



T.C
MERSİN ÜNİVERSİTESİ
ERDEMLİ UYGULAMALI TEKNOLOJİ VE İŞLETMECİLİK YÜKSEKOKULU
BİLGİSAYAR TEKNOLOJİSİ VE BİLİŞİM SİSTEMLERİ BÖLÜMÜ

BTS404-Bilgisayar Ağ Güvenliği

İçerik:

Wireshark Temel İstatistik Araçları

Kasım Bölücü
16-701-005

Dr. Öğr. Üyesi EVRİM ERSİN KANGAL

Mersin, 2020

WIRESHARK

Wireshark Nedir

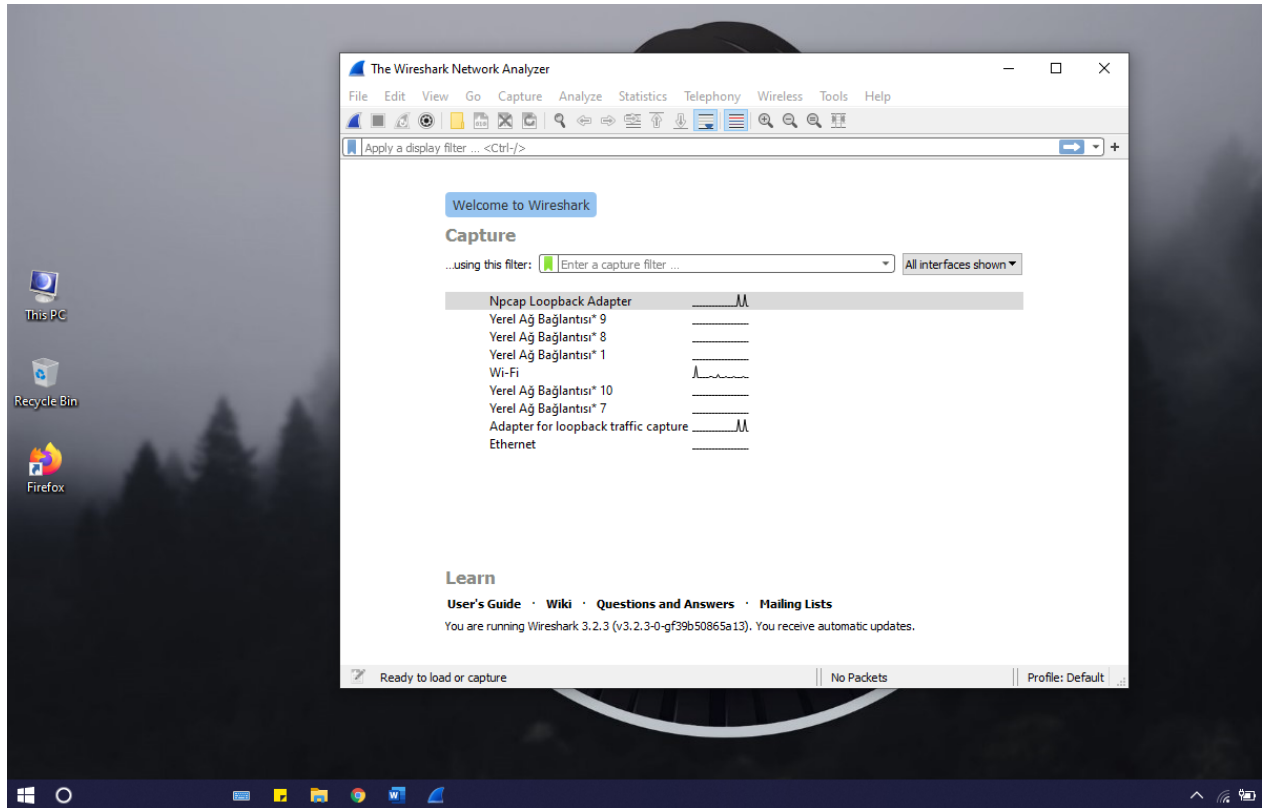
Wireshark, network trafiğinin veya ağ protokolünü, bir grafik arayüz üzerinden izlenmesini ve analiz etmenizi sağlayan, önemli bir programdır. Uygulamanın kurulu olduğu bilgisayar üzerinden anlık network trafiği izlenebileceği gibi, Wireshark daha önce kaydedilmiş dosyaların incelenmesi amacı ile de kullanılabilir. Unix, Linux, Windows ve MacOS işletim sistemlerinde çalışabilir. Wireshark, tamamen ücretsiz ve açık kaynak kodludur. 2006 yılına kadar Ethereal adıyla yayınlanan yazılım, 2006 yılından sonra Wireshark adıyla yayınlanmaya ve geliştirilmeye devam edilmiştir.

Wireshark temel istatistik araçlarını kullanma

Wireshark'ta bize temel ağ istatistiklerini sağlayan basit araçlar vardır.

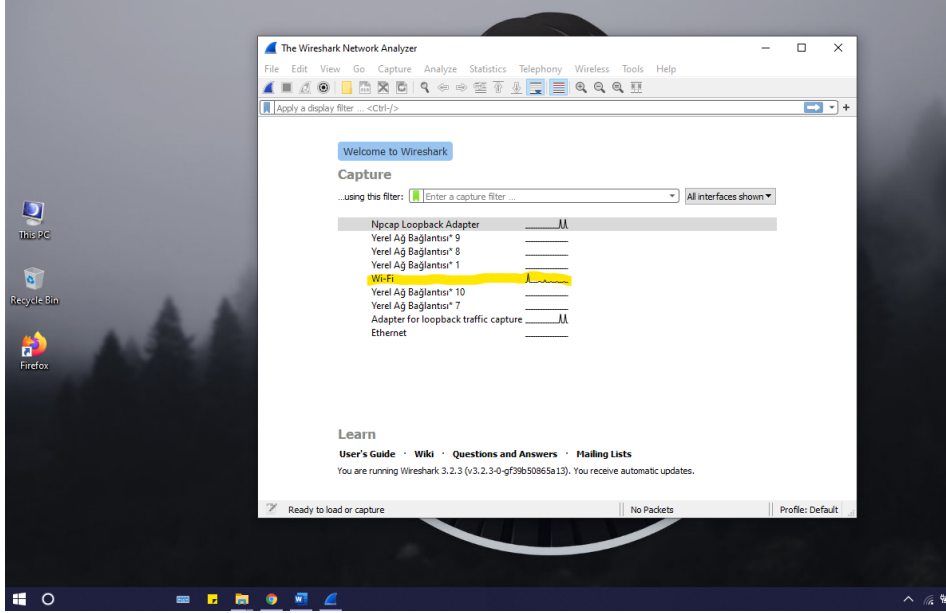
Bu araçlar ağ üzerinden kimler ile kimlerin konuştuğunu, konuşan cihazların neler olduğunu, ağ üzerinden hangi paketler ve hangi boyutlar da çalıştığını inceleyebiliriz.

Wireshark açıldığında bizi aşağıdaki gibi bir görüntü bekliyecektir.

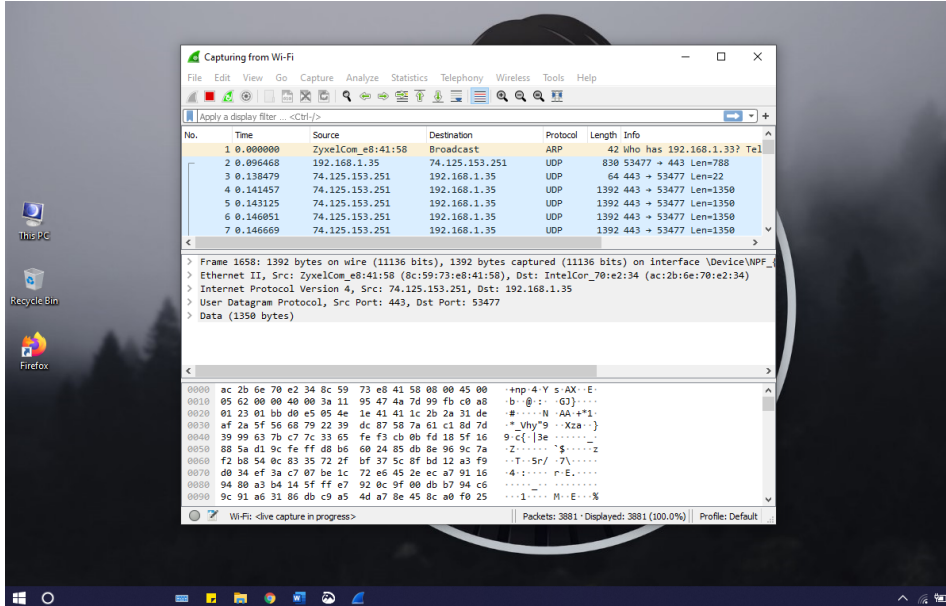


Wireshark'ta ağ istatistiklerini gerçekleştirmek için öncelikle bir ağı yakalamalıyız “Capture”.

Aşağıdaki resimde sarı ile çizilmiş olduğum üzerinde çalışacağım sizde herhangi birine çift tıklayarak yakalama işlemini başlatabilirsiniz.



Eğer herhangi bir sorun olmadığı taktirde sizi aşağıdaki resimde olduğu gibi bir ekran karşılayacaktır.

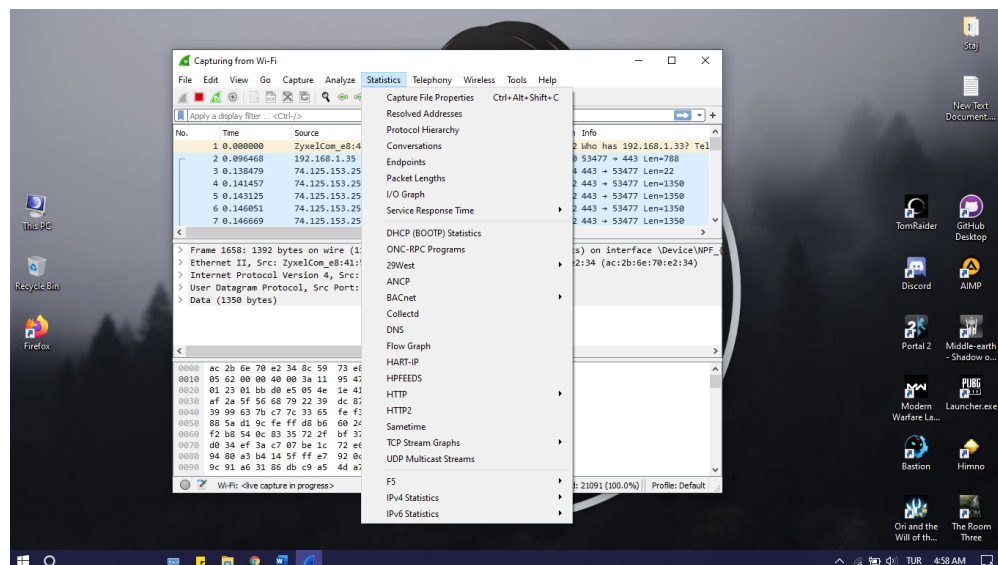


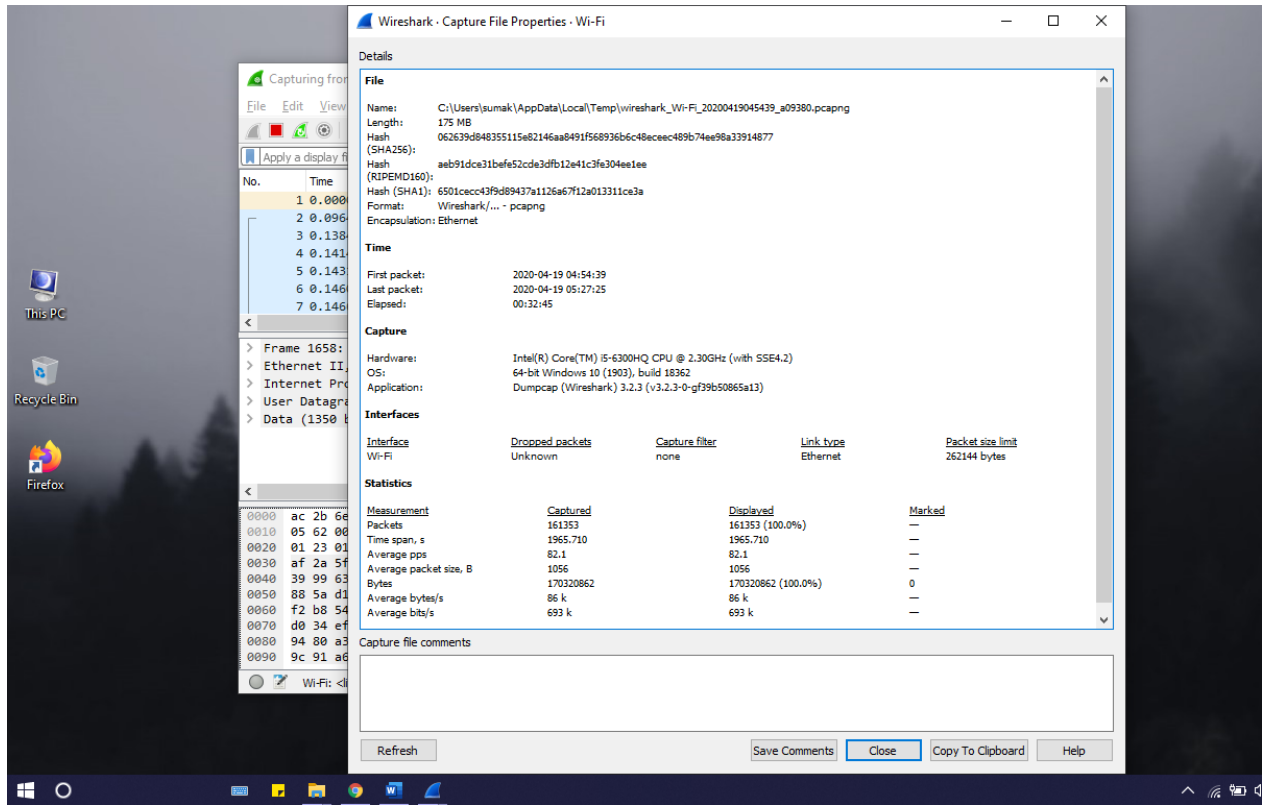
The screenshot displays the Wireshark network protocol analyzer interface. The main window is titled "Capturing from Wi-Fi". The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The top toolbar contains icons for various functions like opening files, saving, and capturing. The main display area is divided into three panes:

- Packet List:** Shows a list of captured packets. The first packet is a broadcast ARP request from 192.168.1.35 to 192.168.1.337. Subsequent packets are UDP datagrams from 192.168.1.35 to 192.168.1.337.
- Packet Details:** Shows the hierarchical structure of the selected packet (Frame 1658). It includes Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (1350 bytes).
- Packet Bytes:** Shows the raw data of the selected packet in hexadecimal and ASCII format.

The status bar at the bottom indicates "Wi-Fi (live capture in progress)" and "Packets: 7103 - Displayed: 7103 (100.0%)".

Açılan menüde ise en üstte bulunan “Capture File Properties” sekmesine tıklayınız.





Açılan pencere içerisindeki başlıkları inceleyecek olursak kısaca şu şekilde olacaktır,

File: Dosya adı ve yolu, uzunluk vb. Gibi dosya verileri sağlar

Time: Başlangıç zamanı, bitiş zamanı ve çekim süresi bilgilerini vermekte.

Capture: Wireshark'ın kullanılmakta olduğu PC için donanım bilgileri mevcut.

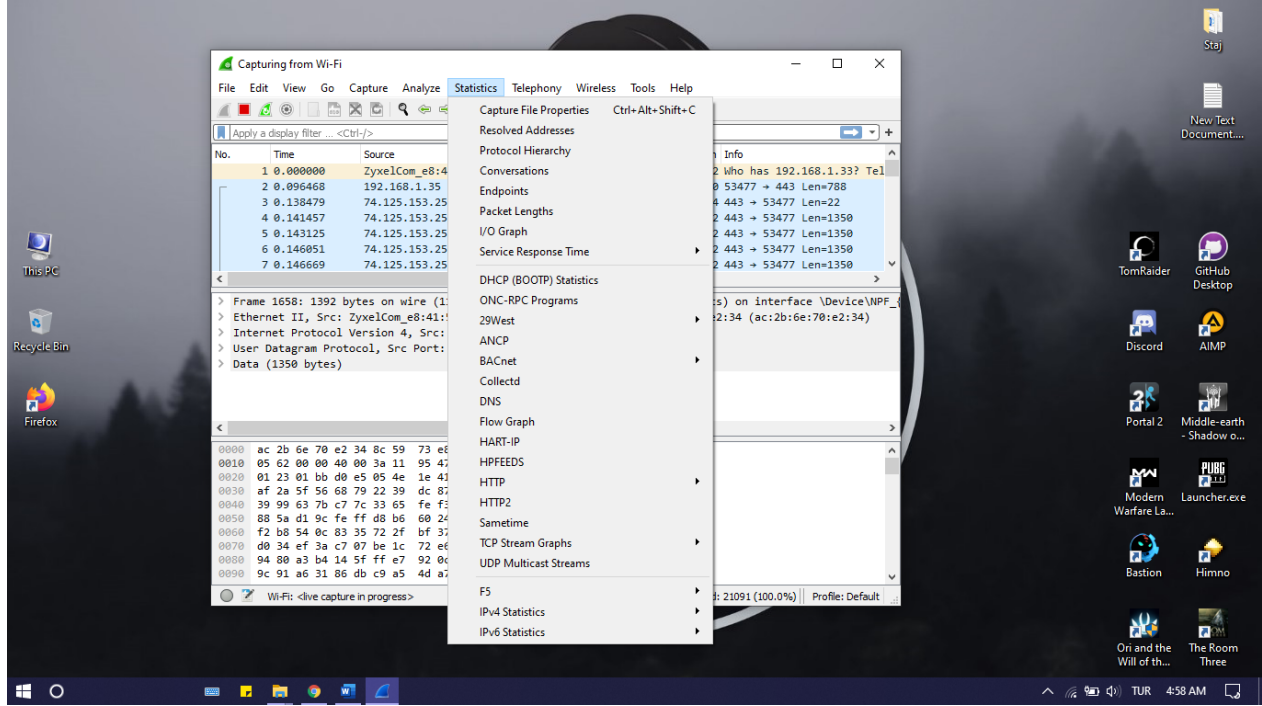
Interfaces: Arayüz bilgisi — soldaki arayüz kayıt defteri tanımlayıcısı, yakalama filtresi “Açık-Kapalı”, arayüz tipi ve paket boyutu sınırı

Statistics: Yakalanan ve görüntülenen paketler dahil genel yakalama istatistikleri.

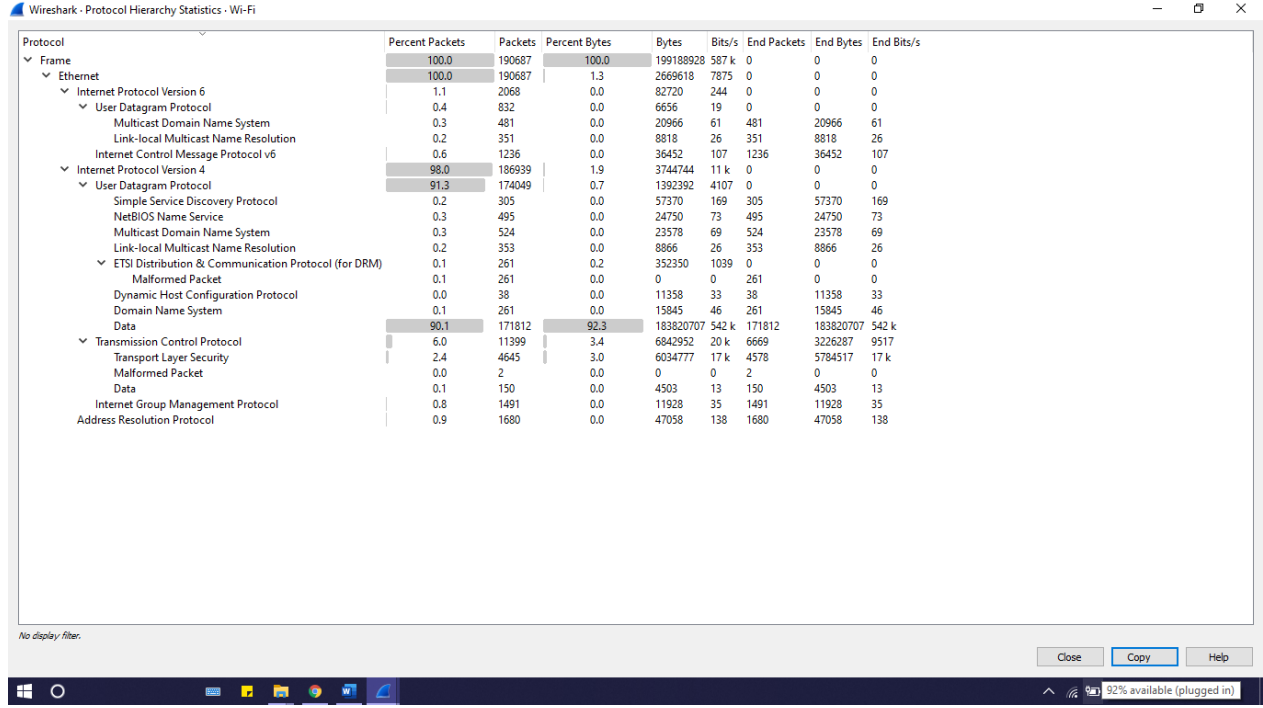
Protocol Hierarchy

Burada karşımıza gelecek olan veriler, yakalanan dosyadaki protokol dağılımı hakkındaki verilerdir. Yakalanan verilerin protokol dağıtımını göreceğiz.

Menü içindeki “Protocol Hierarchy” sekmesini seçerek ulaşabiliriz.



Burada, protokol bazında yakalanan paketlerin istatistiklerini görebiliriz.



Wireshark - Protocol Hierarchy Statistics - Wi-Fi

| Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes | End Bits/s |
|--|-----------------|---------|---------------|-----------|--------|-------------|-----------|------------|
| Frame | 100.0 | 190687 | 100.0 | 199188928 | 587 k | 0 | 0 | 0 |
| Ethernet | 100.0 | 190687 | 1.3 | 2669618 | 7875 | 0 | 0 | 0 |
| Internet Protocol Version 6 | 1.1 | 2068 | 0.0 | 82720 | 244 | 0 | 0 | 0 |
| User Datagram Protocol | 0.4 | 832 | 0.0 | 6656 | 19 | 0 | 0 | 0 |
| Multicast Domain Name System | 0.3 | 481 | 0.0 | 20966 | 61 | 481 | 20966 | 61 |
| Link-local Multicast Name Resolution | 0.2 | 351 | 0.0 | 8818 | 26 | 351 | 8818 | 26 |
| Internet Control Message Protocol v6 | 0.6 | 1236 | 0.0 | 36452 | 107 | 1236 | 36452 | 107 |
| Internet Protocol Version 4 | 98.0 | 186939 | 1.9 | 3744744 | 11 k | 0 | 0 | 0 |
| User Datagram Protocol | 91.3 | 174049 | 0.7 | 1392392 | 4107 | 0 | 0 | 0 |
| Simple Service Discovery Protocol | 0.2 | 305 | 0.0 | 57370 | 169 | 305 | 57370 | 169 |
| NetBIOS Name Service | 0.3 | 495 | 0.0 | 24750 | 73 | 495 | 24750 | 73 |
| Multicast Domain Name System | 0.3 | 524 | 0.0 | 23578 | 69 | 524 | 23578 | 69 |
| Link-local Multicast Name Resolution | 0.2 | 353 | 0.0 | 8866 | 26 | 353 | 8866 | 26 |
| ETSI Distribution & Communication Protocol (for DRM) | 0.1 | 261 | 0.2 | 352350 | 1039 | 0 | 0 | 0 |
| Malformed Packet | 0.1 | 261 | 0.0 | 0 | 0 | 261 | 0 | 0 |
| Dynamic Host Configuration Protocol | 0.0 | 38 | 0.0 | 11358 | 33 | 38 | 11358 | 33 |
| Domain Name System | 0.1 | 261 | 0.0 | 15845 | 46 | 261 | 15845 | 46 |
| Data | 90.1 | 171812 | 92.3 | 183820707 | 542 k | 171812 | 183820707 | 542 k |
| Transmission Control Protocol | 6.0 | 11399 | 3.4 | 6842952 | 20 k | 6669 | 3226287 | 9517 |
| Transport Layer Security | 2.4 | 4645 | 3.0 | 6034777 | 17 k | 4578 | 5784517 | 17 k |
| Malformed Packet | 0.0 | 2 | 0.0 | 0 | 0 | 2 | 0 | 0 |
| Data | 0.1 | 150 | 0.0 | 4503 | 13 | 150 | 4503 | 13 |
| Internet Group Management Protocol | 0.8 | 1491 | 0.0 | 11928 | 35 | 1491 | 11928 | 35 |
| Address Resolution Protocol | 0.9 | 1680 | 0.0 | 47058 | 138 | 1680 | 47058 | 138 |

No display filter.

Close Copy Help

92% available (plugged in)

Açılan pencere içerisindeki başlıkları inceleyecek olursak kısaca şu şekilde olacaktır,

Protocol: Protokol adı.

Percent Packets: Toplam yakalanan paketlerden protokol paketlerinin yüzdesi.

Packets: Toplam yakalanan paketlerden protokol paketi sayısı

Percent Bytes: Toplam yakalanan paketlerden protokol bayt yüzdesi

Bytes: Toplam yakalanan paketlerin protokol baytlarının sayısı

Bit/s: Yakalama süresine göre bu protokolün bant genişliği

End Packets: Bu protokolün mutlak paket sayısı (kod çözme dosyasındaki en yüksek protokol için)

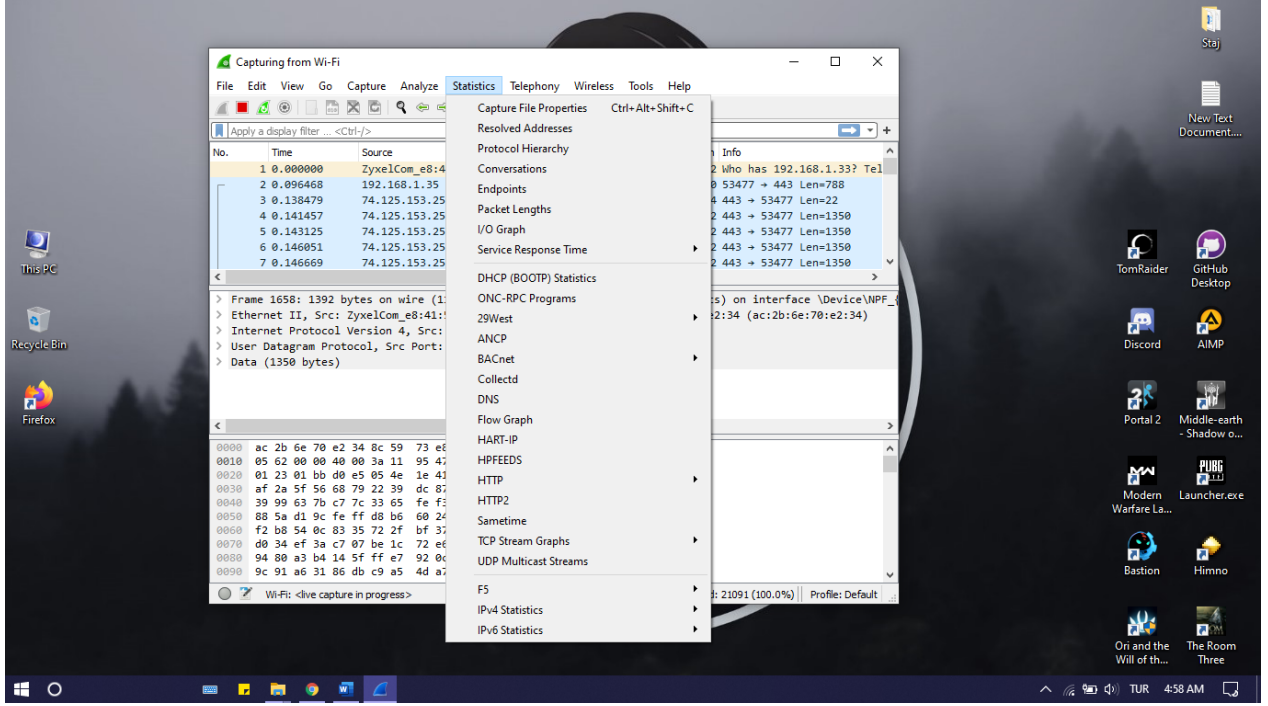
End Bytes: Bu protokolün mutlak bayt sayısı (kod çözme dosyasındaki en yüksek protokol için)

End Bit/s: Yakalama paketlerine ve zamana göre bu protokolün bant genişliği (kod çözme dosyasındaki en yüksek protokol için)

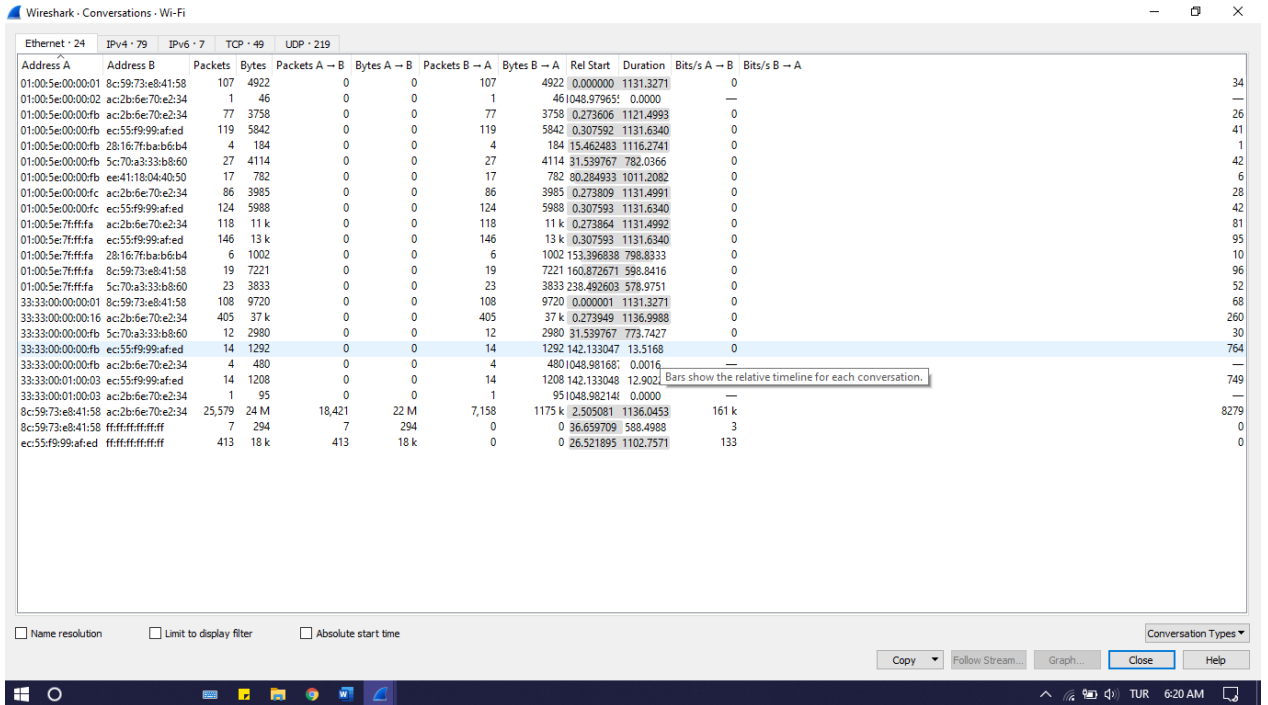
Son sütunlar, protokol paketindeki son protokol olduğunda (yani, protokol çerçevesinin sonuna geldiğinde) sayar. Bunlar, üst katman protokollerini taşıyan, yükü olmayan TCP paketleri (örneğin, SYN paketleri) olabilir. Bu nedenle Ethernet, IPv4 ve UDP uç paketleri için sıfır sayısını görüyorsunuz; bu protokollerin çerçevedeki son protokol olduğu çerçeveler yoktur.

Conversations

Bu bölümde, ağ üzerinden çalışan verilerin konuşma bilgilerini nasıl alacağımızı öğreneceğiz.



Burada “conversations” sekmesini tıklayarak ulaşabiliriz.



Bir ağ görüşmesi, iki belirli uç nokta arasındaki trafiktir. Örneğin, IP görüşmesi iki IP adresi arasındaki tüm trafiktir ve TCP görüşmeleri tüm TCP bağlantılarını sunar.

Yukarıda resimde görüldüğü gibi bizi bu pencerede

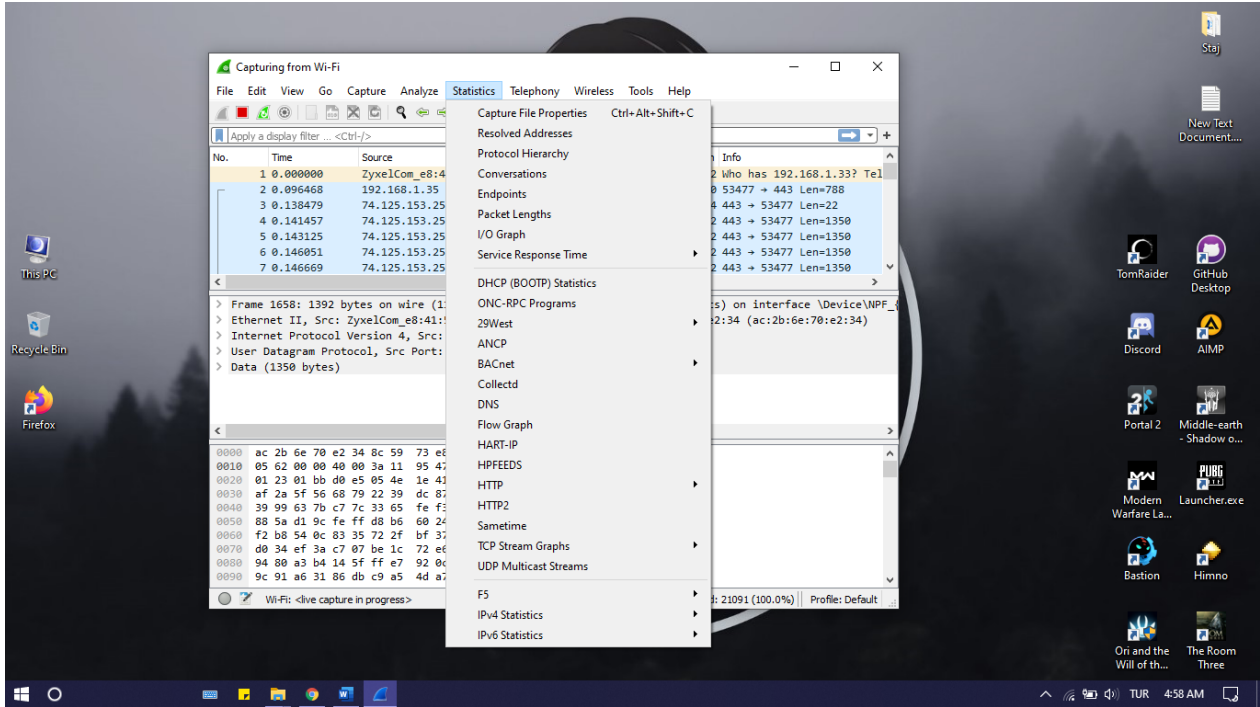
Ethernet istatistikleri, IP istatistikleri, TCP veya UDP istatistikleri yer almakta, bu sekmeler arasında geçiş yapılarak istenen veriler inceleyebilirsiniz.

(Ethernet): Yayın akışlarını bulmak ve izole etmek için kullanılır.

(TCP/IP): İnternet yönlendirici bağlantı noktasına paralel olarak bağlanmak ve hattı ISS'ye kimin yüklediğini kontrol etmek için kullanılır.

Endpoints

Bu bölümde, yakalanan verilerin uç nokta istatistik bilgilerini nasıl alacağımızı öğreneceğiz.



Burada “endpoints” sekmesini tıklayarak ulaşabiliriz.

| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | Country | City | AS Number | AS Organization |
|-----------------|---------|--------|------------|----------|------------|----------|---------|------|-----------|-----------------|
| 13.107.3.254 | 30 | 3764 | 15 | 1848 | 15 | 1916 | — | — | — | — |
| 13.107.18.11 | 40 | 14 k | 22 | 7702 | 18 | 7200 | — | — | — | — |
| 13.107.18.254 | 1 | 54 | 1 | 54 | 0 | 0 | — | — | — | — |
| 13.227.223.66 | 53 | 13 k | 31 | 11 k | 22 | 2622 | — | — | — | — |
| 40.90.23.154 | 48 | 25 k | 25 | 18 k | 23 | 6927 | — | — | — | — |
| 51.11.168.232 | 44 | 12 k | 20 | 9150 | 24 | 3337 | — | — | — | — |
| 51.105.249.228 | 21 | 3038 | 7 | 1575 | 14 | 1463 | — | — | — | — |
| 51.141.33.202 | 1 | 54 | 1 | 54 | 0 | 0 | — | — | — | — |
| 52.109.8.21 | 17 | 8623 | 9 | 7065 | 8 | 1558 | — | — | — | — |
| 52.109.32.23 | 52 | 30 k | 24 | 15 k | 28 | 14 k | — | — | — | — |
| 52.109.68.21 | 78 | 45 k | 36 | 23 k | 42 | 21 k | — | — | — | — |
| 52.114.132.23 | 28 | 11 k | 11 | 7114 | 17 | 4012 | — | — | — | — |
| 52.218.112.184 | 75 | 23 k | 41 | 16 k | 34 | 6578 | — | — | — | — |
| 52.222.141.11 | 39 | 9860 | 21 | 7673 | 18 | 2187 | — | — | — | — |
| 52.222.141.42 | 1,008 | 869 k | 613 | 840 k | 395 | 28 k | — | — | — | — |
| 52.222.141.128 | 62 | 17 k | 34 | 14 k | 28 | 3333 | — | — | — | — |
| 54.192.86.118 | 1,488 | 1290 k | 874 | 1245 k | 614 | 45 k | — | — | — | — |
| 74.125.11.74 | 4,745 | 5652 k | 4,046 | 5583 k | 699 | 69 k | — | — | — | — |
| 74.125.13.41 | 6,617 | 7710 k | 5,496 | 7611 k | 1,121 | 98 k | — | — | — | — |
| 74.125.153.43 | 7,281 | 8152 k | 5,790 | 8003 k | 1,491 | 148 k | — | — | — | — |
| 74.125.154.73 | 22,250 | 24 M | 17,646 | 24 M | 4,604 | 403 k | — | — | — | — |
| 74.125.154.104 | 1,447 | 1748 k | 1,253 | 1722 k | 194 | 26 k | — | — | — | — |
| 104.16.133.229 | 116 | 74 k | 69 | 70 k | 47 | 3808 | — | — | — | — |
| 104.22.1.175 | 54 | 41 k | 42 | 38 k | 12 | 2776 | — | — | — | — |
| 104.26.11.240 | 982 | 540 k | 600 | 509 k | 382 | 31 k | — | — | — | — |
| 104.73.62.206 | 296 | 214 k | 168 | 205 k | 128 | 9882 | — | — | — | — |
| 104.90.105.29 | 72 | 33 k | 41 | 29 k | 31 | 3583 | — | — | — | — |
| 104.90.149.226 | 1,260 | 1131 k | 756 | 1099 k | 504 | 32 k | — | — | — | — |
| 104.104.185.46 | 71 | 21 k | 37 | 17 k | 34 | 3745 | — | — | — | — |
| 131.253.33.254 | 39 | 10 k | 19 | 8426 | 20 | 2050 | — | — | — | — |
| 151.101.61.140 | 387 | 181 k | 210 | 140 k | 177 | 40 k | — | — | — | — |
| 151.101.241.132 | 79 | 21 k | 41 | 19 k | 38 | 3844 | — | — | — | — |
| 151.101.241.140 | 1,836 | 1547 k | 1,099 | 1494 k | 737 | 52 k | — | — | — | — |
| 151.101.242.109 | 53 | 11 k | 27 | 8533 | 26 | 2618 | — | — | — | — |

Bu pencerede “conversations” bölümünde olduğu gibi Ethernet istatistikleri, IP istatistikleri, TCP veya UDP istatistikleri yer almakta, bu sekmeler arasında geçiş yapılarak istenen veriler inceleyebilirsiniz.

Burada bu bilgisayardaki uç nokta IP adresi ve bağlantı noktası numarası ve bilgisayarınıza gönderilen ve gönderilen toplam paketler ve bayt sayısı gibi istatistiksel veriler mevcut.

IO Graph

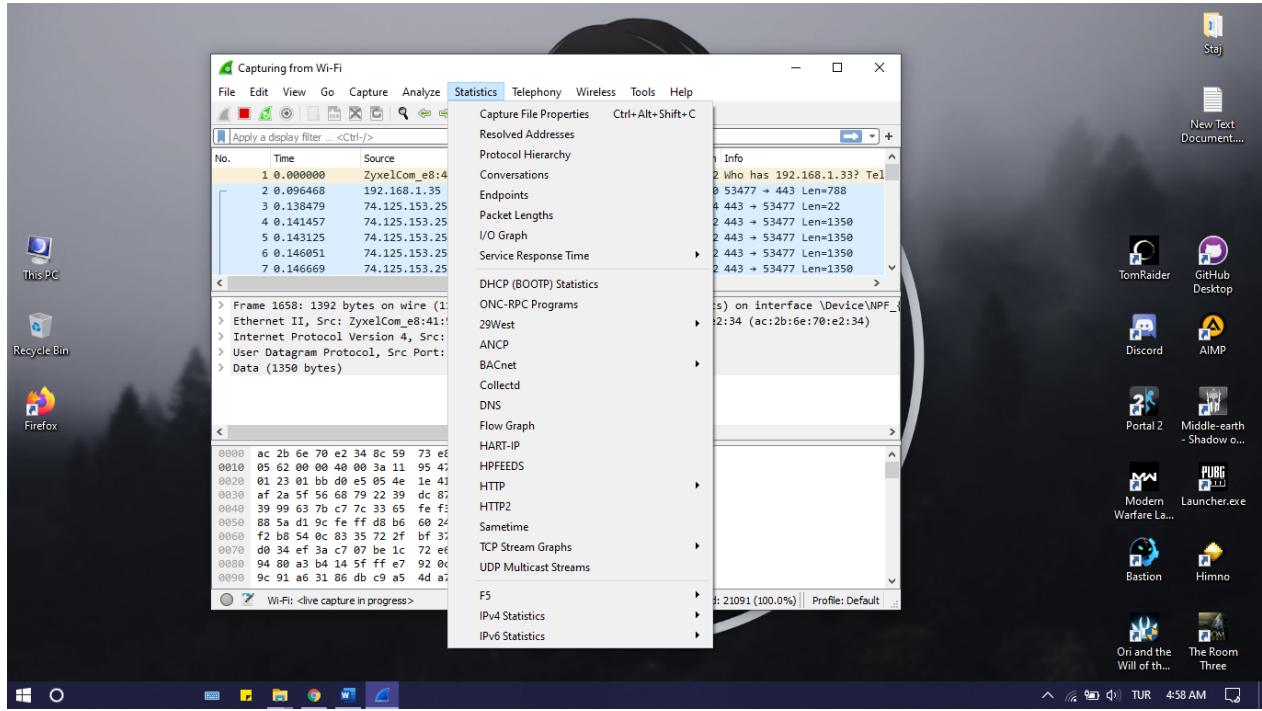
IO Graph aracı, önceden tanımlanmış herhangi bir filtre için istatistiksel grafikleri görüntülememizi sağlar.

Örneğin, Tek bir IP adresindeki verim,

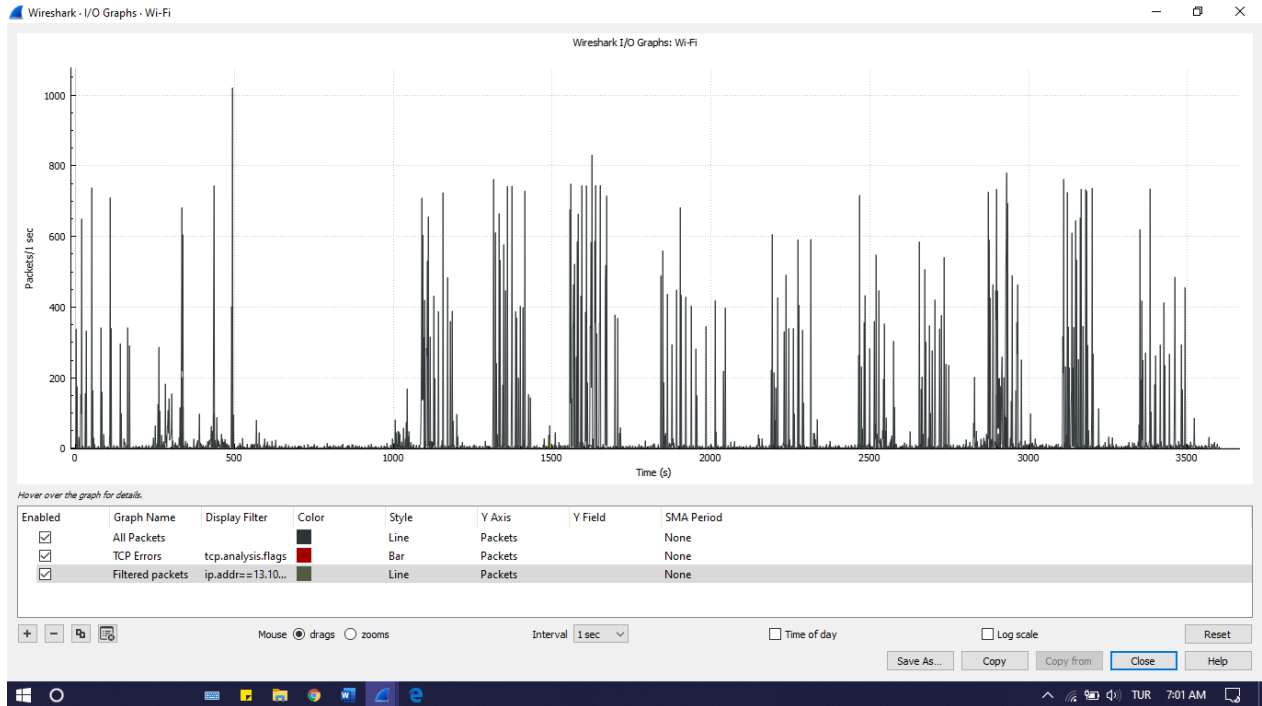
İki veya daha fazla ana bilgisayar arasındaki yükü görebilme,

Uygulama verimliliği,

TCP olayı dağılımı ve daha fazlası.



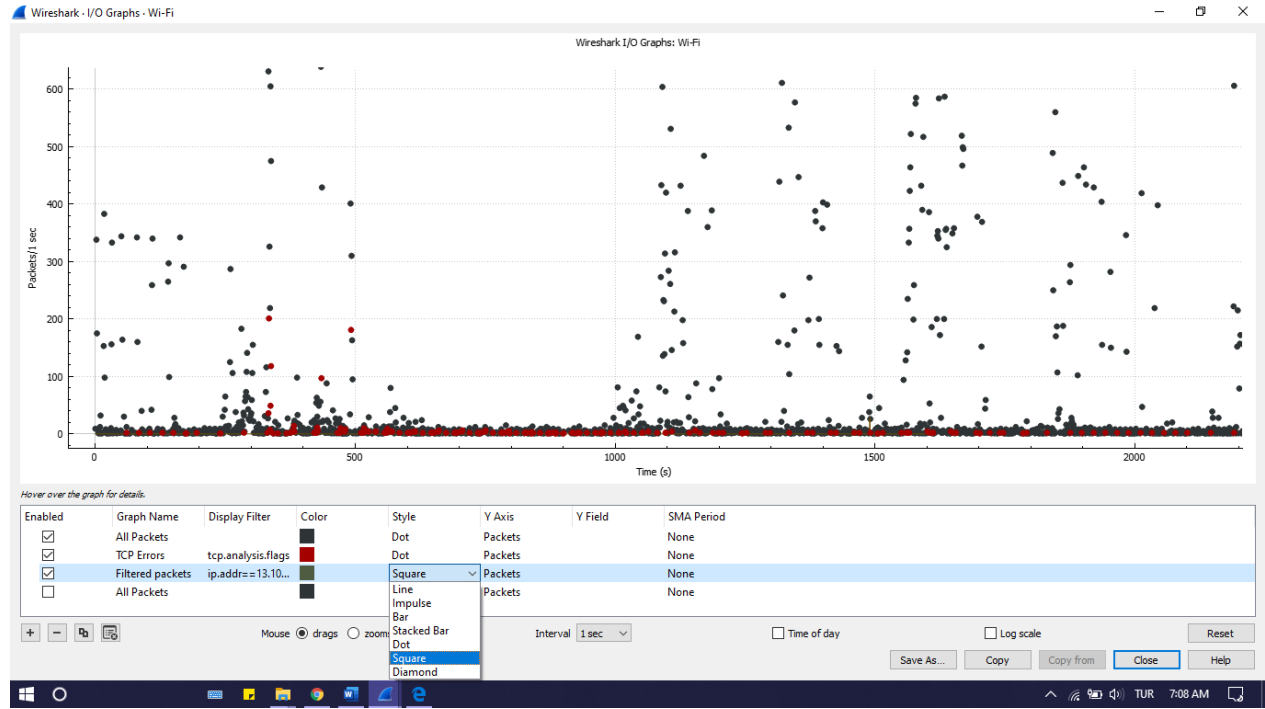
İstatistik menüsü altında, IO Grafiği'ni tıklayarak IO Grafiği aracını açın. Bunu çevrimiçi dosya yakalama sırasında veya daha önce yakaladığınız bir dosyada yapabilirsiniz. IO Graph aracını canlı bir yakalamada kullanırken, yakalanan veriler hakkında canlı istatistikler elde edersiniz. Burada 1 saniyede kaç paket yakalandığını görebiliriz.



Alt kısımda grafik verilerinin nerden geldiğini görebiliyoruz ve aktif veya pasif durumda bırakabiliyoruz. Aynı alanda yer alan “Style” bölümü ile grafik verilerinin ne şekilde gösterileceğini seçebilirsiniz sadece üstüne tıklamanız yeterli.

Hemen “Style” yan tarafında bulunan “Y Axis” ile grafik üzerinde gösterilen verinin kaynağını yani türünü ve biçimini değiştirebilirsiniz.

Örneğin;



Interval seçeneği ile grafiğin yapılandırma aralığını belirleyebiliyoruz. Ölçek 0.001 saniye ile 10 dakika arasında olabilir.

Yine alt tarafta yer alan “Time of Day” ile grafik içerisinde zamansal olarak bilgi gösterilecektir.