Bilgi Toplama

Necmettin ÇARKACI – Ahmet Alperen BULUT

Biz kimiz

İstihbarat Çeşitleri

Pasif Bilgi Toplama

- Hedef sistemden bağımsız

Aktif Bilgi Toplama

- Hedef sistemle doğrudan iletişime geçerek

Aktif Bilgi Toplama

Traceroute

- Traceroute bir paketin istediği adrese gidene kadar hangi hostlar ve yönlendirmelerden geçtiğini gösteren programdır.

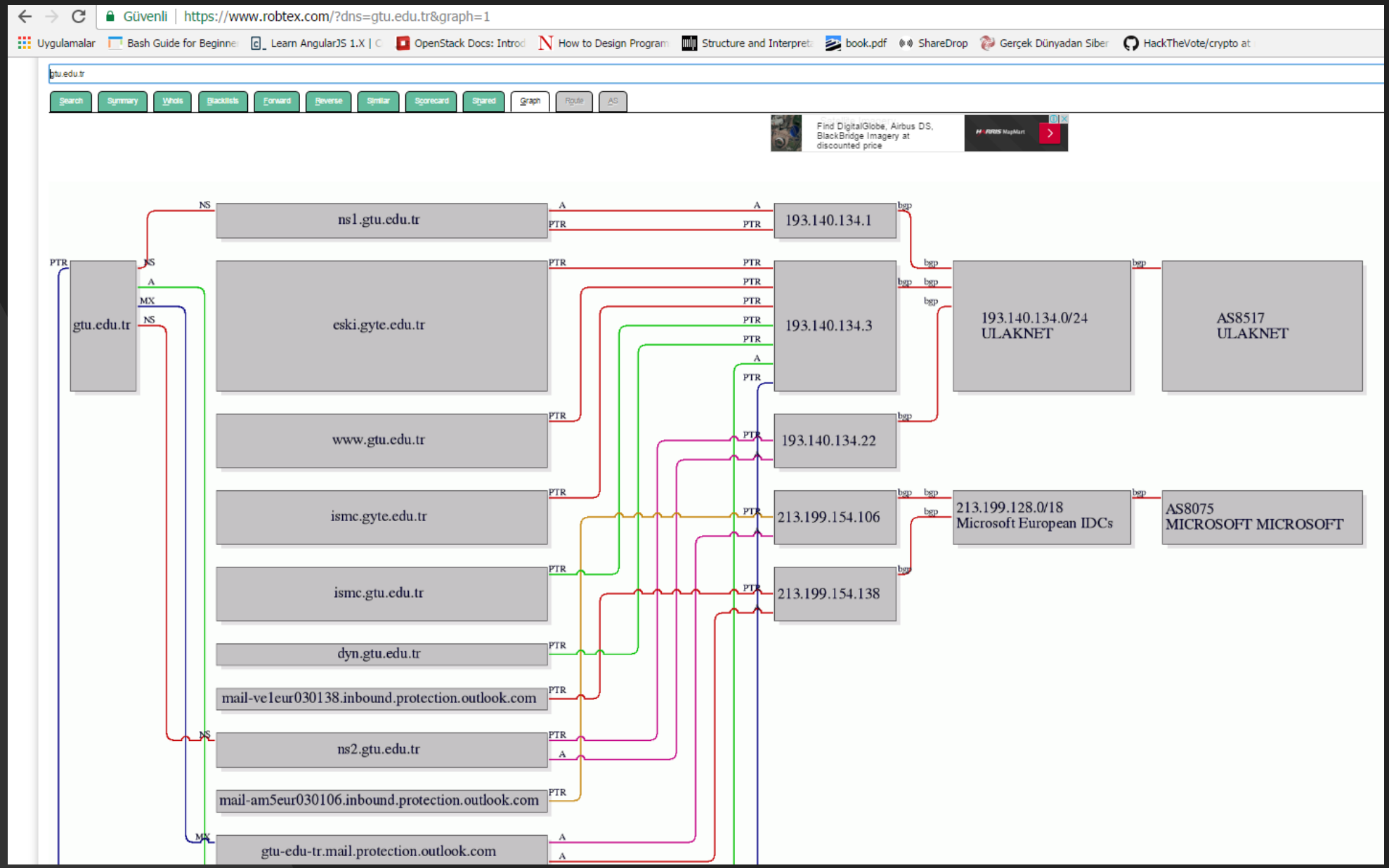
Dig

- Detaylı DNS sorgulaması yapan gelişmiş bir araçtır.

Dirbuster

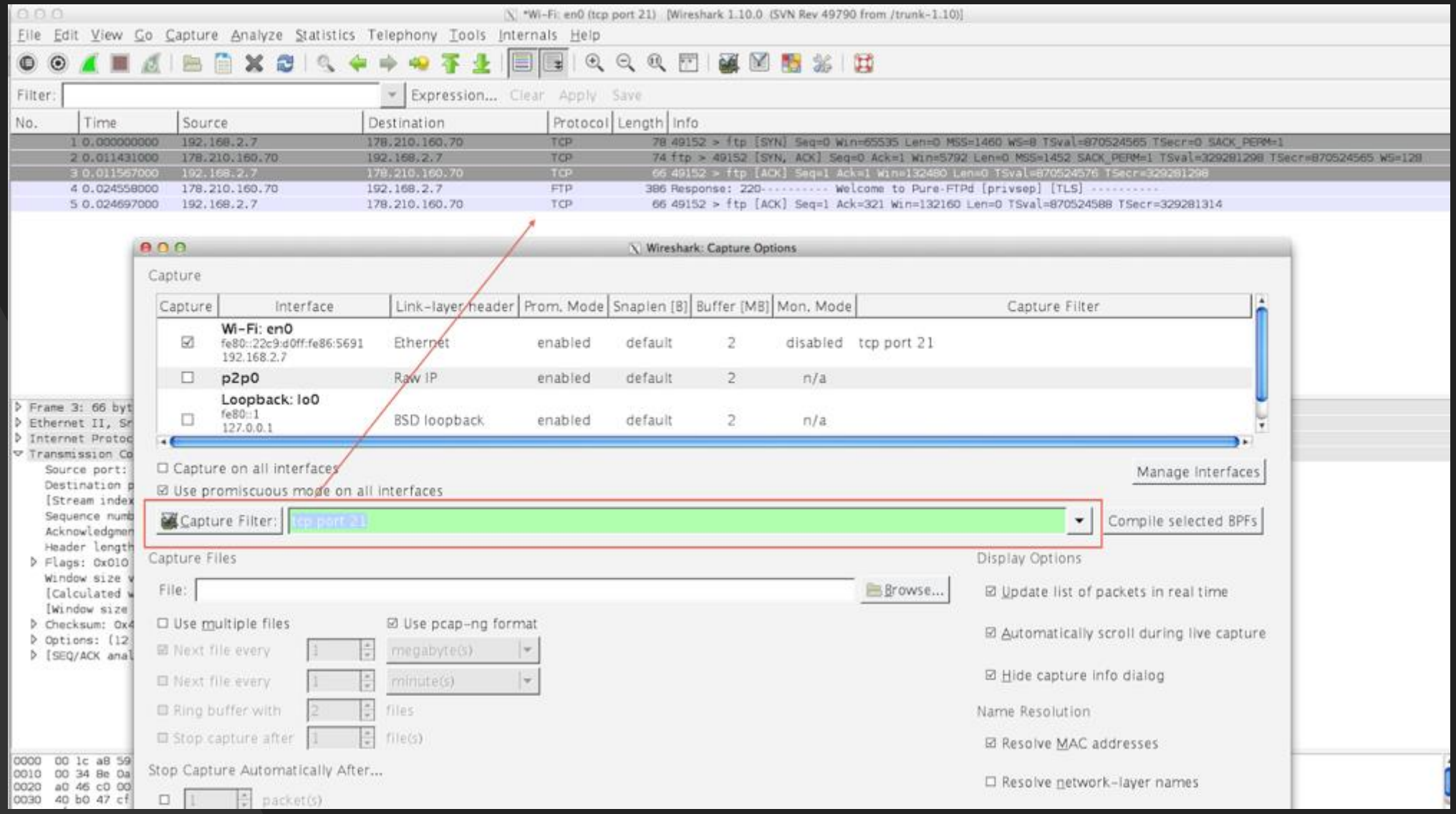
- Hedef adresin alt dizinlerini bulmak için kullanılır.

Robtex


Güvenli | https://www.robtex.com/?dns=gtu.edu.tr&graph=1
Uygulamalar
Bash Guide for Beginne
Learn AngularJS 1.X | C
OpenStack Docs: Introd
How to Design Program
Structure and Interpreta
book.pdf
ShareDrop
Gerçek Dünyadan Siber
HackTheVote/crypto at
gtu.edu.tr
Search
Summary
Whois
Blacklists
Forward
Reverse
Similar
Scorecard
Shared
Graph
Route
AS
Find DigitalGlobe, Airbus DS, BlackBridge Imagery at discounted price
gtu.edu.tr
ns1.gtu.edu.tr
eski.gyte.edu.tr
www.gtu.edu.tr
ismc.gyte.edu.tr
ismc.gtu.edu.tr
dyn.gtu.edu.tr
mail-ve1eur030138.inbound.protection.outlook.com
ns2.gtu.edu.tr
mail-am5eur030106.inbound.protection.outlook.com
gtu-edu-tr.mail.protection.outlook.com
193.140.134.1
193.140.134.3
193.140.134.22
213.199.154.106
213.199.154.138
193.140.134.0/24
ULAKNET
AS8517
ULAKNET
213.199.128.0/18
Microsoft European IDCs
AS8075
MICROSOFT MICROSOFT

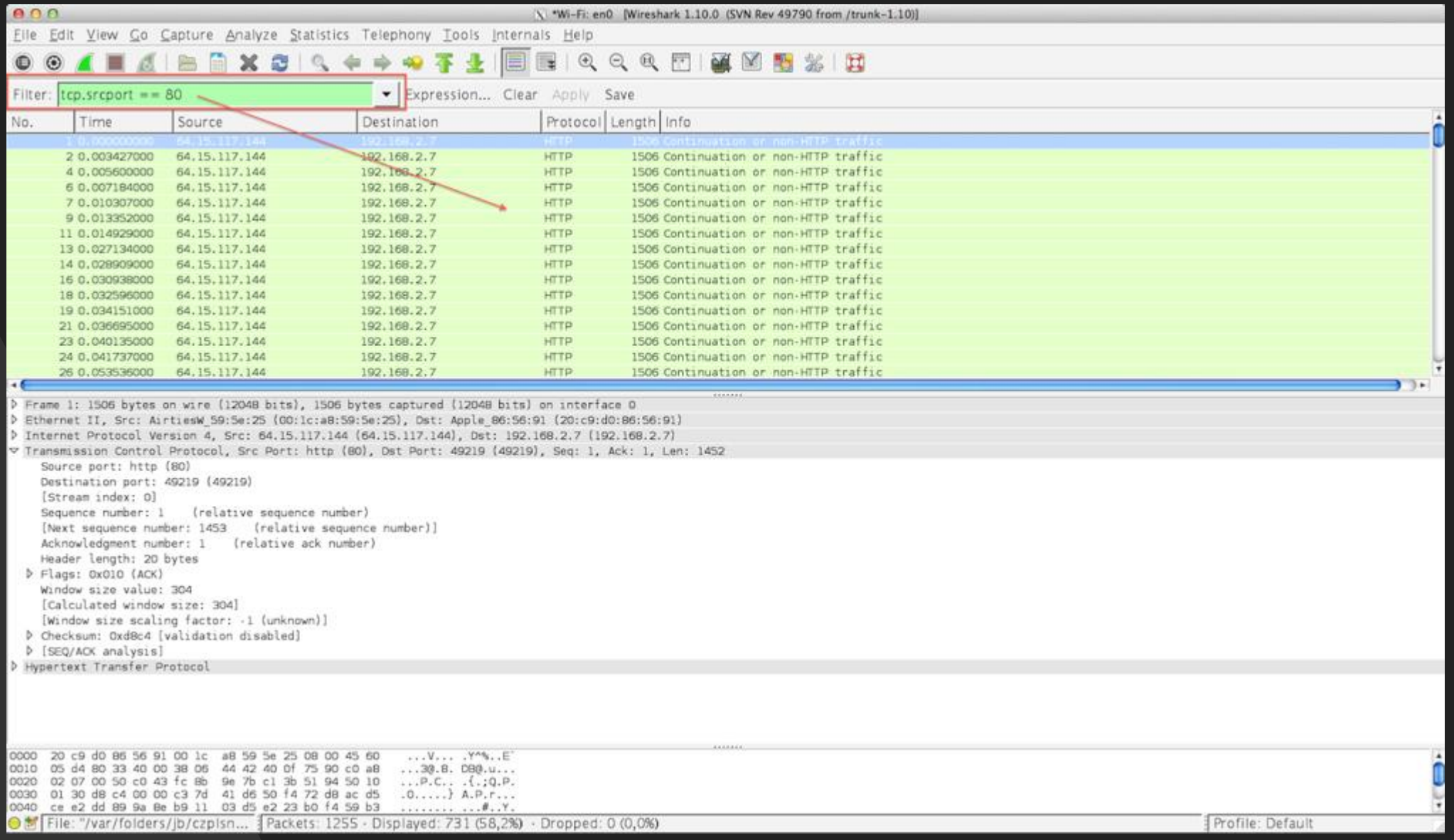
Wireshark

Capture Filter: Yakalanacak paketlerin türü portu protokol bilgisi önceden belirtilerek hedef odaklı bir paket analizi yapılabilir.



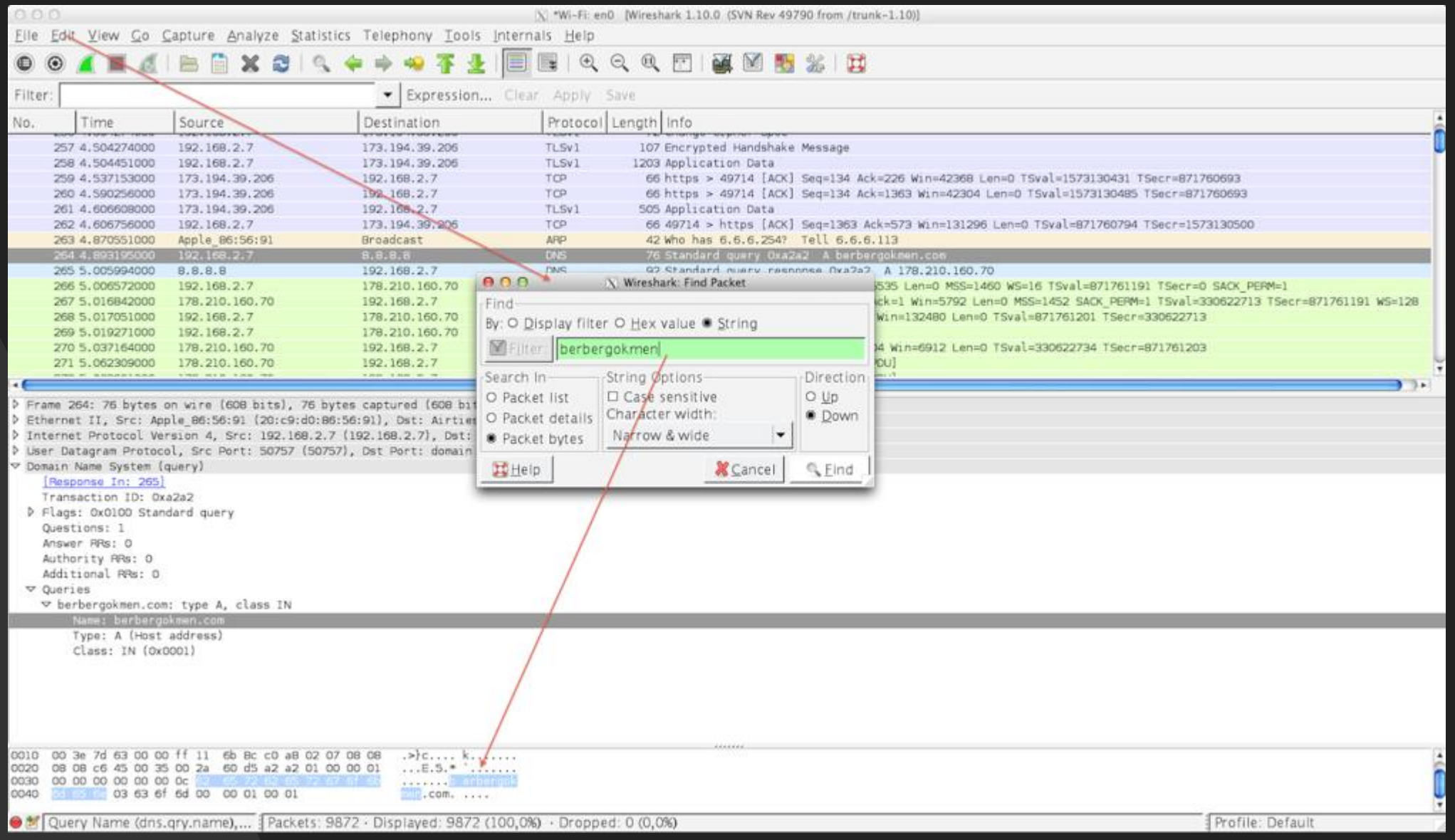
Wireshark

Display Filter: Yakalanan paketlerin içerisinden istenilen özelliklerdeki paketlerin ayıklanması kısmında kullanılabilir.



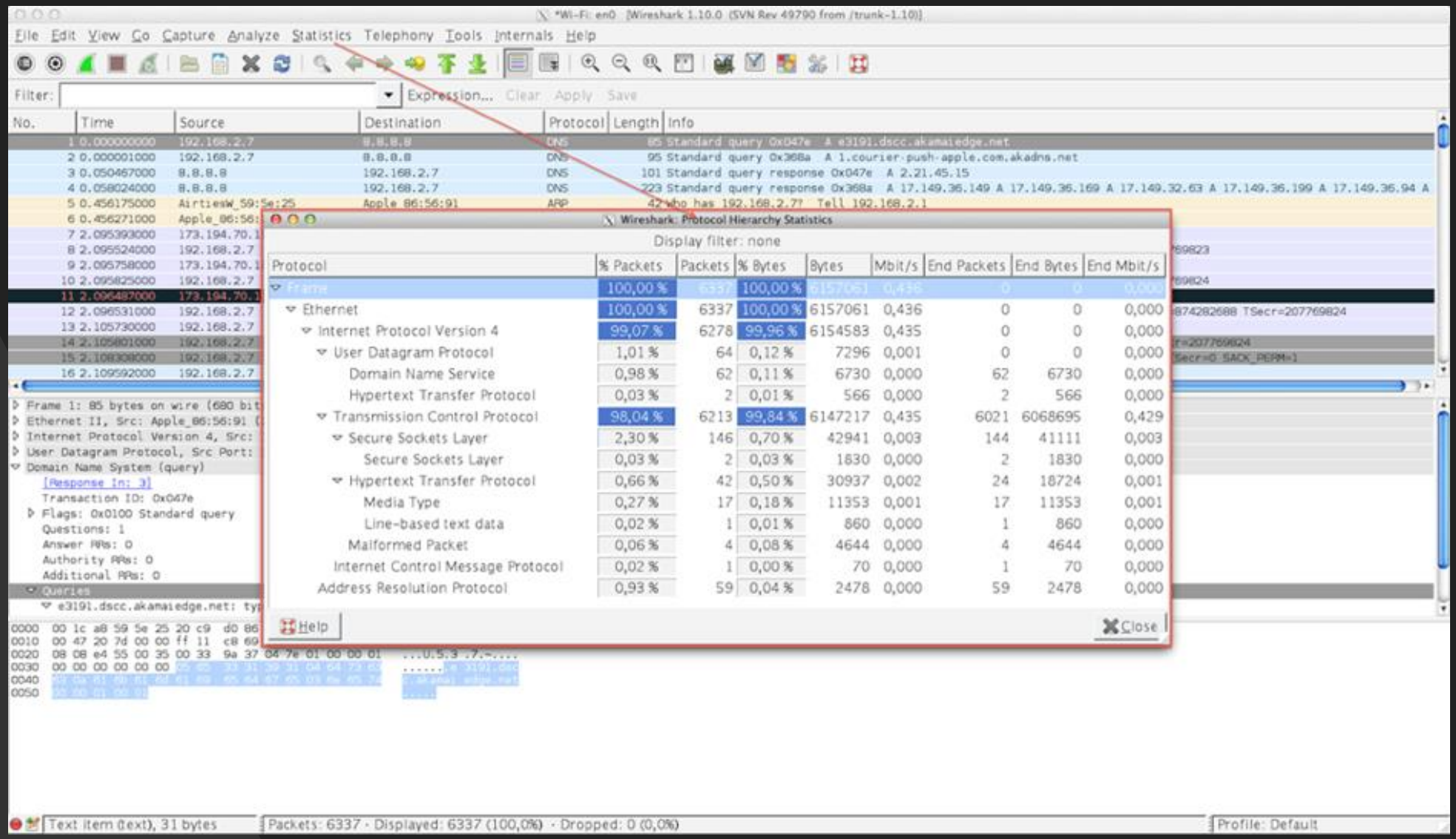
Wireshark

Kelime arama : İzlenen trafik içerisinde kelime arama;



Wireshark

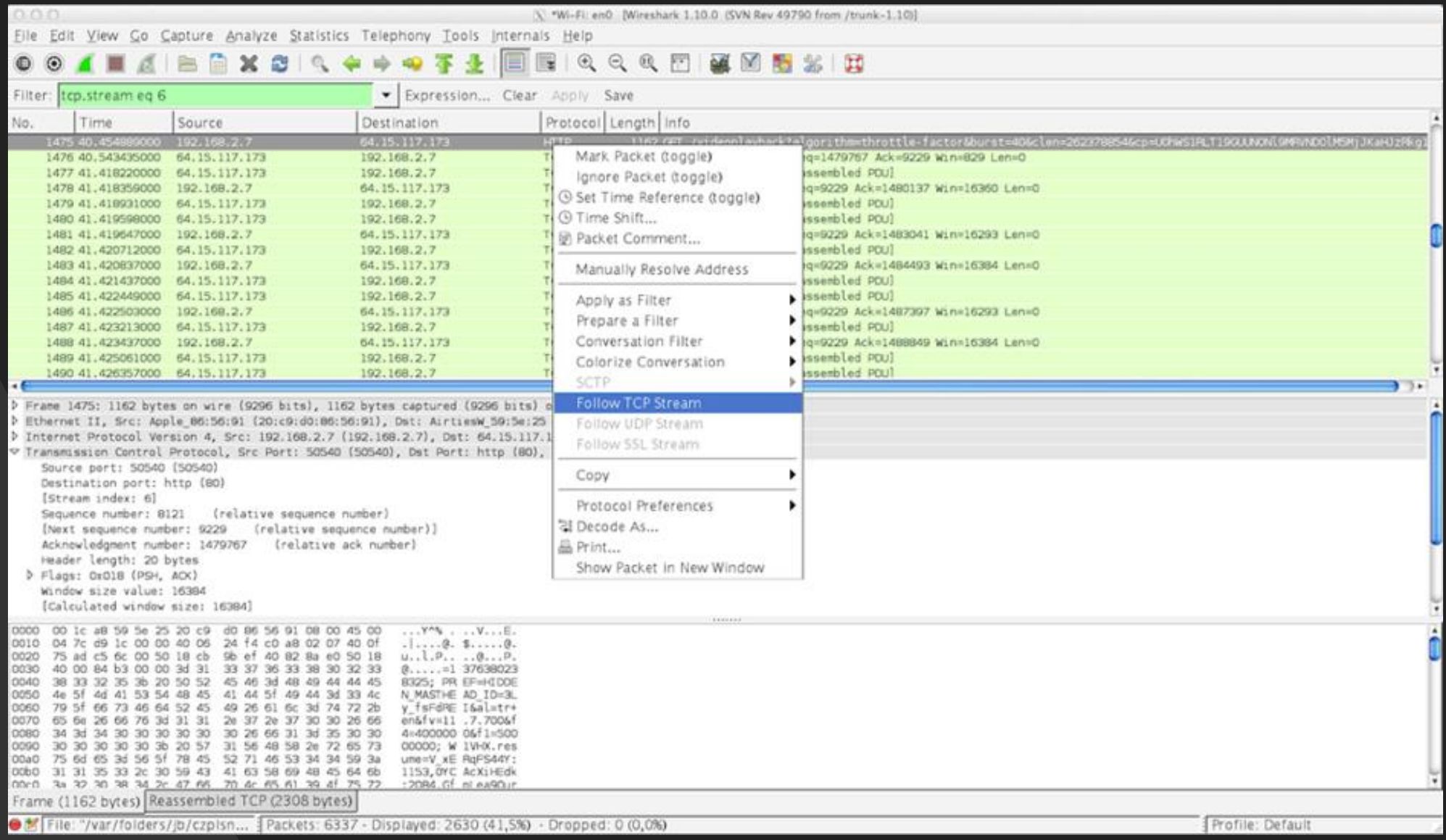
Protokol detayı : Protokol detaylarının gösterilmesi. Özellikle DDOS saldırılarında saldırı tipini belirlemek için kullanılır.



TCP follow : TCP oturumlarında paket birleştirme, HTTP bağlantısındaki tüm giden gelen paketlerin birleştirilip session hakkında bilgi verilmesi.

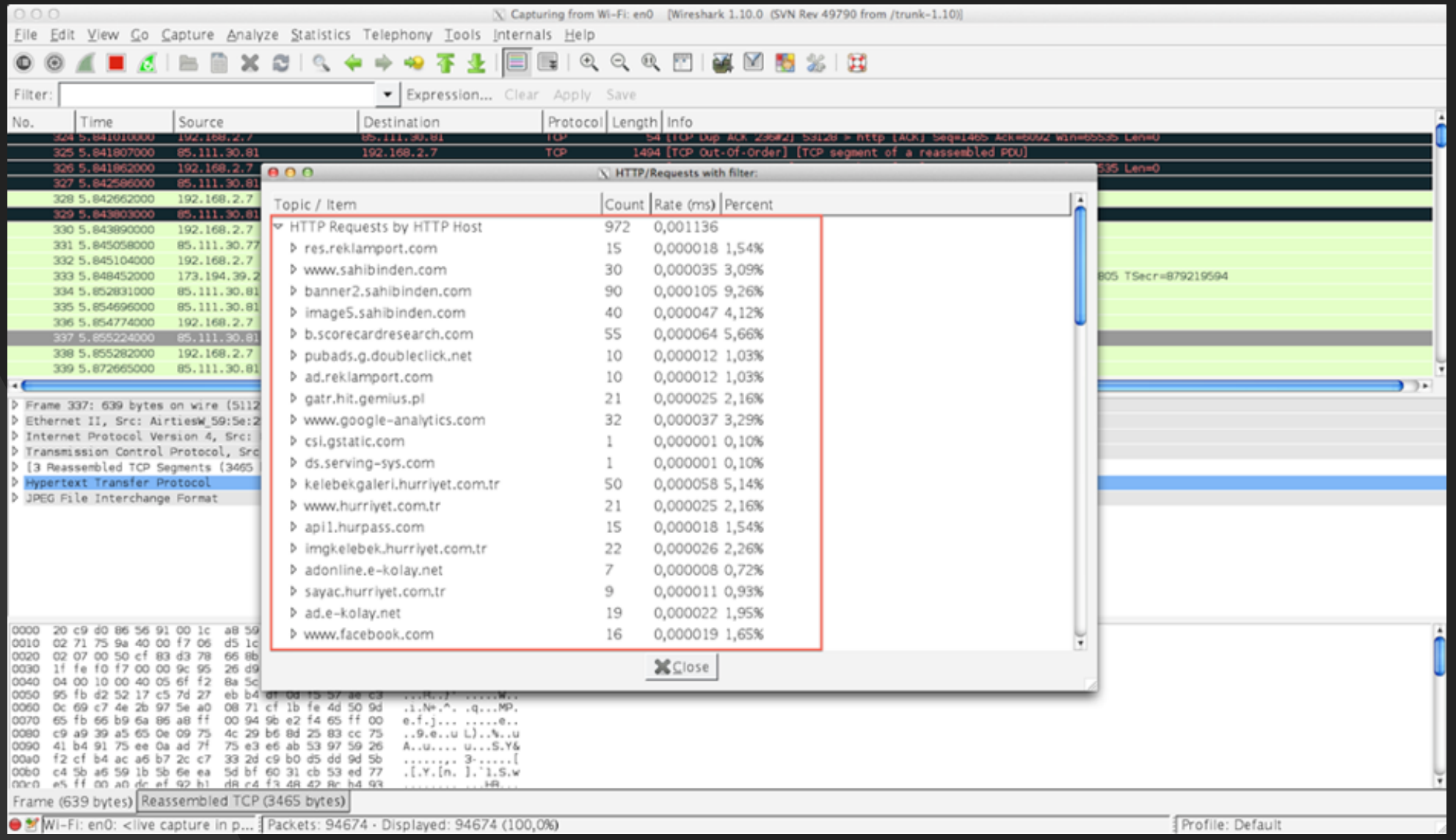
Wireshark

Birleştirilmek istenilen protokol paketi üzerinde sağ tıklanır ve "Follow TCP Stream" seçeneği seçilir.



Wireshark

İstek sayıları : http istek sayılarının görüntülenmesi.



Kaynakça

- Paket/Protokol Analizi Amaçlı Wireshark Kullanımı, http://wiki.bgasecurity.com/Paket/Protokol_Analizi_Amaçlı_Wireshark_Kullanımı