**🧠 1. Arkime Nedir?**

**Arkime**, büyük miktarda ağ trafiğini (PCAP) toplayıp saklayabilen ve web arayüzü üzerinden bu trafiği **arama, filtreleme, analiz** etmenize olanak tanıyan açık kaynaklı bir ağ izleme (network forensics) platformudur.

📌 Özellikleri:

* Yüksek performanslı paket yakalama
* Elasticsearch + Viewer mimarisi
* Web tabanlı analiz ekranı
* Güçlü filtreleme ve etiketleme

**🎯 2. Ne İşe Yarar?**

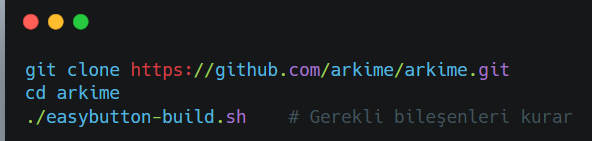
| **İşlev** | **Açıklama** |
| --- | --- |
| 📥 Ağ trafiğini kaydeder | Tüm gelen/giden paketleri diske yazar |
| 🔎 Web üzerinden analiz | Arayüz üzerinden IP, port, hostname filtreleme |
| 🧩 Protokol çözümleme | HTTP, TLS, DNS, FTP, SSH, SIP, SMTP vs. |
| 📁 PCAP dosyası dışa aktarım | Belirli trafiği .pcap olarak indirebilme |
| 📊 Trafik istatistikleri | Oturum sayısı, veri hacmi, hedef portlar |

**🧱 3. Bileşenler**

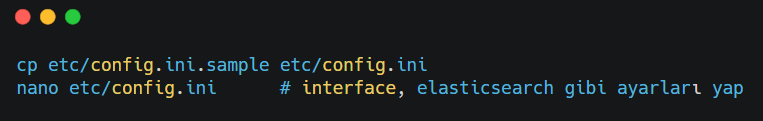
| **Bileşen** | **Açıklama** |
| --- | --- |
| ✳️ **Capture** | Paketi yakalar (libpcap ile) ve diske yazar |
| 🔎 **Viewer** | Web tabanlı analiz arayüzü |
| 📊 **Elasticsearch** | Verilerin indekslenmesini ve aranmasını sağlar |

**⚙️ 4. Kurulum (Kali Linux / Ubuntu)**

**✅ Temel adımlar:**



✅ Config dosyasını düzenle:



**✅ Elasticsearch başlat:**

sudo systemctl start elasticsearch

**✅ Arkime başlat:**

./db.pl --init # Elasticsearch şemasını hazırla

sudo ./capture -c etc/config.ini

sudo ./viewer -c etc/config.ini

**🌐 5. Web Arayüzü**

Web arayüzüne tarayıcıdan eriş:

http://localhost:8005

Kullanıcı adı ve şifre:

admin / password

Buradan canlı ağ trafiği, geçmiş sorgular, oturum detayları, DNS/HTTP sorguları gibi tüm verileri filtreleyebilirsin.

**📋 6. Örnek Kullanım Senaryoları**

| **Senaryo** | **Açıklama** |
| --- | --- |
| 🕵️‍♂️ Olay müdahalesi | Şüpheli trafiklerin geçmişe dönük analizi |
| 🧪 Sızma testi sonrası iz takibi | Hangi sistemle ne zaman bağlantı kuruldu |
| 🎯 Protokol istihbaratı | HTTP başlıkları, DNS talepleri, TLS handshake |
| 📦 Ağ güvenliği araştırması | Hangi IP’ler en çok veri gönderiyor? |
| 🧾 Kullanıcı davranış takibi | İçerik filtreleme, dosya indirme analizleri |

**🛡️ 7. Güvenlik ve Performans Notları**

* ElasticSearch RAM kullanımı yüksektir (4GB+ önerilir)
* Ağ arayüzü üzerindeki tüm trafik yazıldığından **disk alanı çok önemlidir**
* Viewer arayüzü parola ile korunmalıdır
* HTTPS yapılandırması desteklenir (reverse proxy önerilir)

**🎯 8. Öğrenim Kazanımları**

* Ağ trafiği yakalama ve analiz altyapısını öğrenme
* Web arayüzlü forensics mantığını kavrama
* DNS, HTTP, TLS gibi protokolleri analiz etme becerisi
* Elasticsearch temelli sorgu diline giriş
* Log toplama ve trafik geçmişi üzerinden saldırı izi sürme