**🔍 Wireshark Nedir?**

Wireshark, ağ üzerindeki tüm veri trafiğini **gerçek zamanlı** izlemeye yarayan güçlü bir **ağ analiz aracıdır**.  
Siber güvenlik, ağ yönetimi ve hata ayıklama gibi birçok alanda profesyoneller tarafından kullanılır.

* Protokol katmanlarını detaylı inceler (Ethernet, IP, TCP, HTTP, DNS vb.)
* Filtreleme özelliği sayesinde yüzlerce paket arasında ilgilendiğin trafiği seçebilirsin.
* Arayüzü kullanıcı dostudur ve grafiksel görünüme sahiptir.

🔧 **Kurulum (Kali Linux)**

Wireshark çoğu zaman Kali ile birlikte gelir. Yine de manuel kurmak istersen:

sudo apt-get update

sudo apt-get install wireshark

Kurulumdan sonra terminale şu komutu yazarak başlatabilirsin:

wireshark

ekran görüntüsü, yazılım, multimedya yazılımı, metin içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🔍 Temel Filtreler (Paket Seçmek İçin)**

| **Filtre** | **Ne İşe Yarar** |
| --- | --- |
| http | HTTP istek ve yanıtlarını gösterir |
| dns | DNS sorgularını listeler |
| ip.addr == X.X.X.X | Belirli IP adresine ait trafiği gösterir |
| tcp.port == 80 | Belirli port numarasındaki TCP trafiği |
| udp | UDP protokolüne ait tüm trafiği |
| icmp | Ping paketlerini (Echo request/reply) |

**🔎 Paket Yapısı**

Wireshark’ta bir pakete tıkladığında 3 ana bölüm vardır:

1. **Üstte**: Tüm paketlerin listesi
2. **Ortada**: Seçilen paketin protokol detayları (katman katman)
3. **Altta**: Paketin ham (hex ve ASCII) verisi

Bu sayede bir paket içeriğinde **hangi verinin**, **hangi protokolden geçtiği**, **hangi portlarla iletişim kurduğu** anlaşılır.

**🧪 Uygulama Senaryosu (Sınıf İçi Deney)**

1. Öğrenciler aynı ağda çalışır.
2. Bir cihaz Wireshark’ta dns filtresi ile izlemeye başlar.
3. Diğer bir öğrenci youtube.com gibi bir siteye gider.
4. DNS paketi yakalanır ve sorgulanan alan adı gözlemlenir.
5. Ardından http gibi filtrelerle hangi veriler çağrıldığı incelenebilir.
6. HTTPS bağlantı varsa yalnızca **alan adı** (SNI) gözükür, içerik şifreli olur.

**🧪 Uygulama Senaryosu (Sınıf İçi Deney)**

1. Öğrenciler aynı ağda çalışır.
2. Bir cihaz Wireshark’ta dns filtresi ile izlemeye başlar.
3. Diğer bir öğrenci youtube.com gibi bir siteye gider.
4. DNS paketi yakalanır ve sorgulanan alan adı gözlemlenir.
5. Ardından http gibi filtrelerle hangi veriler çağrıldığı incelenebilir.
6. HTTPS bağlantı varsa yalnızca **alan adı** (SNI) gözükür, içerik şifreli olur.