# Wireshark - Mustso Final Raporu

## Ders Hakkında:

**Ders:** Bilgi Sistemleri ve Güvenliği [YMH321]

**Danışman:** Doç.Dr.Fatih ÖZKAYNAK

**Fakülte/Bölüm:** Teknoloji Fakültesi/Yazılım Mühendisliği

**Üniversite:** Fırat Üniversitesi/Elazığ

**Github:**
https://github.com/burakd81/bsvg/blob/5c329a2ab0cf42a2fa91cd2bb035b25d4d8caa43/mus_ticaret_sanayi_odasi.pcapng

## Çalışma Ekibi:

| Öğrenci No | Ad ve Soyadı |
|---|---|
| **190541021** | Zeynep DEMİR |
| **175541038** | Ali Fuat KARAASLAN |
| **16541044** | Furkan BAŞAN |
| **185542003** | Burak DEMİRER |
| **190541017** | Rumeysa KOÇAK |
| **175541006** | Osman USLU |
| **185541094** | Alihan EYMİRLİ |
| **16541071** | Hazel OKTAY |
| **15541061** | Hidayet Can ULUBAŞ |
| **175541611** | Mohammad Amin ASLAMI |
| **175541009** | Alihan KOÇ |

## Wireshark Nedir?

Wireshark bir ağ paket analiz aracıdır. Bir ağ paket analiz aracı, yakalanan paketlerin verilerini mümkün olduğunca ayrıntılı sunar. **Wireshark özgür ve açık kaynaklı bir paket çözümleyicisidir.** Ağ sorunlarını giderme, çözümleme, yazılım ve iletişim protokolü geliştirme ve eğitim amaçlı olarak kullanılır.

## Wireshark'ın Özellikleri

Windows,Unix,OS X,Solaris,FreeBSD,NetBSD ve birçok işletim sistemleri için uygundur.

## Wireshark ne için kullanılır?

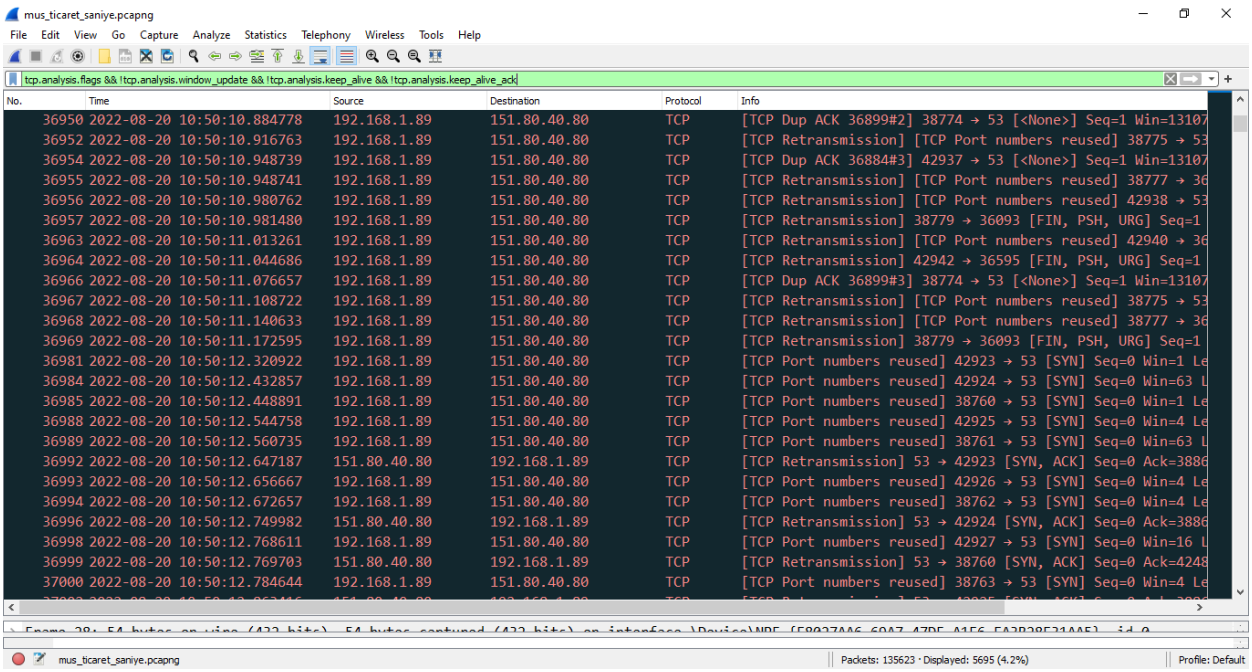
Performans sorunları olan ağlarda sorun giderme de dahil olmak üzere birçok kullanıma sahiptir. Siber güvenlik uzmanları genellikle bağlantıları izlemek, şüpheli ağ işlemlerinin içeriğini görüntülemek ve ağ trafiği patlamalarını belirlemek için bu yazılımı kullanır. Bu yazılım herhangi bir BT uzmanının araç setinin önemli bir parçasıdır.

### 1. Bad TCP (Yakalama)

Varsayılan Wireshark yüklemesi, siyah bir arka plan üzerinde kırmızı metin kullanan "Hatalı TCP" adlı bir renklendirme kuralına sahiptir. Bu renklendirme kuralı "tcp" koşuluyla eşleşir.analiz.bayraklar". Muhtemelen gördüğün şey budur. Kendi başına, bu bilgi muazzam derecede yararlı değildir, çünkü tcp.analiz.bayraklar birkaç farklı TCP koşuluyla eşleşir.

Bunlardan bazıları kendiliğinden kötü değildir ve sorun gidermeye çalıştığınız sorunla doğrudan ilgili olmayabilir.  Aşağıda bir kaç tane (Bad TCP) paketini **mustso'dan** yakaladık.

Bad TCP (Komutu) - **`tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack`**

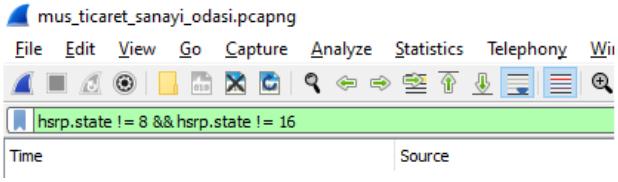



Mustso IP Adresi - 151.80.40.80

**Bad TCP 54** tane taradımız ağ'da bulduk, bunları göremek için github linkin'den ulaşabilirsiniz.

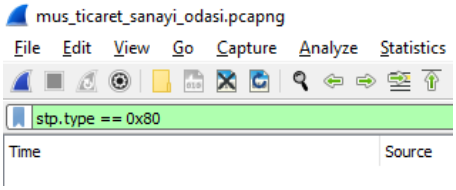
### 2. HSRP State Change (Hot Standby Redundancy Protocol)

HSRP paketini **mustso'dan** her hangi bir ağ veya problem yakalamadık. Yani HSRP ile ilgili her hangi bir düzenleme gerek yoktur.




### 3. Spanning Tree Topology Change (STP)

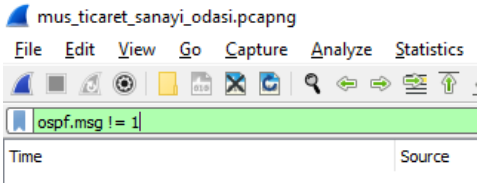
STP paketini **mustso'dan** her hangi bir ağ veya problem yakalamadık. Yani STP ile ilgili herhangi bir düzenleme gerek yoktur.




### 4. OSPF State Change (open shortest path first)

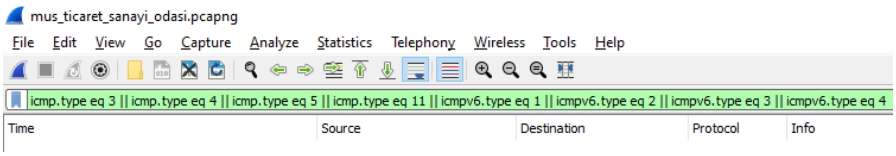
dinamik bir yönlendirme protokolüdür. Bir iç ağ geçidi protokolüdür (IGP). Yönlendiriciler, yönetici müdahalesine gerek kalmadan rotaları otomatik olarak öğrenmek için kullanır.

OSPF ile ilgili herhangi bir düzenleme gerek yoktur.




### 5. ICMP errors

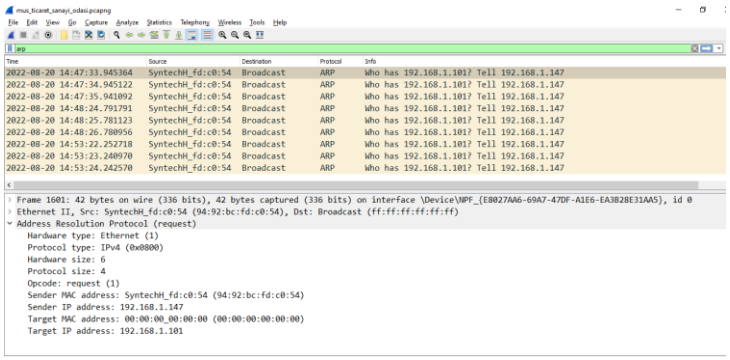
ICMP'deki hata verileri iki değerde taşınır: type ve code. Bir ICMP paketinin tipi, mesajın iletmeyi amaçladığı genel mesajı içerir. **Örneğin, 3 türündeki bir değer, amaçlanan varış noktasına ulaşılamadığı anlamına gelir,** ama bize herhangi ağ tarfını vermedi için düzgün çalıştını bize göstermektedir.



## 6. ARP (Address Resulation Protocol)

Adres Çözümleme Protokolü, katman 3 (protokol) ve katman 2 (donanım) adresi arasındaki eşlemeyi dinamik olarak keşfetmek için kullanılır. Tipik bir kullanım, bir IP adresinin (ör. 192.168.0.10) temel Ethernet adresine (ör. 01:02:03:04:05:06) eşlenmesidir. ARP bu adreslerin keşfedilme şekli olduğundan, genellikle bir konuşmanın başında ARP paketlerini görürsünüz.

Aşağıda 9 tane (ARP) paketini **mustso'dan** yakaladık. ARP bizim için önemli bir bilgidir.



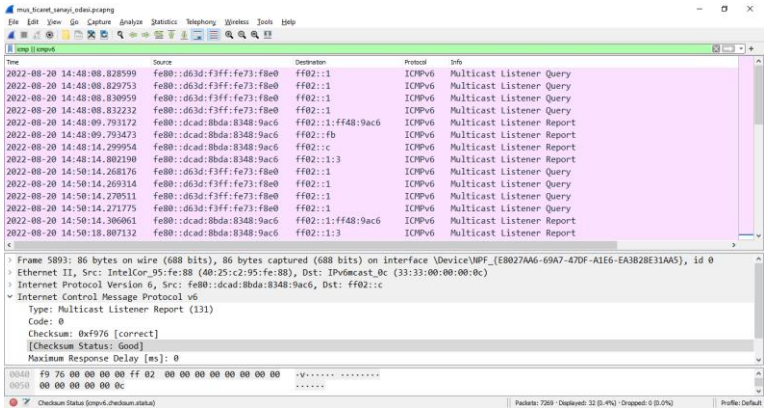

## 7. ICMP (Internet Control Message Protocol)

ICMP trafiği esas olarak hata mesajlarını taşımaya yöneliktir, bu nedenle ağdaki herhangi bir ICMP trafiği ilgi çekici olabilir. Ancak ICMP, bir saldırgan tarafından kasıtlı olarak kötüye kullanılabilir ve tarama ve veri hırsızlığı için kullanılabilir.

[Checksum Status: **Good**]

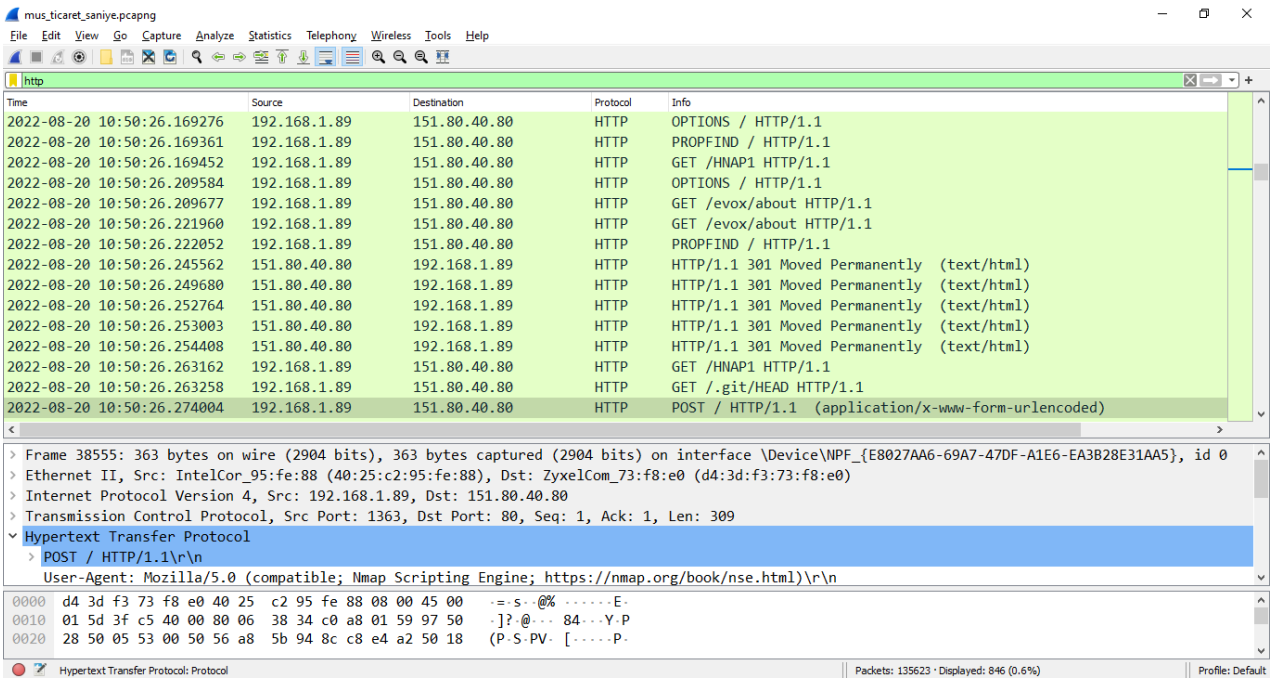
> Birkaç ağ protokolü, veri bütünlüğünü sağlamak için sağlama toplamları kullanır. Burada açıklandığı gibi sağlama toplamlarının uygulanması, artıklık denetimi olarak da bilinir.

**[Good]**, durumu iyi olduğu için bu bilgileri saldırgan kötü amaçlı olarak kullanılamıyor.



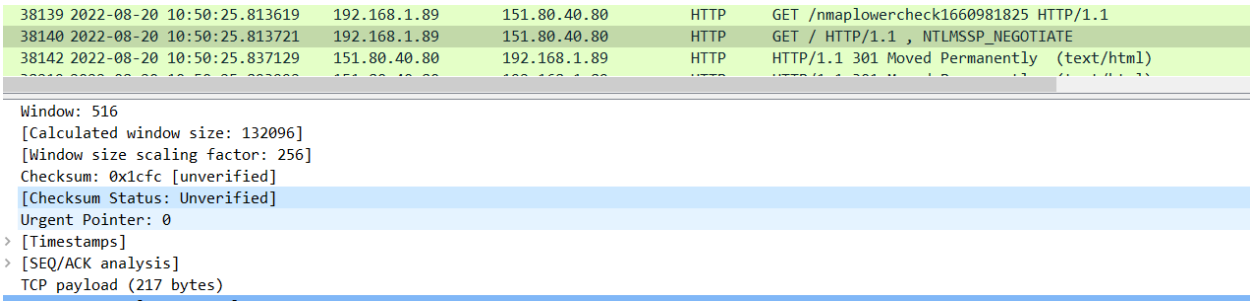

| | | |
|---|---|---|
| 8. TCP RST | 9. SCTP ABORT | 10. TLL low or unexpected |
| 11. Checksum Errors | 12. SMB | **8 - 12'ye kadar bir şey yakalamadık.** |

## 12. HTTP (Hypertext Transfer Protocol)

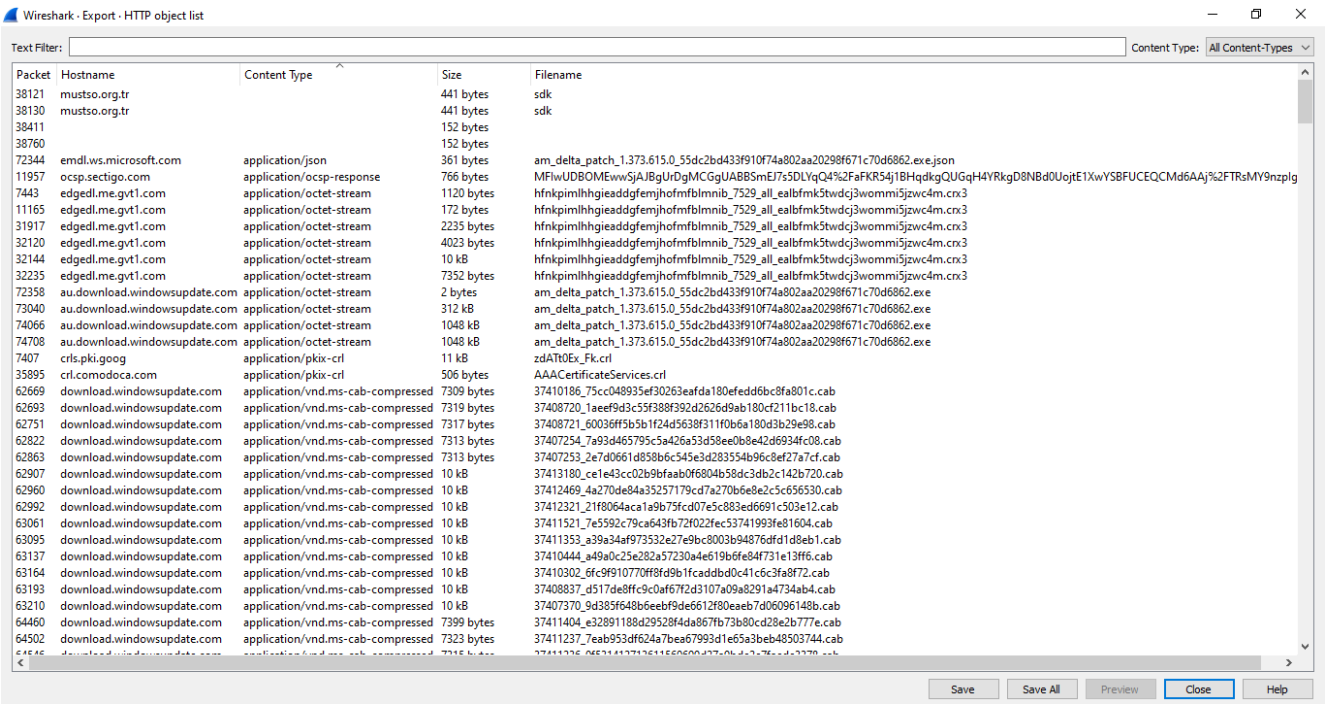



Buradan tüm dosya isteklerini görebilirsiniz ama isterseniniz dosyaya gitmeniz gereken asıl dosya ve bu seçenek denir.

**Nesneleri dışa** aktarır ve tüm **HTTP'yi** görebilirsiniz



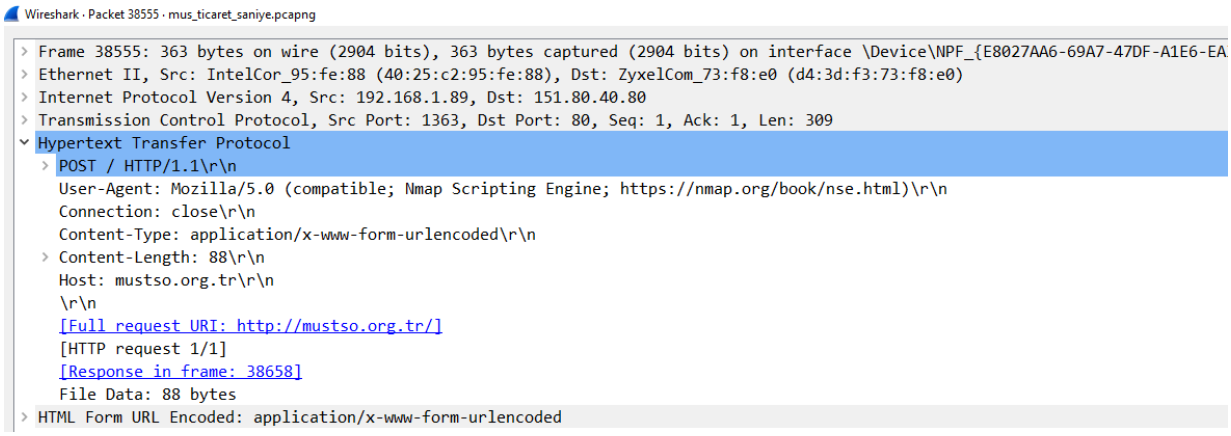

[Checksum Status: **Unverified**]




Çok fazla içerik türü(**content types**) **En kiritik buldumuz kısımda Application** buldundu kısımdır.

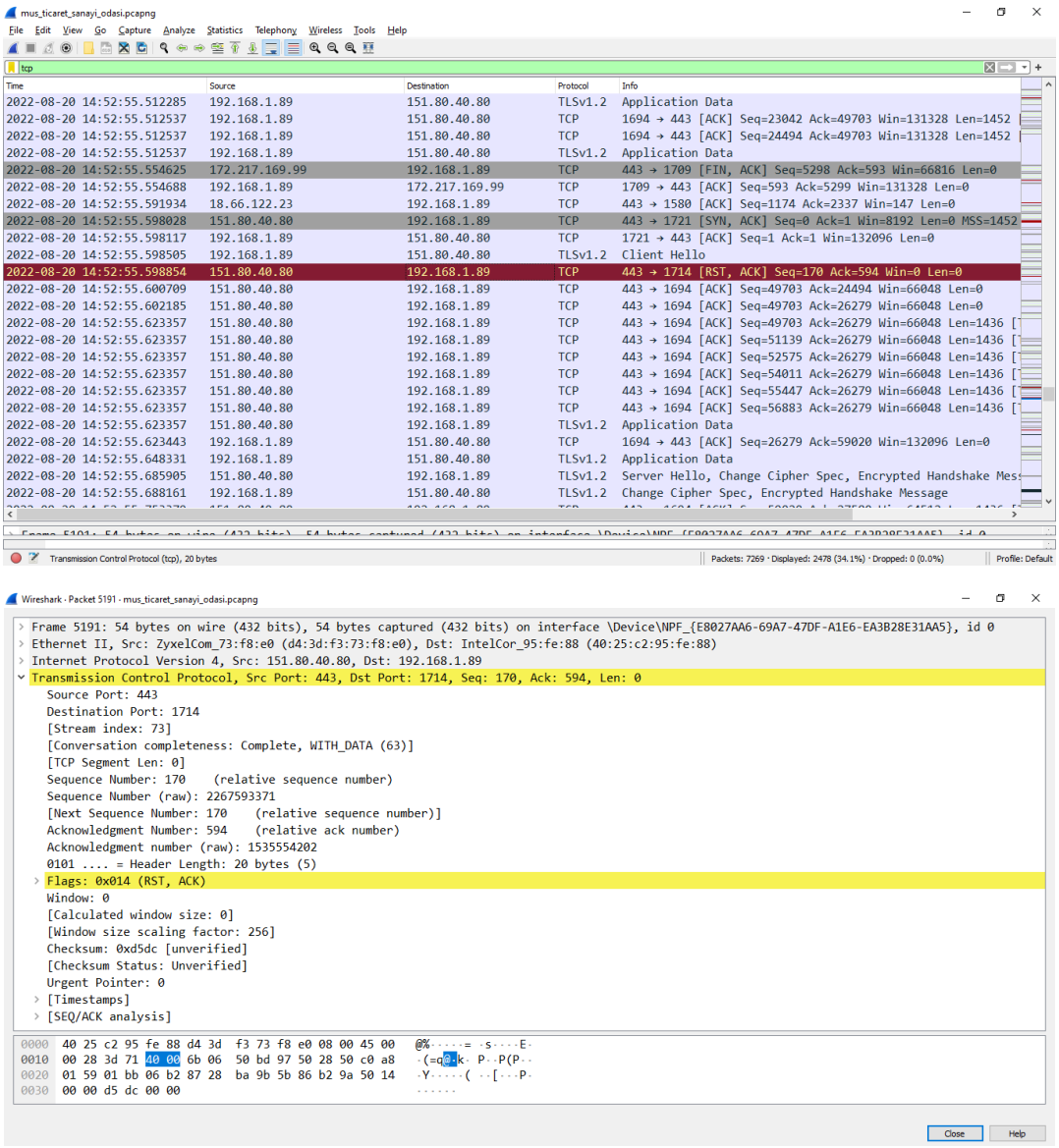
Kötü amaçlı ve yazılım ararken kullandığınız etiket **içerik türü** ve **uygulama türüdür**.

Genelikle **application** ile başlayanları kötü amaçlı olarak kullanabiliriz, onları indirip ondan sonra deneyebiliriz ve eğer o uygulama çalışırsa hack ve kötü amaçlı olarak kullanabilir, o yüzden http protokolü çok önemli bir protokoldür.




## 13. TCP (Transmission Control Protocol)

Varsayılan olarak, Wireshark'ın TCP ayırıcısı her TCP oturumunun durumunu izler ve sorunlar veya olası sorunlar algılandığında ek bilgi sağlar. Bir yakalama dosyası ilk açıldığında analiz her TCP paketi için bir kez yapılır. Paketler, paket listesinde göründükleri sırayla işlenir.




Yukardaki bilgileri heme iyi amaç ile ve hem kötü amaç ile kullanabiliriz, hack kavramını bildiğiniz gibi beyaz şapkalı ve siyah şabkalı hacker iki'sde bilgileri toplar, ama birisi iyi niyet ve birisi kötü niyet ile kullanabilir.

**1. Bad TCP**

Kısmında [Checksum Status: **Unverified**] olduğundan dolayı bu kısımları mustso'nun düzeltemsi gerekiyor.

**12. HTTP**

Kısmında [Checksum Status: **Unverified**] olduğundan dolayı bu kısımları mustso'nun düzeltemsi gerekiyor.