e2264653-report

by ismail sahin

Submission date: 25-Nov-2020 11:54PM (UTC+0300)

Submission ID: 1449825187

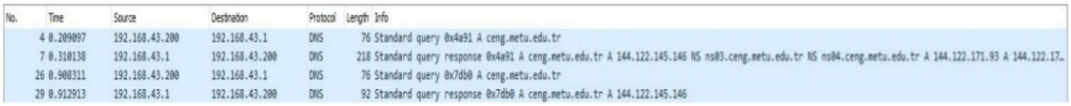
File name: 22117_ismail_sahin_e2264653-report_67008_479808101.pdf (185.88K)

Word count: 343

Character count: 1482

HTTP & DNS

Q1)



```
No.   Time        Source          Destination     Protocol Length Info
    4 0.209097    192.168.43.200  192.168.43.1    DNS      76 Standard query 0x4a91 A ceng.metu.edu.tr
    7 0.310138    192.168.43.1    192.168.43.200  DNS      218 Standard query response 0x4a91 A ceng.metu.edu.tr A 144.122.145.146 NS ns03.ceng.metu.edu.tr NS ns04.ceng.metu.edu.tr A 144.122.171.93 A 144.122.17…
   26 0.908311    192.168.43.200  192.168.43.1    DNS      76 Standard query 0x7db0 A ceng.metu.edu.tr
   29 0.912913    192.168.43.1    192.168.43.200  DNS      92 Standard query response 0x7db0 A ceng.metu.edu.tr A 144.122.145.146
```

2 queries were sent from your computer to the DNS server.

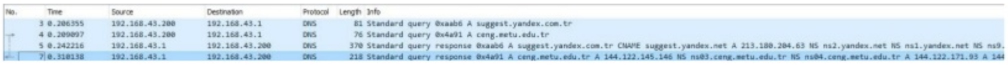
Q2)

The destination address is 192.168.43.1.

Bonus)

We use DNS server to find server address and if it was cached, we do not use that anymore we can use http get request to get web paces so it was not cached.

Q3)



```
No.   Time        Source          Destination     Protocol Length Info
    3 0.206355    192.168.43.200  192.168.43.1    DNS      81 Standard query 0xaab6 A suggest.yandex.com.tr
    4 0.209097    192.168.43.200  192.168.43.1    DNS      76 Standard query 0x4a91 A ceng.metu.edu.tr
    5 0.242216    192.168.43.1    192.168.43.200  DNS      370 Standard query response 0xaab6 A suggest.yandex.com.tr CNAME suggest.yandex.net A 213.180.204.63 NS ns2.yandex.net NS ns1.yandex.net NS ns9.
    7 0.310138    192.168.43.1    192.168.43.200  DNS      218 Standard query response 0x4a91 A ceng.metu.edu.tr A 144.122.145.146 NS ns03.ceng.metu.edu.tr NS ns04.ceng.metu.edu.tr A 144.122.171.93 A 144
```

The first request No:4 and first response is No:7.

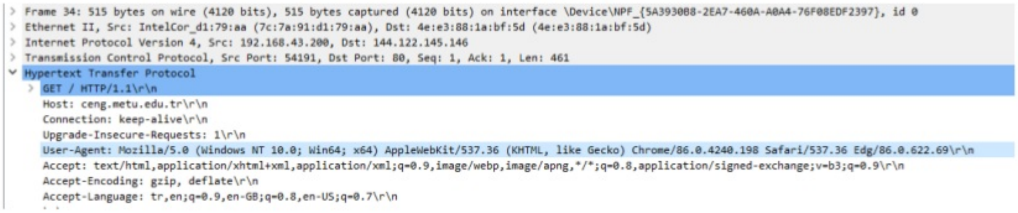
The first request is to find out IP addresses of domain name and it is send by UDP protocol to DNS server. HTTP get request is for getting web pages or contents from web server and this works on TCP protocol.

Q4)

No. Beucause, cookies are created to identify you when you visit a new website. We entered first time to that site so there is no cookie sent with this request.

Q5)

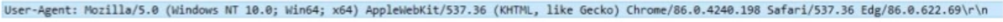
a)



```
> Frame 34: 515 bytes on wire (4120 bits), 515 bytes captured (4120 bits) on interface \Device\NPF_{5A3930B8-2EA7-460A-A0A4-76F08EDF2397}, id 0
> Ethernet II, Src: IntelCor_d1:79:aa (7c:7a:91:d1:79:aa), Dst: 4e:e3:88:1a:bf:5d (4e:e3:88:1a:bf:5d)
> Internet Protocol Version 4, Src: 192.168.43.200, Dst: 144.122.145.146
> Transmission Control Protocol, Src Port: 54191, Dst Port: 80, Seq: 1, Ack: 1, Len: 461
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: ceng.metu.edu.tr\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36 Edg/86.0.622.69\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
```

A user agent string of browsers helps to identify that which browser, what version are being used and on which operating system is the browser.

b)



```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36 Edg/86.0.622.69\r\n
```

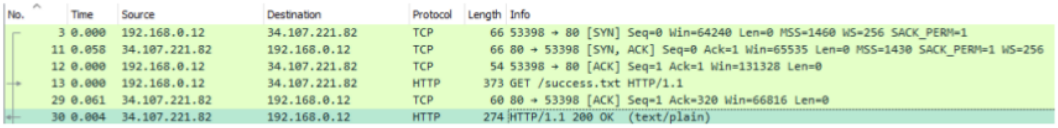
Yes, it includes the browser I am using. (Microsoft Edge).

Yes other browsers are mentioned. Because of history of user agents and browsers. Some servers tend to be see some words as Mozilla to send all supported frames and modern web pages. So some other bwowrsers are mentioned.

HTTPS & TLS

Q1)

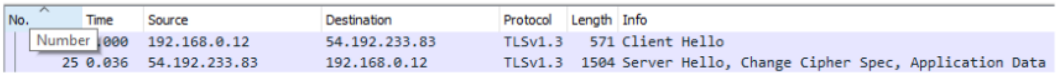
First successful request and response nos are 13 and 30.



No.	Time	Source	Destination	Protocol	Length	Info
3	0.000	192.168.0.12	34.107.221.82	TCP	66	53398 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	0.058	34.107.221.82	192.168.0.12	TCP	66	80 → 53398 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
12	0.000	192.168.0.12	34.107.221.82	TCP	54	53398 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
13	0.000	192.168.0.12	34.107.221.82	HTTP	373	GET /success.txt HTTP/1.1
29	0.061	34.107.221.82	192.168.0.12	TCP	60	80 → 53398 [ACK] Seq=1 Ack=320 Win=66816 Len=0
30	0.004	34.107.221.82	192.168.0.12	HTTP	274	HTTP/1.1 200 OK (text/plain)

When I edit time configurations in milliseconds;
I see that there is 0.04 ms that so, there is 0.00004 second between first request and response.

Q2)



No.	Time	Source	Destination	Protocol	Length	Info
Number	000	192.168.0.12	54.192.233.83	TLSv1.3	571	Client Hello
25	0.036	54.192.233.83	192.168.0.12	TLSv1.3	1504	Server Hello, Change Cipher Spec, Application Data

In the info part of request and response, text written in that box is above. From that we can understand that they are in the first part of comminication, such as getting know each other.

Q3)

13 “hello” message sent by client and 13 “hello” message sent by server. First messages cannot be reached or maybe it is not answered. So new hello messaje can be send. When connection is lost it can be send again to reconnect to server by new hello message.