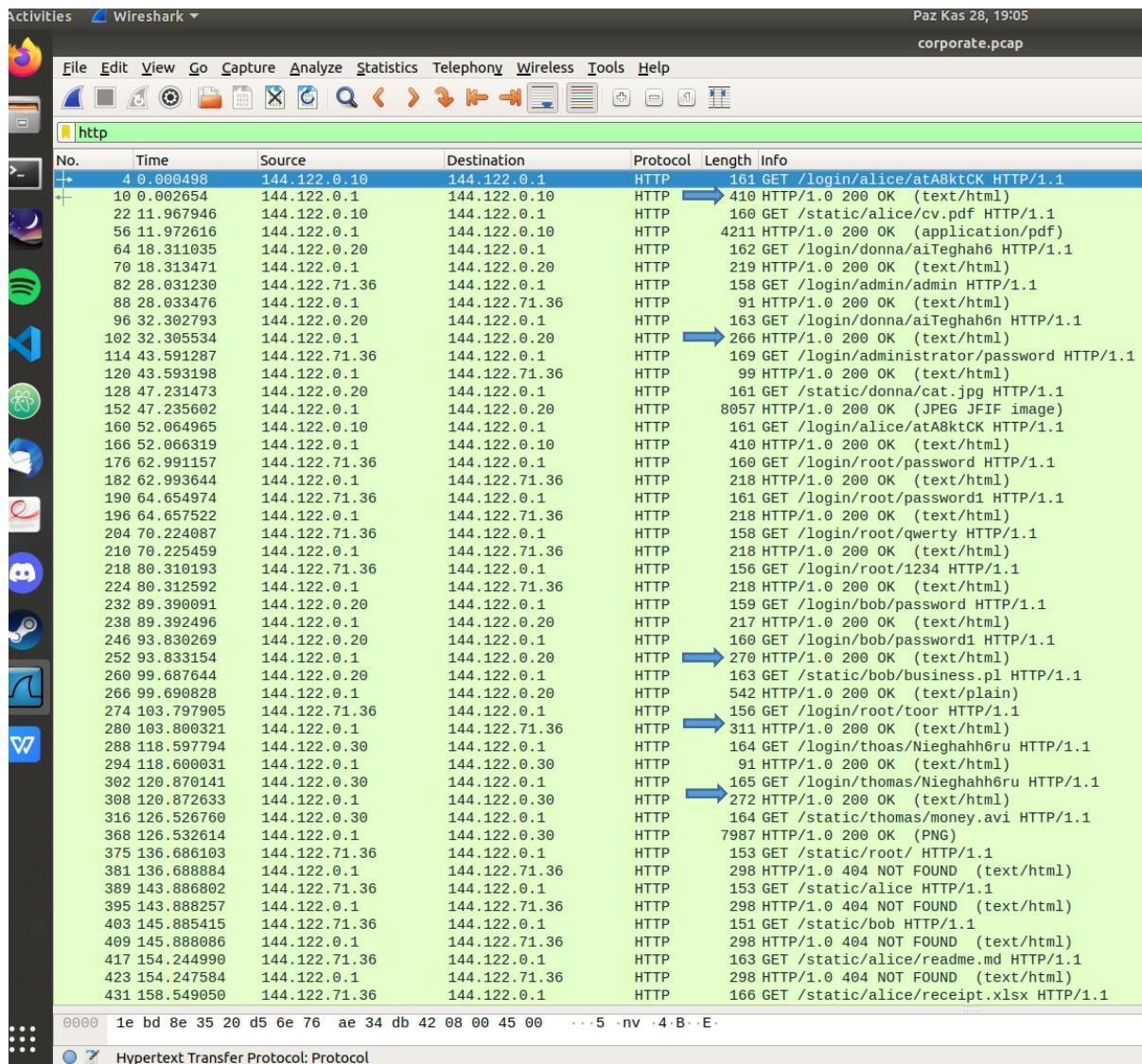


435 THE 1 SOLUTIONS

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.

Screenshot of Wireshark showing network traffic analysis for the HTTP protocol. A blue arrow points to the reassembled TCP segment containing the HTML response.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000498	144.122.0.10	144.122.0.1	HTTP	161	GET /login/alice/atA8ktCK HTTP/1.1
10	0.002654	144.122.0.1	144.122.0.10	HTTP	410	HTTP/1.0 200 OK (text/html)
22	11.967946	144.122.0.10	144.122.0.1	HTTP	160	GET /static/alice/cv.pdf HTTP/1.1
56	11.972616	144.122.0.1	144.122.0.10	HTTP	4211	HTTP/1.0 200 OK (application/pdf)
64	18.311035	144.122.0.20	144.122.0.1	HTTP	162	GET /login/donna/aiTeghah6 HTTP/1.1
70	18.313471	144.122.0.1	144.122.0.20	HTTP	219	HTTP/1.0 200 OK (text/html)
82	28.031230	144.122.71.36	144.122.0.1	HTTP	158	GET /login/admin/admin HTTP/1.1
88	28.033476	144.122.0.1	144.122.71.36	HTTP	91	HTTP/1.0 200 OK (text/html)
96	32.302793	144.122.0.20	144.122.0.1	HTTP	163	GET /login/donna/aiTeghah6n HTTP/1.1
102	32.305534	144.122.0.1	144.122.0.20	HTTP	266	HTTP/1.0 200 OK (text/html)
114	43.591287	144.122.71.36	144.122.0.1	HTTP	169	GET /login/administrator/password HTTP/1.1
120	43.593198	144.122.0.1	144.122.71.36	HTTP	99	HTTP/1.0 200 OK (text/html)
128	47.231473	144.122.0.20	144.122.0.1	HTTP	161	GET /static/donna/cat.jpg HTTP/1.1
152	47.235602	144.122.0.1	144.122.0.20	HTTP	9057	HTTP/1.0 200 OK (JPEG image)

Frame 10: 410 bytes on wire (3280 bits), 410 bytes captured (3280 bits)
Ethernet II, Src: 1e:bd:8e:35:20:d5 (1e:bd:8e:35:20:d5), Dst: 6e:76:ae:34:db:42 (6e:76:ae:34:db:42)
Internet Protocol Version 4, Src: 144.122.0.1, Dst: 144.122.0.10
Transmission Control Protocol, Src Port: 80, Dst Port: 57176, Seq: 155, Ack: 96, Len: 344
[3 Reassembled TCP Segments (498 bytes): #6(17), #8(137), #10(344)]
Hypertext Transfer Protocol
Line-based text data: text/html (16 lines)
<!doctype html>
<title>Corporate File Server</title>
<h1>Welcome to the file server, alice</h1>
<h2>File listing:</h2>

cv.pdf
paycheck.docx
receipt.xlsx

Frame (410 bytes) Reassembled TCP (498 bytes)
Hypertext Transfer Protocol (http), 154 bytes

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”

Wireshark - corporate.pcap

Paz Kas 28, 19:27

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000498	144.122.0.10	144.122.0.1	HTTP	161	GET /login/alice/atA8ktCK HTTP/1.1
10	0.002654	144.122.0.1	144.122.0.10	HTTP	410	HTTP/1.0 200 OK (text/html)
22	11.967946	144.122.0.10	144.122.0.1	HTTP	160	GET /static/alice/cv.pdf HTTP/1.1
56	11.972616	144.122.0.1	144.122.0.10	HTTP	4211	HTTP/1.0 200 OK (application/pdf)
64	18.311035	144.122.0.20	144.122.0.1	HTTP	162	GET /login/donna/aiTeghah6 HTTP/1.1
70	18.313471	144.122.0.1	144.122.0.20	HTTP	219	HTTP/1.0 200 OK (text/html)
82	28.031230	144.122.71.36	144.122.0.1	HTTP	158	GET /login/admin/admin HTTP/1.1
88	28.033476	144.122.0.1	144.122.71.36	HTTP	91	HTTP/1.0 200 OK (text/html)
96	32.302793	144.122.0.20	144.122.0.1	HTTP	163	GET /login/donna/aiTeghah6n HTTP/1.1
102	32.305534	144.122.0.1	144.122.0.20	HTTP	266	HTTP/1.0 200 OK (text/html)
114	43.591287	144.122.71.36	144.122.0.1	HTTP	169	GET /login/administrator/password HTTP/1.1
120	43.593198	144.122.0.1	144.122.71.36	HTTP	99	HTTP/1.0 200 OK (text/html)
128	47.231473	144.122.0.20	144.122.0.1	HTTP	161	GET /static/donna/cat.jpg HTTP/1.1
152	47.235602	144.122.0.1	144.122.0.20	HTTP	8057	HTTP/1.0 200 OK (JPEG/JFIF image)
160	52.064965	144.122.0.10	144.122.0.1	HTTP	161	GET /login/alice/atA8ktCK HTTP/1.1
166	52.066319	144.122.0.1	144.122.0.10	HTTP	410	HTTP/1.0 200 OK (text/html)
176	62.991157	144.122.71.36	144.122.0.1	HTTP	160	GET /login/root/password HTTP/1.1
182	62.993644	144.122.0.1	144.122.71.36	HTTP	218	HTTP/1.0 200 OK (text/html)
190	64.654974	144.122.71.36	144.122.0.1	HTTP	161	GET /login/root/password1 HTTP/1.1
196	64.657522	144.122.0.1	144.122.71.36	HTTP	218	HTTP/1.0 200 OK (text/html)
204	70.224087	144.122.71.36	144.122.0.1	HTTP	158	GET /login/root/qwerty HTTP/1.1
210	70.225459	144.122.0.1	144.122.71.36	HTTP	218	HTTP/1.0 200 OK (text/html)
218	80.310193	144.122.71.36	144.122.0.1	HTTP	156	GET /login/root/1234 HTTP/1.1
224	80.312592	144.122.0.1	144.122.71.36	HTTP	218	HTTP/1.0 200 OK (text/html)
232	89.390091	144.122.0.20	144.122.0.1	HTTP	159	GET /login/bob/password HTTP/1.1
238	89.392496	144.122.0.1	144.122.0.20	HTTP	217	HTTP/1.0 200 OK (text/html)
246	93.830269	144.122.0.20	144.122.0.1	HTTP	160	GET /login/bob/password1 HTTP/1.1
252	93.833154	144.122.0.1	144.122.0.20	HTTP	270	HTTP/1.0 200 OK (text/html)
260	99.687644	144.122.0.20	144.122.0.1	HTTP	163	GET /static/bob/business.pl HTTP/1.1
266	99.690828	144.122.0.1	144.122.0.20	HTTP	542	HTTP/1.0 200 OK (text/plain)
274	103.797905	144.122.71.36	144.122.0.1	HTTP	156	GET /login/root/toor HTTP/1.1
280	103.800321	144.122.0.1	144.122.71.36	HTTP	311	HTTP/1.0 200 OK (text/html)
288	118.597794	144.122.0.30	144.122.0.1	HTTP	164	GET /login/thoas/Nieghahh6ru HTTP/1.1
294	118.600031	144.122.0.1	144.122.0.30	HTTP	91	HTTP/1.0 200 OK (text/html)
302	120.870141	144.122.0.30	144.122.0.1	HTTP	165	GET /login/thomas/Nieghahh6ru HTTP/1.1
308	120.872633	144.122.0.1	144.122.0.30	HTTP	272	HTTP/1.0 200 OK (text/html)
316	126.526760	144.122.0.30	144.122.0.1	HTTP	164	GET /static/thomas/money.avi HTTP/1.1
368	126.532614	144.122.0.1	144.122.0.30	HTTP	7987	HTTP/1.0 200 OK (PNG)
375	136.686103	144.122.71.36	144.122.0.1	HTTP	153	GET /static/root/ HTTP/1.1
381	136.688884	144.122.0.1	144.122.71.36	HTTP	298	HTTP/1.0 404 NOT FOUND (text/html)
389	143.886802	144.122.71.36	144.122.0.1	HTTP	153	GET /static/alice HTTP/1.1
395	143.888257	144.122.0.1	144.122.71.36	HTTP	298	HTTP/1.0 404 NOT FOUND (text/html)
403	145.885415	144.122.71.36	144.122.0.1	HTTP	151	GET /static/bob HTTP/1.1
409	145.888086	144.122.0.1	144.122.71.36	HTTP	298	HTTP/1.0 404 NOT FOUND (text/html)
417	154.244990	144.122.71.36	144.122.0.1	HTTP	163	GET /static/alice/readme.md HTTP/1.1
423	154.247584	144.122.0.1	144.122.71.36	HTTP	298	HTTP/1.0 404 NOT FOUND (text/html)
431	158.549050	144.122.71.36	144.122.0.1	HTTP	166	GET /static/alice/receipt.xlsx HTTP/1.1
441	158.552347	144.122.0.1	144.122.71.36	HTTP	2094	HTTP/1.0 200 OK
449	163.064229	144.122.71.36	144.122.0.1	HTTP	166	GET /static/alice/receipt.xlsx HTTP/1.1

Hypertext Transfer Protocol: Protocol

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.

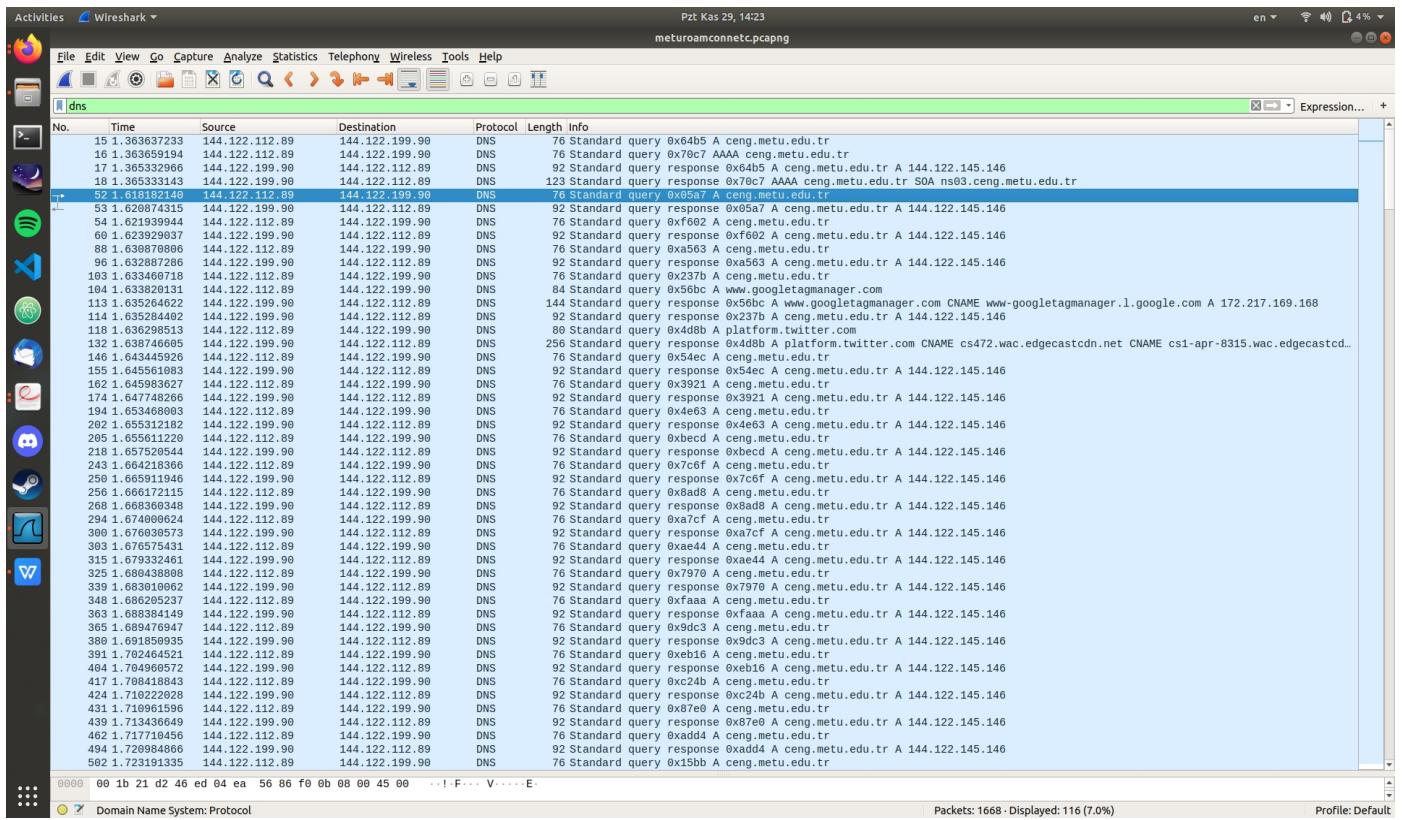
After some time same ip address tries to get information about users in the system. He/she fails at first but we can see he/she gets receipt.xlsx file which belongs to alice by using root privileges.

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.

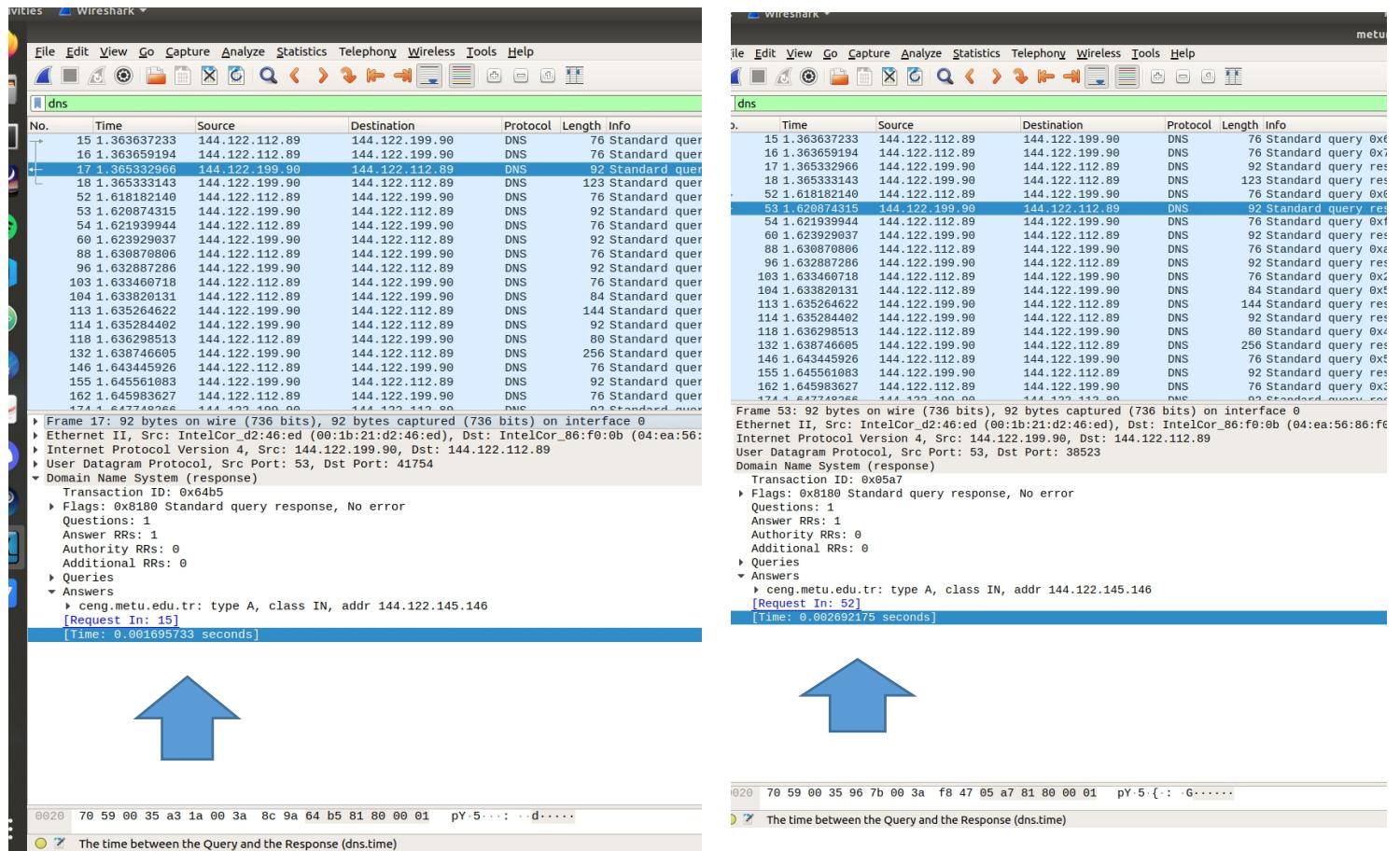
Other flaw is although from same ip address there are multiple failed attempt for entering the system, system lets the user. It does not prevent any user even if they failed to enter for multiple times.

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 address and goes to the same ip address which is 144.122.112.90. We can conclude that there is only one server queried for DNS requests.



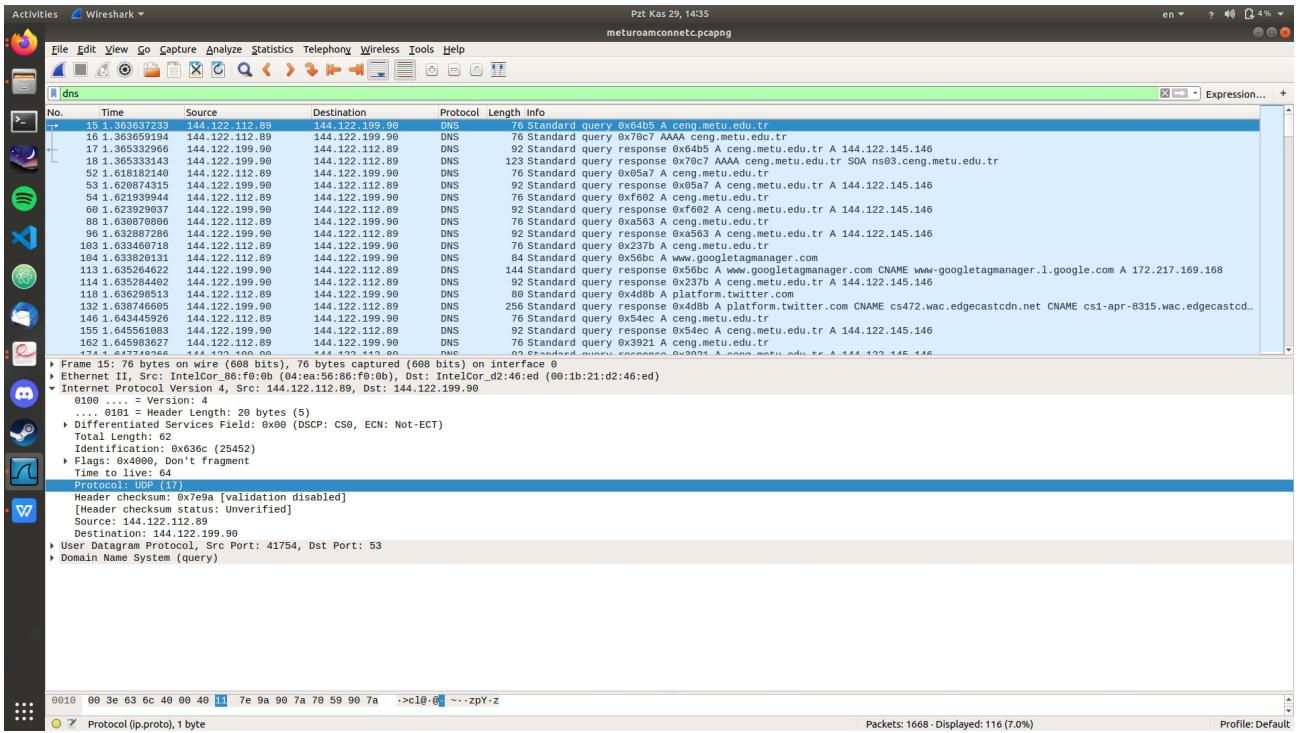
2.4)



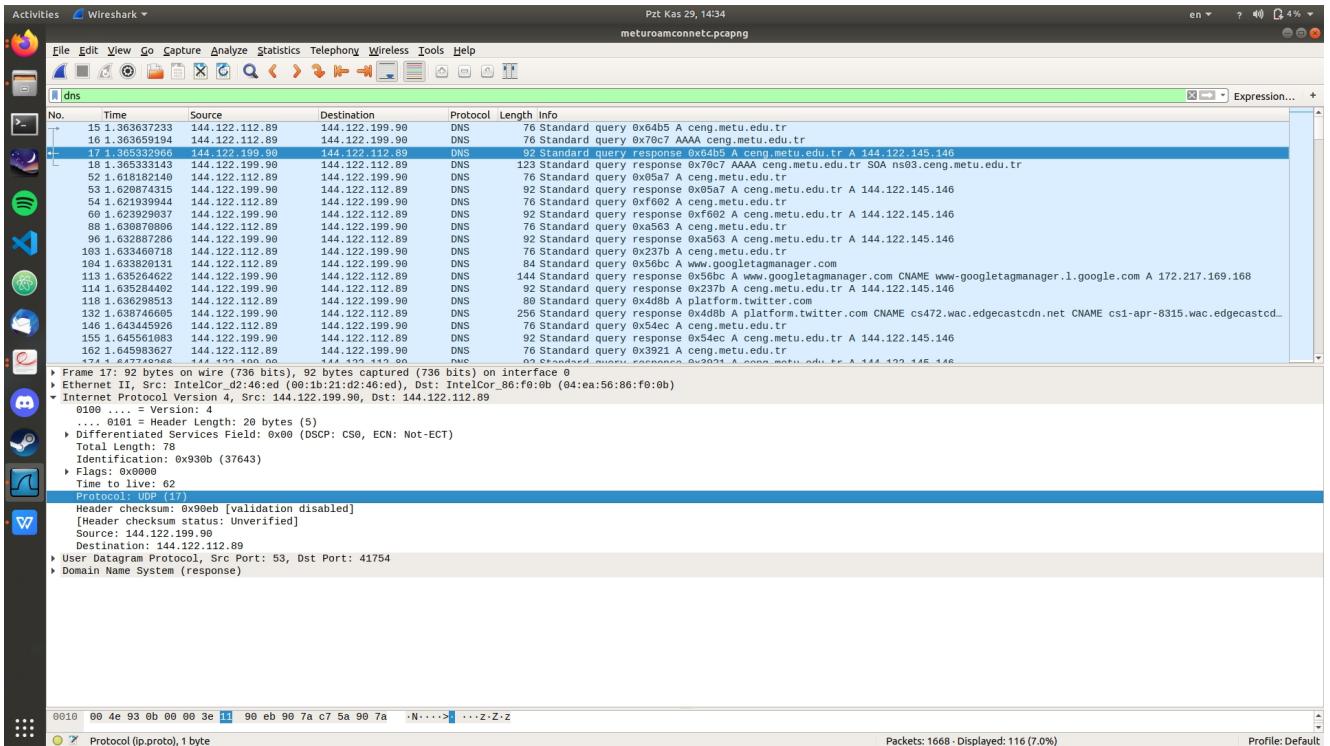
By looking at the screenshots of first and second A type responses, we can conclude the website is already cached in the local DNS server when we make request for its IP. Moreover, the second response takes more time to arrive than the first one.

2.5)

First Request



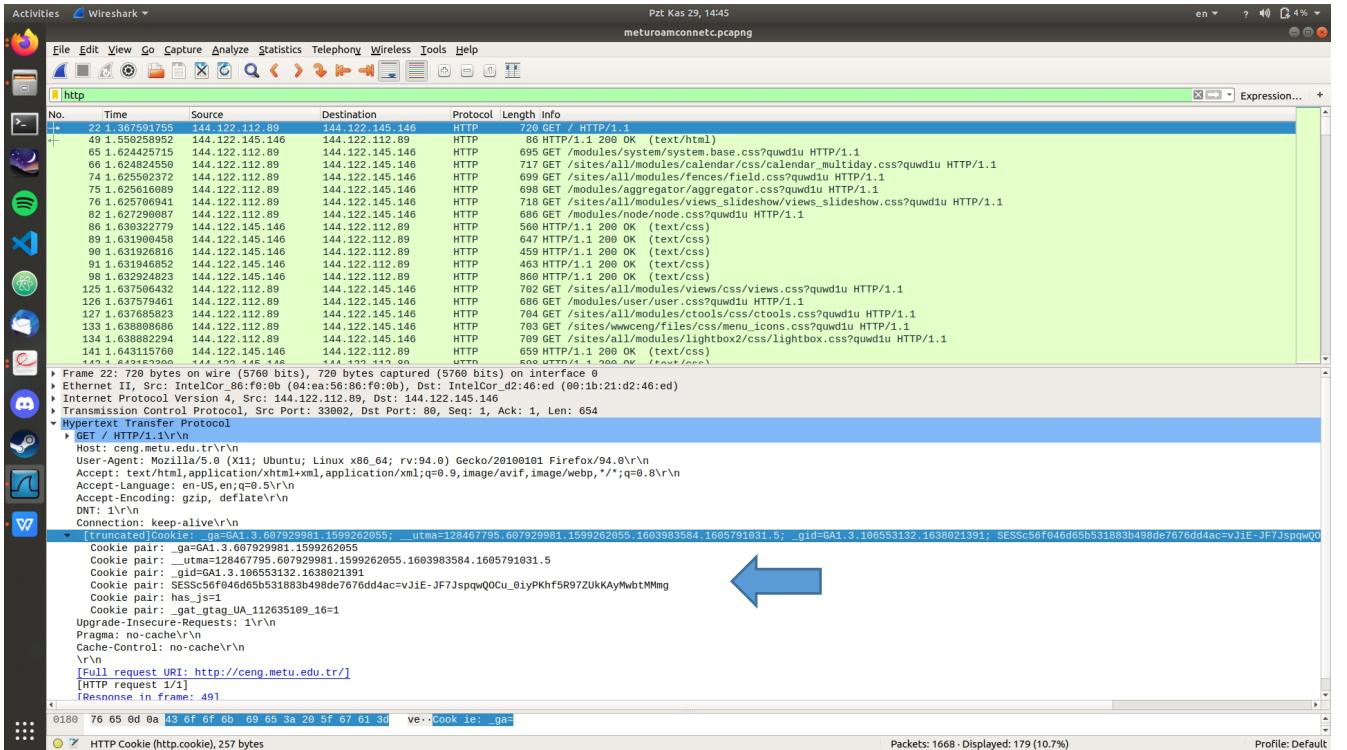
First Response



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.

The screenshot shows the Wireshark interface with several network packets listed in the main pane. A specific packet is selected, highlighted with a blue arrow pointing upwards, which is expanded in the lower-right pane. This selected packet is an HTTP request from the user agent "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:94.0) Gecko/20100101 Firefox/94.0" to the host "ceng.metu.edu.tr". The request is for the URL "http://ceng.metu.edu.tr/modules/system/base.css?quwd1u". The expanded view shows the full header and part of the body of this request.

No.	Time	Source	Destination	Protocol	Length	Info
22	1.367591755	144.122.112.89	144.122.145.146	HTTP	720	HTTP / 1.1
49	1.559258952	144.122.145.146	144.122.112.89	HTTP	86	HTTP / 1.1 200 OK (text/html)
65	1.624425715	144.122.112.89	144.122.145.146	HTTP	695	GET /modules/system/system.base.css?quwd1u HTTP/1.1
66	1.624822455	144.122.112.89	144.122.145.146	HTTP	717	GET /sites/all/modules/calendar/css/calendar_multiday.css?quwd1u HTTP/1.1
74	1.625502372	144.122.112.89	144.122.145.146	HTTP	699	GET /sites/all/modules/fences/field.css?quwd1u HTTP/1.1
75	1.625616088	144.122.112.89	144.122.145.146	HTTP	698	GET /modules/aggregator/aggregator.css?quwd1u HTTP/1.1
76	1.625706941	144.122.112.89	144.122.145.146	HTTP	718	GET /sites/all/modules/views_slideshow/views_slideshow.css?quwd1u HTTP/1.1
82	1.627290087	144.122.112.89	144.122.145.146	HTTP	686	GET /modules/node/node.css?quwd1u HTTP/1.1
86	1.630322779	144.122.145.146	144.122.112.89	HTTP	569	HTTP / 1.1 200 OK (text/css)
89	1.631900450	144.122.145.146	144.122.112.89	HTTP	647	HTTP / 1.1 200 OK (text/css)
90	1.631926814	144.122.145.146	144.122.112.89	HTTP	459	HTTP / 1.1 200 OK (text/css)
91	1.631946852	144.122.145.146	144.122.112.89	HTTP	463	HTTP / 1.1 200 OK (text/css)
98	1.632924802	144.122.145.146	144.122.112.89	HTTP	868	HTTP / 1.1 200 OK (text/css)
125	1.637505432	144.122.112.89	144.122.145.146	HTTP	762	GET /sites/all/modules/views/css/views.css?quwd1u HTTP/1.1
126	1.637579461	144.122.112.89	144.122.145.146	HTTP	696	GET /sites/all/modules/user/user.css?quwd1u HTTP/1.1
127	1.637685823	144.122.112.89	144.122.145.146	HTTP	704	GET /sites/all/modules/ctools/ctools.css?quwd1u HTTP/1.1
133	1.638898686	144.122.112.89	144.122.145.146	HTTP	703	GET /sites/wwwceng/files/css/menu.icons.css?quwd1u HTTP/1.1
134	1.638882294	144.122.112.89	144.122.145.146	HTTP	709	GET /sites/all/modules/lightbox2/css/lightbox.css?quwd1u HTTP/1.1
141	1.643115764	144.122.112.89	144.122.145.146	HTTP	659	HTTP / 1.1 200 OK (text/css)
142	1.642352264	144.122.145.146	144.122.112.89	HTTP	690	HTTP / 1.1 200 OK (text/css)

[Full request URI: http://ceng.metu.edu.tr/modules/system/base.css?quwd1u]
[HTTP request 1/1]
[Response in frame: 98]

0080 67 2e 6d 65 74 75 2e 65 64 75 2e 74 72 0d 0a 55 g.metu.e du.tr..

HTTP User-Agent header (http.user_agent), 90 bytes

Packets: 1668 · Displayed: 179 (10.7%)

Profile: Default