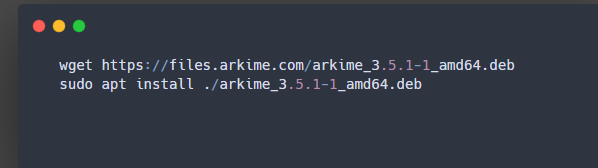
- Siber olay inceleme (Incident Response)  
- Ağ tehdit avcılığı (Threat Hunting)  
- Adli bilişim analizi  
- Güvenlik ihlali tespiti ve analiz  
- SOC eğitim ortamları

# 💻 Kurulum (Kali Linux üzerinde örnek)

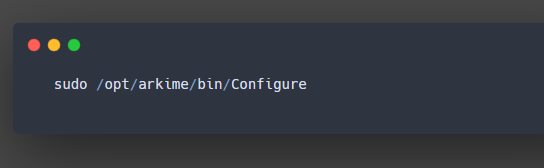
1. Sistem güncellemesi:

******

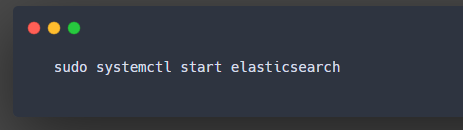
2. Arkime (Moloch) paketini indir ve kur:

******

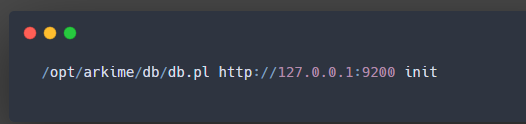
3. Setup script çalıştır:

******

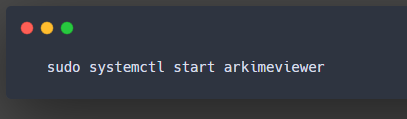
4. Elasticsearch’i kur ve başlat:

******

5. Arkime veritabanını oluştur:

******

6. Viewer başlat:

******

7. Capture başlat:

# 

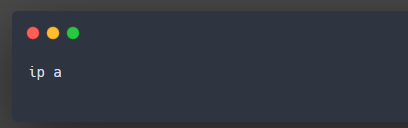
# 🌐 Web Arayüz Erişimi

Varsayılan olarak web arayüzü `http://localhost:8005` adresinden erişilir. İlk oturum açma bilgileri:  
Kullanıcı adı: admin   
Parola: arkime

# 🧪 Örnek Komut ve Çıktılar

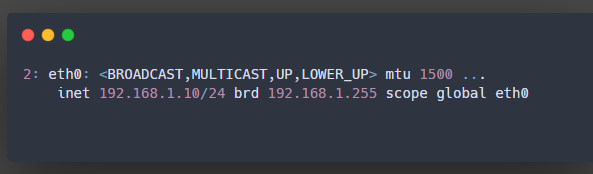
✅ 1. Ağ Arayüzlerini Listeleme

Komut:



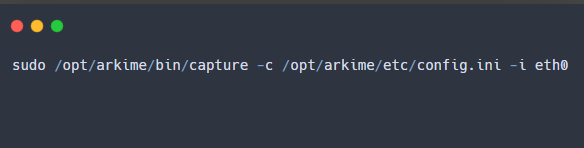
**Amaç:**  
Hangi ağ arayüzünün kullanılacağını belirlemek için ağ kartlarını görüntüler (örneğin eth0, ens33).

Çıktı:



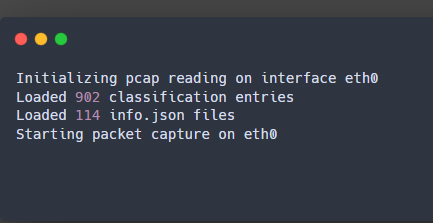
✅ 2. Canlı Trafik Yakalama (Capture)

Komut:



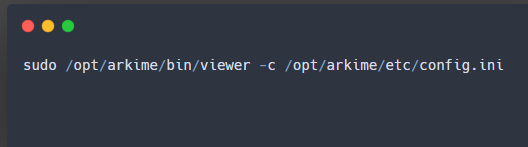
**Amaç:**  
eth0 arayüzünden canlı trafik yakalayarak Arkime veritabanına aktarır.

Çıktı:

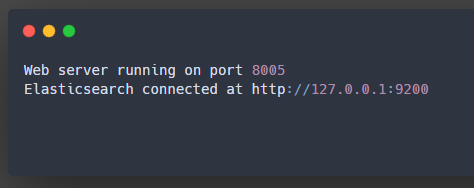


**✅ 3. Arkime Viewer Hızlı Başlatma (manuel)**

**Komut:**

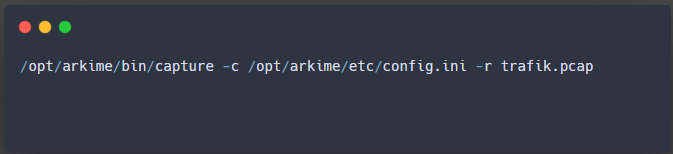


**Amaç:**  
Arkime web arayüzünü elle başlatır. Sistem servisleri yerine terminalden başlatmak için kullanılır.

Çıktı:  


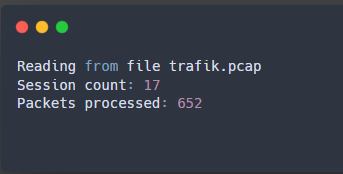
**✅ 4. PCAP Dosyasını Manuel Yükleme**

**Komut:**



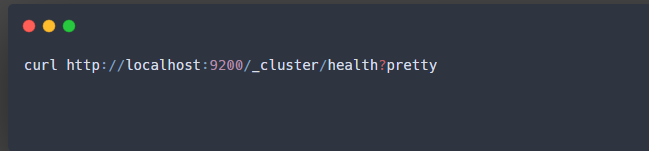
**Amaç:**  
Daha önce kaydedilmiş bir .pcap dosyasını Arkime’ye analiz için yükler.

Çıktı:



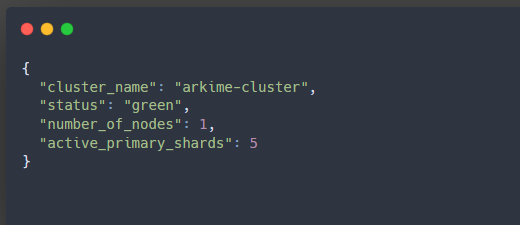
**✅ 5. Elasticsearch Durum Kontrolü**

**Komut:**



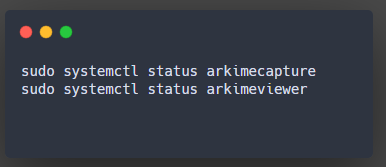
**Amaç:**  
Arkime’nin bağlı olduğu Elasticsearch veri motorunun çalışıp çalışmadığını test eder.

Çıktı:



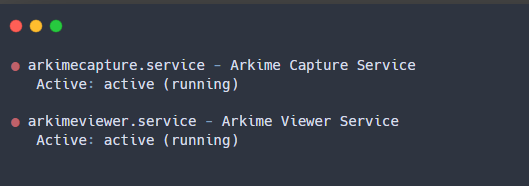
✅ 6. Arkime Capture ve Viewer Servis Durumu

Komut:



**Amaç:**  
Arkime’nin arka planda çalışan servislerinin aktif olup olmadığını kontrol eder.

Çıktı:



📎 Notlar

- Arkime yüksek disk alanı kullanabilir. PCAP'ler saklandığı için minimum 100 GB önerilir.  
- ElasticSearch RAM ve CPU yoğun çalışır, sistem kaynağı yeterli olmalıdır.  
- Kullanıcı arayüzü üzerinden IP, port, oturum filtrelemesi kolaydır.