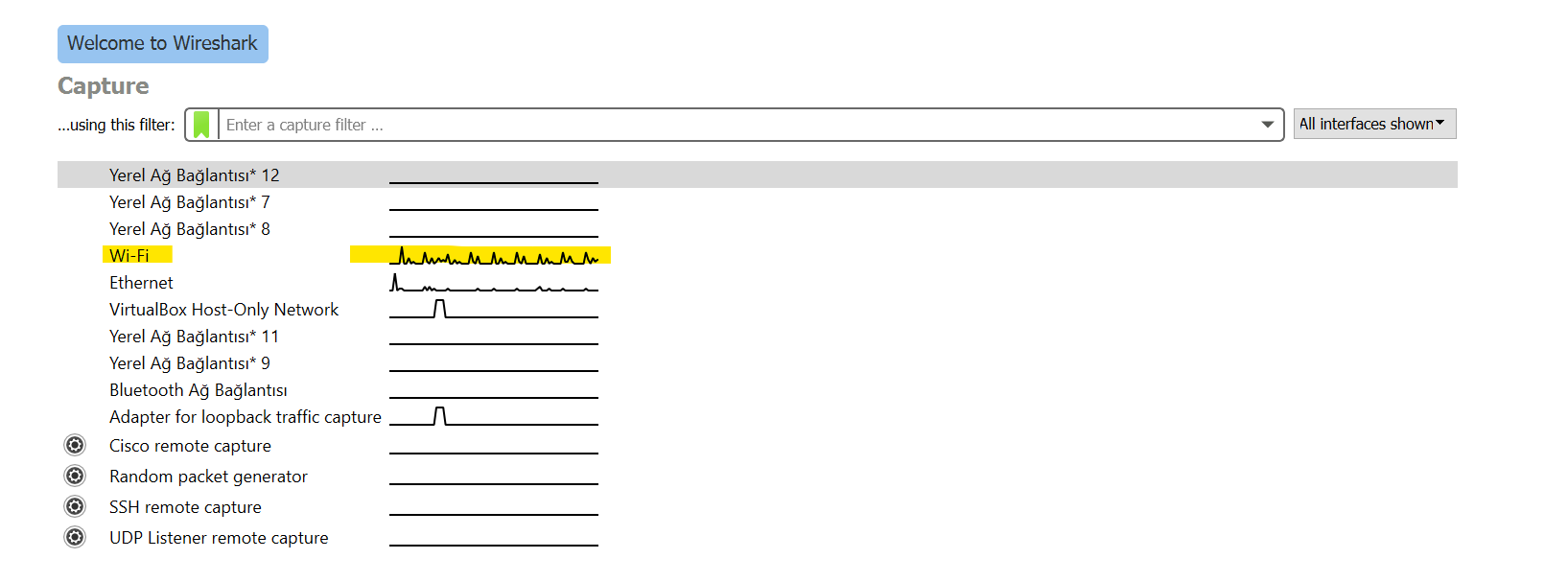
## WİRESHARK İLE PAKET YAKALAMA

Wireshark programını başlattığınızda karşınıza bilgisayarınızdaki ağ bağlantılarının da listelendiği bir hoş geldiniz ekranı gelir. Canlı trafiğin olduğu ağ bağlantılarında EKG grafiklerine benzer çizgiler görünür.

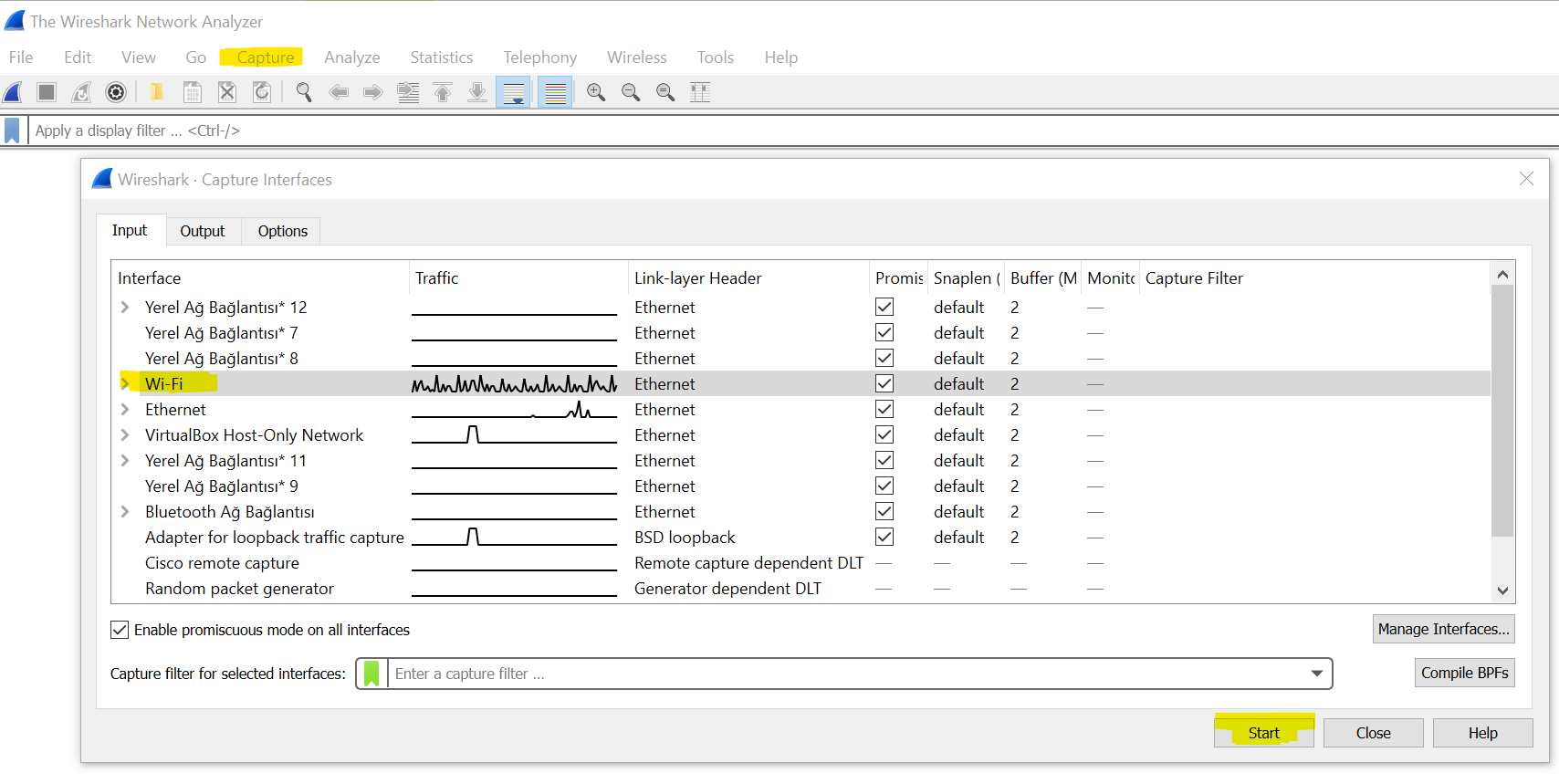
[](https://www.siberguvenlik.web.tr/wp-content/uploads/2020/03/welcome.png)

Wireshark ile paketleri yakalamaya başlamak için birkaç yöntem vardır. İsterseniz ilgili ağ kartının üzerine çift tıklayarak yakalama işlemini başlatabilirsiniz.

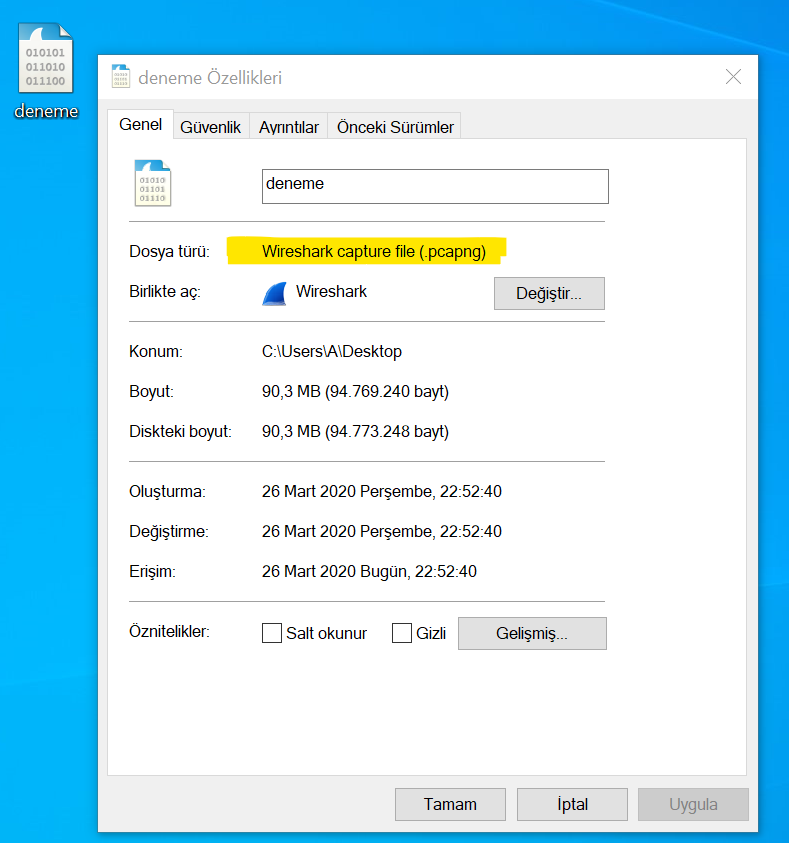
Ya da ağ kartı üzerinde sağ tıklayıp start capture’a tıklayarak ta yakalama işlemini başlatabilirsiniz. Son olarak ağ kartını seçip yukarıdaki menüden  Capture seçeneğine tıklayıp ardından Start’a tıklayarak (Kısa yol tuşu CTRL+E) ile de yakalama işlemini başlatabilirsiniz.

*Birden fazla ağ kartını Shift tuşu ile birlikte seçerek aynı anda birden fazla ağ kartından geçen trafiği yakalayabilirisiniz.*

Ayrıca Capture/Option menüsünden açılan pencerede ilgili ağ kartını seçip start düğmesine tıklayarak başka bir şekilde de paket yakalayabilirsiniz.

[](https://www.siberguvenlik.web.tr/wp-content/uploads/2020/03/start.png)

Yakalanan Paketleri kaydetmek için öncelikle işlemi durdurmamız gerekir. Bunun için Ctrl+E kısa yol tuşuna basabilir ya da Capture/Stop menüsünü kullanabiliriz. Ayrıca menü ekranındaki kırmızı stop düğmesine de basabiliriz. Sonrasında File/Save menüsünden belirlediğimiz klasöre dosya ismi vererek pcapng uzantısı ile yakalanan paketleri kayıt edebiliriz.

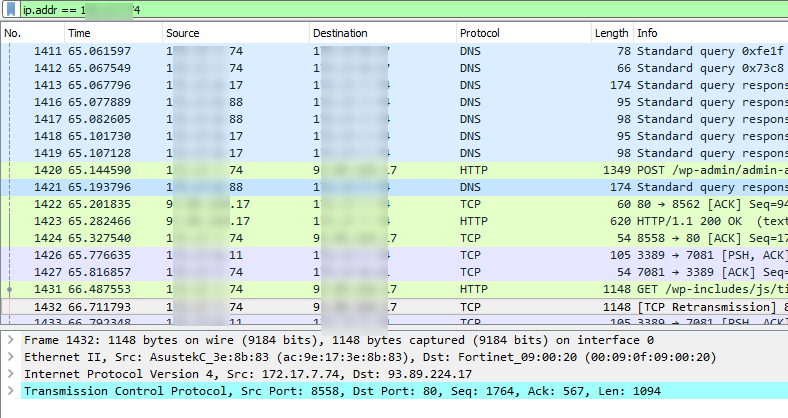
[](https://www.siberguvenlik.web.tr/wp-content/uploads/2020/03/kayit.png)

Filtreleme: Wireshark, filtreler kullanarak tüm bu rastgele canlı verileri dilimleme ve küp şeklinde doğrama yeteneğine sahiptir. Bir filtre uygulayarak, yalnızca görmeniz gereken bilgileri elde edebilirsiniz.

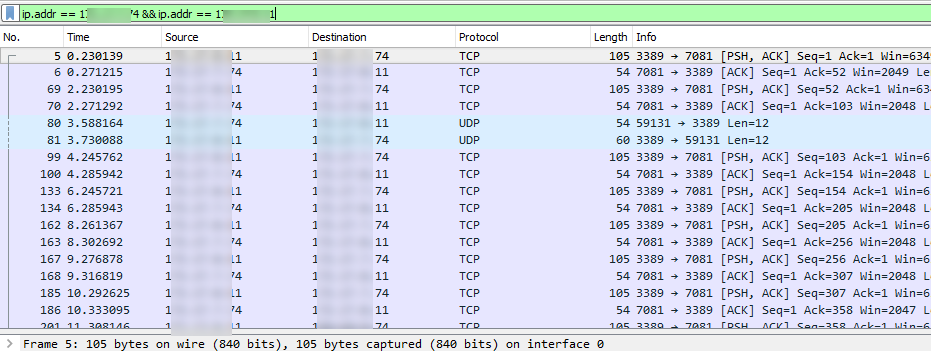
**10 Wireshark Filtresi**

1. **ip.addr == 192.168.1.1**

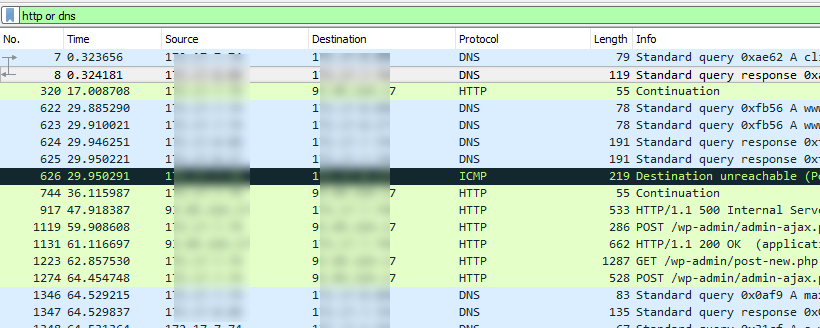
Bu filtreleme gerek kaynak gerekse hedef ip adresinde 192.168.1.1 olan tüm satırları filtreler.

[](http://www.astronur.com/wp-content/uploads/2018/06/kullanisli-wireshark-filtreleri-1.png)

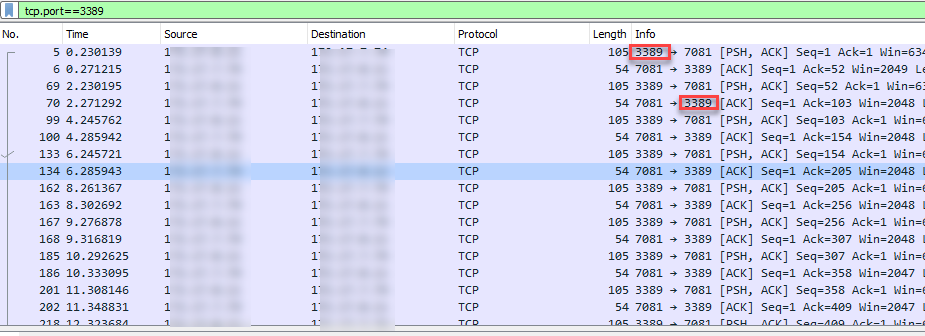
1. **ip.addr==192.168.1.1 && ip.addr==192.168.1.55**  
   Bu filtreleme ile iki ip adresi arasındaki konuşmayı filtreleyebilirsiniz.

[](http://www.astronur.com/wp-content/uploads/2018/06/kullanisli-wireshark-filtreleri-2.png)

1. **http** **or** **dns**  
   Bu filtreleme ile ip kısıtı olmaksızın sadece http ve dns protokolleir ile ilgili streamleri filtreleyebilirsiniz.

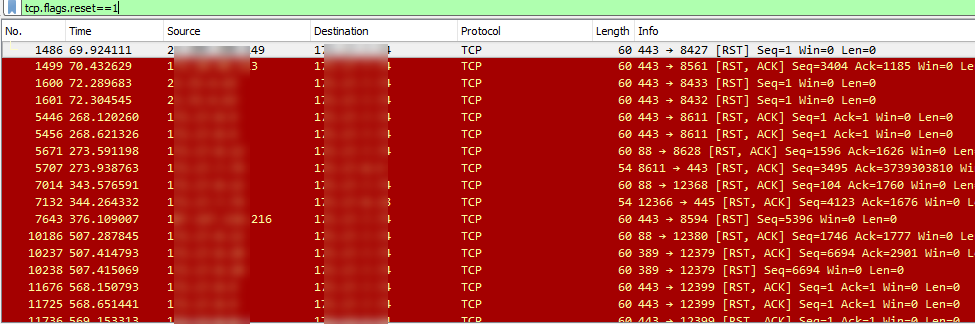
[](http://www.astronur.com/wp-content/uploads/2018/06/kullanisli-wireshark-filtreleri-3.png)

1. **tcp.port==3389**  
   Bu filtre ile ip kısıtı olmaksızın TCP/3389portu ile ilgili tüm stream leri filtreleyebilirsiniz. Burada 3389 değerini izleyeceğiniz port ile değiştirmeniz gerek

[](http://www.astronur.com/wp-content/uploads/2018/06/kullanisli-wireshark-filtreleri-4.png)

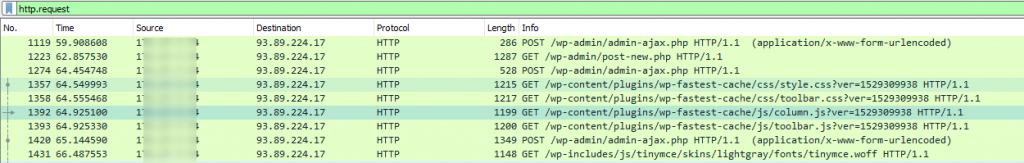
1. **tcp.flags.reset==1**

Bu filtre ile TCP Reset stream lerini filtreleyebilirsiniz.

[](http://www.astronur.com/wp-content/uploads/2018/06/kullanisli-wireshark-filtreleri-5.png)

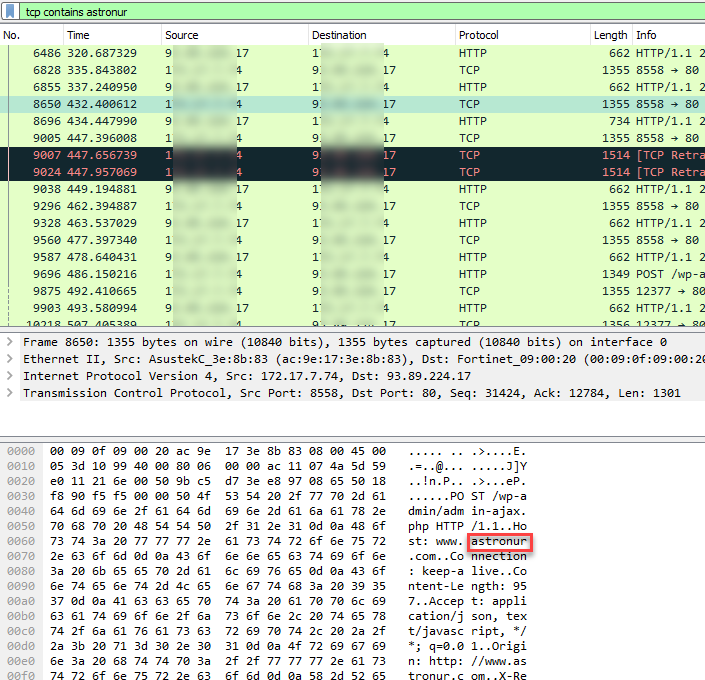
1. **http.request**

Bu filtre ile http GET request lerini filtreleyebilirsiniz.

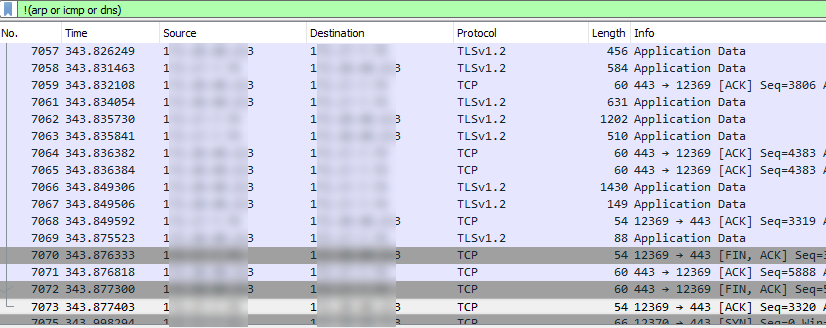
[](http://www.astronur.com/wp-content/uploads/2018/06/kullanisli-wireshark-filtreleri-6.png)

1. **tcp contains traffic**

Bu filtre ile tüm TCP paketlerinin içinde “astronur” ifadesi geçenleri filtreleyebilirsiniz.

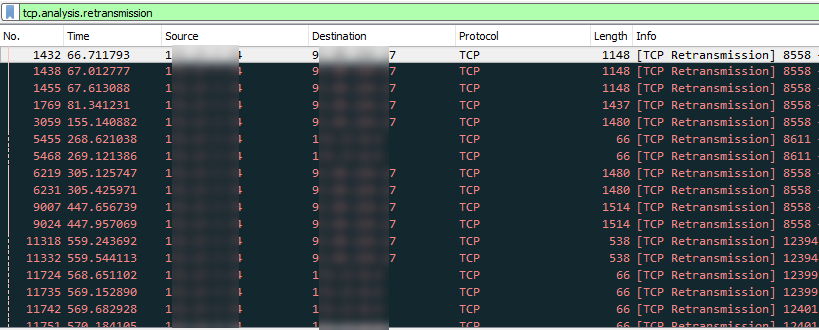
[](http://www.astronur.com/wp-content/uploads/2018/06/kullanisli-wireshark-filtreleri-7.png)

1. **!(arp or icmp or dns)**Bu filtre ile tüm stream lerin arasında aslında ihtiyacımız olmayan ve en çok göreceğimiz ARP, DNS ve ICMP satırlarını filtreleyebilirsiniz. Örneğin Wiresharkı RDP ile bağlandığınız bir sunucuda çalıştırdıysanız bu filtreye RDP yi de ekleyebilirsiniz. Böylece RDP satırlarıda gizlenecektir.

[](http://www.astronur.com/wp-content/uploads/2018/06/kullanisli-wireshark-filtreleri-8.png)

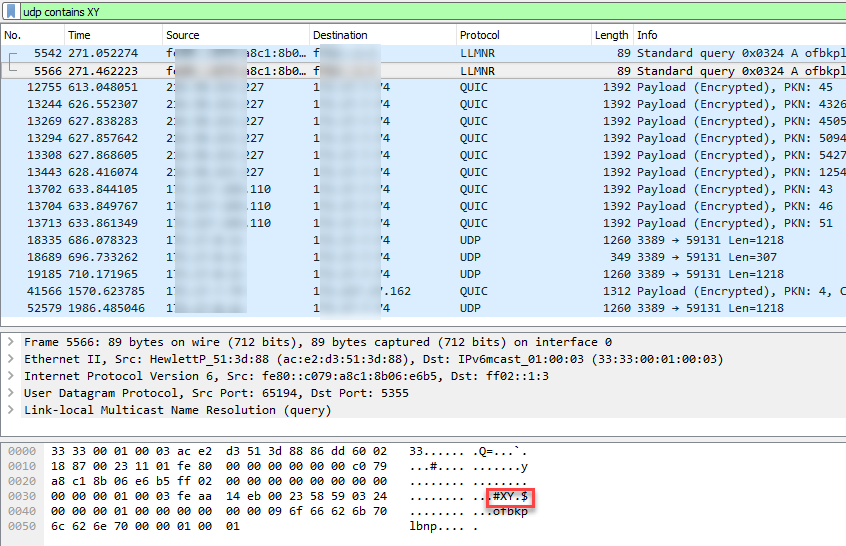
1. **tcp.analysis.retransmission**

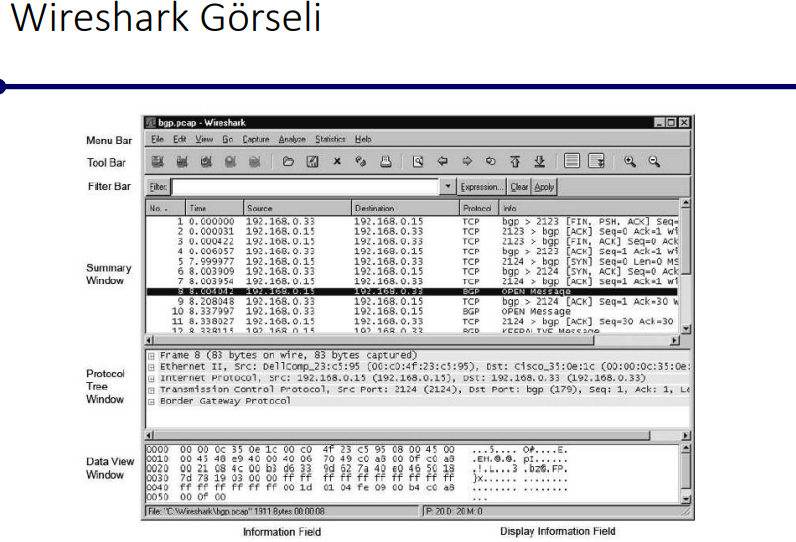
Bu filtre ile TCP ReTransmission stream lerini görebilirsiniz.

[](http://www.astronur.com/wp-content/uploads/2018/06/kullanisli-wireshark-filtreleri-9.png)

1. **udp contains XY**

Bu filtre ile UDP paketinin HEX içeriğinde “XY” geçen stream leri filtreleyebilirsiniz. Buradaki XY değerini ihtiyacınız olan değerler değiştirmeniz gerekmektedir.

[](http://www.astronur.com/wp-content/uploads/2018/06/kullanisli-wireshark-filtreleri-10.png)



**Menu Bar** Menudeki maddelerin, grafiksel ara yüzünü içeren klasik bir uygulamadır.

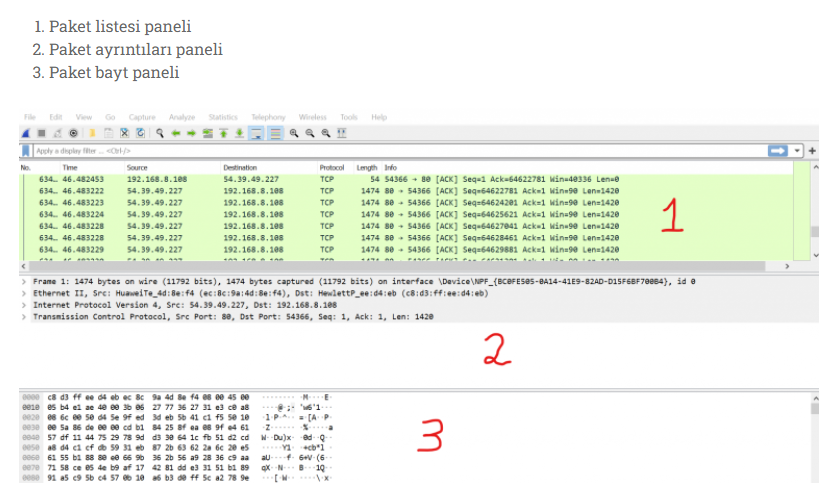
**Tool Bar** Wireshark’ın sık kullanılan fonksiyonlarının kısa yollarını içerir. Kullanıcıya göre ayarlanabilir. Filter Bar Yakalanan paketleri, istenilen sekilde ayrılarak gösterilmesini sağlar.

**Summary Window** Yakalan paketlerin her biri için, bir satırlık özet bilgi sunar.

**Protocol Tree Window** Summary window ’da seçili olan paketin detaylı bilgilerini, kullanıcıların anlayacağı şekilde düzenleyerek sunar.

**Data View Window** Summary Window ‘da seçili olan paketin, detaylı bilgilerini, herhangi bir düzenleme yapmadan sunar.

Display Information Field Yakalanmış paketlerin numaralarını, güncel olarak gösterir.



* **No** : Bu alan, hangi paketlerin aynı görüşmenin parçası olduğunu gösterir. Bir paket seçinceye kadar boş kalır.
* **Time:** Paketin alındığı zaman damgası bu sütunda görüntülenir. Varsayılan biçim, bu belirli yakalama dosyasının ilk oluşturulmasından bu yana geçen saniye sayısıdır.
* **Source:** Bu sütun, paketin kaynaklandığı adresi (IP veya diğer) içerir.
* **Destination:** Bu sütun paketin gönderildiği adresi içerir.
* **Protocol:** Paketin TCP gibi protokol adını bu sütunda bulabilirsiniz.
* **Length:** Paket uzunluğu, bayt cinsinden, bu sütunda görüntülenir.
* **Info:** Paket hakkında ek ayrıntılar burada sunulmaktadır. Bu sütunun içeriği paket içeriğine bağlı olarak büyük ölçüde değişebilir.

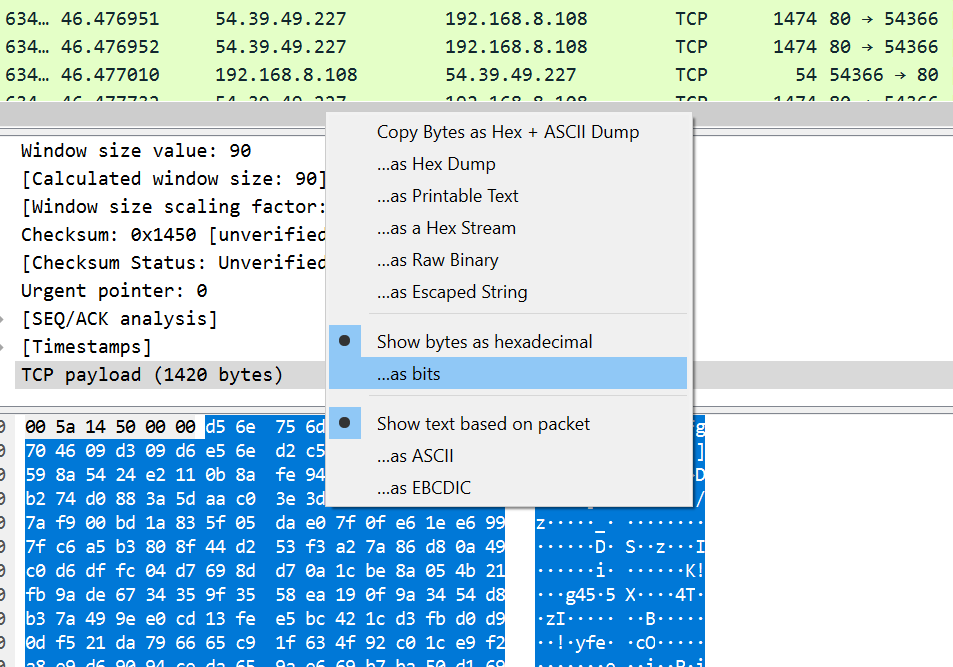
### PAKET DETAYLARI PANELİ

Ortada bulunan ayrıntılar bölmesi, seçilen paketin protokollerini ve protokol alanlarını daraltılabilir bir biçimde sunar. Her seçimi genişletmeye ek olarak, belirli ayrıntılara dayalı olarak ayrı Wireshark filtreleri uygulayabilir ve istenen öğeye sağ tıklayarak protokol türüne göre veri akışlarını takip edebilirsiniz.

### PAKET BAYT PANELİ

Altta, seçilen paketin ham verilerini onaltılık görünümde görüntüleyen paket bayt bölmesi bulunur. Buradaki  veriler hexadecimal  ve text based olarak görüntülenir.

Bu verileri onaltılıdan farklı olarak bit formatında görüntülemek için bölmenin herhangi bir yerine sağ tıklayın ve **bit olarak** seçin .

[](https://www.siberguvenlik.web.tr/wp-content/uploads/2020/03/bits.png)

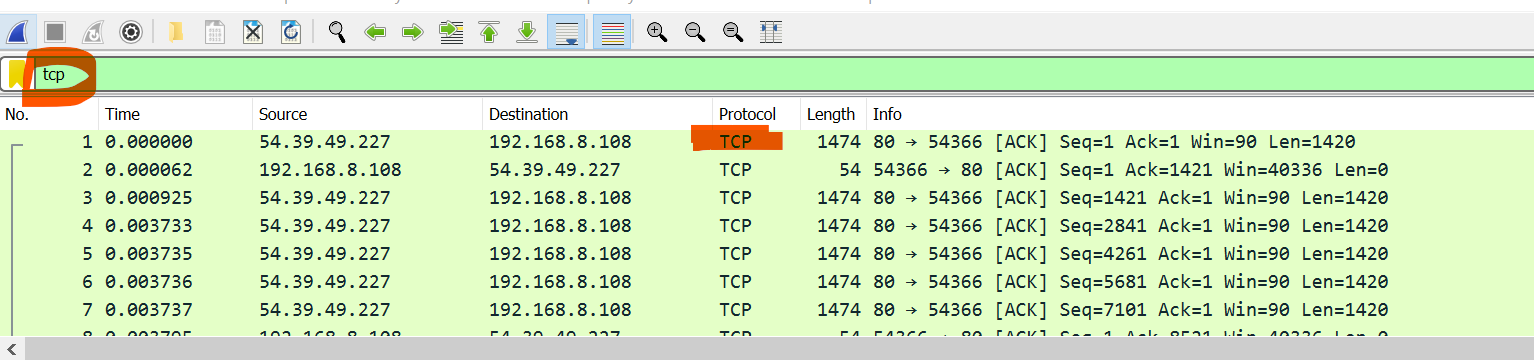
Bu verilerin belirli bir bölümünün seçilmesi, paket ayrıntıları bölmesinde karşılık gelen bölümünü otomatik olarak vurgular ve bunun tersi de geçerlidir. Yazdırılamayan baytlar bir nokta ile gösterilir.

## WİRESHARK FİLTRELERİ NASIL KULLANILIR

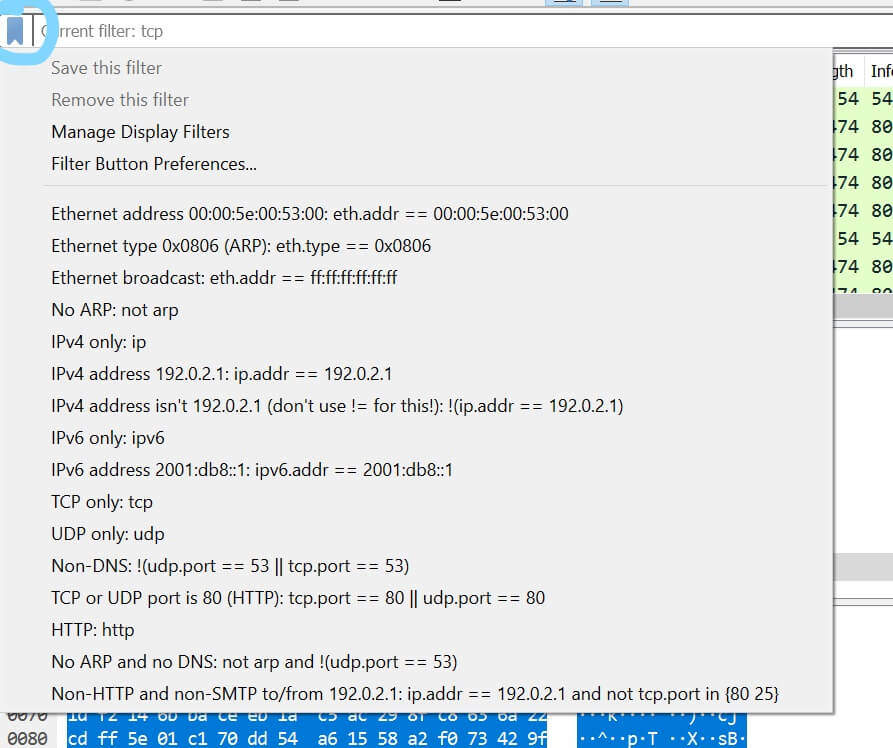
Yakalama filtreleri Wireshark’a yalnızca belirtilen ölçütleri karşılayan paketleri kaydetmesi talimatını verir. Filtreler, yalnızca belirli paketlerin gösterilmesi için oluşturulmuş bir yakalama dosyasına da uygulanabilir. Bunlara ekran filtreleri denir.

Wireshark, varsayılan olarak çok sayıda önceden tanımlanmış filtre sağlar. Bu mevcut filtrelerden birini kullanmak için, adını Wireshark araç çubuğunun altında bulunan **Apply a display filter** giriş alanına veya karşılama ekranının ortasında bulunan **Enter a capture filter** alanına girin .

Örneğin, TCP paketlerini görüntülemek istiyorsanız, **tcp**yazın ve entere basın . Wireshark otomatik tamamlama özelliği, yazmaya başladığınızda önerilen adları gösterir, böylece aradığınız filtre için doğru takma adın bulunmasını kolaylaştırır.

[](https://www.siberguvenlik.web.tr/wp-content/uploads/2020/03/tcpfiltre.png)

Filtre seçmenin bir başka yolu , giriş alanının sol tarafındaki **bookmark** seçmektir . **Filtre** eklemek, kaldırmak veya düzenlemek için **Manage Filter Expressions** veya **Manage Display Filters ‘i** seçin .

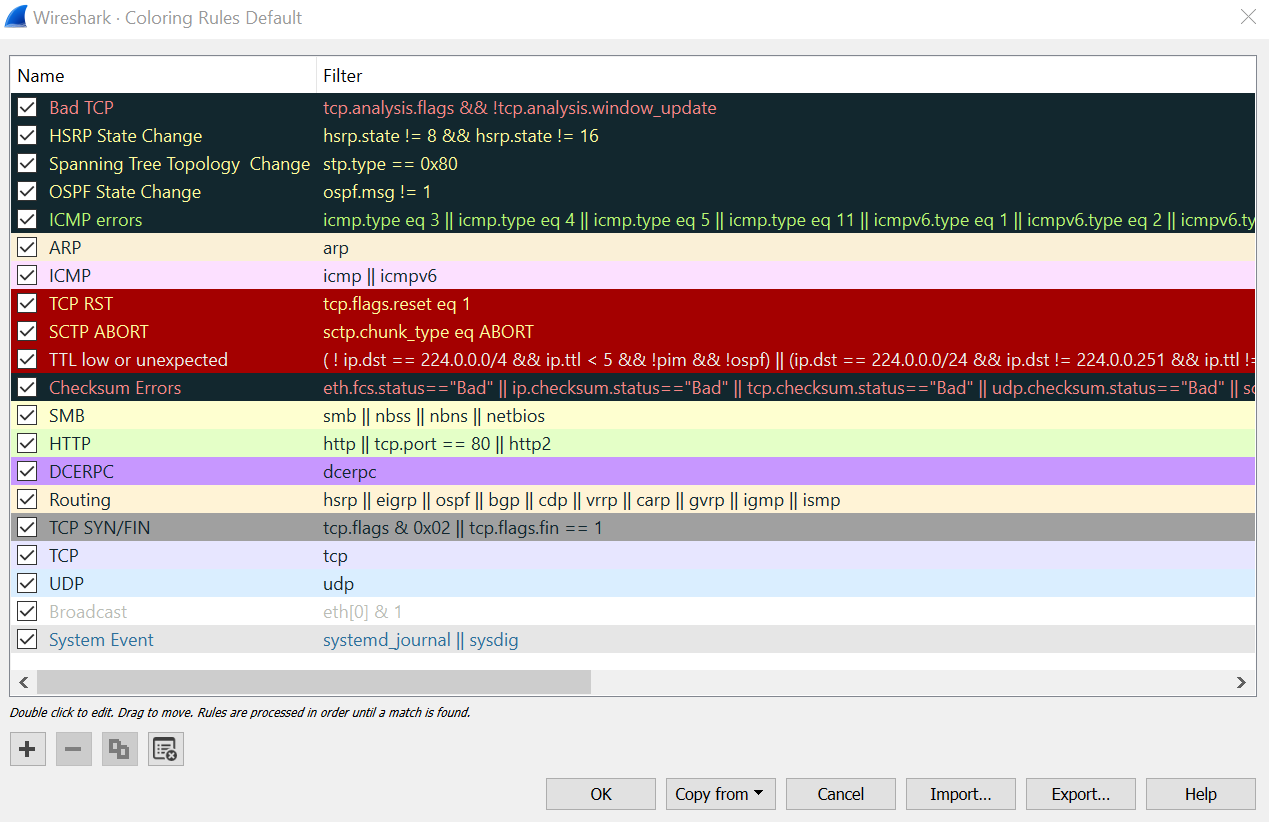
[](https://www.siberguvenlik.web.tr/wp-content/uploads/2020/03/filtre2.jpg)

## WİRESHARK RENK KURALLARI

Wireshark yaklaşık 20 varsayılan renklendirme kuralıyla birlikte gelir, her biri düzenlenebilir, devre dışı bırakılabilir veya silinebilir. Her rengin ne anlama geldiğine genel bakış için **View** > **Coloring Rules** seçin . Ayrıca kendi renk tabanlı filtrelerinizi de ekleyebilirsiniz.

Varsayılan olarak, açık mor TCP trafiğidir, açık mavi UDP trafiğidir ve siyah paketleri hatalı olarak tanımlar – örneğin, düzensiz teslim edilmiş olabilirler.

Yeşil, Mavi ve Siyah renkleri, yakalanan paketlerin türünü ayırt eder. Geleneksel olarak yeşil renk, İletim Denetimi Protokolü (TCP) trafiğini gösterir. Diğer yandan koyu mavi, Ad Sistemi (DNS) trafiğidir, açık mavi ise Kullanıcı Datagram Protokolü (UDP) trafiğini gösterir. Siyah, TCP paketlerini sipariş dışı gibi sorunlarla gösterir.

[](https://www.siberguvenlik.web.tr/wp-content/uploads/2020/03/renkler.png)