Mehmet Berk Türkçapar
21902570 - Section 1

Wireshark Lab:

1. List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
    1. DTLS
    2. ARP
    3. MDNS
    4. SSDP
    5. LLC
    6. QUIC
    7. TLSv1.2
    8. TCP
    9. UDP
    10. HTTP

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.)

Time	Info
15:19:43.808580	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
15:19:43.956703	HTTP/1.1 200 OK (text/html)

As it can be seen in the picture it approximately took 0.15 seconds.

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?

The internet address of gaia.cs.umass.edu is: 128.119.245.12
The internet address of my computer is: 139.179.55.144

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.

```
/Users/berkturkcapar/Desktop/bilkent-wifi-wireshark-lab1.pcapng 540 total packets, 2 shown

No.     Time              Info
Source              Destination           Protocol Length
    378 15:19:43.808580    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
139.179.55.144        128.119.245.12        HTTP     545
Frame 378: 545 bytes on wire (4360 bits), 545 bytes captured (4360 bits) on interface en0, id 0
Ethernet II, Src: Apple_a0:7c:73 (f0:18:98:a0:7c:73), Dst: SuperMic_8e:b3:84 (0c:c4:7a:
8e:b3:84)
Internet Protocol Version 4, Src: 139.179.55.144, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56608, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
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 (Macintosh; Intel Mac OS X 10_15_7) 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\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: 386]
```

Mehmet Berk Türkçapar
21902570 - Section 1

HTTP Lab:

The Basic HTTP GET/response Interaction:

```
No.     Time              Info
Source               Destination          Protocol Length
    150 15:54:59.729802    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
139.179.55.144       128.119.245.12       HTTP     574
Frame 150: 574 bytes on wire (4592 bits), 574 bytes captured (4592 bits) on interface en0, id 0
Ethernet II, Src: Apple_a0:7c:73 (f0:18:98:a0:7c:73), Dst: SuperMic_8e:b3:84 (0c:c4:7a:
8e:b3:84)
Internet Protocol Version 4, Src: 139.179.55.144, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56800, Dst Port: 80, Seq: 1, Ack: 1, Len: 508
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/
1.1\r\n]
            [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) 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,de;q=0.6\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: 181]
```

```
No.     Time              Info
Source               Destination          Protocol Length
    181 15:54:59.877744    HTTP/1.1 200 OK  (text/html)
128.119.245.12       139.179.55.144       HTTP     552
Frame 181: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
Ethernet II, Src: SuperMic_8e:b3:84 (0c:c4:7a:8e:b3:84), Dst: Apple_a0:7c:73 (f0:18:98:a0:7c:
73)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.55.144
Transmission Control Protocol, Src Port: 80, Dst Port: 56800, Seq: 1, Ack: 509, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Tue, 14 Mar 2023 12:54:59 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: Tue, 14 Mar 2023 05:59:01 GMT\r\n
    ETag: "80-5f6d5ec9bcf0b"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
        [Content length: 128]
    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: 0.147942000 seconds]
    [Request in frame: 150]
    [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)
```

Mehmet Berk Türkçapar
21902570 - Section 1

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

HTTP version is 1.1

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

It accepts Turkish (tr-TR, tr), English (en-US, en) and German (de).

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

```
Internet Protocol Version 4, Src: 139.179.55.144, Dst: 128.119.245.12
```

The internet address of gaia.cs.umass.edu is: 128.119.245.12
The internet address of my computer is: 139.179.55.144

4. What is the status code returned from the server to your browser?
The status code returned from the server is 200.

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

14 March 2023 05:59:01.

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

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, there are not any headers within the data that are not displayed in the packet-listing window.

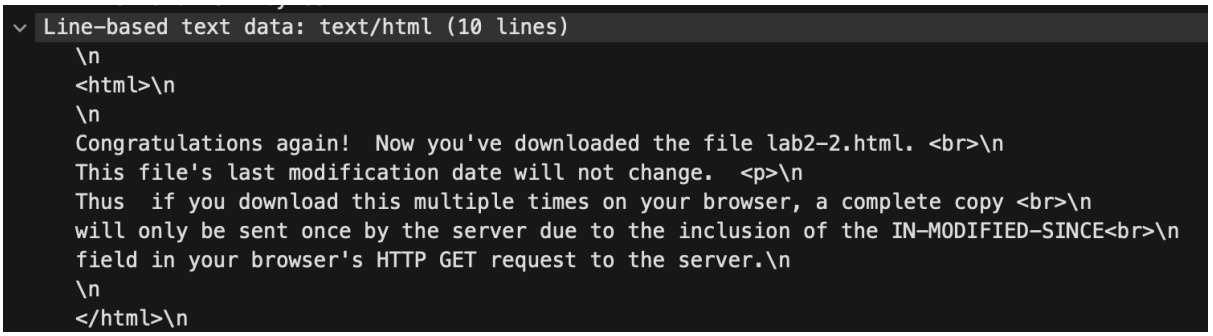
Mehmet Berk Türkçapar
21902570 - Section 1

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, it does not contain an “IF-MODIFIED-SINCE” line.

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



Yes, the server explicitly returns the contents of the file.

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?

Yes, in the second HTTP GET I see an “IF-MODIFIED-SINCE:” line. It contains the date of the Last-Modified date of the current content.

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.

It returns 304 Not Modified which indicates that the content requested has not been modified since the last request. The server did not return the contents of the file since they have not been modified. So, the already existing data from the previous HTTP GET request was shown.

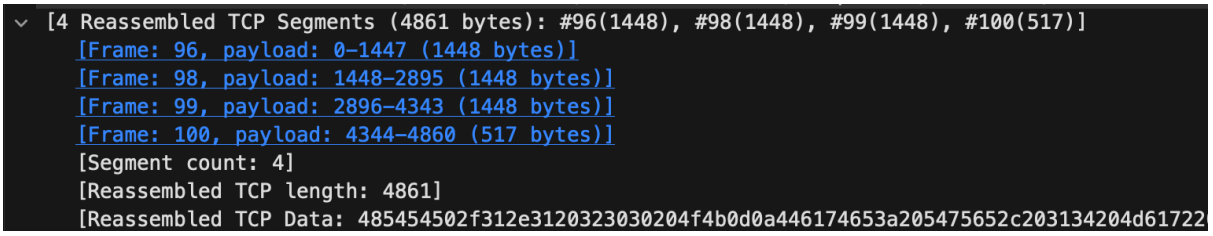
Mehmet Berk Türkçapar
21902570 - Section 1

Retrieving Long Documents:

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

Only one HTTP GET request message was sent by the browser.

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



4 data-containing TCP segments were needed to carry the single HTTP response.

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

The status code is 200 and the phrase is OK.

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

No, there are not any HTTP status lines in the transmitted data associated with a TCPinduced “Continuation”.

Mehmet Berk Türkçapar
21902570 - Section 1

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?

No.	Time	Info	Source	Destination	Protocol
427	17:33:26.090022	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1	139.179.55.144	128.119.245.12	HTTP
429	17:33:26.238155	HTTP/1.1 200 OK (text/html)	128.119.245.12	139.179.55.144	HTTP
431	17:33:26.269141	GET /pearson.png HTTP/1.1	139.179.55.144	128.119.245.12	HTTP
443	17:33:26.356946	GET /8E_cover_small.jpg HTTP/1.1	139.179.55.144	178.79.137.164	HTTP
452	17:33:26.417416	HTTP/1.1 200 OK (PNG)	128.119.245.12	139.179.55.144	HTTP
457	17:33:26.440382	HTTP/1.1 301 Moved Permanently	178.79.137.164	139.179.55.144	HTTP

In total 3 HTTP GET request messages were sent. First two GET requests were sent to 128.119.245.12 and the last one was sent to 178.79.137.164 .

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

The browser downloaded the two images from the two websites in parallel. As it can be seen from the screenshot the HTTP GET request for the second image was sent before the response came for the first HTTP GET request.

HTTP Authentication:

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

No.	Time	Info	Source	Destination
314	17:57:33.531302	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.ht…	139.179.55.144	128.119.245.12
318	17:57:33.681034	HTTP/1.1 401 Unauthorized (text/html)	128.119.245.12	139.179.55.144
679	17:57:45.586108	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.ht…	139.179.55.144	128.119.245.12
684	17:57:45.735183	HTTP/1.1 200 OK (text/html)	128.119.245.12	139.179.55.144

401 Unauthorized

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

```
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
   Credentials: wireshark-students:network
```

Authorization field was added in the second HTTP GET message.

Mehmet Berk Türkçapar
21902570 - Section 1

DNS:

nslookup:

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

```
Berks-MacBook-Pro-3:~ berkturkcapar$ nslookup www.gmarket.co.kr
Server:         139.179.30.24
Address:        139.179.30.24#53

Non-authoritative answer:
www.gmarket.co.kr       canonical name = www.gmarket.co.kr.gccdn.net.
Name:   www.gmarket.co.kr.gccdn.net
Address: 212.154.20.35
```

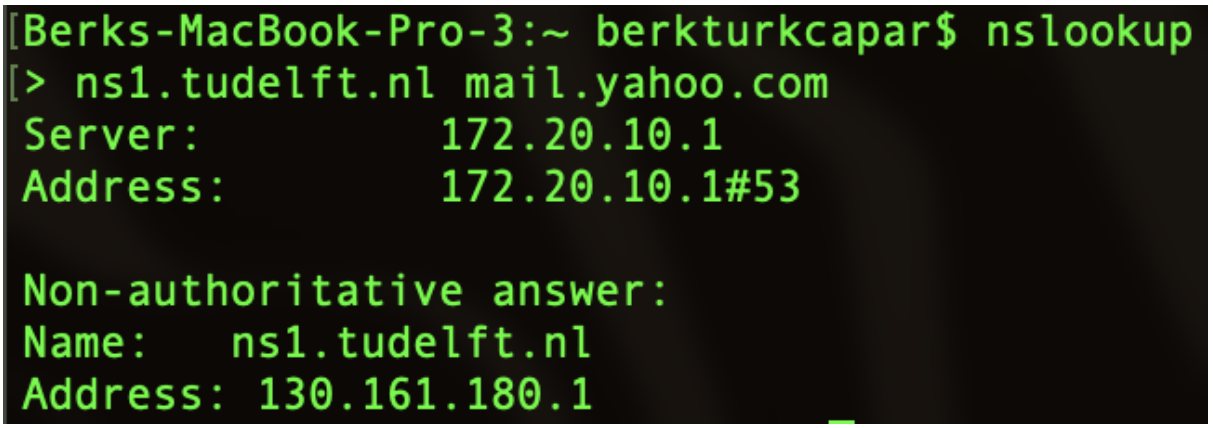
As it can be seen the IP address of gmarket.co.kr which is an ecommerce website in South Korea is 212.154.20.35

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

```
Berks-MacBook-Pro-3:~ berkturkcapar$ nslookup -type=NS tudelft.nl
Server:         139.179.30.24
Address:        139.179.30.24#53

Non-authoritative answer:
tudelft.nl      nameserver = ns1.tudelft.nl.
tudelft.nl      nameserver = ns2.tudelft.nl.

Authoritative answers can be found from:

Berks-MacBook-Pro-3:~ berkturkcapar$ nslookup ns1.tudelft.nl
Server:         139.179.30.24
Address:        139.179.30.24#53

Non-authoritative answer:
Name:   ns1.tudelft.nl
Address: 130.161.180.1

Berks-MacBook-Pro-3:~ berkturkcapar$ nslookup ns2.tudelft.nl
Server:         139.179.10.13
Address:        139.179.10.13#53

Non-authoritative answer:
Name:   ns2.tudelft.nl
Address: 130.161.180.65
```

The alias of TU Delft is www.tudelft.nl. First I checked the name servers by using `nslookup -type=NS`. Then, I used nslookup to get the authoritative addresses of TU Delft. There were two server names and their addresses were as follows:
ns1.tudelft.nl: 130.161.180.1
ns2.tudelft.nl: 130.161.180.65

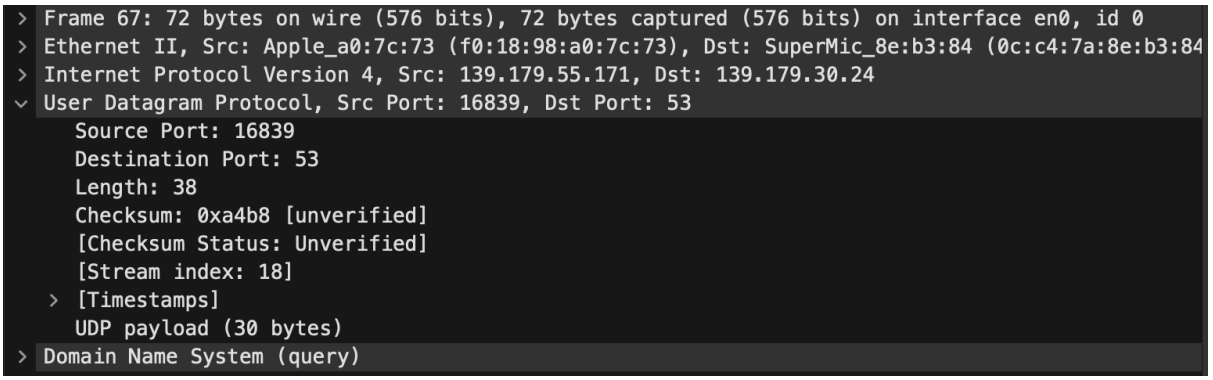
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail.



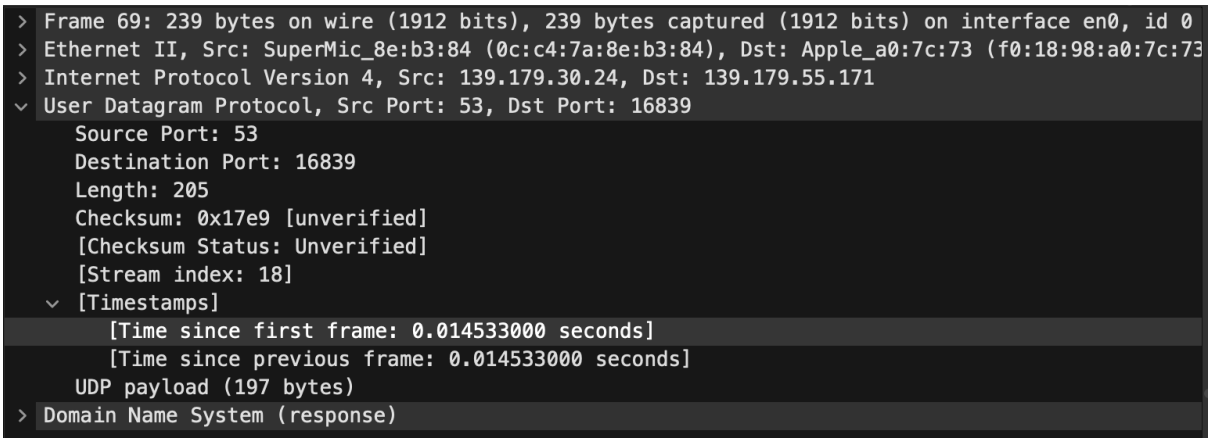
Mehmet Berk Türkçapar
21902570 - Section 1

Tracing DNS with Wireshark

Query:



Response:



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

They are sent over UDP.

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

Destination port of the DNS query message: 53
Source port of DNS response message: 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 DNS query message is sent to 139.179.30.24 which is the same as the address of my default local DNS server.

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

```
Domain Name System (query)
    Transaction ID: 0x897e
  > 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 (Host Address) (1)
        Class: IN (0x0001)
```

It is classified as Type A. The query message does not contain any “answers”.

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

There are three answers provided. The first answer contains information about the alias of the DNS of the host which is www.ietf.org.cdn.cloudflare.net . The next two contain Type A addresses which are host addresses. The first answer contains the address 104.16.44.99 and the second answer contains the address 104.16.45.99 .

```
Answers
  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: 1381 (23 minutes, 1 second)
    Data length: 33
    CNAME: www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
    Address: 104.16.44.99
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
    Address: 104.16.45.99
```

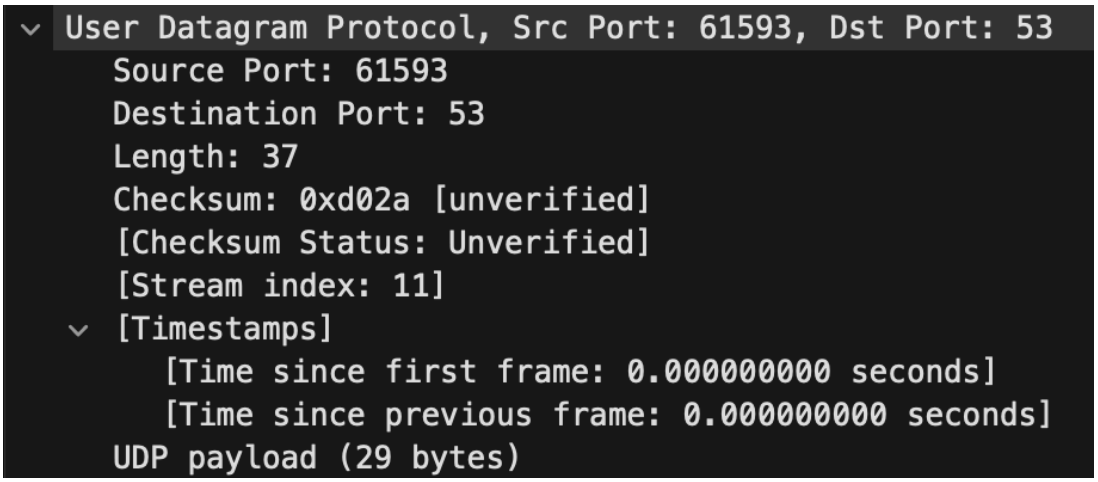
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

The destination IP address of the TCP SYN packet is 104.16.44.99 which is the same IP address in the second answer.

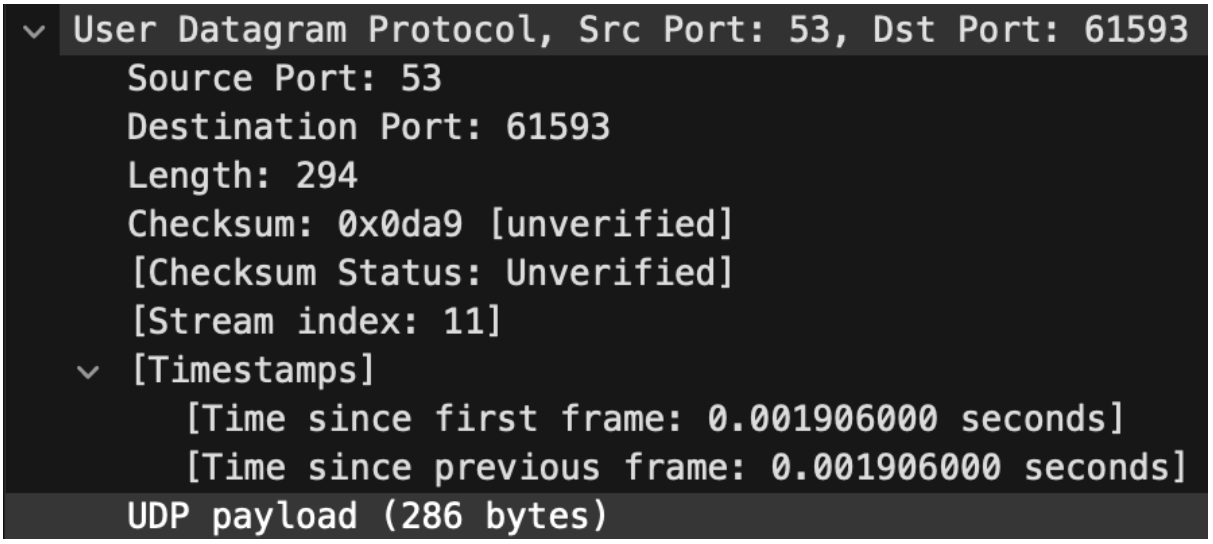
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Yes, it issues new DNS queries before retrieving each image.

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



Destination port of the DNS query message: 53



Source port of DNS response message: 53

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

```
64 16:48:34.246083 Standard query 0x7ed5 A www.mit.edu                          139.179.55.171      139.179.30.24
68 16:48:34.247989 Standard query response 0x7ed5 A www.mit.edu CNAME www.mit.… 139.179.30.24       139.179.55.171
```

The DNS query message is sent to 139.179.30.24 which is the same as the address of my default local DNS server.

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

```
Domain Name System (query)
    Transaction ID: 0x7ed5
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

It is classified as Type A. The query message does not contain any “answers”.

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

There are three answers provided. The first two answers contain information about the alias of the DNS servers. The first one is www.mit.edu.edgekey.net and the second is e9566.dscb.akamaiedge.net . The third answer contains A type address which is 23.0.93.177 .

15. Provide a screenshot.

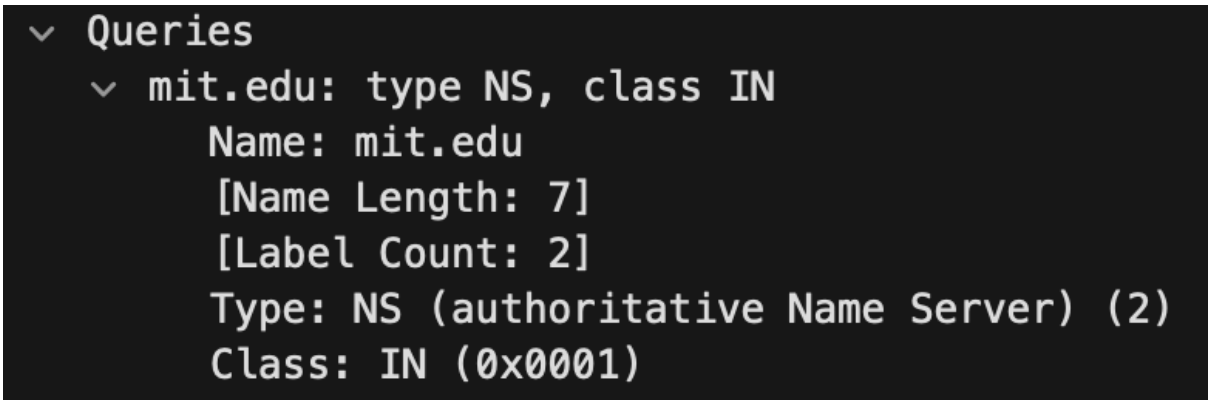
```
Answers
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1576 (26 minutes, 16 seconds)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 57 (57 seconds)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type A, class IN, addr 23.0.93.177
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 17 (17 seconds)
      Data length: 4
      Address: 23.0.93.177
```

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

```
17:18:16.868963  Standard query 0x9b93 NS mit.edu                              139.179.55.171   139.179.30.24   DNS
17:18:16.873775  Standard query response 0x9b93 NS mit.edu NS ns1-37.akam.ne…  139.179.30.24    139.179.55.171  DNS
```

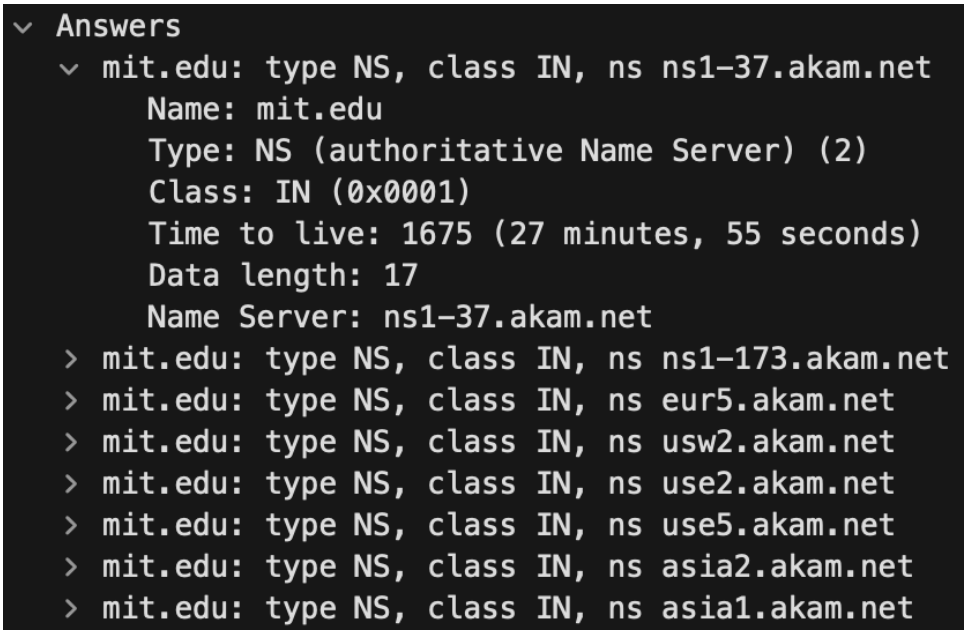
The DNS query message is sent to 139.179.30.24 which is the same as the address of my default local DNS server.

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



It is classified as Type NS. The query message does not contain any “answers”.

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?



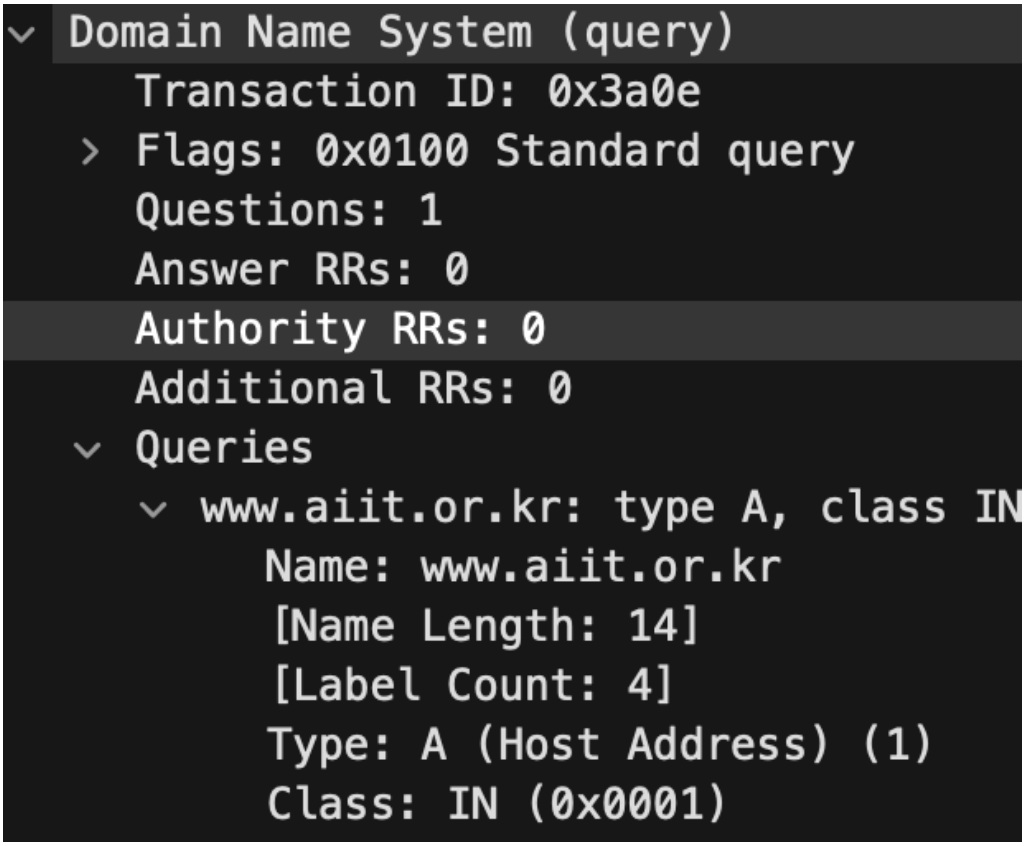
The names are indicated in the screenshot. The IP addresses are not provided.

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?

```
45 17:38:03.515027  Standard query 0x3a0e A www.aiit.or.kr                      139.179.55.171   139.179.30.24
46 17:38:03.533077  Standard query response 0x3a0e A www.aiit.or.kr A 58.229.6.… 139.179.30.24   139.179.55.171
```

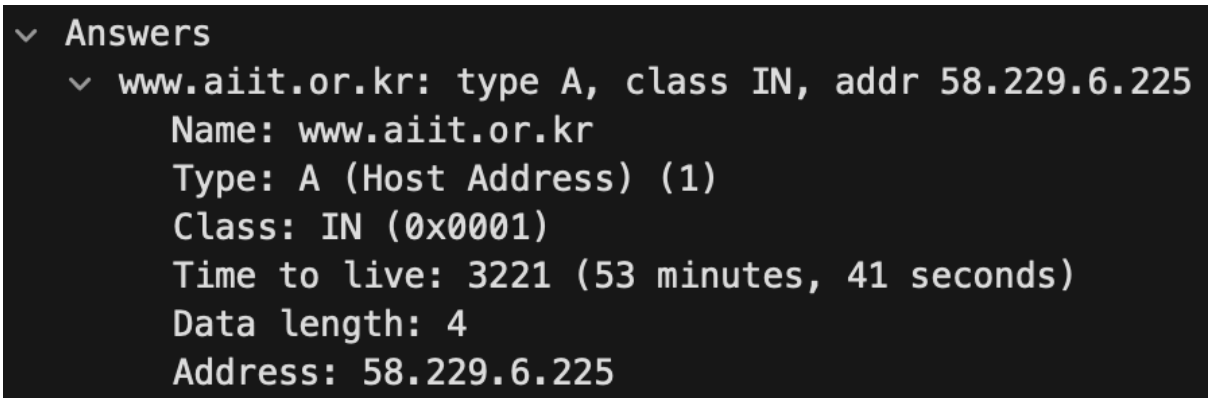
The DNS query message is sent to 139.179.30.24 which is the same as the address of my default local DNS server.

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



It is classified as Type A. The query message does not contain any “answers”.

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



Only one answer which contains a type A address is provided. The address is 58.229.6.225 .