Student Information

Full Name: Ozan Akın
Id Number: 2309599

HTTP & DNS (70 Points)

Type your answers under the appropriate subsections.

1. (8 Points)

1 query was sent from my computer to DNS server to get "ceng.metu.edu.tr".

No.	Time	Source	Destination	Protocol	Length	Info
6	0.0045…	192.168.1.45	1.1.1.1	DNS	87	Standard query 0xefd4 A ceng.metu.edu.tr OPT

DNS query for ceng.metu.edu.tr

2. (10 Points)

Destination address of the server where the DNS query was answered is 1.1.1.1.

2. (Bonus) (10 Bonus Points)

Server address was found in Cloudflare DNS server, 1.1.1.1. Later it was cached by my local DNS server since there is only one dns query for ceng.metu.edu.tr.

3. (15 Points)

The query with no 8 is the first request was sent, and the query with no 17 is the first response was received.

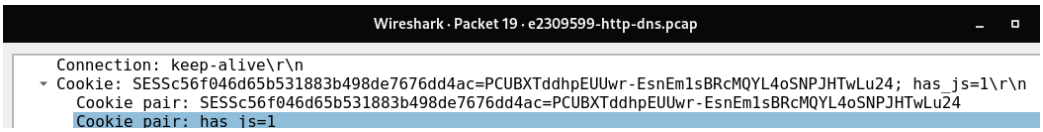
No.	Time	Source	Destination	Protocol	Length	Info
8	0.0199…	192.168.1.45	144.122.145.146	TCP	74	35720 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=132160880 TSecr=0 WS=128
17	0.0358…	144.122.145.146	192.168.1.45	TCP	74	80 → 35720 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 TSval=88287395 TSecr=132160880 WS=1024

The first request and response queries

It is not a HTTP request since HTTP is an application layer protocol based on top of TCP. A TCP handshake (SYN, SYN-ACK) is required before sending the HTTP packet.

4. (15 Points)

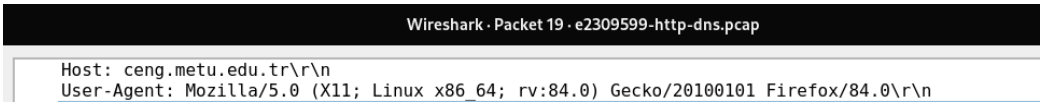
Yes, a cookie was sent with the first HTTP request. The first HTTP request's no is 19 and there is a cookie field inside the HTTP protocol.



The Cookie was sent with the first HTTP package

5a. (7 Points)

The user agent string is "Mozilla/5.0 (X11; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0".



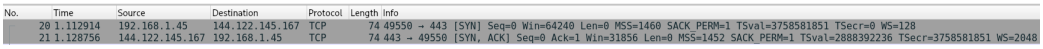
The User-Agent was sent with HTTP requests

5b. (15 Points)

Yes, it includes my browser, which is Mozilla Firefox. Also there are some other things have mentioned, "Mozilla and Gecko". However these are not browsers. "Gecko/20100101" is the browser/render engine with its version which Firefox is based on. And "Mozilla/5.0" is the Mozilla token which is found in most modern browsers. These browser strings other than my actual browser are sent to resolve possible compatibility problems.

HTTPS & TLS (30 Points)

1. (10 Points)



No.	Time	Source	Destination	Protocol	Length	Info
20	1.112914	192.168.1.45	144.122.145.167	TCP	74	49550 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3758581851 TSecr=0 WS=128
21	1.128756	144.122.145.167	192.168.1.45	TCP	74	443 → 49550 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1452 SACK_PERM=1 TSval=2888392236 TSecr=3758581851 WS=2048

The first request and response pair.

The time difference between the first request and response is 0.015842.

2. (10 Points)

The first requests's info field is "Client Hello", and the first response's info field is "Server Hello, Change Cipher Spec, Application Data". They are in the handshake part for TLS based encrypted communication.

3. (10 Points)

There are 6 client hello and 6 server hello packages. These client hello and server hello packages are actually handshakes belong to different connections, which can be proved by looking theirs source port numbers. Each connection has its own handshake.