

# Bilkent University

## CS421 Wireshark Assignment

Emre Uncu

22003884

### What to hand in

1. List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

- ARP
- TLSv1.2
- TCP
- MDNS
- UDP
- SSDP
- IGMPv2
- TLSv1.3
- DNS
- ICMP

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packetlisting window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

14:37:20,795252 GET  
14:37:20,926717 OK  
0,131465 seconds

89	14:37:20,795252	139.179.243.93	128.119.245.12	HTTP	463	GET /wireshark-labs/INTRO-wireshar
91	14:37:20,926717	128.119.245.12	139.179.243.93	HTTP	492	HTTP/1.1 200 OK (text/html)

3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)?  
What is the Internet address of your computer?

128.119.245.12 gaia.cs.umass.edu  
139.179.243.93 my computer

89	14:37:20,795252	139.179.243.93	128.119.245.12	HTTP	463	GET /wireshark-labs/INTRO-wireshar
91	14:37:20,926717	128.119.245.12	139.179.243.93	HTTP	492	HTTP/1.1 200 OK (text/html)

4. Print the two HTTP messages displayed in step 9 above. To do so, select Print from the Wireshark File command menu, and select “Selected Packet Only” and “Print as displayed” and then click OK.

C:\Users\Emre\AppData\Local\Temp\wireshark\_Wi-Fi 2V0O812.pcapng 383 total packets, 1 shown

```
No.      Time                Source                Destination            Protocol Length Info
 89 14:37:20.795252    139.179.243.93        128.119.245.12        HTTP      463    GET /wireshark-labs/INTRO-wireshark-file1.html
HTTP/1.1
Frame 89: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface \Device\NPF_{F30844EB-6737-49E2-8E0B-6D0F904D8E2E},
id 0
Ethernet II, Src: Intel_58:10:4c (64:6e:e0:58:10:4c), Dst: SuperMicroCo_8e:b3:84 (0c:c4:7a:8e:b3:84)
Internet Protocol Version 4, Src: 139.179.243.93, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 65434, Dst Port: 80, Seq: 1, Ack: 1, Len: 409
Hypertext Transfer Protocol
  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Priority: u=0, i\r\n
\r\n
[Response in frame: 91]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

C:\Users\Emre\AppData\Local\Temp\wireshark\_Wi-Fi 2V0O812.pcapng 383 total packets, 1 shown

```
No.      Time                Source                Destination            Protocol Length Info
 91 14:37:20.926717    128.119.245.12        139.179.243.93        HTTP      492    HTTP/1.1 200 OK (text/html)
Frame 91: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{F30844EB-6737-49E2-8E0B-6D0F904D8E2E},
id 0
Ethernet II, Src: SuperMicroCo_8e:b3:84 (0c:c4:7a:8e:b3:84), Dst: Intel_58:10:4c (64:6e:e0:58:10:4c)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.243.93
Transmission Control Protocol, Src Port: 80, Dst Port: 65434, Seq: 1, Ack: 410, Len: 438
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Mon, 24 Feb 2025 11:37:17 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: Mon, 24 Feb 2025 06:59:01 GMT\r\n
  ETag: "51-62edde007f376"\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
[Request in frame: 89]
[Time since request: 0.131465000 seconds]
[Request URI: /wireshark-labs/INTRO-wireshark-file1.html]
[Full 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)
```

## HTTP

### 1. The Basic HTTP GET/response interaction

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

HTTP/1.1      My browser  
HTTP/1.1      the server

```
2247 139.179.243.93 128.119.245.12 HTTP      462 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
7004 128.119.245.12 139.179.243.93 HTTP      540 HTTP/1.1 200 OK (text/html)
```

2. What languages (if any) does your browser indicate that it can accept to the server?

Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3  
Turkish and English

```
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3\r\n
```

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

139.179.243.93      my computer  
128.119.245.12      gaia.cs.umass.edu

```
21 14:46:32,912247 139.179.243.93 128.119.245.12 HTTP 462 GET /wireshark-labs/HTTP-wireshark
24 14:46:33,047004 128.119.245.12 139.179.243.93 HTTP 540 HTTP/1.1 200 OK (text/html)
```

4. What is the status code returned from the server to your browser?

Status Code: 200  
[Status Code Description: OK]

```
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
```

5. When was the HTML file that you are retrieving last modified at the server?

Last-Modified: Mon, 24 Feb 2025 06:59:01 GMT

```
Last-Modified: Mon, 24 Feb 2025 06:59:01 GMT\r\n
```

6. How many bytes of content are being returned to your browser?

Content-Length: 128  
128 bytes

```
[Content length: 128]
File Data: 128 bytes
```

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

No, I don't see any headers.

## 2. The HTTP CONDITIONAL GET/response interaction

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

No, I don't see an "IF-MODIFIED-SINCE" line in the HTTP GET.

```
▼ Hypertext Transfer Protocol
  ▼ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.html
    Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    \r\n
    [Response in frame: 1420]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Yes. It includes a Line-based test data section and 10-line content.

```
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Mon, 24 Feb 2025 11:59:42 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: Mon, 24 Feb 2025 06:59:01 GMT\r\n
    ETag: "173-62edde0080ece"\r\n
    Accept-Ranges: bytes\r\n
    ▶ Content-Length: 371\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
    [Request in frame: 1418]
    [Time since request: 0.131174000 seconds]
    [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
    [Full 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)
    \n
    <html>\n
    \n
    Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change. <p>\n
    Thus if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

If-Modified-Since: Mon, 24 Feb 2025 06:59:01 GMT

```
▼ Hypertext Transfer Protocol
  ▶ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Mon, 24 Feb 2025 06:59:01 GMT\r\n
    If-None-Match: "173-62edde0080ece"\r\n
    Priority: u=0, i\r\n
    \r\n
    [Response in frame: 1467]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Status Code: 304

Response Phrase: Not Modified

The server didn't return the file's contents because it was not modified and exists in the cache.

```
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
```

### 3. Retrieving Long Documents

12. How many HTTP GET request messages were sent by your browser?

One HTTP GET request was sent by my browser.

```
51 15:07:15,799579 139.179.243.93 128.119.245.12 HTTP 462 GET /wireshark-labs/HTTP-wireshark
56 15:07:15,933771 128.119.245.12 139.179.243.93 HTTP 535 HTTP/1.1 200 OK (text/html)
```

13. How many data-containing TCP segments were needed to carry the single HTTP response?

[Segment count: 4]

4 TCP segments were needed.

```
▼ [4 Reassembled TCP Segments (4861 bytes): #53(1460), #54(1460), #55(1460), #56(481)]
  [Frame: 53, payload: 0-1459 (1460 bytes)]
  [Frame: 54, payload: 1460-2919 (1460 bytes)]
  [Frame: 55, payload: 2920-4379 (1460 bytes)]
  [Frame: 56, payload: 4380-4860 (481 bytes)]
  [Segment count: 4]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data [...]: 485454502f312e3120323030204f4b0d0a446174653a204d6f6e2c203234204665622f
```

**14. What is the status code and phrase associated with the response to the HTTP GET request?**

Status Code: 200  
Response Phrase: OK



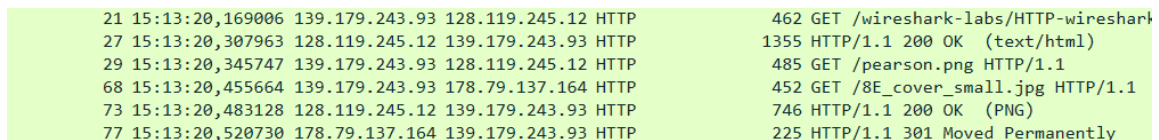
**15. Are there any HTTP status lines in the transmitted data associated with a TCPinduced “Continuation”?**

No, there were no “Continuation” lines.

## 4. HTML Documents with Embedded Objects

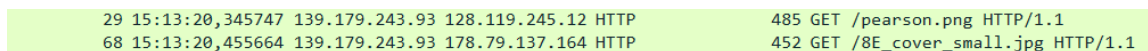
**16. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?**

Three HTTP GET requests were sent, two to `gaia.cs.umass.edu` and one to `kurose.cslash.net`  
128.119.245.12      `gaia.cs.umass.edu`  
178.79.137.164      `kurose.cslash.net`



**17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.**

Two separate GET requests were sent at different times; therefore, the images were downloaded serially.



## 5. HTTP Authentication

**18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?**

Status Code: 401  
Response Phrase: Unauthorized



19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm5=  
Credentials: wireshark-students:network

```
▼ Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm5=\r\n
  Credentials: wireshark-students:network 01d0
  01e0
```

## DNS

### 1. nslookup

1. Run nslookup to obtain the IP address of a Web server in Asia.

```
C:\Users\Emre>nslookup www.emba.cuhk.edu.hk
Server: manyas.bcc.bilkent.edu.tr
Address: 139.179.30.24

Non-authoritative answer:
Name:    www.emba.cuhk.edu.hk
Address: 172.104.167.152
```

2. Run nslookup to determine the authoritative DNS servers for a university in Europe.

```
C:\Users\Emre>nslookup -type=NS tum.de
Server: manyas.bcc.bilkent.edu.tr
Address: 139.179.30.24

Non-authoritative answer:
tum.de nameserver = dns2.lrz.bayern
tum.de nameserver = dns3.lrz.eu
tum.de nameserver = dns1.lrz.de
```

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail.

```
C:\Users\Emre>nslookup -type=mx yahoo.com dns2.lrz.bayern
Server: dns2.lrz.de
Address: 141.40.9.211

*** dns2.lrz.de can't find yahoo.com: Query refused

C:\Users\Emre>nslookup -type=mx yahoo.com dns3.lrz.eu
Server: UnKnown
Address: 78.128.211.180

*** UnKnown can't find yahoo.com: Query refused

C:\Users\Emre>nslookup -type=mx yahoo.com dns1.lrz.de
Server: dns1.lrz.de
Address: 129.187.19.183

*** dns1.lrz.de can't find yahoo.com: Query refused
```

```

C:\Users\Emre>nslookup mail.yahoo.com dns1.lrz.de
Server: dns1.lrz.de
Address: 129.187.19.183

*** dns1.lrz.de can't find mail.yahoo.com: Query refused

C:\Users\Emre>nslookup mail.yahoo.com dns3.lrz.eu
Server: UnKnown
Address: 78.128.211.180

*** UnKnown can't find mail.yahoo.com: Query refused

C:\Users\Emre>nslookup mail.yahoo.com dns2.lrz.bayern
Server: dns2.lrz.bayern
Address: 141.40.9.211

*** dns2.lrz.bayern can't find mail.yahoo.com: Query refused

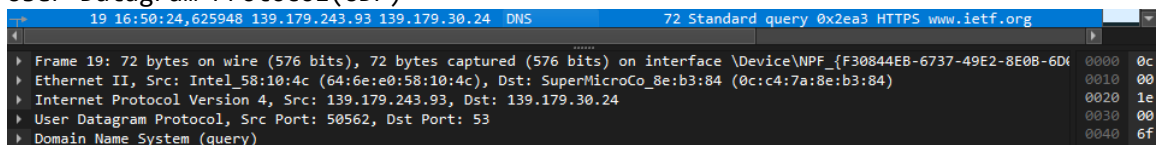
```

## 2. ipconfig

## 3. Tracing DNS with Wireshark

### 4. Locate the DNS query and response messages. Are they sent over UDP or TCP?

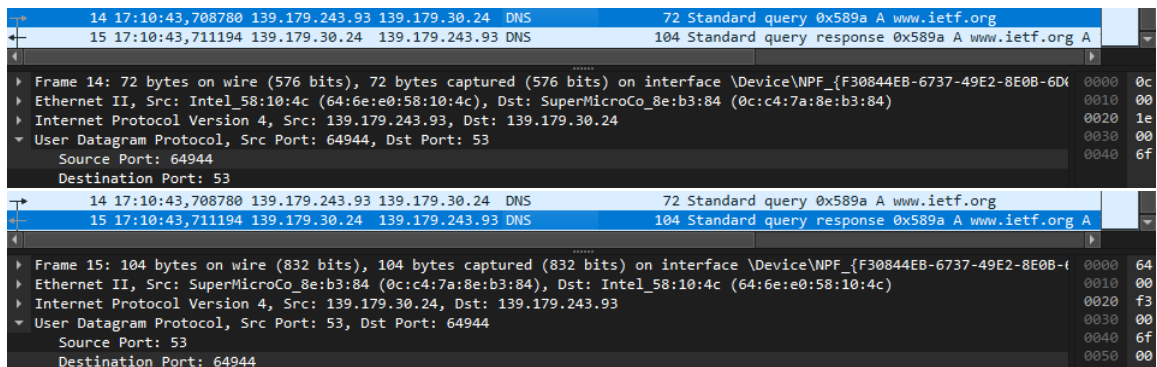
User Datagram Protocol(UDP)



### 5. What is the destination port for the DNS query message? What is the source port of DNS response message?

Destination port for the DNS query: 53

Source port of DNS response: 53



### 6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

The destination IP: 139.179.30.34

One of my local DNS servers: 139.179.30.34

These IP addresses are the same.



No.	Time	Source	Destination	Protocol	Length	Info
14	17:10:43,708780	139.179.243.93	139.179.30.24	DNS	72	Standard query 0x589a A www.ietf.org

DNS Servers . . . . .	: 139.179.30.24
	139.179.10.13

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Type A

It doesn’t contain any “answers”.

▼ Domain Name System (query)
Transaction ID: 0x589a
► Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
▼ www.ietf.org: type A, class IN
Name: www.ietf.org
[Name Length: 12]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)

8. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

It provides two answers that contain Name, Type, Class, TTL, Data length, and Address.

▼ Answers
► www.ietf.org: type A, class IN, addr 104.16.44.99
▼ www.ietf.org: type A, class IN, addr 104.16.45.99
Name: www.ietf.org
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 250 (4 minutes, 10 seconds)
Data length: 4
Address: 104.16.45.99

9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

The destination IP address of the SYN packet: 104.16.44.99

One of the IP addresses provided in the DNS response: 104.16.44.99

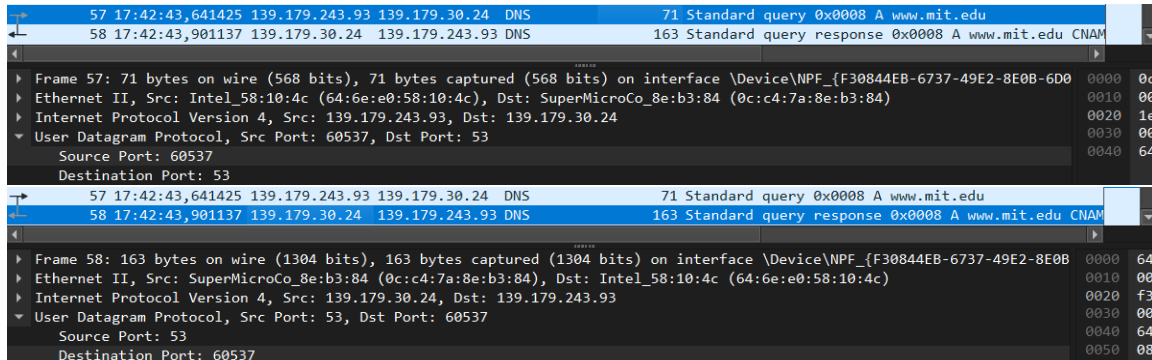
14	17:10:43,708780	139.179.243.93	139.179.30.24	DNS	72	Standard query 0x589a A www.ietf.org
15	17:10:43,711194	139.179.30.24	139.179.243.93	DNS	104	Standard query response 0x589a A www.ietf.org A 1
16	17:10:43,712578	139.179.243.93	104.16.44.99	TCP	66	59799 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

No, the host doesn’t issue new DNS queries.

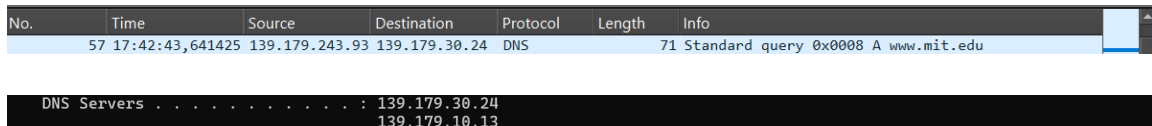
11. What is the destination port for the DNS query message? What is the source port of DNS response message?

Destination port for the DNS query: 53  
 Source port of DNS response: 53



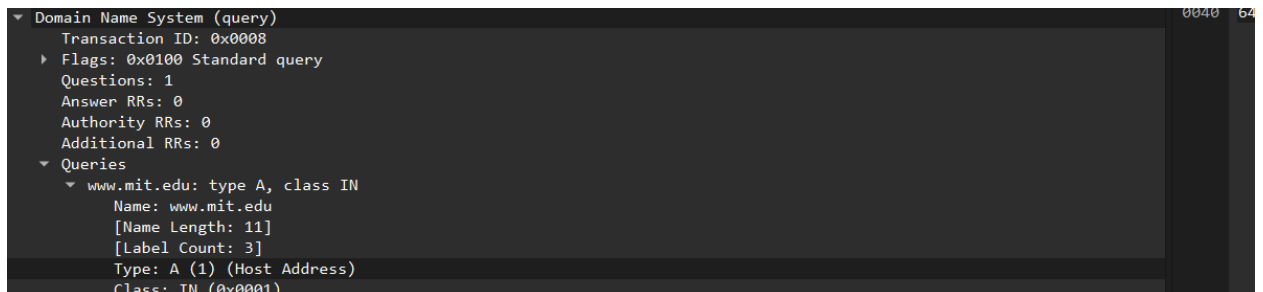
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The destination IP: 139.179.30.34  
 One of my local DNS servers: 139.179.30.34 (I used public DNS)



13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Type A  
 It doesn’t contain any “answers”.



14. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

It provides three answers that contain Name, Type, Class, TTL, Data length, and CNAME or Address.

```

  Answers
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    Name: www.mit.edu.edgekey.net
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 60 (1 minute)
    Data length: 27
    CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type A, class IN, addr 184.29.225.160
    Name: e9566.dscb.akamaiedge.net
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 20 (20 seconds)
    Data length: 4
    Address: 184.29.225.160

```

## 15. Provide a screenshot

No.	Time	Source	Destination	Protocol	Length	Info
57	17:42:43,641425	139.179.243.93	139.179.30.24	DNS	71	Standard query 0x0008 A www.mit.edu
58	17:42:43,901137	139.179.30.24	139.179.243.93	DNS	163	Standard query response 0x0008 A www.mit.edu CNAME

```

  Frame 58: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface \Device\NPF_{F30844EB-6737-49E2-8E0B-...}
  Ethernet II, Src: SuperMicroCo_8e:b3:84 (0c:c4:7a:8e:b3:84), Dst: Intel_58:10:4c (64:6e:e0:58:10:4c)
  Internet Protocol Version 4, Src: 139.179.30.24, Dst: 139.179.243.93
  User Datagram Protocol, Src Port: 53, Dst Port: 60537
  Domain Name System (response)
    Transaction ID: 0x0008
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    Queries
    Answers
      www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 1800 (30 minutes)
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
      www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        Name: www.mit.edu.edgekey.net
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 60 (1 minute)
        Data length: 27
        CNAME: e9566.dscb.akamaiedge.net
      e9566.dscb.akamaiedge.net: type A, class IN, addr 184.29.225.160
        Name: e9566.dscb.akamaiedge.net
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 4
        Address: 184.29.225.160
    [Request In: 57]
    [Time: 0.259712000 seconds]

```

## 16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The destination IP: 76.76.19.19

One of my local DNS servers: 76.76.19.19 (I used public DNS)

No.	Time	Source	Destination	Protocol	Length	Info
13	20:56:30,077483	192.168.1.71	76.76.19.19	DNS	67	Standard query 0x0003 NS mit.edu

```

DNS Servers . . . . . : 76.76.19.19
                       76.223.122.150

```

17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Type NS

It doesn't contain any “answers”.

```
▼ Domain Name System (query)
  Transaction ID: 0x0003
  ▶ Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ mit.edu: type NS, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
```

18. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?

The answers provide 8 MIT name servers. The Additional records provide the IP addresses of the MIT name servers.

```
▼ Answers
  ▶ mit.edu: type NS, class IN, ns use5.akam.net
  ▶ mit.edu: type NS, class IN, ns eur5.akam.net
  ▶ mit.edu: type NS, class IN, ns use2.akam.net
  ▶ mit.edu: type NS, class IN, ns asia2.akam.net
  ▶ mit.edu: type NS, class IN, ns ns1-37.akam.net
  ▶ mit.edu: type NS, class IN, ns usw2.akam.net
  ▶ mit.edu: type NS, class IN, ns asia1.akam.net
  ▶ mit.edu: type NS, class IN, ns ns1-173.akam.net
  ▼ Additional records
    ▶ eur5.akam.net: type A, class IN, addr 23.74.25.64
    ▶ use2.akam.net: type A, class IN, addr 96.7.49.64
    ▶ use5.akam.net: type A, class IN, addr 2.16.40.64
    ▶ usw2.akam.net: type A, class IN, addr 184.26.161.64
    ▶ asia1.akam.net: type A, class IN, addr 95.100.175.64
    ▶ asia2.akam.net: type A, class IN, addr 95.101.36.64
    ▶ ns1-37.akam.net: type A, class IN, addr 193.108.91.37
    ▶ ns1-173.akam.net: type A, class IN, addr 193.108.91.173
```

19. Provide a screenshot.

No.	Time	Source	Destination	Protocol	Length	Info
13	20:56:30,077483	192.168.1.71	76.76.19.19	DNS	67	Standard query 0x0003 NS mit.edu
14	20:56:30,217139	76.76.19.19	192.168.1.71	DNS	446	Standard query response 0x0003 NS mit.edu NS use5

Domain Name System (response)  
Transaction ID: 0x0003  
Flags: 0x8180 Standard query response, No error  
Questions: 1  
Answer RRs: 8  
Authority RRs: 0  
Additional RRs: 11  
Queries  
Answers

mit.edu: type NS, class IN, ns use5.akam.net  
Name: mit.edu  
Type: NS (2) (authoritative Name Server)  
Class: IN (0x0001)  
Time to live: 1776 (29 minutes, 36 seconds)  
Data length: 15  
Name Server: use5.akam.net

mit.edu: type NS, class IN, ns eur5.akam.net  
mit.edu: type NS, class IN, ns use2.akam.net  
mit.edu: type NS, class IN, ns asia2.akam.net  
mit.edu: type NS, class IN, ns ns1-37.akam.net  
mit.edu: type NS, class IN, ns usw2.akam.net  
mit.edu: type NS, class IN, ns asia1.akam.net  
mit.edu: type NS, class IN, ns ns1-173.akam.net

Additional records

eur5.akam.net: type A, class IN, addr 23.74.25.64  
Name: eur5.akam.net  
Type: A (1) (Host Address)  
Class: IN (0x0001)  
Time to live: 80614 (22 hours, 23 minutes, 34 seconds)  
Data length: 4  
Address: 23.74.25.64

use2.akam.net: type A, class IN, addr 96.7.49.64  
use5.akam.net: type A, class IN, addr 2.16.40.64  
usw2.akam.net: type A, class IN, addr 184.26.161.64  
asia1.akam.net: type A, class IN, addr 95.100.175.64  
asia2.akam.net: type A, class IN, addr 95.101.36.64  
ns1-37.akam.net: type A, class IN, addr 193.108.91.37  
ns1-173.akam.net: type A, class IN, addr 193.108.91.173

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

The destination IP: 18.0.72.3  
This IP address corresponds to: bitsy.mit.edu

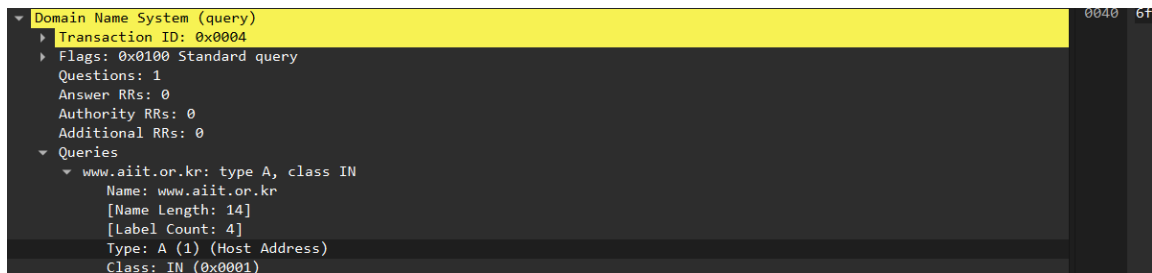
No.	Time	Source	Destination	Protocol	Length	Info
20	21:07:36,555122	192.168.1.71	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr

C:\Users\Emre>nslookup 18.0.72.3  
Server: modem.home  
Address: 192.168.1.1  
  
Name: bitsy.mit.edu  
Address: 18.0.72.3

21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Type A  
It doesn't contain any “answers”.



22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

Even though I manually tried the public DNSs I found on the internet from my computer's network settings, like the previous question, I could not get a response to this query.

No.	Time	Source	Destination	Protocol	Length	Info
2	21:07:30,539109	192.168.1.71	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
8	21:07:32,541811	192.168.1.71	18.0.72.3	DNS	79	Standard query 0x0002 A www.aiit.or.kr.home
18	21:07:34,547824	192.168.1.71	18.0.72.3	DNS	79	Standard query 0x0003 AAAA www.aiit.or.kr.home
20	21:07:36,555122	192.168.1.71	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
21	21:07:38,562658	192.168.1.71	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

```

C:\Users\Emre>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 18.0.72.3

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
  
```

But later, in the command I ran, I replaced the expression bitsy.mit.edu with Google's public DNS (8.8.4.4) and obtained the following prompt.

```

C:\Users\Emre>nslookup www.aiit.or.kr 8.8.4.4
Server: dns.google
Address: 8.8.4.4

Non-authoritative answer:
Name: www.aiit.or.kr
Address: 58.229.6.225
  
```

So, I was able to view the response message via Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
9	21:33:48,093420	192.168.1.71	8.8.4.4	DNS	74	Standard query 0x0004 A www.aiit.or.kr
10	21:33:48,145588	8.8.4.4	192.168.1.71	DNS	90	Standard query response 0x0004 A www.aiit.or.kr A

The response message provides one answer that contains the Name, Type, Class, TTL, Data length, and Address of www.aiit.or.kr.

```
Answers
  www.aiit.or.kr: type A, class IN, addr 58.229.6.225
    Name: www.aiit.or.kr
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 2726 (45 minutes, 26 seconds)
    Data length: 4
    Address: 58.229.6.225
```

### 23. Provide a screenshot.

No.	Time	Source	Destination	Protocol	Length	Info
9	21:33:48,093420	192.168.1.71	8.8.4.4	DNS	74	Standard query 0x0004 A www.aiit.or.kr
10	21:33:48,145588	8.8.4.4	192.168.1.71	DNS	90	Standard query response 0x0004 A www.aiit.or.kr A

Frame 10: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF\_{F30844EB-6737-49E2-8E08-6D08} 0000 64

Ethernet II, Src: HuaweiTechno\_93:c3:34 (60:7e:cd:93:c3:34), Dst: Intel\_58:10:4c (64:6e:e0:58:10:4c) 0010 00

Internet Protocol Version 4, Src: 8.8.4.4, Dst: 192.168.1.71 0020 01

User Datagram Protocol, Src Port: 53, Dst Port: 57778 0030 00

Domain Name System (response) 0040 6f

Transaction ID: 0x0004 0050 00

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

www.aiit.or.kr: type A, class IN

Name: www.aiit.or.kr

[Name Length: 14]

[Label Count: 4]

Type: A (1) (Host Address)

Class: IN (0x0001)

Answers

www.aiit.or.kr: type A, class IN, addr 58.229.6.225

Name: www.aiit.or.kr

Type: A (1) (Host Address)

Class: IN (0x0001)

Time to live: 2726 (45 minutes, 26 seconds)

Data length: 4

Address: 58.229.6.225

[Request In: 9]

[Time: 0.052168000 seconds]