CS 421- Computer Networks

Homework 1 Report

20.03.2023

Instructor: Ezhan Karaşan

Section: 01

Zeynep Selcen Öztunç - 21902941

A-Wireshark Test Run

1. TCP, MDNS, UDP, DNS, QUIC, ARP, SSDP, TLSv1.2, NBNS, HTTP.
2. It took 0.139505 seconds from when HTTP GET message was sent and HTTP OK message was received.
3. Internet address of gaia.cs.umass.edu is 128.119.245.12 and the internet address of my computer is 192.168.1.47.
4. The printed get message is:

```
No.     Time           Source                Destination           Protocol Length Info
    670 38.548955      192.168.1.47          128.119.245.12        HTTP     548    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1
Frame 670: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits) on interface \Device\NPF_{66E478DD-5665-452F-BF0D-
B247B4117F3E}, id 0
Ethernet II, Src: IntelCor_33:65:c6 (d0:ab:d5:33:65:c6), Dst: zte_05:1e:2c (30:cc:21:05:1e:2c)
Internet Protocol Version 4, Src: 192.168.1.47, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50310, Dst Port: 80, Seq: 1, Ack: 1, Len: 494
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-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/111.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7\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/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 699]
```

The printed ok message is:

```
No.     Time           Source                Destination           Protocol Length Info
    699 38.688460      128.119.245.12        192.168.1.47          HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 699: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{66E478DD-5665-452F-BF0D-
B247B4117F3E}, id 0
Ethernet II, Src: zte_05:1e:2c (30:cc:21:05:1e:2c), Dst: IntelCor_33:65:c6 (d0:ab:d5:33:65:c6)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.47
Transmission Control Protocol, Src Port: 80, Dst Port: 50310, Seq: 1, Ack: 495, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Wed, 15 Mar 2023 15:20:31 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 15 Mar 2023 05:59:01 GMT\r\n
    ETag: "51-5f6ea0a6f5373"\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: 0.139505000 seconds]
    [Request in frame: 670]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

WireShark Lab: HTTP

1. The Basic HTTP GET/response interaction

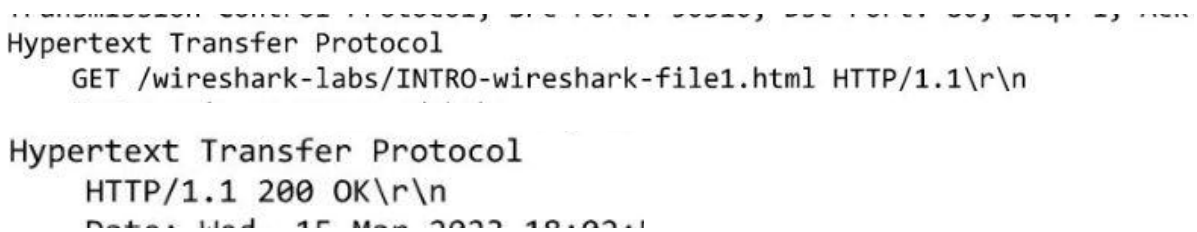
The GET message in the printed form is:

```
No.     Time           Source                Destination           Protocol Length Info
    670 38.548955      192.168.1.47          128.119.245.12        HTTP     548    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1
Frame 670: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits) on interface \Device\NPF_{66E478DD-5665-452F-BF0D-
B247B4117F3E}, id 0
Ethernet II, Src: IntelCor_33:65:c6 (d0:ab:d5:33:65:c6), Dst: zte_05:1e:2c (30:cc:21:05:1e:2c)
Internet Protocol Version 4, Src: 192.168.1.47, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50310, Dst Port: 80, Seq: 1, Ack: 1, Len: 494
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-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/111.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7\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/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 699]
```

The response message in the printed form is:

```
No.     Time              Source                Destination           Protocol Length Info
    168 21:02:55,096302   128.119.245.12        192.168.1.47          HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 168: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{66E478DD-5665-452F-BF0D-
B247B4117F3E}, id 0
Ethernet II, Src: zte_05:1e:2c (30:cc:21:05:1e:2c), Dst: IntelCor_33:65:c6 (d0:ab:d5:33:65:c6)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.47
Transmission Control Protocol, Src Port: 80, Dst Port: 58369, Seq: 1, Ack: 494, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Wed, 15 Mar 2023 18:02:55 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 15 Mar 2023 05:59:01 GMT\r\n
    ETag: "80-5f6ea0a6f7a84"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\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: 0.147479000 seconds]
    [Request in frame: 158]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

1. My browser is running HTTP version 1.1. The server is also running HTTP version 1.1



2. My browser indicates that it can accept Turkish and English to the server.

```
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
\r\n
```

3. Internet address of gaia.cs.umass.edu is 128.119.245.12 and the internet address of my computer is 192.168.1.47.

```
Source                  Destination
192.168.1.47            128.119.245.12
```

4. The status code returned from the server to my browser is 200, which stands for OK.

```
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
```

5. The file was last modified at the server at: Wed, 15 Mar 2023 05:59:01 GMT

```
Last-Modified: Wed, 15 Mar 2023 05:59:01 GMT\r\n
```

6. 128 bytes of content are returned to my browser.

```
Content-Length: 128\r\n
```

7. No, all of the raw data is included in the packet listing window.

2. The HTTP CONDITIONAL GET/response interaction

8. No, I have not seen any "IF-MODIFIED-SINCE" line in the first GET message.

9. Yes, I know that the server explicitly returned the contents of the file since the HTTP status code of the first response message was 200 which stands for "OK", indicating that the get request has succeeded. Also, the content can be seen at Line-based text data

```
144 03:14:55,967218 192.168.1.57    128.119.245.12    HTTP    547 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1
170 03:14:56,110192 128.119.245.12  192.168.1.57      HTTP    784 HTTP/1.1 200 OK  (text/html)
214 03:14:58,667223 192.168.1.57    128.119.245.12    HTTP    659 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1
```

```
[Request in frame: 144]
[Next request in frame: 214]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
> Line-based text data: text/html (10 lines)
```

10. Yes, there is an "IF-MODIFIED-SINCE" line in the second GET message. It is followed by the date value Wed, 15 Mar 2023 05:59:01 GMT which is the date of the last modification in the previous response.

```
> Frame 214: 659 bytes on wire (5272 bits), 659 bytes captured (5272 bits) on interface \Device\NPF_{66E478DD-5665-452F-BF0D-B247E
> Ethernet II, Src: IntelCor_33:65:c6 (d0:ab:d5:33:65:c6), Dst: zte_05:1e:2c (30:cc:21:05:1e:2c)
> Internet Protocol Version 4, Src: 192.168.1.57, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49996, Dst Port: 80, Seq: 494, Ack: 731, Len: 605
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\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/111.0.0.0 Safari/537.36\r
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-e
    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
    If-None-Match: "173-5f72663f76abd"\r\n
    If-Modified-Since: Sat, 18 Mar 2023 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 144]
```

11. The server responds with the status code 304 with the phrase “Not Modified”. No, this time the server did not explicitly return the contents of the file. This is because, in the first response message from the server, the contents of the file are cached. The cache also stores the Last-Modified date. When the browser sends the second GET request, the cache checks performs an up-to-date check by issuing a conditional GET. It sees that the value of the IF-MODIFIED-SINCE is equal to the value of the Last-Modified. That means that the object has not been changed since the server first sent the object, hence the value of the object in the cache can be used. So in the second response message, the server does not include the requested object. 304 status messages tells the cache that it can forward the cached copy of the object [1].

3. Retrieving Long Documents

12. Only one request message was sent.

No.	Time	Source	Destination	Protocol	Length	Info
140	00:40:17,215433	192.168.1.47	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.
164	00:40:17,361167	128.119.245.12	192.168.1.47	HTTP	559	HTTP/1.1 200 OK (text/html)

13. 4 TCP segments were needed to carry the single response.

No.	Time	Source	Destination	Protocol	Length	Info
140	00:40:17,215433	192.168.1.47	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.
164	00:40:17,361167	128.119.245.12	192.168.1.47	HTTP	559	HTTP/1.1 200 OK (text/html)

```
> Frame 164: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{66E478DD-5665-452F-BF0D-B247B4
> Ethernet II, Src: zte_05:1e:2c (30:cc:21:05:1e:2c), Dst: IntelCor_33:65:c6 (d0:ab:d5:33:65:c6)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.47
> Transmission Control Protocol, Src Port: 80, Dst Port: 50159, Seq: 4357, Ack: 494, Len: 505
v [4 Reassembled TCP Segments (4861 bytes): #161(1452), #162(1452), #163(1452), #164(505)]
    [Frame: 161, payload: 0-1451 (1452 bytes)]
    [Frame: 162, payload: 1452-2903 (1452 bytes)]
    [Frame: 163, payload: 2904-4355 (1452 bytes)]
    [Frame: 164, payload: 4356-4860 (505 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205765642c203135204d61722032…]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

14. The associated status code and phrases of the response are 200 and “OK”.

No.	Time	Source	Destination	Protocol	Length	Info
140	00:40:17,215433	192.168.1.47	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.
164	00:40:17,361167	128.119.245.12	192.168.1.47	HTTP	559	HTTP/1.1 200 OK (text/html)

15. No, there are no “Continuation” lines.

4. HTML Documents with Embedded Objects

16. There are 3 GET messages sent from my browser. These request messages were sent to internet addresses 128.119.245.12, 128.119.245.12, 178.79.137.64 respectively.

http

No.	Time	Source	Destination	Protocol	Length	Info
48	14:25:04,525699	192.168.1.47	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.
55	14:25:04,685779	128.119.245.12	192.168.1.47	HTTP	1355	HTTP/1.1 200 OK (text/html)
57	14:25:04,732467	192.168.1.47	128.119.245.12	HTTP	493	GET /pearson.png HTTP/1.1
65	14:25:04,806851	192.168.1.47	178.79.137.164	HTTP	460	GET /8E_cover_small.jpg HTTP/1.1
67	14:25:04,869945	178.79.137.164	192.168.1.47	HTTP	225	HTTP/1.1 301 Moved Permanently
70	14:25:04,894404	128.119.245.12	192.168.1.47	HTTP	761	HTTP/1.1 200 OK (PNG)

No.	Time	Source	Destination	Protocol	Length	Info
98	00:16:45,691701	192.168.1.47	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.
102	00:16:45,838735	128.119.245.12	192.168.1.47	HTTP	1355	HTTP/1.1 200 OK (text/html)
104	00:16:45,874336	192.168.1.47	128.119.245.12	HTTP	493	GET /pearson.png HTTP/1.1
115	00:16:46,016201	128.119.245.12	192.168.1.47	HTTP	761	HTTP/1.1 200 OK (PNG)
148	00:16:46,387137	192.168.1.47	178.79.137.164	HTTP	460	GET /8E_cover_small.jpg HTTP/1.1
153	00:16:46,452900	178.79.137.164	192.168.1.47	HTTP	225	HTTP/1.1 301 Moved Permanently

17. The two images were sent in parallel since the get request is sent before the processing of the first one has finished.

http

No.	Time	Source	Destination	Protocol	Length	Info
48	14:25:04,525699	192.168.1.47	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.
55	14:25:04,685779	128.119.245.12	192.168.1.47	HTTP	1355	HTTP/1.1 200 OK (text/html)
57	14:25:04,732467	192.168.1.47	128.119.245.12	HTTP	493	GET /pearson.png HTTP/1.1
65	14:25:04,806851	192.168.1.47	178.79.137.164	HTTP	460	GET /8E_cover_small.jpg HTTP/1.1
67	14:25:04,869945	178.79.137.164	192.168.1.47	HTTP	225	HTTP/1.1 301 Moved Permanently
70	14:25:04,894404	128.119.245.12	192.168.1.47	HTTP	761	HTTP/1.1 200 OK (PNG)

5. HTTP Authentication

18. The server’s response to the initial request was 401 unauthorized.

No.	Time	Source	Destination	Protocol	Length	Info
55	14:07:48,504811	192.168.1.47	128.119.245.12	HTTP	563	GET /wireshark-labs/protected_pages/HTTP-wireshark-fi
64	14:07:48,646976	128.119.245.12	192.168.1.47	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
170	14:08:00,633880	192.168.1.47	128.119.245.12	HTTP	648	GET /wireshark-labs/protected_pages/HTTP-wireshark-fi
176	14:08:00,831800	128.119.245.12	192.168.1.47	HTTP	544	HTTP/1.1 200 OK (text/html)
178	14:08:01,045922	192.168.1.47	128.119.245.12	HTTP	509	GET /favicon.ico HTTP/1.1
179	14:08:01,235180	128.119.245.12	192.168.1.47	HTTP	538	HTTP/1.1 404 Not Found (text/html)

19. Authorization and Cache-Control fields are new.

```
Cache-Control: max-age=0\r\n
› Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
```

Wireshark Lab: DNS

1. nslookup

1. I performed nslookup for www.tohoku.ac.jp

```
C:\Users\admin>nslookup www.tohoku.ac.jp
Server:  csp3.zte.com.cn
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.tohoku.ac.jp
Address:  130.34.41.233
```

2. I performed nslookup for Erasmus University in the Netherlands.

```
C:\Users\admin>nslookup -type=NS eur.nl
Server:  csp1.zte.com.cn
Address:  192.168.1.1

Non-authoritative answer:
eur.nl  nameserver = ns1.surfnet.nl
eur.nl  nameserver = ns2.surfnet.nl
eur.nl  nameserver = ns3.surfnet.nl
eur.nl  nameserver = ns1.zurich.surf.net
```

3. I tried nslookup on the authoritative servers in question 2, but I had a "Query refused" response. Then I tried it with multiple different servers but I always got the "Query refused" response.

```
C:\Users\admin>nslookup mail.yahoo.com ns1.surfnet.nl
Server:  ns1.surfnet.nl
Address:  192.87.106.101

*** ns1.surfnet.nl can't find mail.yahoo.com: Query refused
```

2. ipconfig

DNS request message:

```
No.     Time              Source                Destination           Protocol Length Info
    225 17:16:56,407743   192.168.1.47          192.168.1.1           DNS      72     Standard query 0x2865 A www.ietf.org
Frame 225: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{66E478DD-5665-452F-BF0D-B247B4117F3E},
id 0
Ethernet II, Src: IntelCor_33:65:c6 (d0:ab:d5:33:65:c6), Dst: zte_05:1e:2c (30:cc:21:05:1e:2c)
Internet Protocol Version 4, Src: 192.168.1.47, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 62963, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x2865
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
    [Response In: 229]
```

DNS response message:

```
No.     Time               Source                Destination           Protocol Length Info
    229 17:16:56,414125    192.168.1.1           192.168.1.47          DNS      104    Standard query response 0x2865 A www.ietf.org A
104.16.44.99 A 104.16.45.99
Frame 229: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{66E478DD-5665-452F-BF0D-B247B4117F3E},
id 0
Ethernet II, Src: zte_05:1e:2c (30:cc:21:05:1e:2c), Dst: IntelCor_33:65:c6 (d0:ab:d5:33:65:c6)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.47
User Datagram Protocol, Src Port: 53, Dst Port: 62963
Domain Name System (response)
    Transaction ID: 0x2865
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.ietf.org: type A, class IN
    Answers
    [Request In: 225]
    [Time: 0.006382000 seconds]
```

4. They are sent over UDP.

```
Internet Protocol Version 4, Src: 192.168.1.47, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 62963, Dst Port: 53
Domain Name System (query)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.47
User Datagram Protocol, Src Port: 53, Dst Port: 62963
Domain Name System (response)
```

5. The destination port of the query message and the source port of the response message are both 53.

```
Internet Protocol Version 4, Src: 192.168.1.47, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 62963, Dst Port: 53
Domain Name System (query)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.47
User Datagram Protocol, Src Port: 53, Dst Port: 62963
Domain Name System (response)
```

6. The DNS query is sent to the IP address 192.168.1.1. From ipconfig, I see that the IP address of my DNS server is also 192.168.1.1. So yes, both IP addresses are the same**.**

```
    225 17:16:56,407743 192.168.1.47          192.168.1.1           DNS      72 Standard query 0x2865 A www.ietf.org
    226 17:16:56,408025 192.168.1.47          192.168.1.1           DNS      72 Standard query 0x200f HTTPS www.ietf.org
```

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Physical Address. . . . . . . . . : D0-AB-D5-33-65-C6
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5f55:13b7:125c:3ca9%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.47(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 17 Mart 2023 Cuma 13:17:36
   Lease Expires . . . . . . . . . . : 18 Mart 2023 Cumartesi 13:17:36
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 164670421
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-D7-0C-5C-98-FA-9B-7B-F1-14
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

7. It is a type A query and it does not contain any answers.

```
Domain Name System (query)
    Transaction ID: 0x2865
  > 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: 229]
```

8. The response message contains 2 answers which are of type A. The answers contain information about Name, Type, Class, Time to live, Data length, Address.

```
v Answers
  v www.ietf.org: type A, class IN, addr 104.16.44.99
        Name: www.ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 21 (21 seconds)
        Data length: 4
        Address: 104.16.44.99
  v www.ietf.org: type A, class IN, addr 104.16.45.99
        Name: www.ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 21 (21 seconds)
        Data length: 4
        Address: 104.16.45.99
    [Request In: 225]
```

9. Yes, the destination IP address of the SYN corresponds to one of the IP addresses in the DNS response message (104.16.45.99).

234	17:16:56,431310	192.168.1.1	192.168.1.47	DNS	196	Standard query response 0x2a38 HTTPS www.ietf.o
235	17:16:56,432733	192.168.1.47	104.16.45.99	TCP	66	51826 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=146

10. No, it does not, it uses the answer from the first response. (I have checked this part from the zip file provided in the homework document).

No.	Time	Source	Destination	Protocol	Length	Info
8	00:57:43,582042	128.238.38.160	128.238.29.23	DNS	72	Standard query 0x006e A www.ietf.org
9	00:57:43,582886	128.238.29.23	128.238.38.160	DNS	104	Standard query response 0x006e A www.ietf.org A 132.

11. The destination port for the DNS query message and the source port of the DNS response message is both 53. The DNS query message:

```
> Frame 19: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3742, 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
  > Queries
    [Response In: 20]
```

The DNS response message:

```
> Frame 20: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 128.238.29.22, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3742
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 3
    Additional RRs: 3
  > Queries
  > Answers
  > Authoritative nameservers
  > Additional records
    [Request In: 19]
    [Time: 0.016757000 seconds]
```

12. The DNS query message is sent to the IP address 192.168.1.1 which is also the IP address of my local DNS server. (In the answers 11,13,14,15 I have used the zip provided in the homework assignment, but for this one I did my own packet capturing to see whether the IP addresses are actually the same.)

```
Internet Protocol Version 4, Src: 192.168.1.47, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 50811, Dst Port: 53
```

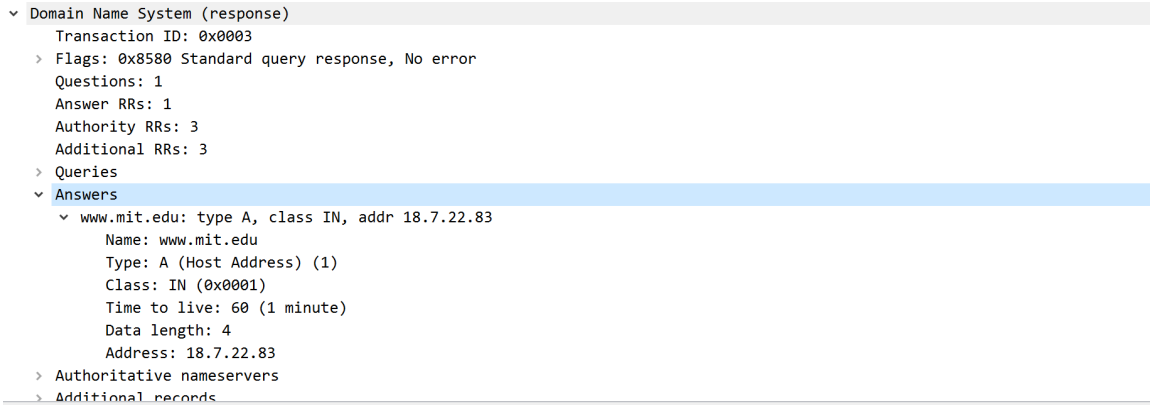
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Physical Address. . . . . . . . . : D0-AB-D5-33-65-C6
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5f55:13b7:125c:3ca9%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.47(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 17 Mart 2023 Cuma 13:17:36
   Lease Expires . . . . . . . . . . : 18 Mart 2023 Cumartesi 13:17:36
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 164670421
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-D7-0C-5C-98-FA-9B-7B-F1-14
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

13. The DNS query message is of type A and it does not contain any answers.

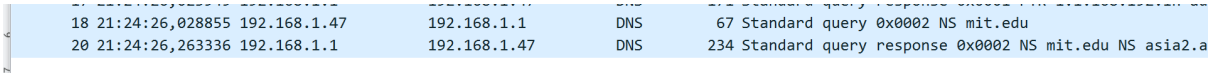
```
> Frame 19: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3742, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.mit.edu: type A, class IN
    [Response In: 20]
```

14. The DNS response message has 1 answer. The answers contain Name, Type, Class, Time to live, Data Length, CNAME lines.

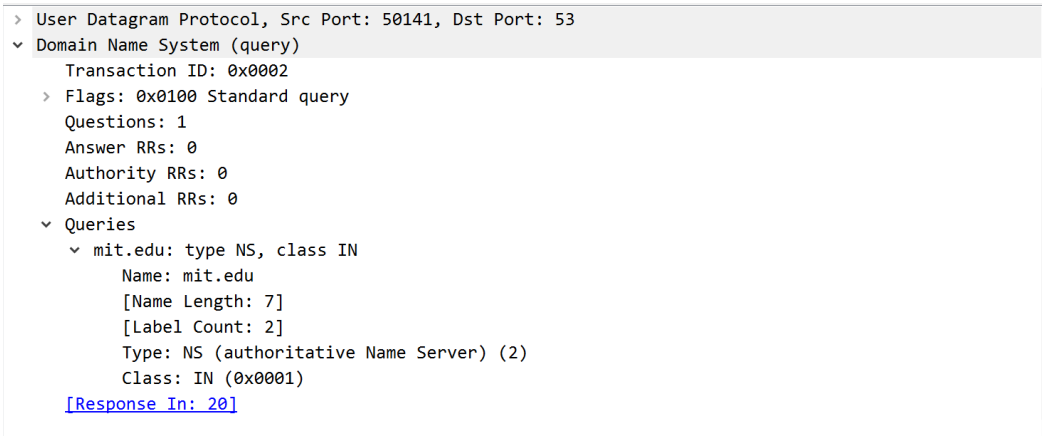
15. Screenshots for answer 14 are provided.



16. The DNS query is sent to the IP address 192.168.1.1. From ipconfig, I see that the IP address of my DNS server is also 192.168.1.1. So yes, both IP addresses are the same**.**



17. The DNS query is of type NS and it does not contain any answers.



18. It provides the names of the authoritative DNS servers which are asia2.akam.net, ns-173.akam.net, usw2.akam.net, ns1-37.akam.net, asia1.akam.net, eur5.akam.net, use5.akam.net, use2.akam.net. The answer does not provide the IP addresses of these servers.

19. The screenshots for answer 18 is given below.

```
Answer RRs: 8
Authority RRs: 0
Additional RRs: 0
Queries
  mit.edu: type NS, class IN
Answers
  mit.edu: type NS, class IN, ns asia2.akam.net
  mit.edu: type NS, class IN, ns ns1-173.akam.net
  mit.edu: type NS, class IN, ns usw2.akam.net
  mit.edu: type NS, class IN, ns ns1-37.akam.net
  mit.edu: type NS, class IN, ns asia1.akam.net
  mit.edu: type NS, class IN, ns eur5.akam.net
  mit.edu: type NS, class IN, ns use5.akam.net
  mit.edu: type NS, class IN, ns use2.akam.net
[Request In: 18]
[Time: 0.234481000 seconds]
```

```
Answer RRs: 8
Authority RRs: 0
Additional RRs: 0
Queries
  mit.edu: type NS, class IN
Answers
  mit.edu: type NS, class IN, ns asia2.akam.net
      Name: mit.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      Data length: 16
      Name Server: asia2.akam.net
  mit.edu: type NS, class IN, ns ns1-173.akam.net
  mit.edu: type NS, class IN, ns usw2.akam.net
  mit.edu: type NS, class IN, ns ns1-37.akam.net
  mit.edu: type NS, class IN, ns asia1.akam.net
```

20. It is sent to the IP address 18.72.03 which is not the IP address of my default local DNS server. It corresponds to the IP address of bitsy.mit.edu.

```
00:36:49,859652 128.238.38.160   18.72.0.3          DNS   74  Standard query 0x0003 A www.aiit.or.kr
00:36:49,873994 18.72.0.3        128.238.38.160     DNS   156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.2…
```

21. It is a standard type A query and it does not contain any answers.

```
Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
User Datagram Protocol, Src Port: 3753, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x0003
  Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.aiit.or.kr: type A, class IN
    [Response In: 105]
```

22. There is one answer provided. The answer contains the Name, Type, Class, Time to live and Address.

23. The screenshots of the answer 22 is given below:

```
> Frame 105: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 18.72.0.3, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3753
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  > Queries
  > Answers
  > Authoritative nameservers
  > Additional records
    [Request In: 104]
    [Time: 0.014342000 seconds]
```

```
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  > Queries
  v Answers
    v www.aiit.or.kr: type A, class IN, addr 218.36.94.200
        Name: www.aiit.or.kr
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3338 (55 minutes, 38 seconds)
        Data length: 4
        Address: 218.36.94.200
  > Authoritative nameservers
  > Additional records
    [Request In: 104]
    [Time: 0.014342000 seconds]
```

References

[1] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 7th ed. Boston, MA: Pearson, 2016.