Department of Computer Engineering

Computer Networks

Homework 2

Dr. Jafari

Parsa Mohammadian — 98102284

May 23, 2022

Contents

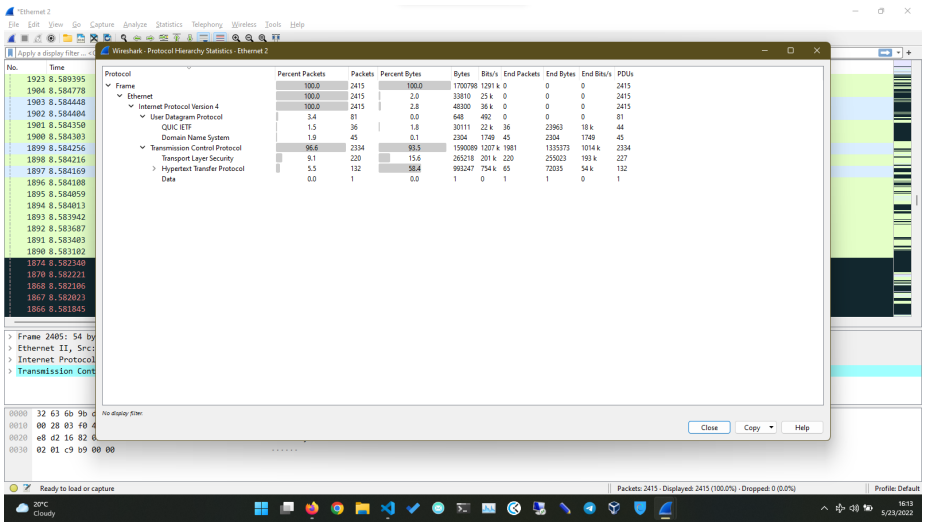

Figure 1: Wireshark Protocol Statistics

1

1.1

As we can see in the figure 1, UDP and TCP are used to transfer data over IPv4. Despite not all of the packets are used for loading `ce.sharif.edu`, browser had used both of them to transfer data. It used UDP for DNS queries and TCP for HTTP requests.

1.2

First, we can sort the packets by the protocol type. Now we can see all of the DNS requests togehter. We can see the first DNS request for `ce.sharif.edu` in the figure 2. As we can see, the first request is sent from `172.20.10.3` to `192.168.250.250` for A record of `ce.sharif.edu`. Both of these IP addresses are private LAN addresses so this request is probably to a local DNS. After that we have the second packet sent from `172.20.10.3` to `8.8.8.8` which is the Google DNS server. Then Google DNS server responds and sends the `81.31.168.124` as the IP address of `ce.sharif.edu`. After that we have exact same packets sent and received but for AAAA record; and the final response is not IP address but it is SOA record (`ns1.sharif.ir`) which is a record that tells the server where to find other records. After that we can see some other DNS request, like those for `ce.sharif.edu`, for subdomains of `ce.sharif.edu` which are hardware, ai, it, and web.

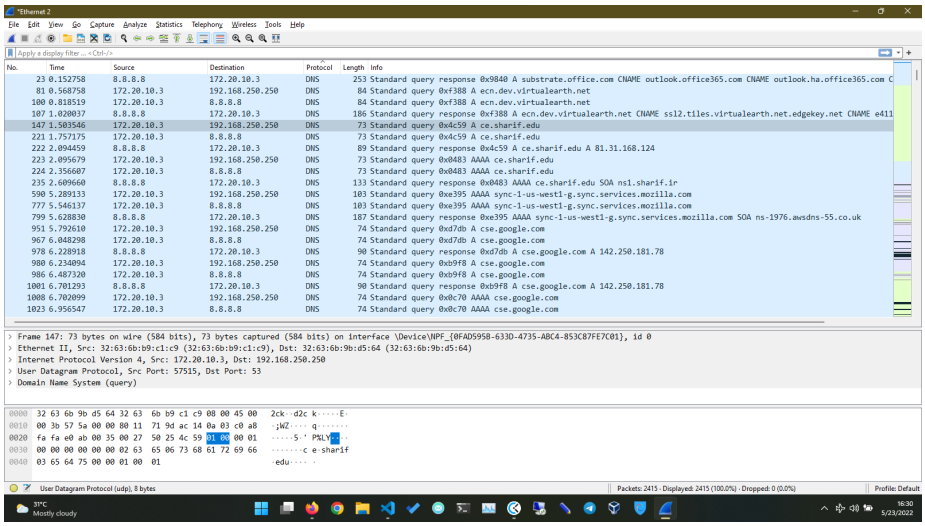

Figure 2: DNS Requests

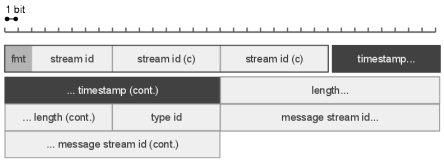

Figure 3: RTMP Packet Structure

2

RTMP or Real-Time Messaging Protocol is a protocol for streaming media over the Internet. It was primarily developed by Micromedia (which is now owned by Adobe Systems) and is used by Adobe Flash Media Server (FMS) to stream media to the client.
RTMP is used in transport-layer protocol like TCP and UDP.
The structure of RTMP packet is shown in the figure 3.
The handshake process is shown in the figure 4.

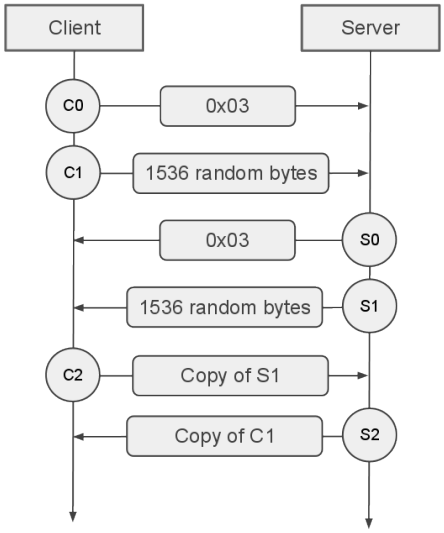

Figure 4: RTMP Handshake Diagram