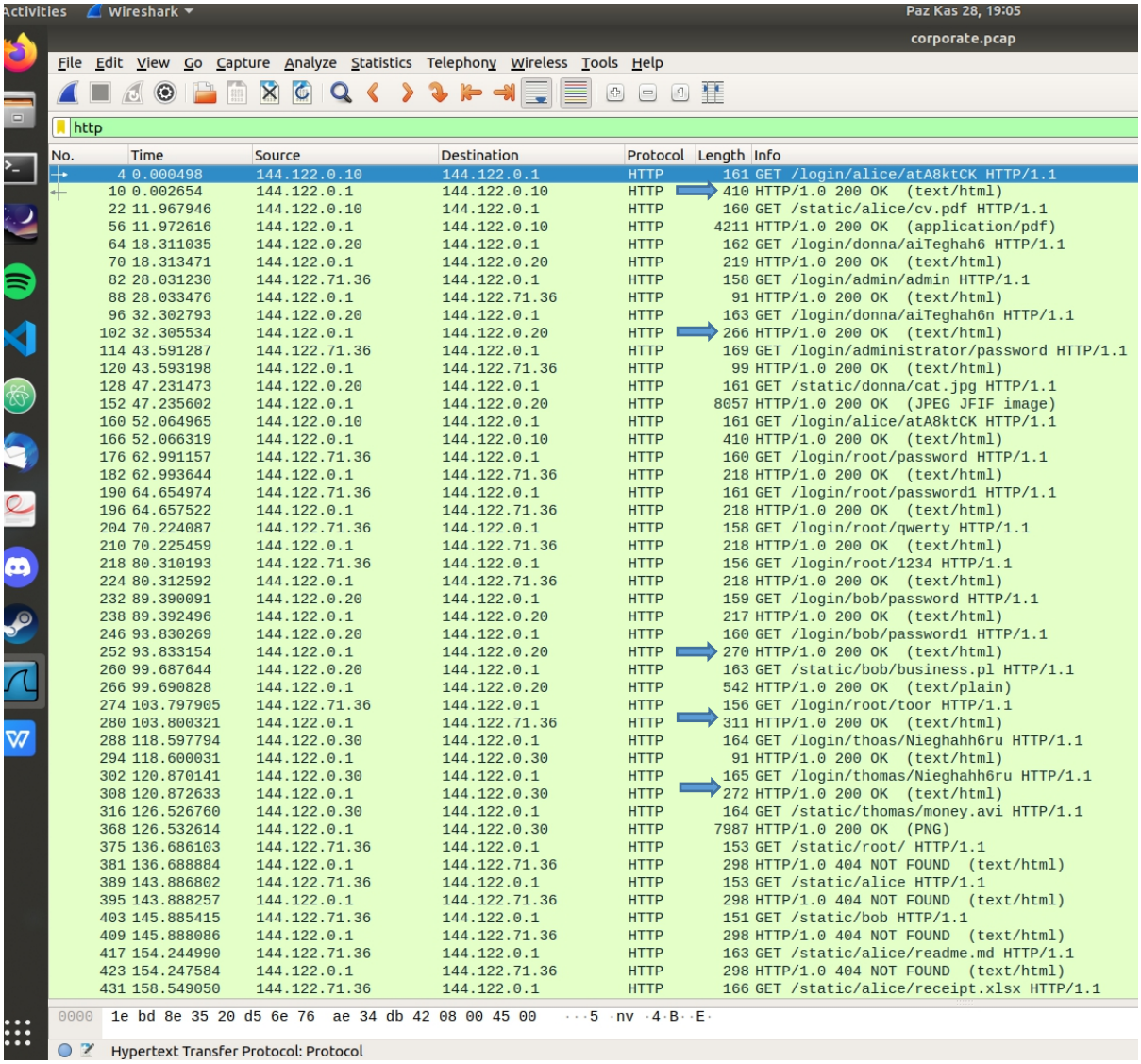
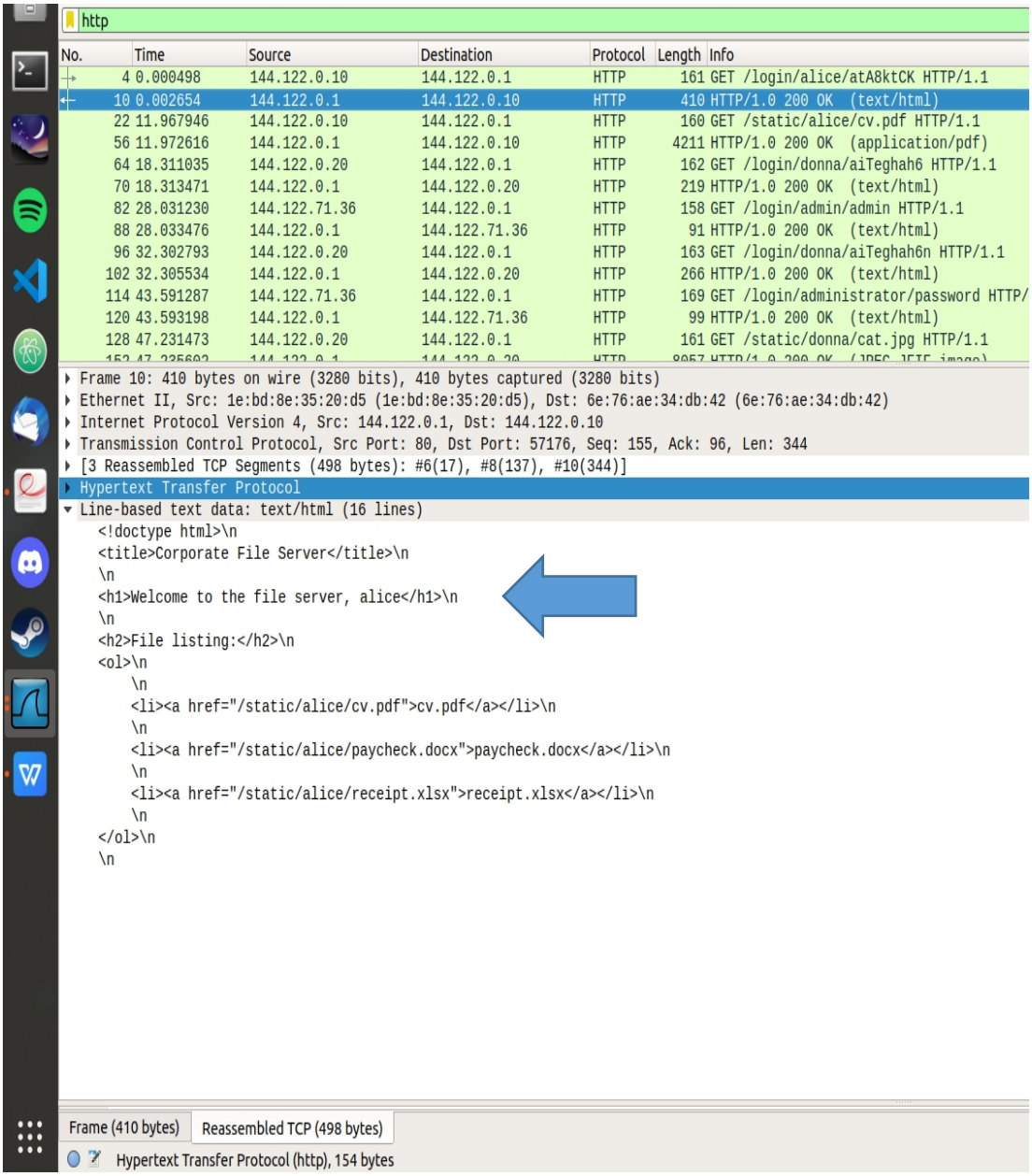
435 THE 1 SOLUTIONS

1.1 and 1.2) I checked the successful logins by looking at responses from 144.122.0.1 ip adressed server. I looked at the line-based text data from wire-shark and checked whether there is welcome message. Marked the screenshot of the successfull logins that writes “Welcome to the file server.” in html file that is recieved. I did not mark the same users twice.

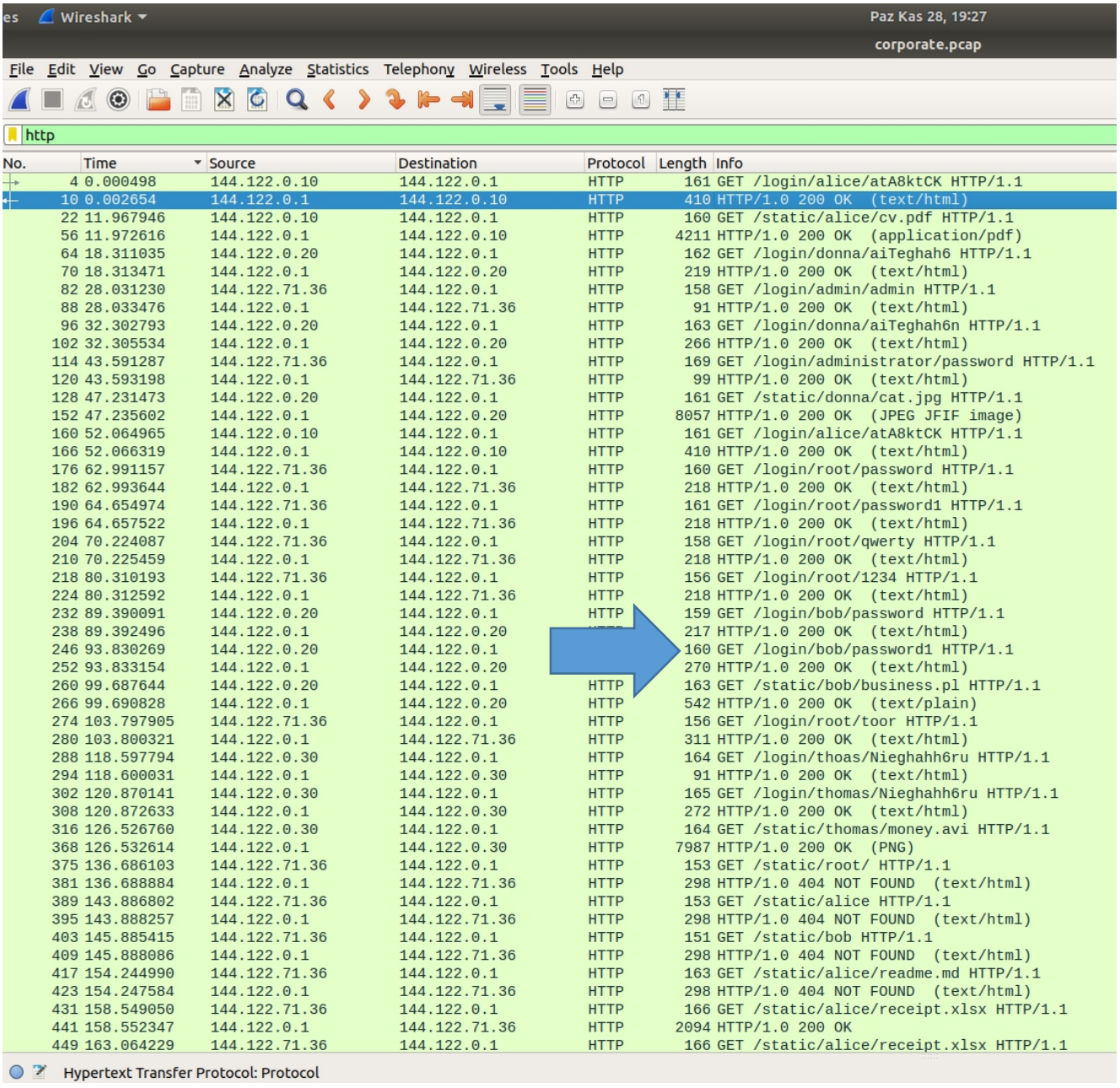
As we can see, there are 5 users that successfully entered the system: alice, donna, root, bob and thomas.



The message i checked for successful enters.



1.3) Looking at the login request that bob send, we can clearly see at first try entering “password” was not successful. After entering “password1” system send welcome message. So bob’s password is “password1”



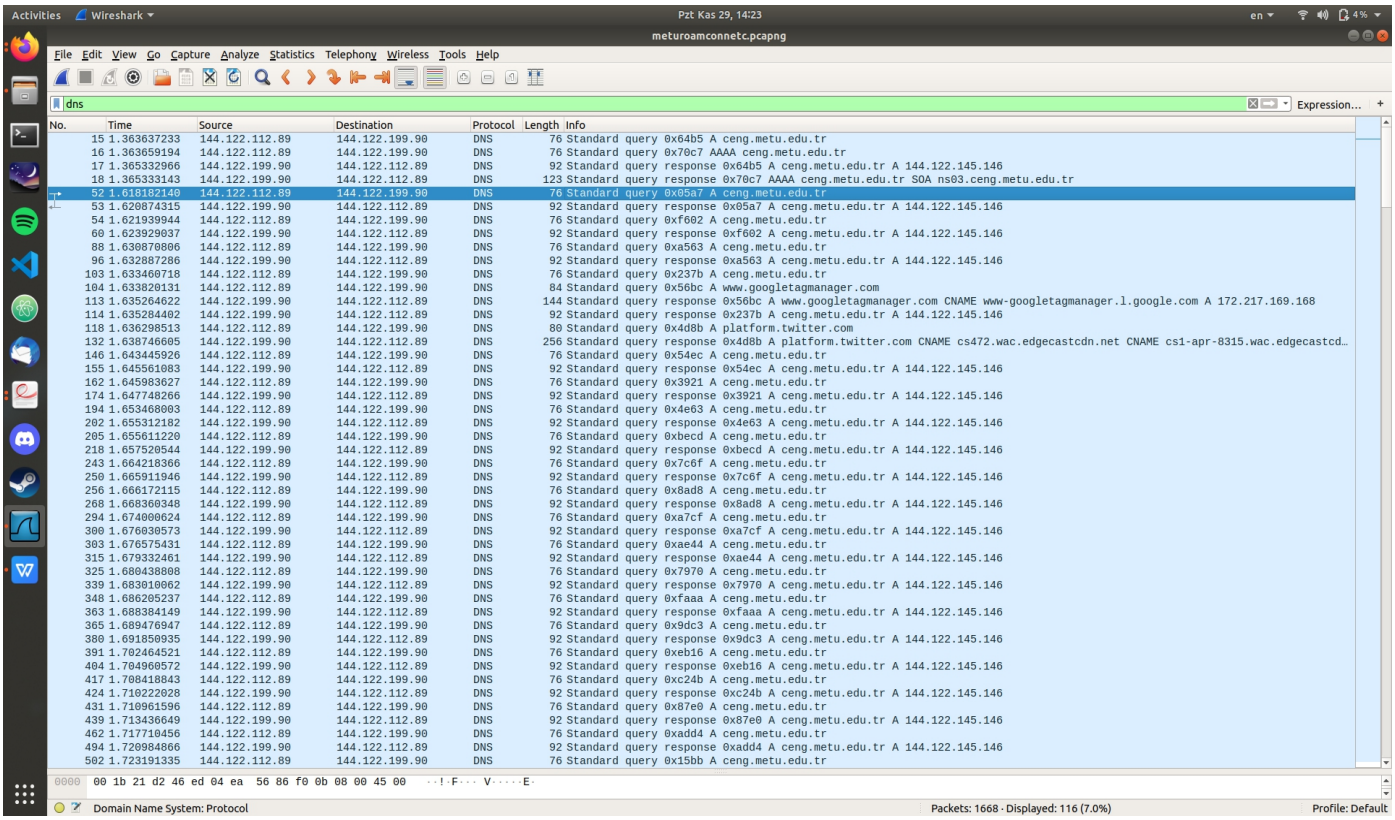
1.4 and 1.5) By looking at the screenshot same ip address (144.122.71.36) tries multiple entries for root user. At first it tries “admin” and “administrator” usernames but fails. After that he/she finds correct username for admin which is “root”, this time he/she enters wrong password for root. After few tries he/she enters system as root user.

After some time same ip adress tries to get information about users in the system. He/she fails at first but we can see he/she gets receipt.xlsx file which belongs to alice by using root privilages.

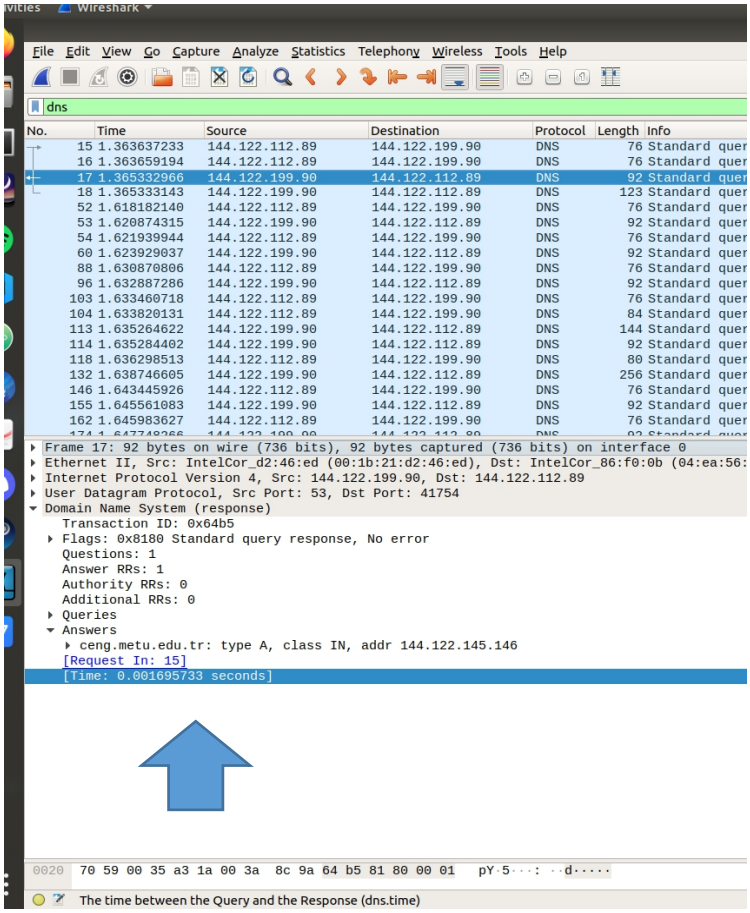
1.6) Since HTTP is not encrypted any person can see the passwords that people uses for entering the system by using correct tools like wireshark application.
Other flaw is although from same ip adress there are multiple failed attemp for entering the system, system lets the user. It does not prevent any user even if they failed to enter for multiple times.

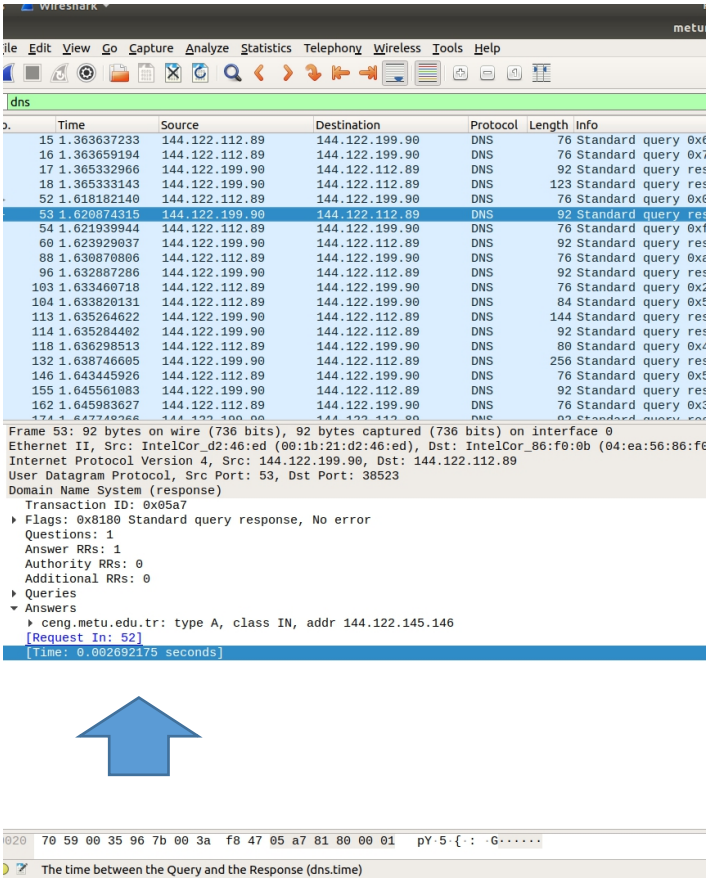
2.1) It is around 50. I believe it is because even if we establish persistent TCP connections for HTTP, for different objects in the website we need make few different HTTP requests. This results in DNS requests for these HTTP requests.

2.2 and 2.3) As seen in this screenshot, every DNS response comes from the same ip adress and goes to the same ip adress which is 144.122.112.90. We can conclude that there is only one server queried for DNS requests.



2.4)

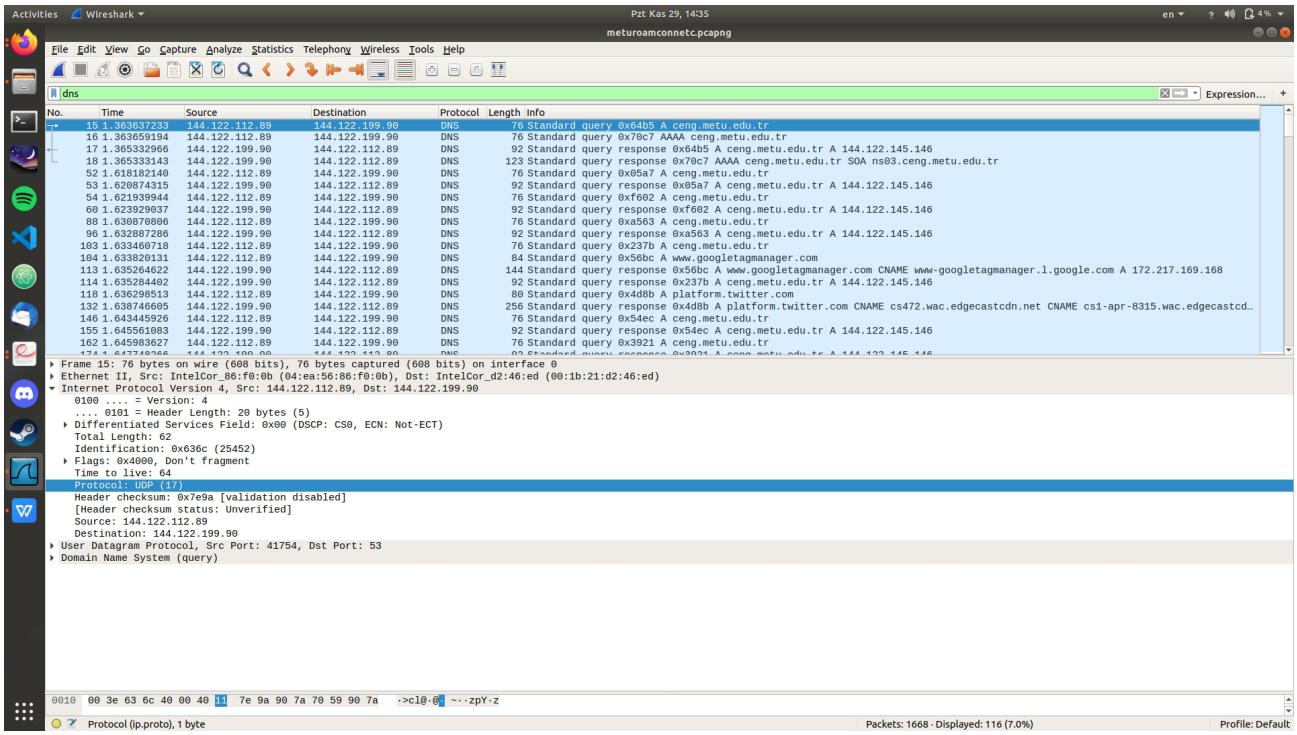




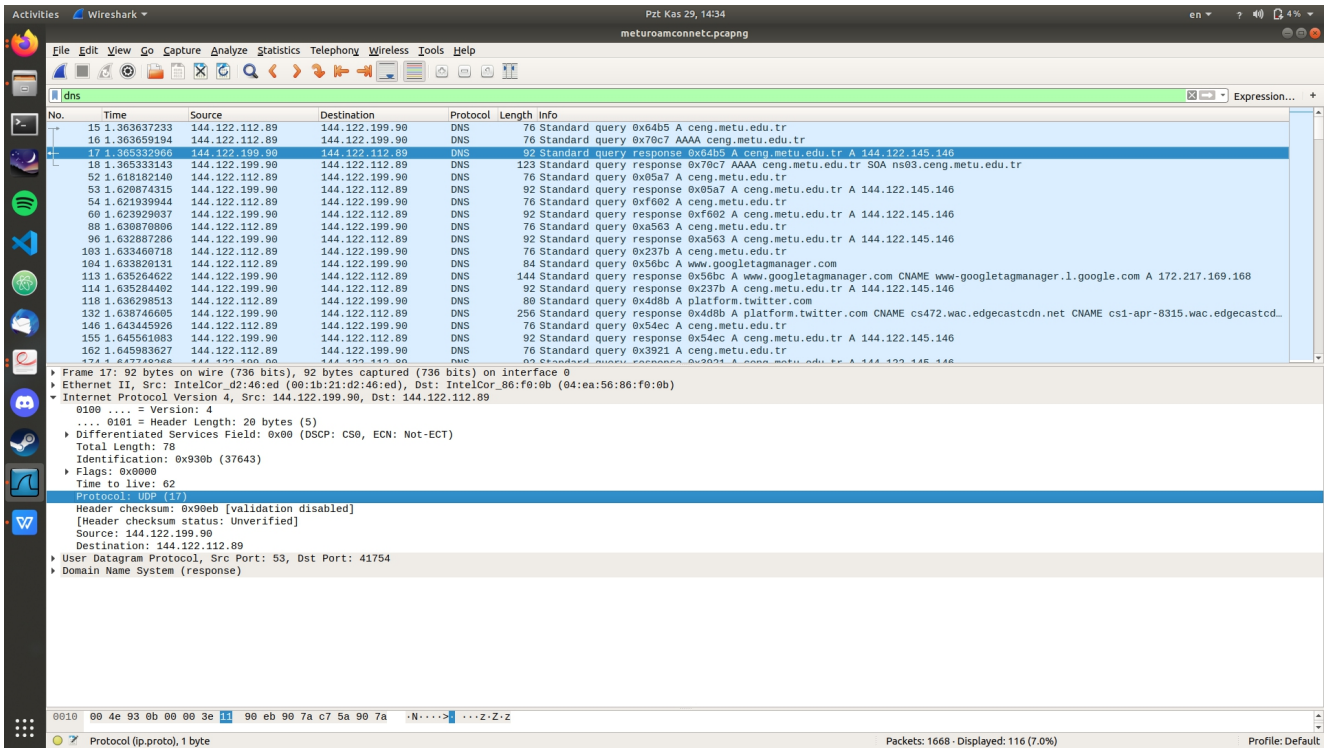
By looking at the screenshots of first and second A type responses, we can conclude the website is already cached in the local DNS server when we make request for its IP. Moreover, the second response takes more time to arrive than the first one.

2.5)

First Request

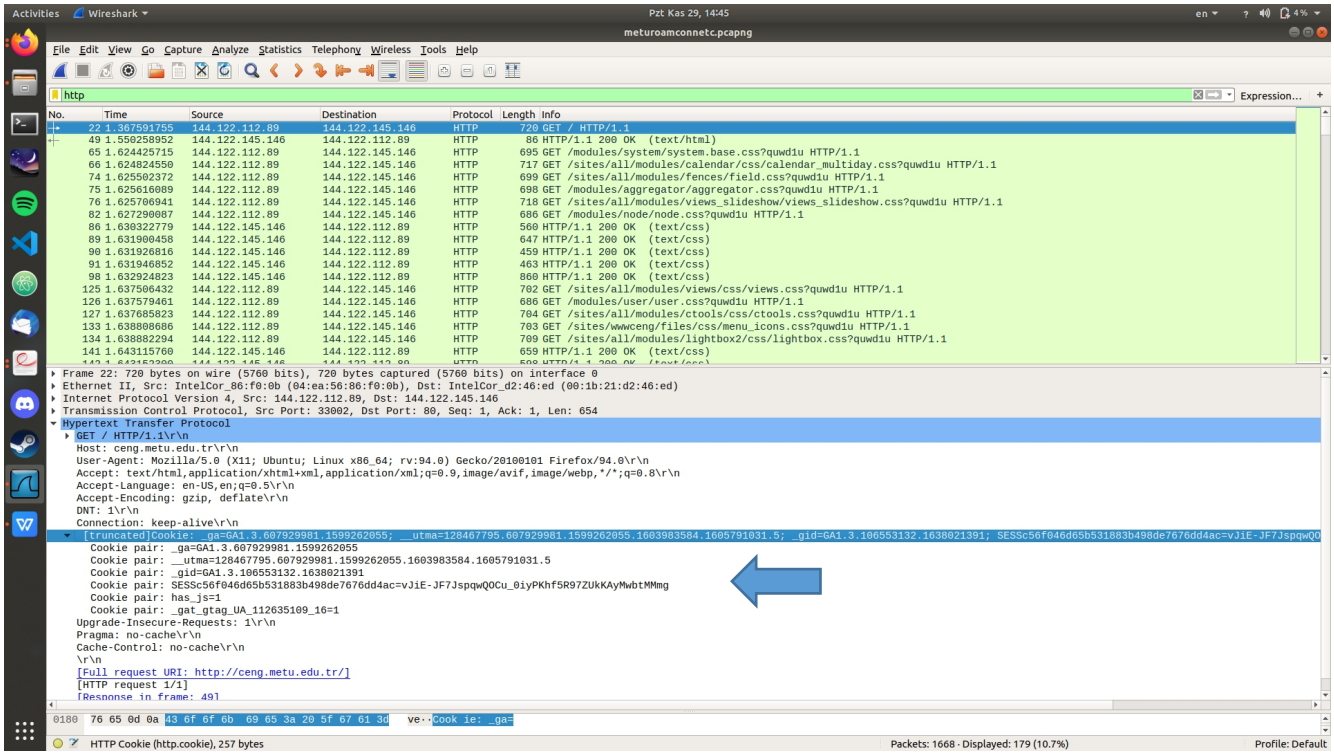


First Response



Both request and response uses UDP. It is because UDP is much faster than TCP connection. In TCP connection we need to first make a handshake between client and server. This kind of connection would DNS servers much slower due to the time it takes to make handshake. UDP on the other hand, is much more faster than TCP. Even if we lose the information on the way, we could send another. Also to me, TCP is unnecessary for small requests and responses such as DNS response and requests. They only carry small information like type, hostname, host ip etc.

2.6)



We see cookies are sent. Probably the webserver knows our IP and cached it. Thats why in the first request we send cookies to the webserver. Normally in the first request we do not send the cookie, after the webserver knows our IP it sends cookies to us than we send it.

2.7)

User agent is shown in screenshot. We see there is browser information, OS information and some other things. It is necessary because the objects we want could have different versions for different browsers. For example same version of an object could work on the Chrome but may not work on the Mozilla Firefox. Thats why it is needed.