**Wireshark**

**Wireshark Nedir?**

Wireshark, ağ üzerindeki veri paketlerini gerçek zamanlı olarak yakalayan ve analiz eden açık kaynaklı bir ağ analiz aracıdır. Ağ trafiğini görselleştirir ve detaylı analiz yapmanı sağlar. Özellikle ağ trafiğini izlemek, sorunları teşhis etmek ve güvenlik zafiyetlerini tespit etmek için kullanılır.

- **Bunu şöyle düşünebilirsin:**  
Wireshark, ağda geçen tüm konuşmaları (veri paketlerini) duyan bir “ağ dedektifi” gibidir.

**Wireshark'ın Özellikleri**

* Gerçek zamanlı ağ trafiği izleme ve kayıt.
* 1000’den fazla ağ protokolünü tanıma ve çözümleme.
* Filtreleme özelliğiyle sadece belirli trafiği görüntüleme.
* Paketlerin zamanlamasını, boyutunu ve içeriğini detaylı analiz etme.
* Hem canlı trafik hem de kayıtlı .pcap dosyaları üzerinde analiz yapma.
* TCP, UDP, HTTP, DNS, ICMP, ARP, SSL/TLS gibi protokolleri çözümleme.

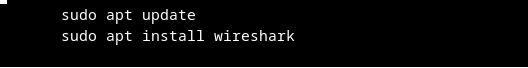
**Kullanım Alanları**

* **Siber güvenlik uzmanları:** Ağ saldırılarını analiz etmek, şüpheli trafiği incelemek.
* **Sistem yöneticileri:** Ağ sorunlarını teşhis etmek, performans kontrolü yapmak.
* **Etik hackerlar (beyaz şapkalı hackerlar):** Ağda geçen verilerin güvenliğini test etmek.
* **Eğitim amaçlı:** Ağ protokollerini öğrenmek isteyen öğrenciler ve araştırmacılar.

**Kurulum Aşamaları:**

**Windows için Kurulum:**

1. Wireshark’ın resmi web sitesine gir:  
   - https://www.wireshark.org/download.html
2. Windows Installer (64-bit) seçeneğini indir.
3. Kurulum sırasında **WinPcap** ya da **Npcap** bileşenini yüklemeyi **unutma**. Bunlar paket yakalamak için gereklidir.
4. Kurulumu “Next” diyerek tamamla ve uygulamayı başlat.

**Linux (Debian/Kali) için Kurulum: **

NOT: Kurulumdan sonra "wireshark" grubuna kullanıcıyı eklemek gerekebilir:



-Ardından sistemi yeniden başlat.

**Dikkat Edilmesi Gerekenler:**

* Wireshark ile **izin alınmadan ağ trafiği izlemek yasal değildir**.
* Büyük ağlarda yoğun trafik olabileceği için filtreleme yapılmazsa analiz zorlaşabilir.
* **Yönetici (admin/root) yetkisi** gerektirdiğinden sistem güvenliği açısından dikkatli kullanılmalıdır.
* SSL/TLS gibi şifreli trafikleri çözümleyebilmek için ek yapılandırmalar gerekebilir.
* Bazı antivirüsler, Wireshark'ı tehlikeli olarak algılayabilir; güvenlik yazılımı ile çakışmalar olabilir.