

**Sonuç**

Bu proje, ağ trafiği analizi için kullanılabilecek basit ve etkili bir araç sunmaktadır.

Elde edilen görselleştirmeler, ağ trafiğinin yapısını kolayca anlamamıza ve

potansiyel güvenlik tehditlerini veya ağ performansı sorunlarını hızlıca tespit etmemize olanak tanır.

Gönderilen paketlerin sayısı, aynı ip adresinden fazla sayıda paket gönderilmesi ve bunu aynı ip adresine göndermesi

gibi bilgilerin görsel olarak gözlemlenmesi analiz işlemini kolaylaştırmaktadır.

Ayrıca, projenin esnek yapısı, farklı ağ trafiği veri kaynaklarını analiz etmek ve gerektiğinde özelleştirmeler yapmak için olanak sağlar.

Analiz edilmek istenen veri dosyası kolayca yüklenip analiz edilebilir. Ayrıca wiresharktan alınan veriler olduğu için

anlık olarak ağ trafiğini dinleyip, dosyayı alıp yükleyerek analiz yapılabilir.

**Kullanılan Yöntemler**

Ağ trafiği veri dosyalarının JSON formatında okunması ve içeriğinin pandas DataFrame'e dönüştürülmesi.

Ağ trafiği veri dosyaları JSON formatında okunur ve içeriği karmaşıklığı azaltmak için veri sözlüğüne dönüştürülür.

Veriler veri sözlüğünden okunarak işlenir.

İlişkilerin görselleştirilmesi için, pyvis kütüphanesinin kullanılması ve paket bağlantılarının ağ grafiği olarak temsil edilmesi.

İlişkiler, kenarlar ve düğümler için pyvis kütüphanesi kullanılır. Paketlerin bağlantıları, renkleri, sayıları ve hareketliliği

pyvis ile sağlanır.

Görselleştirmelerde farklı protokol türlerine göre renklendirme yapılır ve paket sayısına göre kalınlıklar ayarlanır.

Paket sayısı fazla olan kenar daha kalın görselleştirilir. Ayrıca her protokol türü farklı renkler ile temsil edilir ve

graf modelinde farklı renklerde görselleştirilir.

**Projenin Amacı**

Projenin amacı kullanıcılara wiresharktaki ağ paketlerini okumaları ve anlamaları konusunda kolaylık sağlamaktır.

Ağ trafiği veri dosyalarını okuyarak, iletilen paketler arasındaki ilişkileri analiz etmek ve bu ilişkileri graf

yapısıyla görselleştirerek kullanıcıya sunmaktır. Kullanıcı oluşturulan görselde paketleri kolaylıkla inceleyip analiz

yapabilecektir.

İletilen paketlerin özelliklerini, örneğin protokol türlerini, kaynak ve hedef IP adreslerini, iletilen veri miktarını vb.

gibi bilgileri görsel olarak gözlemleyebilecektir.

Toplanan verileri kullanarak, ağdaki bağlantıları görselleştirilecek ve farklı protokol türlerine göre paketler renklendirilecektir.

Hangi ip adresinden hangi ip adresine kaç adet paket gönderildiği de paket sayısına göre görselleştirilip kalınlık sağlanacaktır.

Görselleştirmeler aracılığıyla, ağ trafiğinin genel yapısını anlamak ve potansiyel anormallikleri tespit etmek temel amaçtır.

AĞ PAKETLERİ ANALİZİ ve GÖRSELLEŞTİRİLMESİ

**Projenin Kapsamı**

Proje kapsamında, Python programlama dili kullanılarak bir dizi kütüphane ve araçtan yararlanılmıştır.

Ana kütüphaneler arasında pandas veri analizi için, pyvis ağ görselleştirmesi için,

ve standart kütüphaneler arasında json ve collections bulunmaktadır.

Projede kullanılan temel yöntemler arasında, ağ trafiği veri dosyalarının okunması,

verilerin işlenmesi ve analiz edilmesi, görselleştirmelerin oluşturulması ve sonuçların sunulması yer almaktadır.

**Yorumlar**

Bu projenin avantajları arasında, ağ trafiği verilerini görsel olarak temsil etme yeteneği,

kullanıcı dostu bir arayüz sağlama potansiyeli ve çeşitli ağ protokollerine destek verme esnekliği bulunmaktadır.

Bununla birlikte, büyük veri kümeleriyle çalışırken performansın artırılması gerekebilir ve kullanıcıların daha iyi

anlayabileceği bir dokümantasyon ve rehber sunulması faydalı olabilir.

Ayrıca, daha karmaşık ağ yapılarını analiz etmek için ek fonksiyonlar ve özellikler eklenerek aracın genişletilebilirliği artırılabilir.

**Proje Özeti**

Bu proje wiresharkta yakalanmış ağ paketlerini analiz edip pythonda görselleştirmek amacıyla yapılmıştır.

Ağ trafiği, günümüzün karmaşık bilgi iletişim ağlarında hayati bir rol oynamaktadır.

Bu projede, Python dilinde geliştirilen bir araç, ağ trafiği veri dosyalarını analiz ederek,

iletilen paketler arasındaki ilişkileri ve bu paketlerin özelliklerini görselleştirme amacıyla tasarlanmıştır.

Wiresharkta paketleri izlemek, hangi ip adresinden hangi ip adresine kaç adet paket gönderilmiş ve hangi protokolden gönderilmiş gibi

bilgileri gözlemlemek zahmetli ve zordur. Özellikle ağ analistleri ve diğer kullanıcılar paketleri izlerken daha kolay bir şekilde

gözlem yapabilmeleri amacıyla, bu sistem ağ paketlerini alır ve kullanıcıya graf yapısı olarak görselleştirerek sunar

200541047 - Büşra KARAOZAN

2210541033 - Tuğçe ŞERBETÇİ