Ayhan Okuyan
21601531
CS421-02

Computer Assignment -1

Wireshark Lab

1- ARP, DHCP, DNS, GQUIC, HTTP, NBNS, SSDP, TCP, TLS(v1/v1.2), UDP

2- The get message was sent exactly at 17:56:03.212003 and the packet was received exactly at 17:56:03.363779, which means the transmission took 0.151776 seconds.

3- The internet address of my computer (client) appears to be 139.179.55.96 while the internet address of the server seems to be 128.119.245.12.

4-

```
No. Time Source Destination Protocol Length Info
3892 17:56:03.363779 128.119.245.12 139.179.55.96 HTTP 492 HTTP/1.1 200 OK (text/html)
Frame 3892: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
Ethernet II, Src: SuperMic_8e:b5:5c (0c:c4:7a:8e:b5:5c), Dst: IntelCor_cd:2a:1c (1c:1b:b5:cd:2a:1c)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.55.96
Transmission Control Protocol, Src Port: 80, Dst Port: 51041, Seq: 1, Ack: 534, Len: 438
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Wed, 06 Mar 2019 14:56:03 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Last-Modified: Wed, 06 Mar 2019 06:59:01 GMT\r\n
ETag: "51-58367864cbadf"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.151776000 seconds]
[Request in frame: 3868]
File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

HTTP Lab

- The Basic HTTP GET/response interaction

1- My browser is running HTTP/1.1 as well as the server.

2- The browser accepts Turkish and English Languages, with some variance, given as, tr-TR, tr, en, en-US.

3- The IP address of my computer is 139.179.55.96 while the IP address of the server is 128.119.245.12.

4- The status code returned from the server is 200.

5- This URL was last modified on Wed, 06 Mar 2019 06:59:01 GMT.

6- 128 bytes of data were transferred from the server to client.

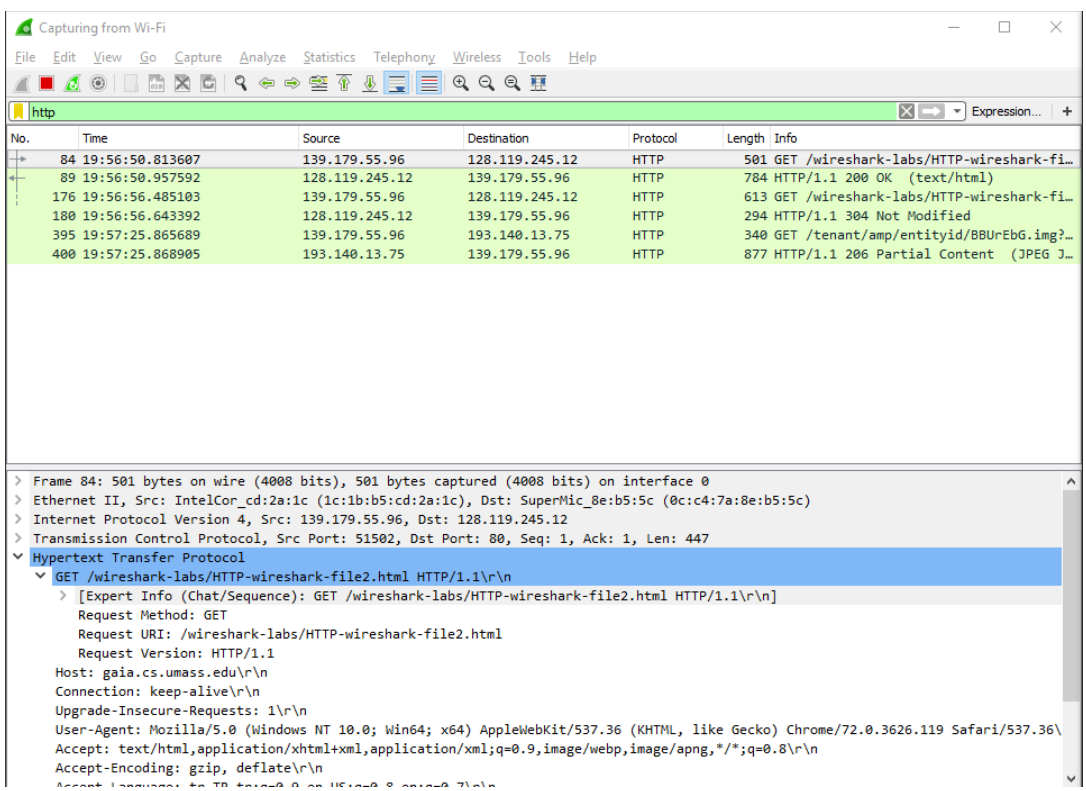
7- No, I don't see any information I don't see on the packet listing window.

Ayhan Okuyan
21601531
CS421-02

```
C :\Users\Dell\AppData\Local\Temp\wireshark_DBD18801-12D F-40A3-9251-BC0B2F072A70_20190306021138_a17652.pcapng 303 total packets, 2 show n
No. Time Source Destination Protocol Length Info
82 02:12:06.385695 139.179.55.83 128.119.245.12 HTTP 501 GET /wireshark-labs/HTTP-wiresharkfile1.
html HTTP/1.1
Frame 82: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface 0
Ethernet II, Src: IntelCor_cd:2a:1c (1c:1b:b5:cd:2a:1c), Dst: SuperMic_8e:b5:5c (0c:c4:7a:8e:b5:5c)
Internet Protocol Version 4, Src: 139.179.55.83, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50557, Dst Port: 80, Seq: 1, Ack: 1, Len: 447
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\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/72.0.3626.119 Safari/
537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 86]
```

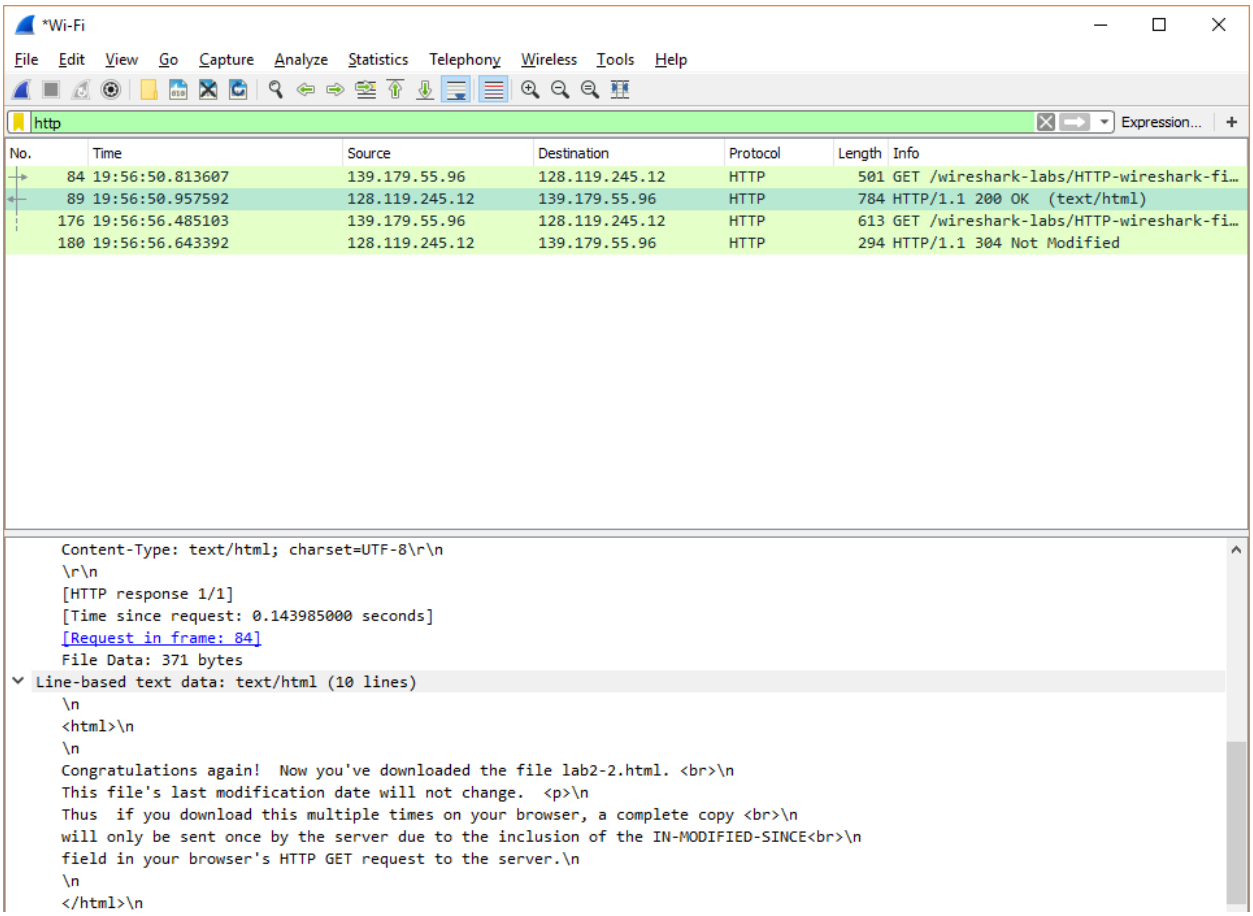
- The HTTP CONDITIONAL GET/response interaction

8- There is no if-modified-since line in the first HTTP GET message.

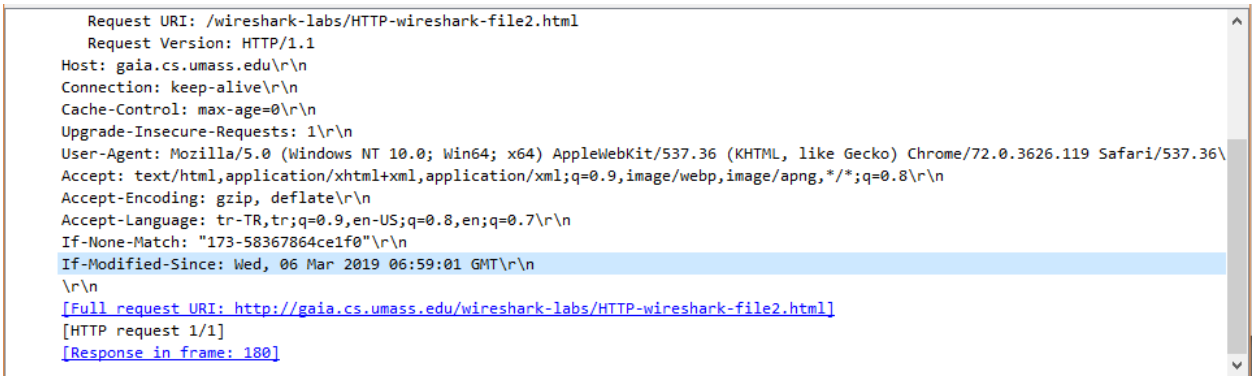


Ayhan Okuyan
21601531
CS421-02

9- The server explicitly returned the contents of the URL, we can observe the line-based text data in HTML language at the end of the server response packet.



10- Yes, in the second GET message, I see an if-modified-since message that contains the data of the date, that is the date of last modification.



11- This time, the status code returned from the server was 304, meaning that the contents of the address was not modified since the last modification. We observe that the contents of the page were not sent by the server again. Simply, the contents were just reloaded on the screen, because the data was indifferent from the one we have requested.

Ayhan Okuyan
21601531
CS421-02

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 51503, Seq: 1, Ack: 560, Len: 240
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Wed, 06 Mar 2019 16:56:56 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-58367864ce1f0"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.158289000 seconds]
    [Request in frame: 176]
```

- Retrieving Long Documents

12- One TCP segment was sent from the client to the server.

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

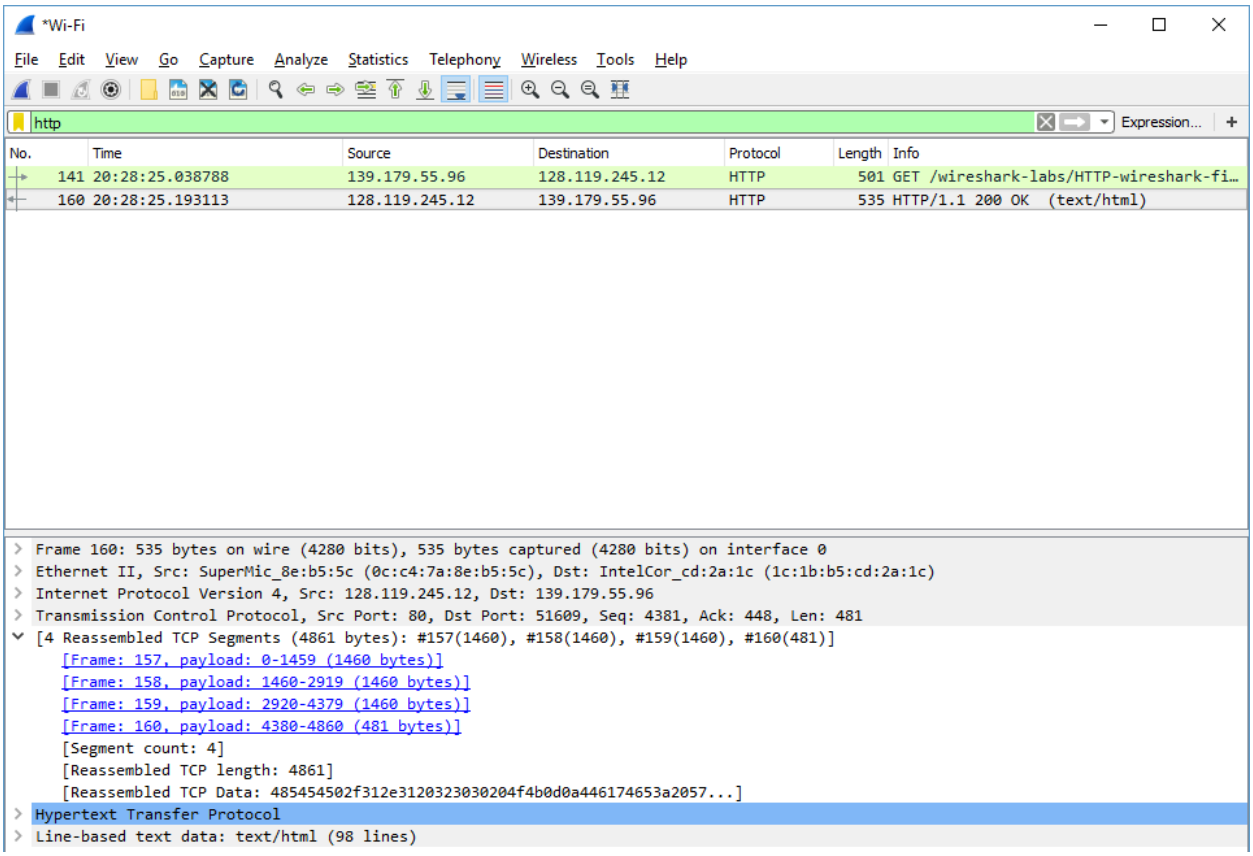
http Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
141	20:28:25.038788	139.179.55.96	128.119.245.12	HTTP	501	GET /wireshark-labs/HTTP-wireshark-fi…
160	20:28:25.193113	128.119.245.12	139.179.55.96	HTTP	535	HTTP/1.1 200 OK (text/html)

```
> Frame 141: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface 0
> Ethernet II, Src: IntelCor_cd:2a:1c (1c:1b:b5:cd:2a:1c), Dst: SuperMic_8e:b5:5c (0c:c4:7a:8e:b5:5c)
> Internet Protocol Version 4, Src: 139.179.55.96, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51609, Dst Port: 80, Seq: 1, Ack: 1, Len: 447
> Hypertext Transfer Protocol
```

13- Four data containing TCP segments were carried to the client from the server. All of them which are reassembled on the analyzer section.

Ayhan Okuyan
21601531
CS421-02



14- The status code that was returned from the server is 200 with the response message OK which is clearly represented on the image for the 13th question.

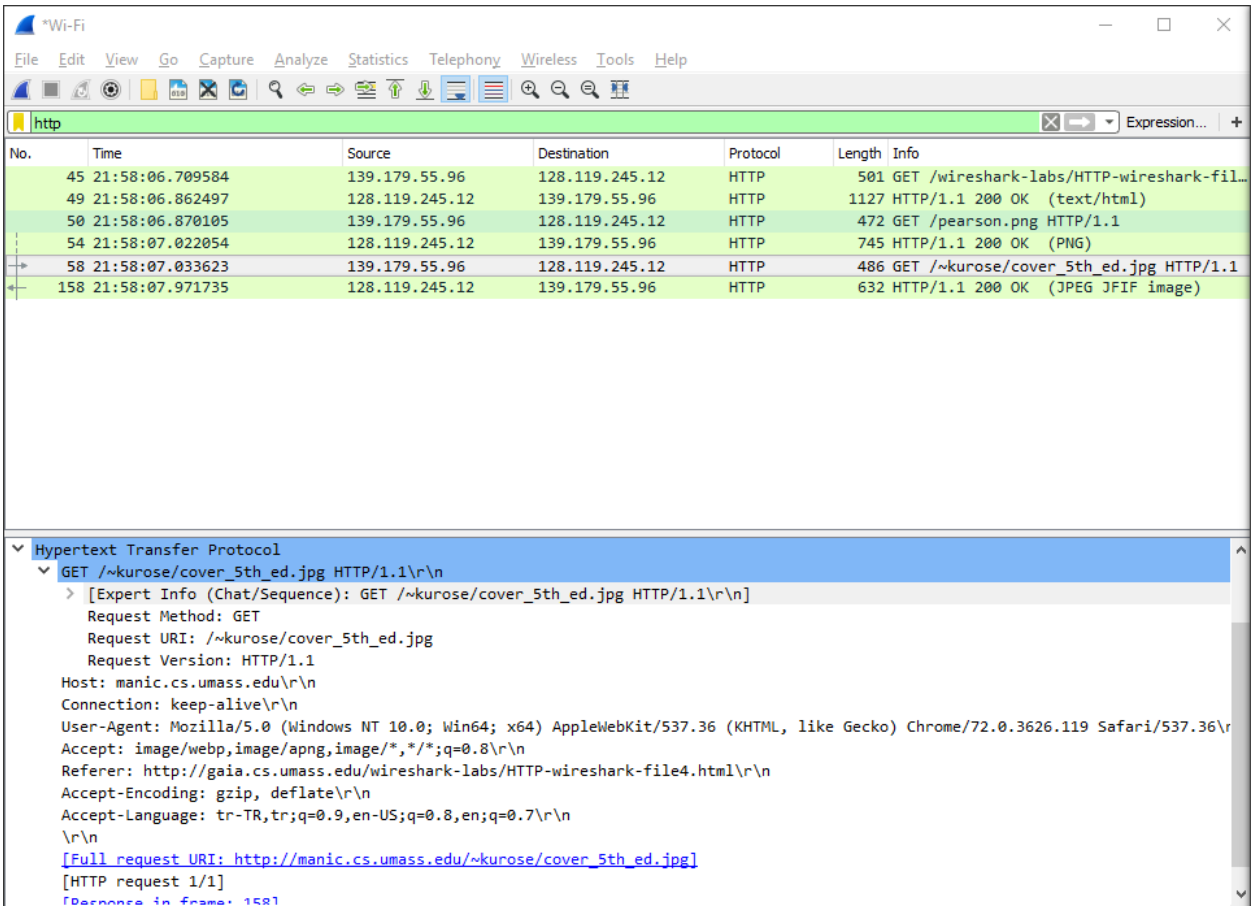
15- No, there are not any HTTP status lines in the transmitted data that are related to continuation.

- HTML Documents with Embedded Objects

16- In total three HTTP GET messages were sent to the server, one for the HTML text, one for the PNG image and one for the JPEG/JFIF image that is contained on the webpage.

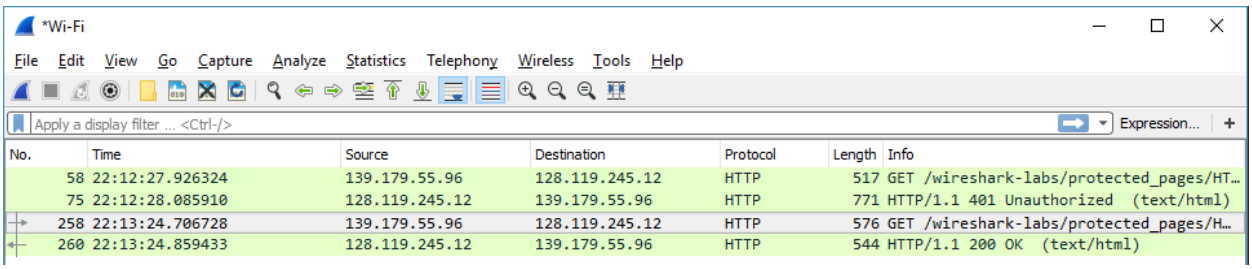
17- We can see that the images are downloaded from the sources separately, in order rather than in parallel. We can see that the GET message for the first image (PNG) is downloaded at 21:58:06.870105 and the server response is documented at the time 21:58:07.022054. Then we look at the GET message for the second image (JPEG), which is done on 21:58:07.033623. Here, we see that the GET request was done after the server fully receives the first image. (The screenshots that are used to answer these questions are given below)

Ayhan Okuyan
21601531
CS421-02



-HTTP Authentication

18- The response message of the server to client is 401, which is described as "Unauthorized".



19- In the second HTTP GET message, the field "Authorization" is added, to the standard HTTP format, with a section "Credentials" with the username and password that I have typed into the browser. (wireshark-students and network)

Ayhan Okuyan
21601531
CS421-02

```
> Transmission Control Protocol, Src Port: 60752, Dst Port: 80, Seq: 1, Ack: 1, Len: 522
v Hypertext Transfer Protocol
  v GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.119 Safari/537.36\r
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
```

DNS Lab

-nslookup

1- I have looked at the server of mit.edu first to get all the servers that are associated with the alias. Then from the servers that I have found, I have searched for the one that has an Asia domain, which is asia1.akam.net. Then I have searched for that address specifically and got the address 95.100.175.64.

```
Command Prompt
Microsoft Windows [Version 10.0.17134.590]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Dell>nslookup www.mit.edu
Server:  dns49.turktelekom.com.tr
Address:  195.175.39.49

Non-authoritative answer:
Name:    e9566.dscb.akamaiedge.net
Addresses:  2a02:26f0:c00:48d::255e
          2a02:26f0:c00:4a4::255e
          104.86.234.56
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net


C:\Users\Dell>nslookup -type=NS mit.edu
Server:  dns49.turktelekom.com.tr
Address:  195.175.39.49

Non-authoritative answer:
mit.edu nameserver = use2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net

C:\Users\Dell>nslookup asia1.akam.net
Server:  dns49.turktelekom.com.tr
Address:  195.175.39.49

Non-authoritative answer:
Name:    asia1.akam.net
Address:  95.100.175.64
```

2- The university that I have found the DNS server for is the EPFL. The alias for its authoritative server is www.epfl.ch. After I have found the alias, I have searched for the name servers by using the -type=NS command. The server names that I have found

were stisun2.epfl.ch and stisun1.epfl.ch. Then I searched them to get the authoritative server addresses which turned out to be 128.178.15.8 for stisun1.epfl.ch and 128.178.15.7 for stisun2.epfl.ch.

```
Command Prompt

C:\Users\Dell>nslookup -type=NS epfl.ch
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
epfl.ch nameserver = stisun1.epfl.ch
epfl.ch nameserver = stisun2.epfl.ch

C:\Users\Dell>nslookup stisun1.epfl.ch
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
Name:    stisun1.epfl.ch
Addresses:  2001:620:618:10f:1:80b2:f08:1
          128.178.15.8


C:\Users\Dell>nslookup stisun2.epfl.ch
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
Name:    stisun2.epfl.ch
Addresses:  2001:620:618:10f:1:80b2:f07:1
          128.178.15.7


C:\Users\Dell>
```

3- After I found the DNS addresses, I have queried that server to search for the mail.yahoo.com which is the Yahoo! Mail server alias. When I did, the server has refused my query. Then I tried a different approach where I queried the EPFL DNS server for the yahoo alias, which has given me the location of a Yahoo mail server from Ireland Dublin. The address is given as 87.248.118.22 which I confirmed from http://whois.domaintools.com/87.248.118.22.

```
Command Prompt
Microsoft Windows [Version 10.0.17134.590]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Dell>nslookup mail.yahoo.com stisun1.epfl.ch
Server:  stisun1.epfl.ch
Address:  128.178.15.8

*** stisun1.epfl.ch can't find mail.yahoo.com: Query refused

C:\Users\Dell>nslookup stisun1.epfl.ch mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  87.248.118.22

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

Ayhan Okuyan
21601531
CS421-02

-Tracing DNS with Wireshark

4- The query messages between my IP address and http://www.ietf.org were sent over User Datagram Protocol (UDP).

ip.addr == 172.20.10.1 Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
4	17:12:19.748962	172.20.10.2	172.20.10.1	DNS	72	Standard query 0x22a7 A www.ietf.org
5	17:12:19.756607	172.20.10.1	172.20.10.2	DNS	149	Standard query response 0x22a7 A www.i…

```
> Frame 4: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: IntelCor_cd:2a:1c (1c:1b:b5:cd:2a:1c), Dst: 3a:65:90:a4:25:64 (3a:65:90:a4:25:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.1
v User Datagram Protocol, Src Port: 62549, Dst Port: 53
    Source Port: 62549
    Destination Port: 53
    Length: 38
    Checksum: 0x6c63 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
> Domain Name System (query)
```

5- The destination port for the DNS query message was 53. The source port of the DNS response message is also given as port 53, which is an indication that the port 53 for UDP listens and responses from the same port.

Query:

```
> Frame 4: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: IntelCor_cd:2a:1c (1c:1b:b5:cd:2a:1c), Dst: 3a:65:90:a4:25:64 (3a:65:90:a4:25:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.1
v User Datagram Protocol, Src Port: 62549, Dst Port: 53
    Source Port: 62549
    Destination Port: 53
    Length: 38
    Checksum: 0x6c63 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
> Domain Name System (query)
```

Response:

```
> Frame 5: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
> Ethernet II, Src: 3a:65:90:a4:25:64 (3a:65:90:a4:25:64), Dst: IntelCor_cd:2a:1c (1c:1b:b5:cd:2a:1c)
> Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.2
v User Datagram Protocol, Src Port: 53, Dst Port: 62549
    Source Port: 53
    Destination Port: 62549
    Length: 115
    Checksum: 0x5a29 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
> Domain Name System (response)
```

6- The DNS query is sent to the IP address 172.20.10.1, which is also the IP address of my local DNS server.

Ayhan Okuyan
21601531
CS421-02

```
Select Command Prompt
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 1E-1B-B5-CD-2A-1C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9462
   Physical Address. . . . . . . . . : 1C-1B-B5-CD-2A-1C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c4b6:2db5:44d7:5f97%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.20.10.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Lease Obtained. . . . . . . . . . : Tuesday, March 12, 2019 4:13:46 PM
   Lease Expires . . . . . . . . . . : Wednesday, March 13, 2019 3:59:25 PM
   Default Gateway . . . . . . . . . : 172.20.10.1
   DHCP Server . . . . . . . . . . . : 172.20.10.1
   DHCPv6 IAID . . . . . . . . . . . : 253500341
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-86-BA-18-3C-2C-30-BC-5C-F3
   DNS Servers . . . . . . . . . . . : 172.20.10.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
```

7- The DNS query message is classified as a type A query. However, it does not contain any answers.

```
Domain Name System (query)
    Transaction ID: 0x22a7
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
    [Response In: 5]
```

8- There are three separate answers on the response message. One is the canonical name, also known as the alias of the DNS of the host. The other two are the host addresses, also known as the A type addresses. The canonical name is given as www.ietf.org.cdn.cloudfare.net and the two host addresses are 104.20.0.85 and 104.20.1.85.

Ayhan Okuyan
21601531
CS421-02

```
> Frame 5: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
> Ethernet II, Src: 3a:65:90:a4:25:64 (3a:65:90:a4:25:64), Dst: IntelCor_cd:2a:1c (1c:1b:b5:cd:2a:1c)
> Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.2
> User Datagram Protocol, Src Port: 53, Dst Port: 62549
v Domain Name System (response)
    Transaction ID: 0x22a7
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
        Name: www.ietf.org
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 140
        Data length: 33
        CNAME: www.ietf.org.cdn.cloudflare.net
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
        Name: www.ietf.org.cdn.cloudflare.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 140
        Data length: 4
        Address: 104.20.0.85
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
        Name: www.ietf.org.cdn.cloudflare.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 140
        Data length: 4
        Address: 104.20.1.85
    [Request In: 4]
    [Time: 0.007645000 seconds]
```

9- Yes, the TCP SYN packets are sent to 104.20.0.85, which is one of the provided answers from the DNS response message.

tcp.port == 80 | Expression... | +

No.	Time	Source	Destination	Protocol	Length	Info
6	17:12:19.758050	172.20.10.2	104.20.0.85	TCP	66	63797 → 80 [SYN] Seq=0 Win=17520 Len=0…
7	17:12:19.758050	172.20.10.2	104.20.0.85	TCP	66	63796 → 80 [SYN] Seq=0 Win=17520 Len=0…
8	17:12:19.800654	104.20.0.85	172.20.10.2	TCP	66	80 → 63797 [SYN, ACK] Seq=0 Ack=1 Win=…
9	17:12:19.800654	104.20.0.85	172.20.10.2	TCP	66	80 → 63796 [SYN, ACK] Seq=0 Ack=1 Win=…
10	17:12:19.800786	172.20.10.2	104.20.0.85	TCP	54	63797 → 80 [ACK] Seq=1 Ack=1 Win=17408…
11	17:12:19.800857	172.20.10.2	104.20.0.85	TCP	54	63796 → 80 [ACK] Seq=1 Ack=1 Win=17408…
12	17:12:19.800923	172.20.10.2	104.20.0.85	HTTP	456	GET / HTTP/1.1
13	17:12:19.836134	104.20.0.85	172.20.10.2	TCP	54	80 → 63797 [ACK] Seq=1 Ack=403 Win=921…
14	17:12:19.904569	104.20.0.85	172.20.10.2	HTTP	769	HTTP/1.1 302 Found (text/html)
18	17:12:19.944086	172.20.10.2	104.20.0.85	TCP	54	63797 → 80 [ACK] Seq=403 Ack=716 Win=1…

10- As, seen from the above image, before sending the HTTP GET messages, the host issues two new DNS queries, which are labeled as [ACK].

11- The destination port for the DNS query message is port 53. The source port for the server is also port 53.

Query:

```
> Frame 9: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
> Ethernet II, Src: IntelCor_cd:2a:1c (1c:1b:b5:cd:2a:1c), Dst: 3a:65:90:a4:25:64 (3a:65:90:a4:25:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.1
v User Datagram Protocol, Src Port: 63401, Dst Port: 53
    Source Port: 63401
    Destination Port: 53
    Length: 33
    Checksum: 0x6c5e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
```

Ayhan Okuyan
21601531
CS421-02

Response:

```
> Frame 10: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface 0
> Ethernet II, Src: 3a:65:90:a4:25:64 (3a:65:90:a4:25:64), Dst: IntelCor_cd:2a:1c (1c:1b:b5:cd:2a:1c)
> Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.2
v User Datagram Protocol, Src Port: 53, Dst Port: 63401
    Source Port: 53
    Destination Port: 63401
    Length: 89
    Checksum: 0x35ac [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
> Domain Name System (response)
```

12- The IP address that the query is sent to is 172.20.10.1, which is the IP address of my default local DNS server.

ip.addr == 172.20.10.1 Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
5	20:33:11.975305	172.20.10.2	172.20.10.1	DNS	84	Standard query 0x0001 PTR 1.10.20.172.…
6	20:33:11.983641	172.20.10.1	172.20.10.2	DNS	138	Standard query response 0x0001 No such…
7	20:33:11.985570	172.20.10.2	172.20.10.1	DNS	67	Standard query 0x0002 A mit.edu
8	20:33:12.183691	172.20.10.1	172.20.10.2	DNS	83	Standard query response 0x0002 A mit.e…
9	20:33:12.186482	172.20.10.2	172.20.10.1	DNS	67	Standard query 0x0003 AAAA mit.edu
10	20:33:12.475344	172.20.10.1	172.20.10.2	DNS	123	Standard query response 0x0003 AAAA m…

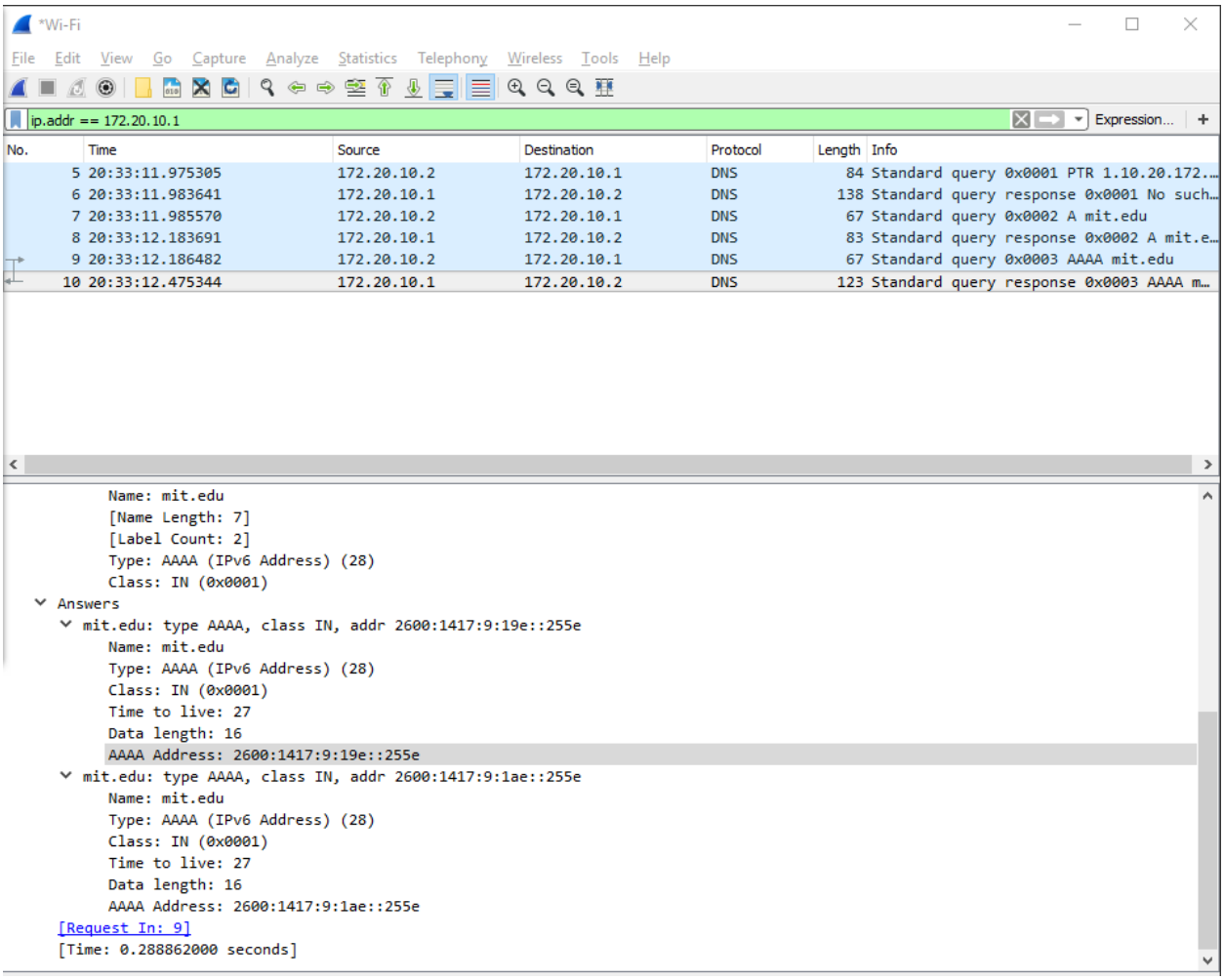
13- The type of query is described as a AAAA type query since the question required us to discard the first two interactions. The query does not contain any answers.

```
> Frame 9: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
> Ethernet II, Src: IntelCor_cd:2a:1c (1c:1b:b5:cd:2a:1c), Dst: 3a:65:90:a4:25:64 (3a:65:90:a4:25:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.1
> User Datagram Protocol, Src Port: 63401, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v mit.edu: type AAAA, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
    [Response In: 10]
```

14- In the response message, two separate answers are received. Both are type AAAA, which are IPv6 addresses. The AAAA addresses are given as 2600:1417:9:19e::255e and 2600:1417:9:1ae::255e

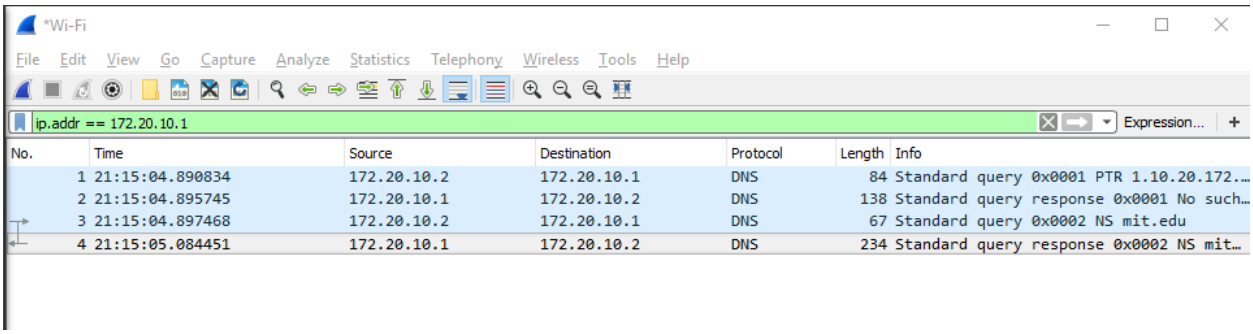
```
  v Answers
    v mit.edu: type AAAA, class IN, addr 2600:1417:9:19e::255e
        Name: mit.edu
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 27
        Data length: 16
        AAAA Address: 2600:1417:9:19e::255e
    v mit.edu: type AAAA, class IN, addr 2600:1417:9:1ae::255e
        Name: mit.edu
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 27
        Data length: 16
        AAAA Address: 2600:1417:9:1ae::255e
```

Ayhan Okuyan
21601531
CS421-02



15-

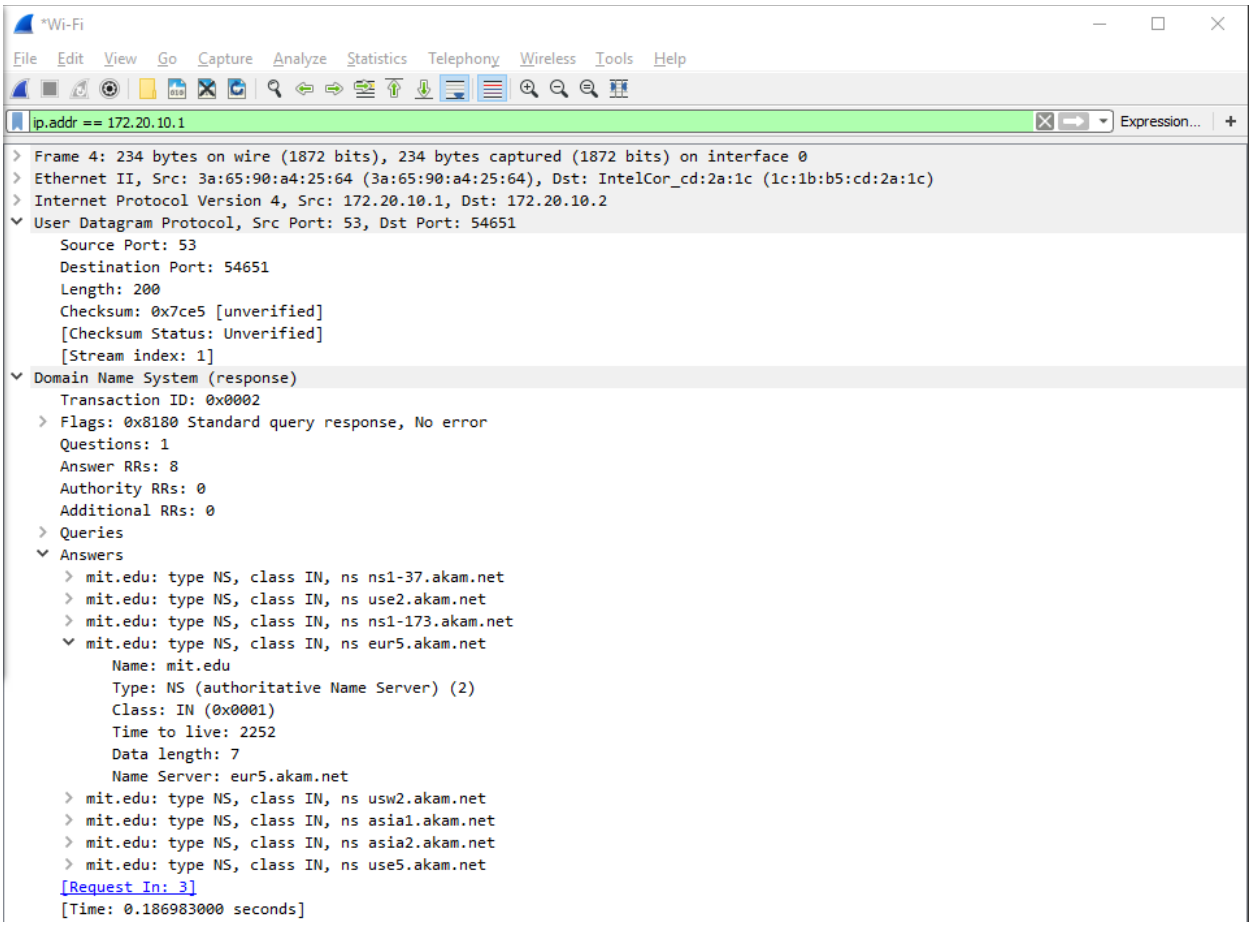
16- The query is sent to the IP address 172.20.10.1, which is my default local DNS server.



17- The query is an NS type query. The query does not contain any answer.

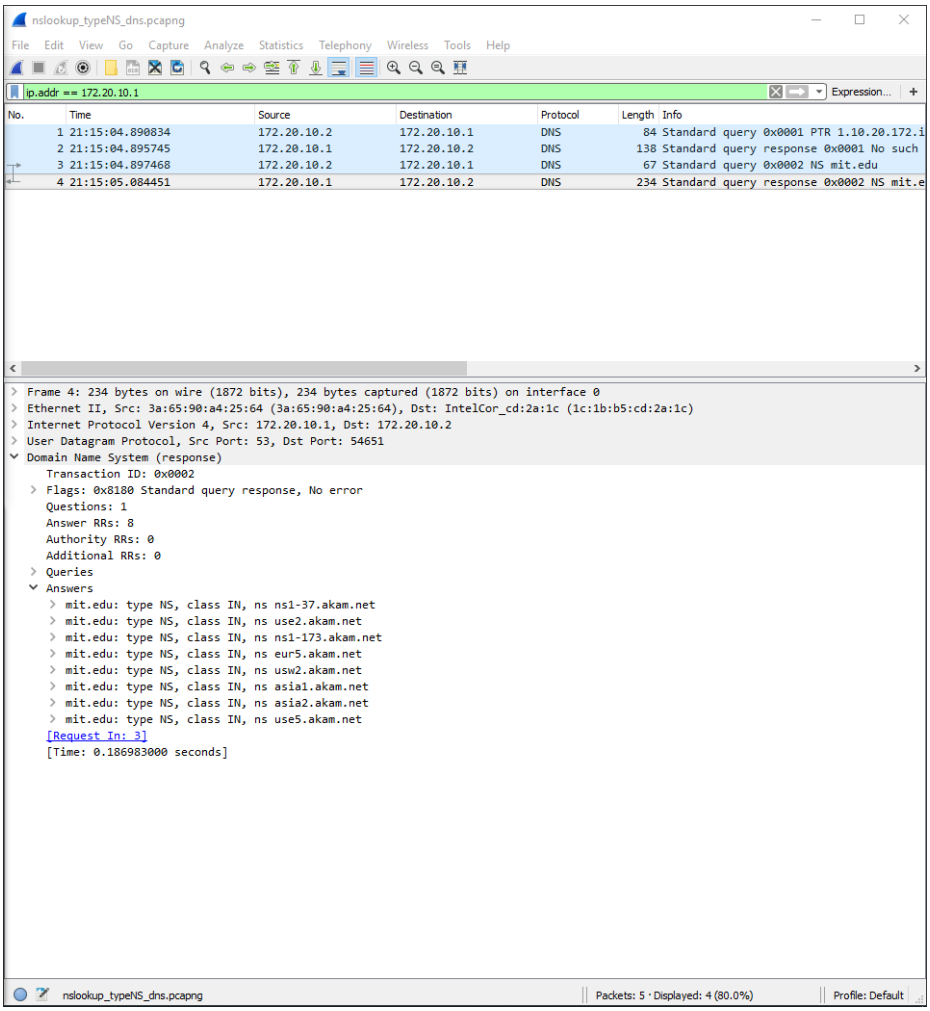
Ayhan Okuyan
21601531
CS421-02

18- The response provides all the name servers for mit.edu which are, ns1-37.akam.net, use2.akam.net, ns1-173.akam.net, eur5.akam.net, usw2.akam.net, asia1.akam.net, asia2.akam.net and use5.akam.net. The response message does not provide the IP addresses of the MIT name servers.



Ayhan Okuyan
21601531
CS421-02

19-



20- The DNS query is sent to the IP address 172.20.10.1, which is the default IP address of my local DNS server.

6	21:28:00.245646	172.20.10.2	172.20.10.1	DNS	73 Standard query 0x6fd0 A bitsy.mit.edu
7	21:28:00.335566	172.20.10.2	172.20.10.1	DNS	73 Standard query 0x6fd0 A bitsy.mit.edu
8	21:28:00.352644	172.20.10.1	172.20.10.2	DNS	89 Standard query response 0x6fd0 A bitsy.
15	21:28:03.503160	172.20.10.2	172.20.10.1	DNS	97 Standard query 0x2006 A array605-prod.d
22	21:28:03.559445	172.20.10.1	172.20.10.2	DNS	113 Standard query response 0x2006 A array6

21- This is a standard query of type A with the given bitsy.mit.edu as an input to the system. No, the query does not contain any answers.

```
Domain Name System (query)
    Transaction ID: 0x6fd0
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        bitsy.mit.edu: type A, class IN
    [Response In: 8]
```

22- The answer section shows only one answer, which is the IP address of the bitsy.mit.edu given as 18.72.0.3.

Ayhan Okuyan
21601531
CS421-02

```
Answers
  bitsy.mit.edu: type A, class IN, addr 18.72.0.3
      Name: bitsy.mit.edu
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 2252
      Data length: 4
      Address: 18.72.0.3
  [Request In: 6]
  [Time: 0.106998000 seconds]
```

23-