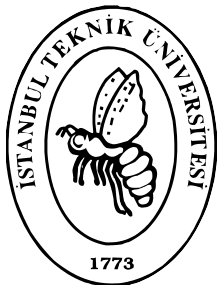
ISTANBUL TECHNICAL UNIVERSITY



BLG 433E

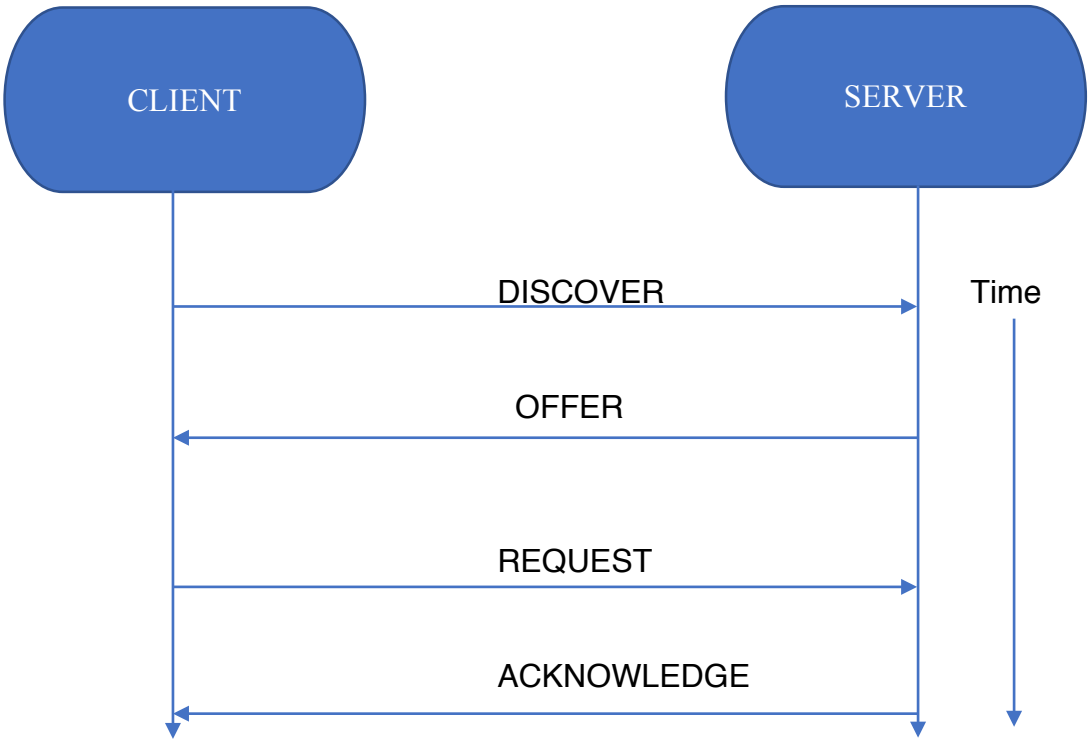
COMPUTER COMMUNICATIONS

NETWORK ANALYZING WITH WIRESHARK

1.DHCP (Dynamic Host Configuration Protocol)

How DHCP Works?

DHCP protocol attaches IP addresses to clients on network automatically. So, it gives the capability of managing IP addresses from a center. DHCP also sends DNS server address and Default Gateway. It finishes the process in a 4-step sequence.

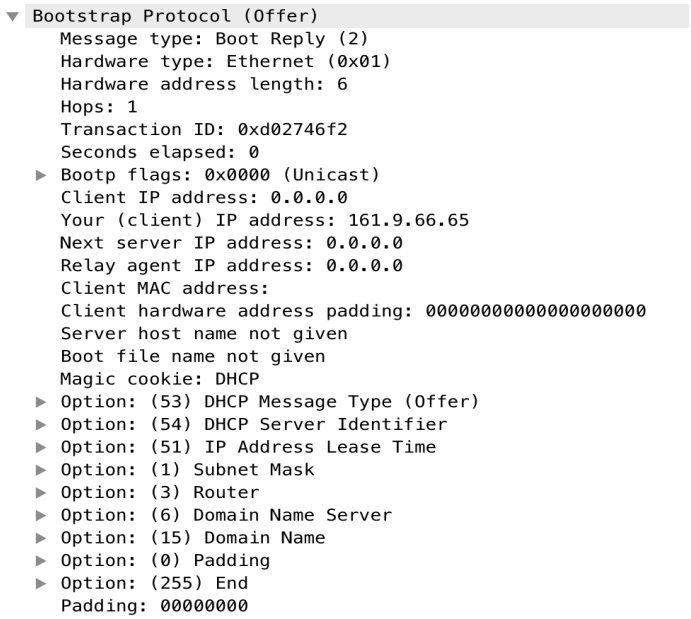


First, client sends a DHCP DISCOVER packet to find DHCP server. The packet contains client computer name and the MAC address.

```
▼ Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xd02746f2
    Seconds elapsed: 0
  ▶ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address:
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (Discover)
  ▶ Option: (55) Parameter Request List
  ▶ Option: (57) Maximum DHCP Message Size
  ▶ Option: (61) Client identifier
  ▶ Option: (51) IP Address Lease Time
  ▶ Option: (12) Host Name
  ▶ Option: (255) End
    Padding: 000000000000000000000000
```

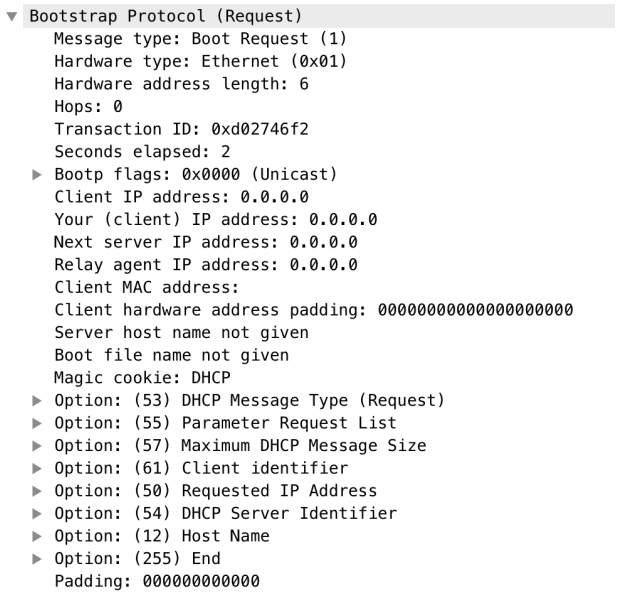
Picture 1 DHCP Discover

Second, DCHP server gets the packet and sends back a DHCP offer packet which includes IP address and Lease Time properties.



Picture 2 DHCP Offer

Third, client accepts the DHCP offer packet and sends back DHCP request packet to say server DHCP offer packet accepted or not.

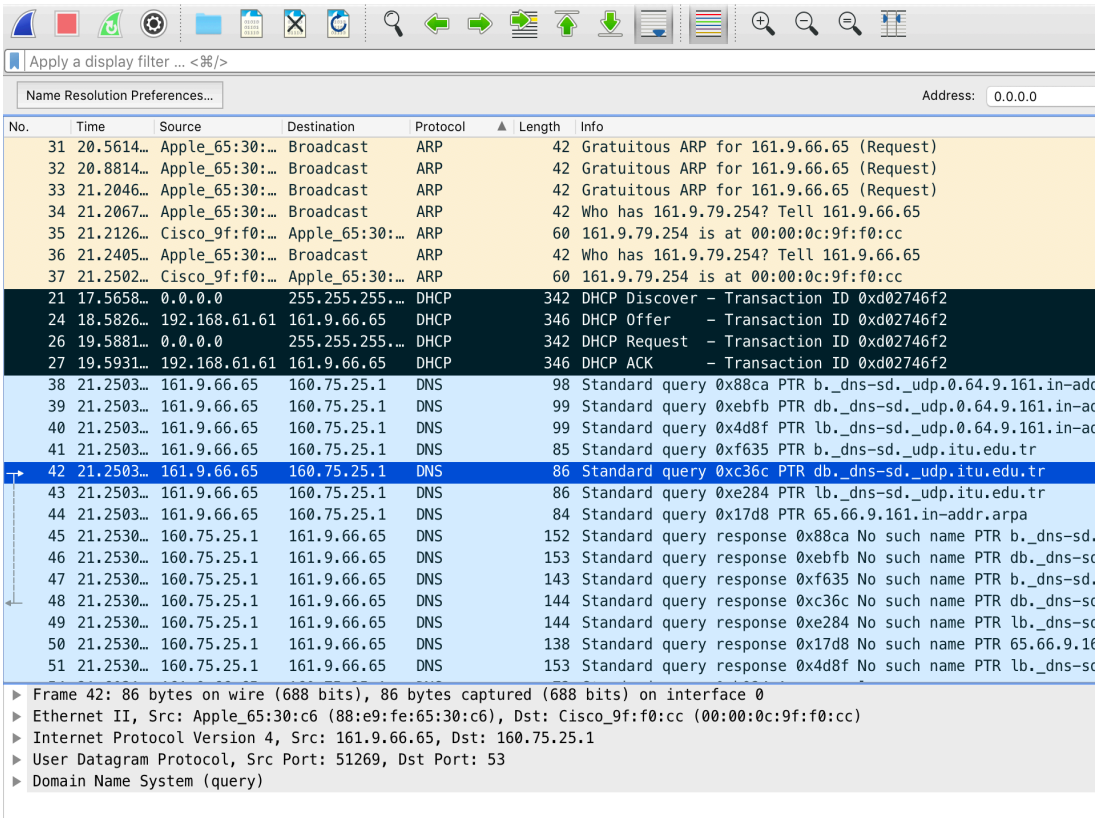


Picture 3 DHCP Request

Fourth, DHCP server attaches the IP address and Lease Time. The client becomes TCP/IP client and participates to network.

```
▼ Bootstrap Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0xd02746f2
    Seconds elapsed: 2
  ▶ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 161.9.66.65
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address:
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (ACK)
  ▶ Option: (54) DHCP Server Identifier
  ▶ Option: (51) IP Address Lease Time
  ▶ Option: (1) Subnet Mask
  ▶ Option: (3) Router
  ▶ Option: (6) Domain Name Server
  ▶ Option: (15) Domain Name
  ▶ Option: (0) Padding
  ▶ Option: (255) End
    Padding: 00000000
```

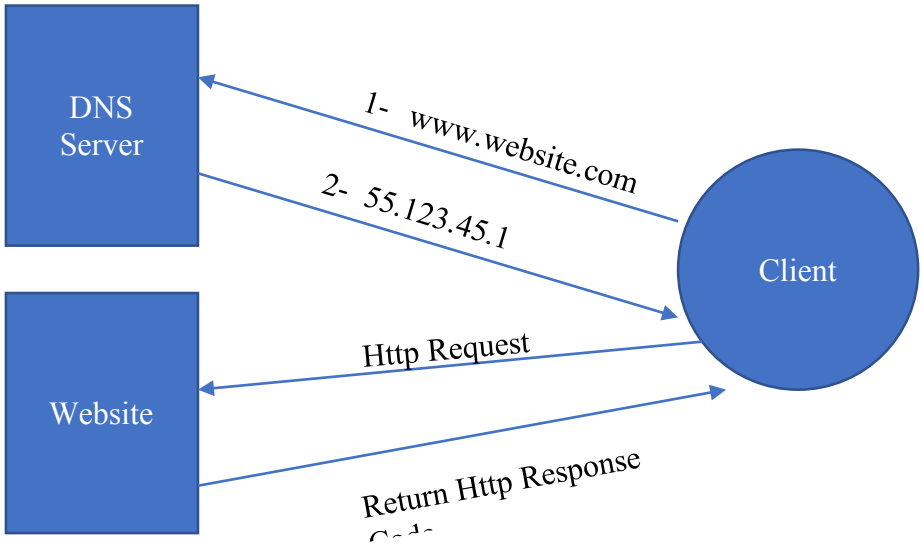
Picture 4 DHCP Acknowledge



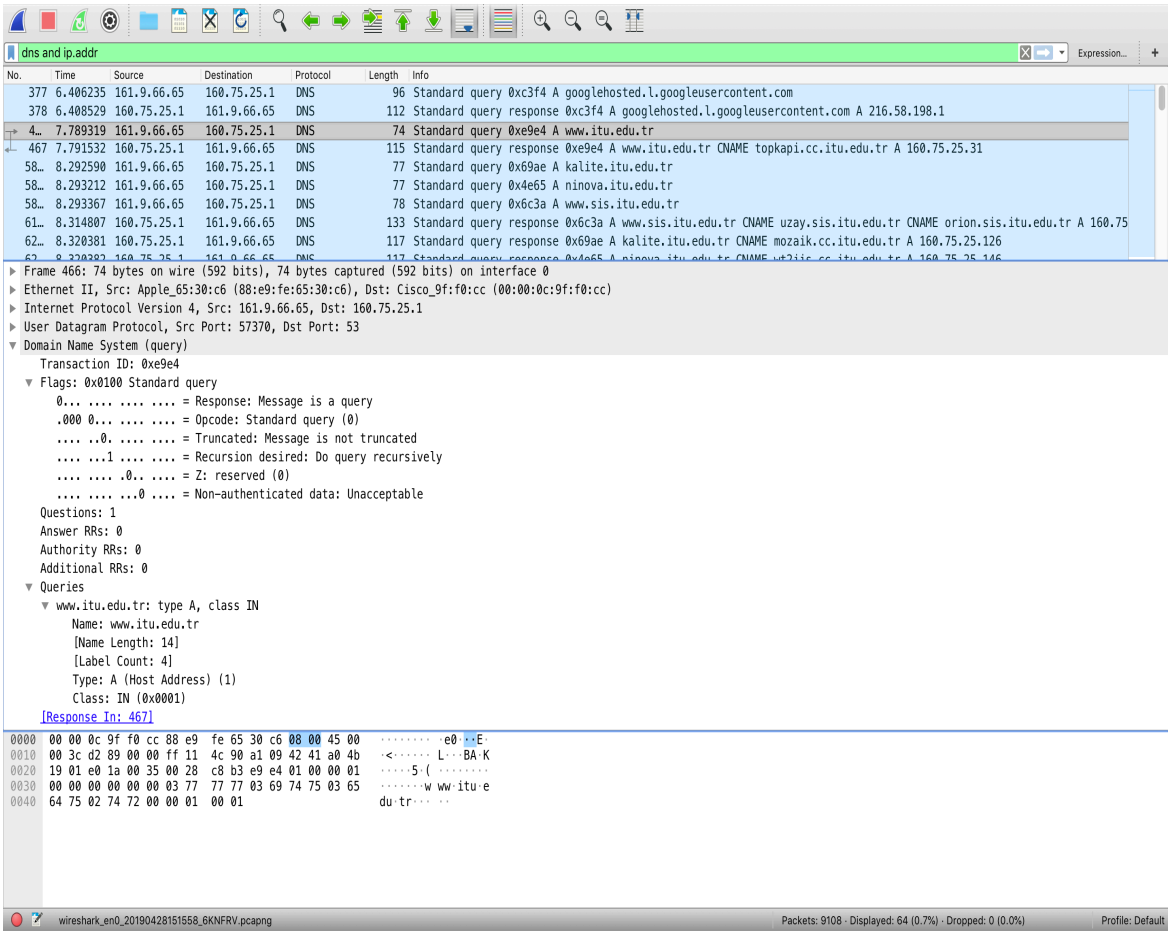
Picture 5 DCHP Protocol

2.DNS (Domain Name System Protocol)

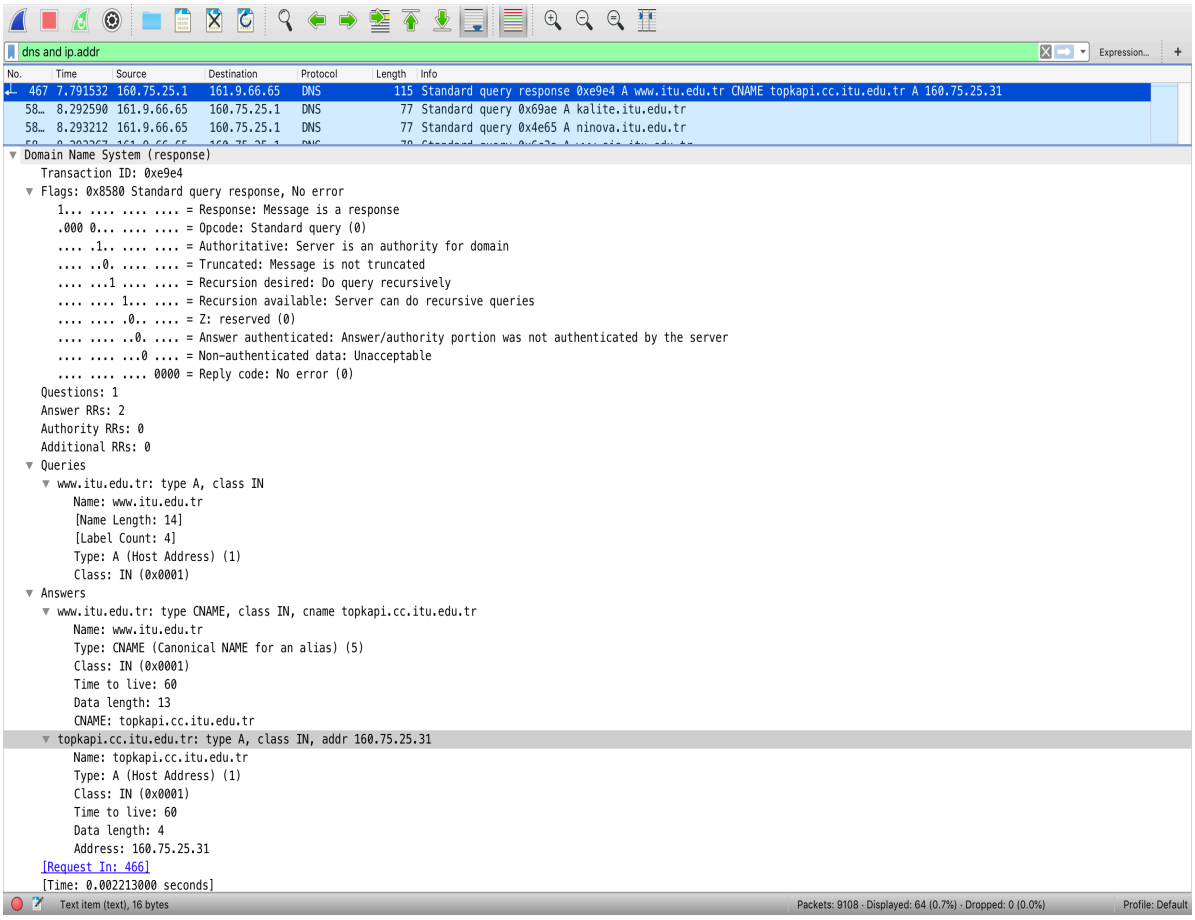
Applications use understandable, easy remember names instead of IP addresses. So, we need a system to resolve and matches names with IP address. Basically, DNS works in the given figure below. Now we will analyze DNS Protocol with Wireshark.



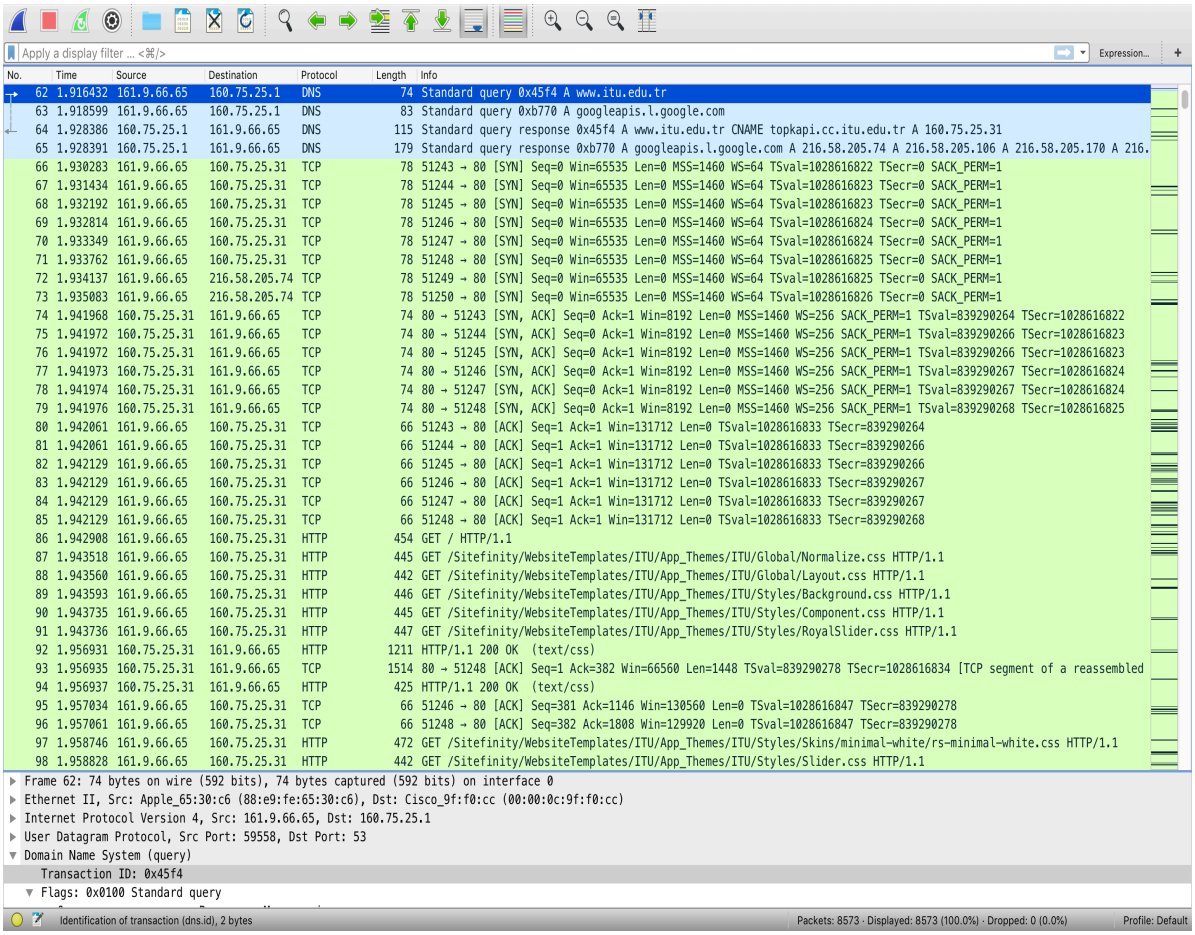
First, I deleted the history of the browser. After that I send a DNS query for www.itu.edu.tr. So, the 1st step completed and Picture 6 shows the query.



Picture 6 DNS Query with Wireshark



Picture 7 Source and Destination IP



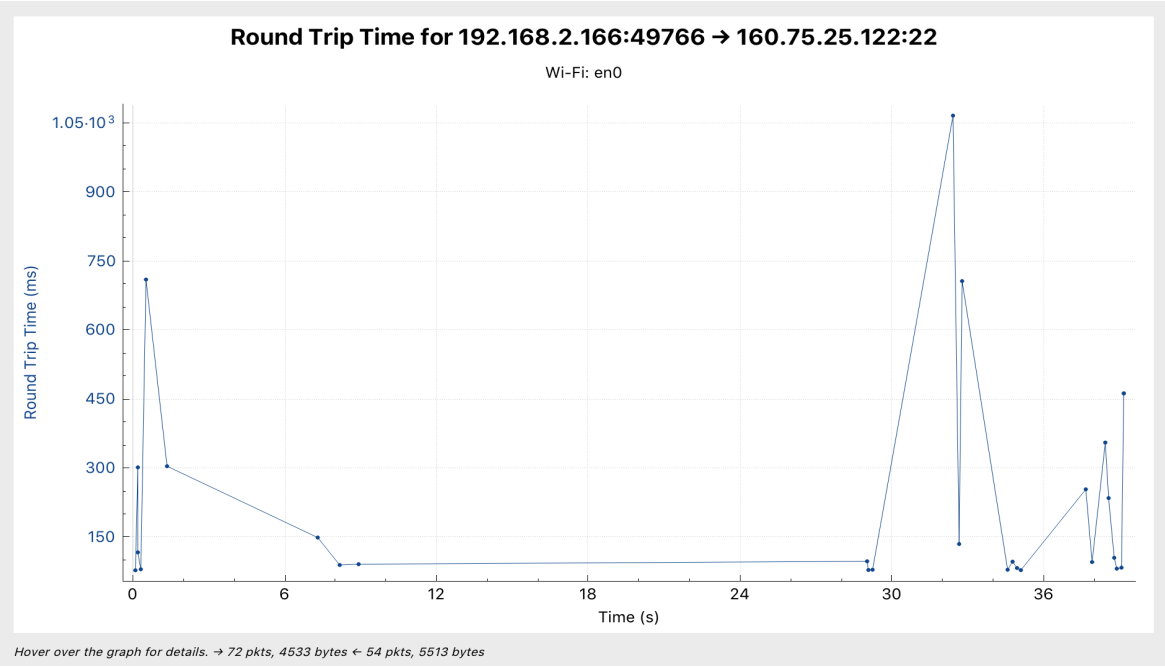
Picture 8 All Stages of DNS Protocol

In Picture 7 we can see that DNS server sent the IP address of the website by resolving it recursively. After that a TCP connection occured between website and my computer. All in all, we can see the DNS server as 160.75.25.1 and IP address of website as 160.75.25.31 from screenshots.

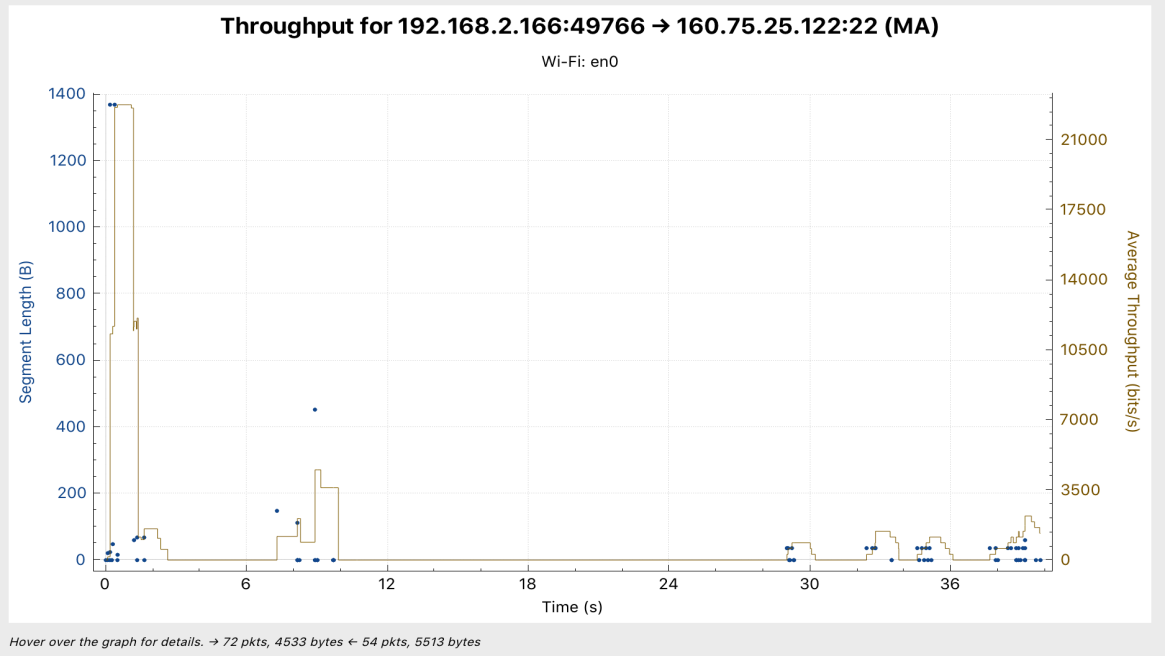
3.TRANSPORT LAYER PROTOCOLS

a.Capture A Session That Uses TCP

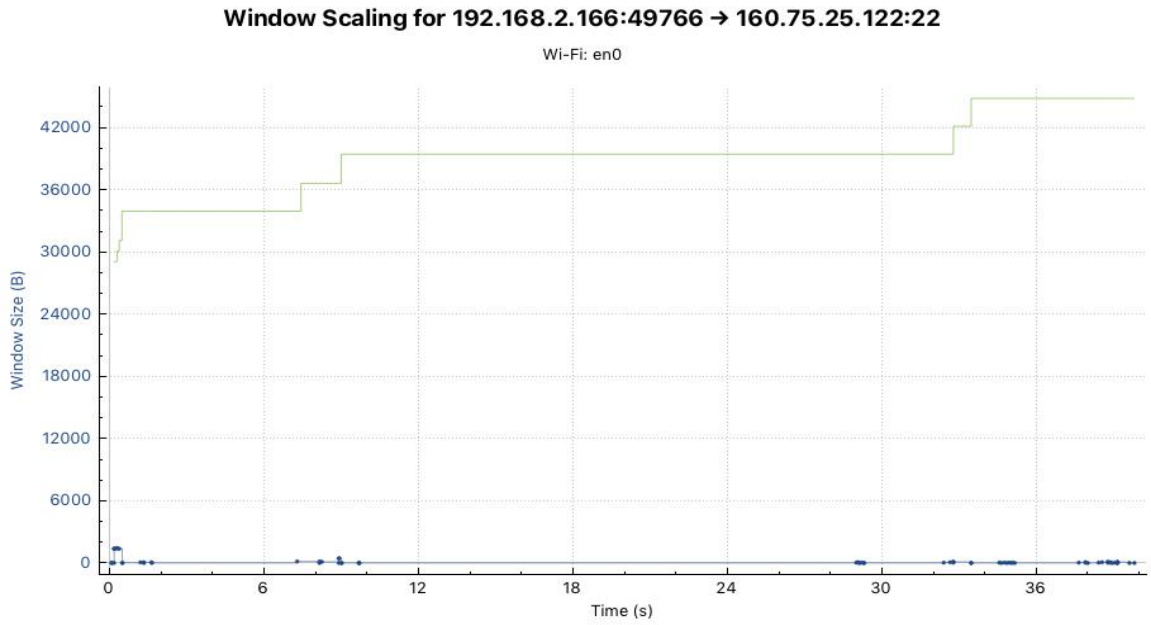
I know SSH uses TCP, so I created a TCP connection between ssh.itu.edu.tr and my computer. I started the Wireshark and made ssh login operation from terminal. After that I stopped the session by using logout command and results are:



Picture 9 Round Trip Time



Picture 10 Throughput

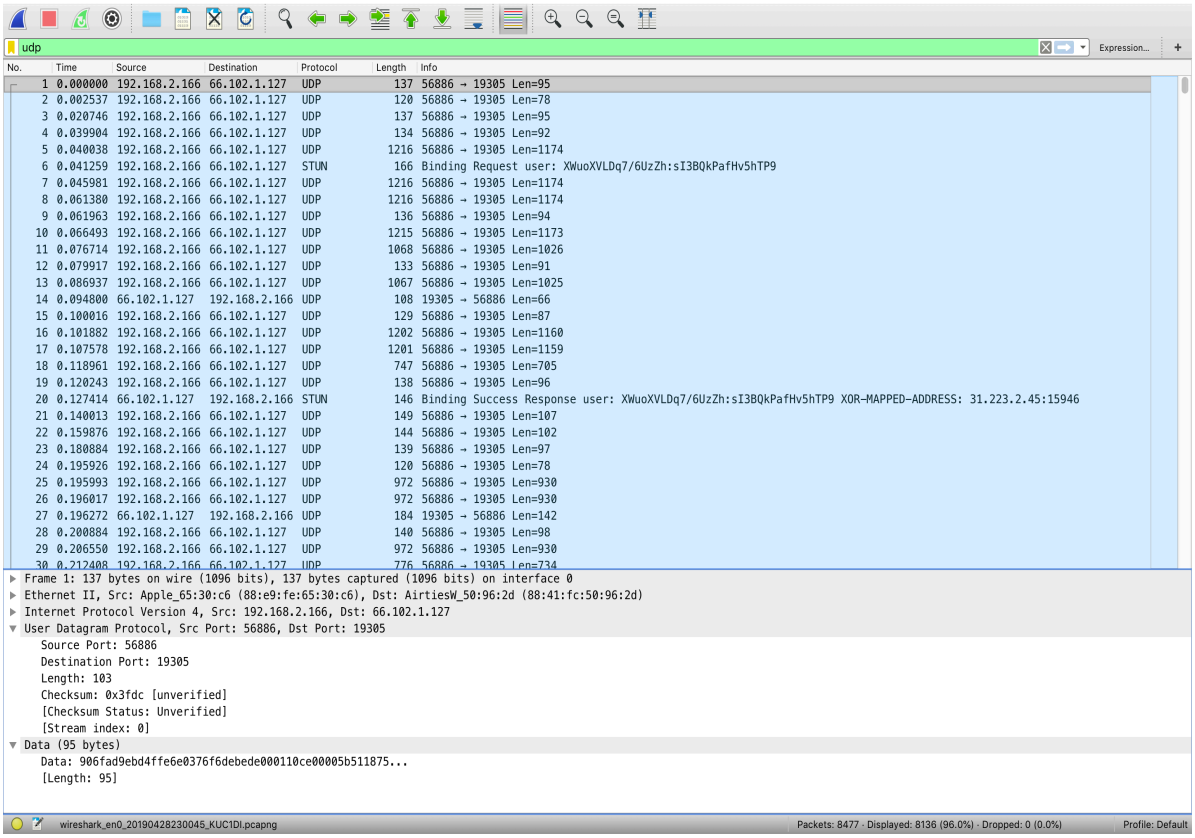


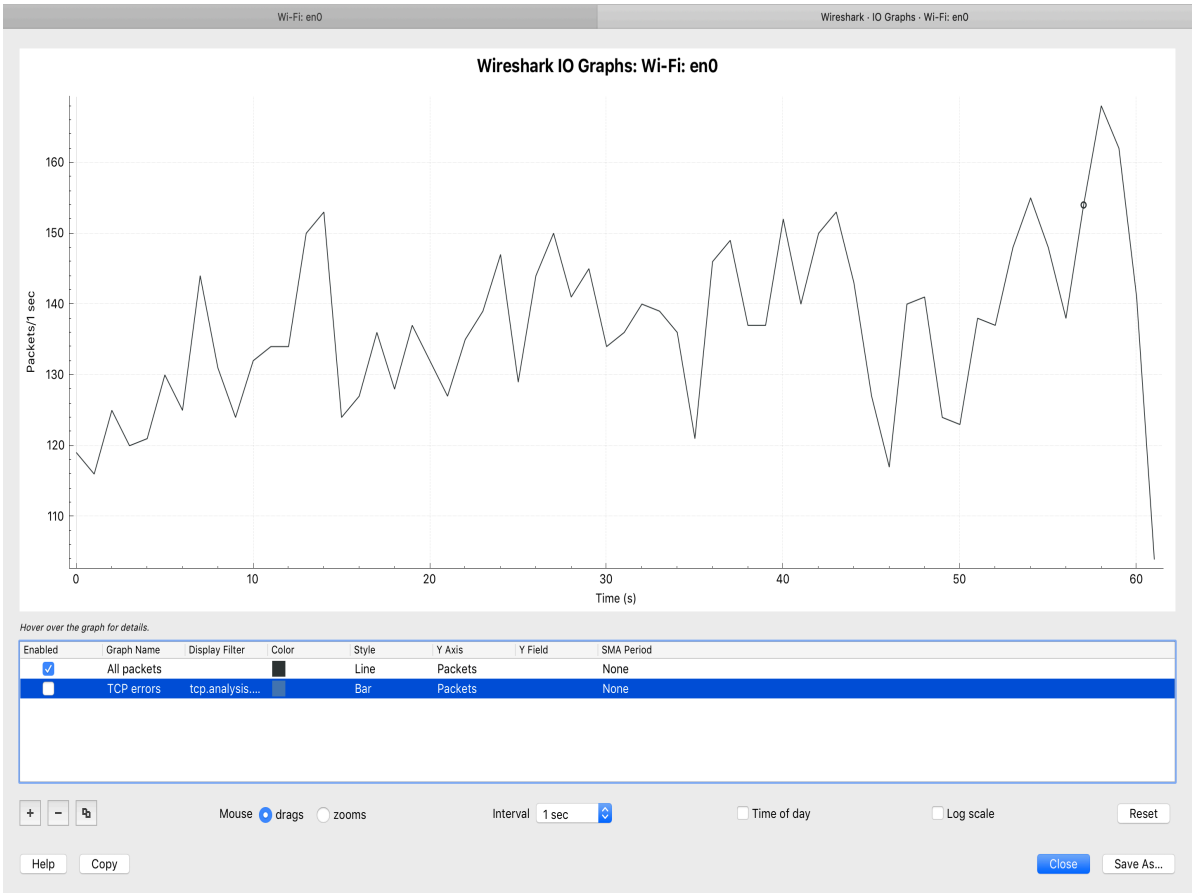
Picture 11 Window Scaling

According to TCP Congestion Mechanism, when the network delivery becomes slow down, it gives warning to sender for slowing down. So according to congestion policy, in slow stop phase it exponentially increases window size. In congestion avoidance phase it increases 1 after reaching threshold. In congestion detection phase sender returns slow start and congestion avoidance phase.

b.Capture A Session That Uses UDP

I used Google Hangouts for capturing UDP packets. I started Wireshark and I called my friend then I used “udp” filter to see UDP packets.





Picture 12 IO Statistics For UDP

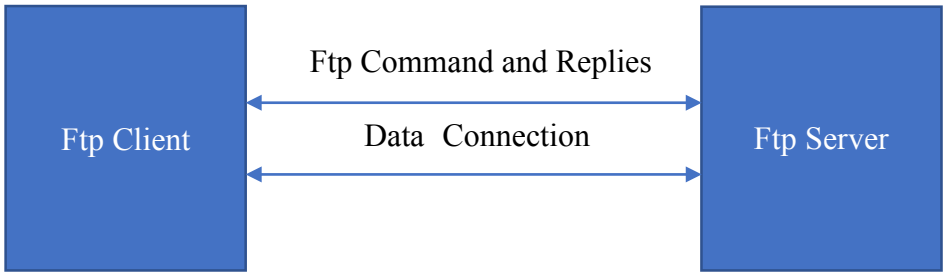
According to my researches, it is not proper to use statistical methods for UDP as in TCP. So, in this step for UDP connections Wireshark gives a practical way to analyze UDP packets named as I/O Graph.
Best Effort Service in UDP means, network does not work for retransmit lost or corrupted packets. Using this method network provides more performance. In TCP connection between client and server guarantees the package delivery, so this causes checking packages and more cost. But in UDP method this is not a problem if package loss occurs.

c.Any Other Transport Layer Protocol During Sessions?

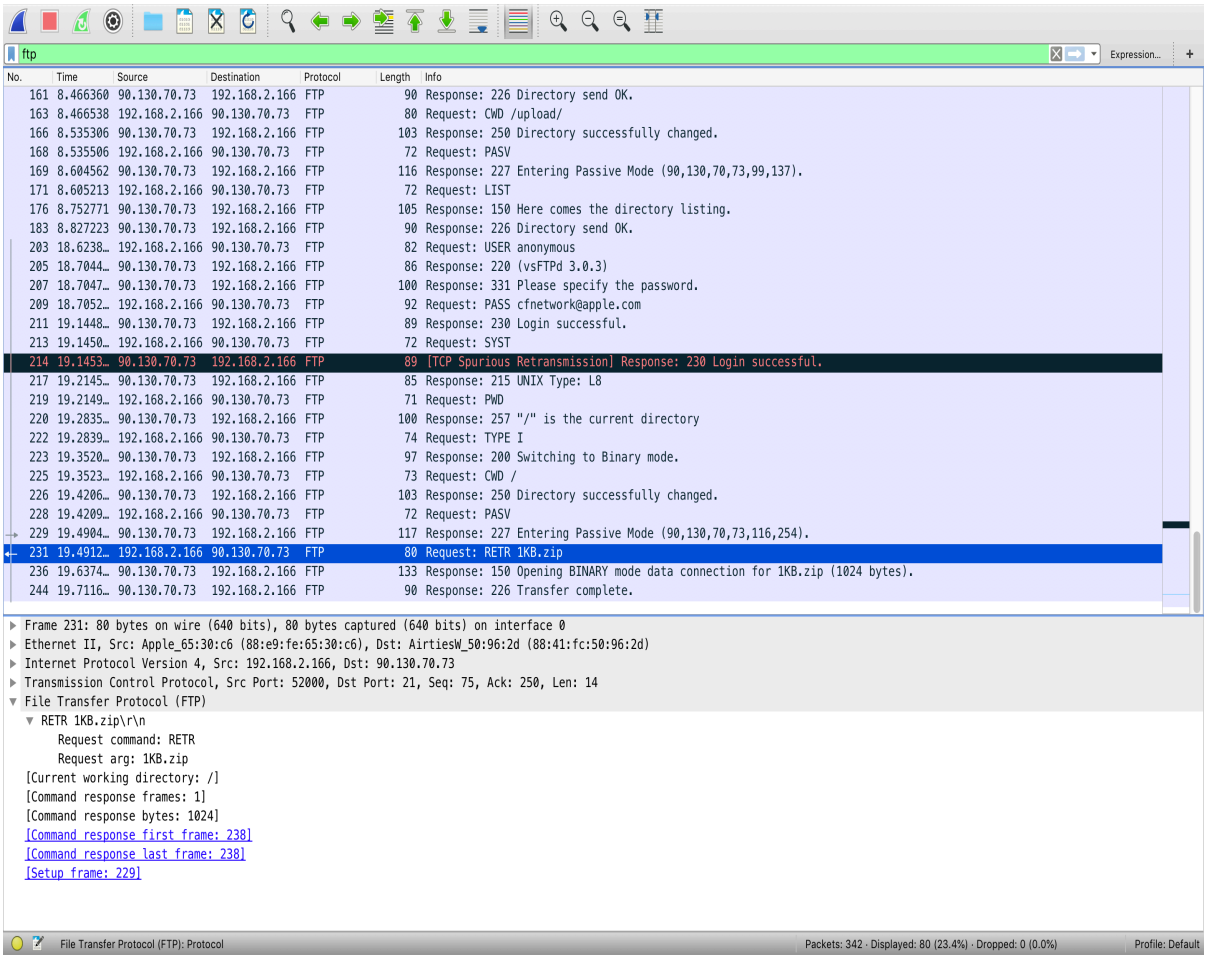
I made a detailed search and I found; AEP, AH, DCCP, ESP, FCP, NETBIOS, IL, ISCSI, NBF, SCTP, SINEC H1, SPX, NBP protocols near TCP and UDP in transport layer. But when I am using Wireshark I could not detected any other transport layer protocols except TCP and UDP.

4.FILE TRANSFER

When I tried to download a file from Ninova Wireshark does not show any FTP protocol it all includes TCP protocols. Because Http supports downloading file.
The reason for this situation is FTP requires a new connection for each new data transfer, so this decreases the performance and increases the cost for a website like Ninova. So basically Http use request-response methodology in file transfer too.



The given Figure represents the Ftp connection and file downloading process. So we can easily see the process by using Wireshark.



Picture 13 Ftp Connection and File Download

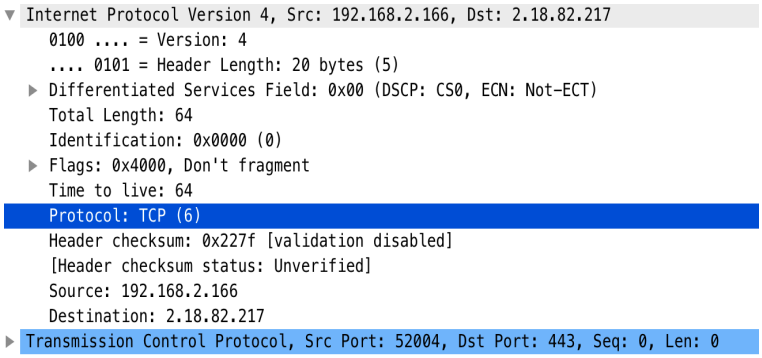
5.PROTOCOL ANALYSIS INTERPRETATION

a.How Many Different Protocols Captured?

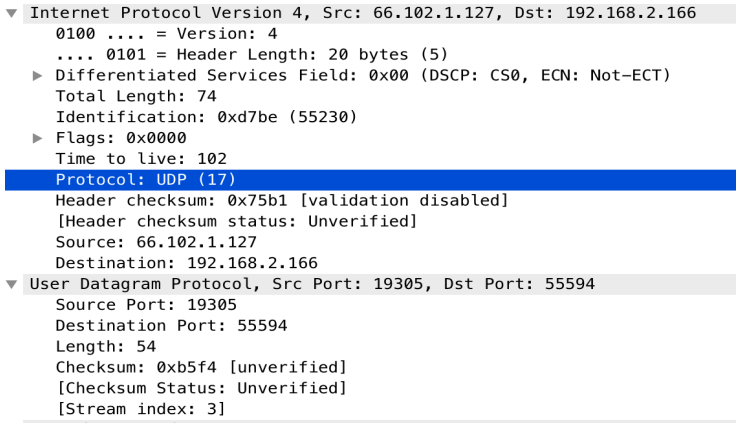
DNS – TCP – HTTP – OCSP – TLSv1.2 – UDP – FTP – SSDP – ARP – STUN - ICMP

b.What Are Specific Protocol Numbers For Transport Protocol?

TCP uses 6 as a protocol number.



UDP uses 17 as a protocol number.



ICMP uses 1 as a protocol number.