CS421 Wireshark Assignment 01

Uğur Erdem Seyfi
21801744

What to hand in

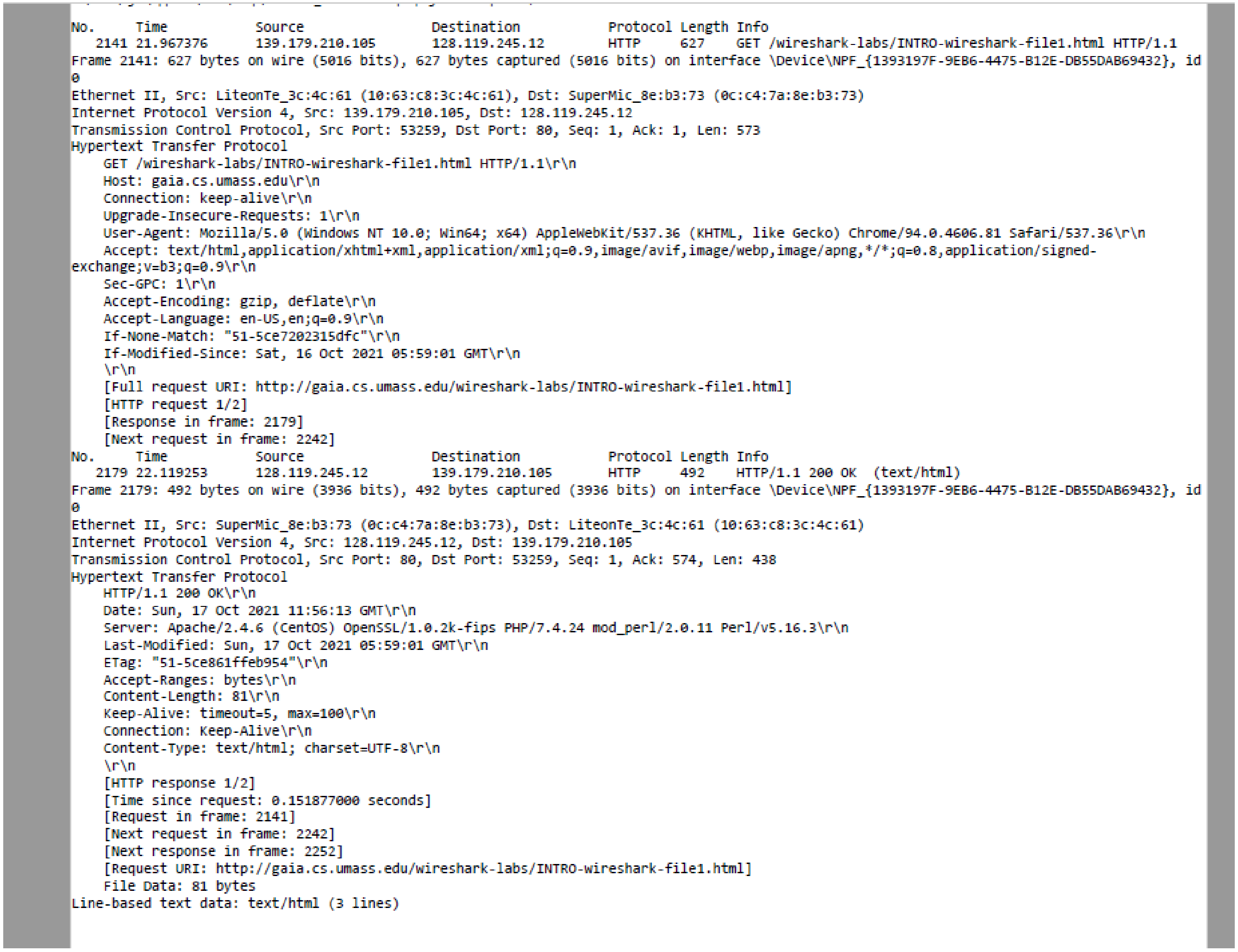
Q1. List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Answer: SSDP, UDP, ARP, MDNS, TCP, NBNS, IGMPv2, LLMNR, DNS, TLSv1.2, ICMPv6

Q2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?
Answer: The difference between arrival time of the packages is around 151ms

Q3. 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?
Answer: Address for gaia.cs.umass.edu is 128.119.245.12, address of my computer is 139.179.210.105

Q4. 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.
Answer: I have printed them. It is in the next page.



```
No.     Time           Source                Destination           Protocol Length Info
   2141 21.967376      139.179.210.105       128.119.245.12        HTTP     627    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 2141: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits) on interface \Device\NPF_{1393197F-9EB6-4475-B12E-DB55DAB69432}, id
0
Ethernet II, Src: LiteonTe_3c:4c:61 (10:63:c8:3c:4c:61), Dst: SuperMic_8e:b3:73 (0c:c4:7a:8e:b3:73)
Internet Protocol Version 4, Src: 139.179.210.105, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53259, Dst Port: 80, Seq: 1, Ack: 1, Len: 573
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/94.0.4606.81 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=0.9\r\n
    Sec-GPC: 1\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "51-5ce7202315dfc"\r\n
    If-Modified-Since: Sat, 16 Oct 2021 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 2179]
    [Next request in frame: 2242]
No.     Time           Source                Destination           Protocol Length Info
   2179 22.119253      128.119.245.12        139.179.210.105       HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 2179: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{1393197F-9EB6-4475-B12E-DB55DAB69432}, id
0
Ethernet II, Src: SuperMic_8e:b3:73 (0c:c4:7a:8e:b3:73), Dst: LiteonTe_3c:4c:61 (10:63:c8:3c:4c:61)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.210.105
Transmission Control Protocol, Src Port: 80, Dst Port: 53259, Seq: 1, Ack: 574, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sun, 17 Oct 2021 11:56:13 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 17 Oct 2021 05:59:01 GMT\r\n
    ETag: "51-5ce861ffeb954"\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 1/2]
    [Time since request: 0.151877000 seconds]
    [Request in frame: 2141]
    [Next request in frame: 2242]
    [Next response in frame: 2252]
    [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)
```

1. The Basic HTTP GET/response interaction

Q1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
Answer: Both of them are running HTTP version 1.1.

Q2. What languages (if any) does your browser indicate that it can accept to the server? ,
Answer: -

Q3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
Answer: Address for gaia.cs.umass.edu is 128.119.245.12, address of my computer is 139.179.210.105

Q4. What is the status code returned from the server to your browser?
Answer: 200 OK

Q5. When was the HTML file that you are retrieving last modified at the server?

Answer: 17 October 2021 05:05:01 GMT

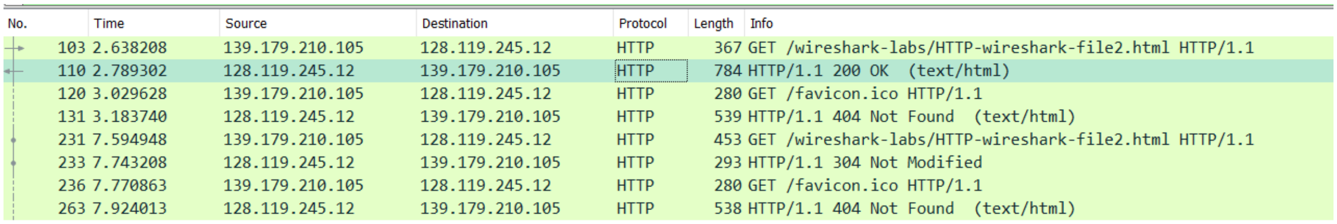
Q6. How many bytes of content are being returned to your browser?
Answer: Content length is 128 bytes

Q7. 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.
Answer: No I did not find any headers that are not in the data.

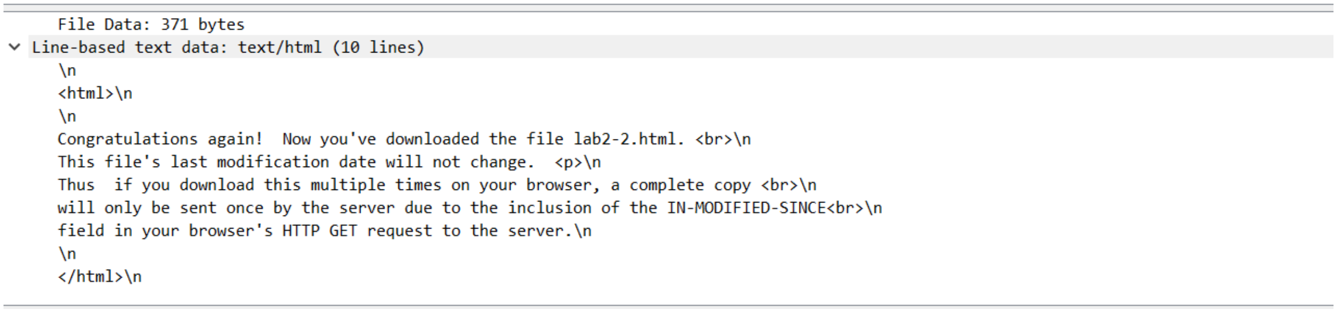
2. The HTTP CONDITIONAL GET/response interaction

Q8. 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?
Answer: No, I don’t see “IF-MODIFIED-SINCE” in the GET request.

Q9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
Answer: Yes, in the packet with the status “200 OK” from server, there is a section called “Line-based text data”, in there I can see the same content as that is shown on my browser.

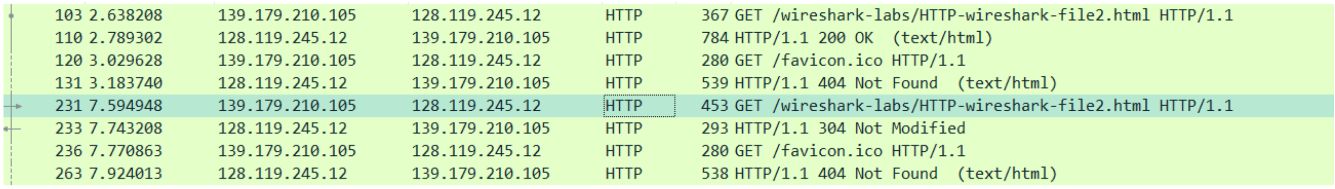


```
No.    Time        Source            Destination       Protocol  Length  Info
  103  2.638208    139.179.210.105   128.119.245.12    HTTP         367  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  110  2.789302    128.119.245.12    139.179.210.105   HTTP         784  HTTP/1.1 200 OK  (text/html)
  120  3.029628    139.179.210.105   128.119.245.12    HTTP         280  GET /favicon.ico HTTP/1.1
  131  3.183740    128.119.245.12    139.179.210.105   HTTP         539  HTTP/1.1 404 Not Found  (text/html)
  231  7.594948    139.179.210.105   128.119.245.12    HTTP         453  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  233  7.743208    128.119.245.12    139.179.210.105   HTTP         293  HTTP/1.1 304 Not Modified
  236  7.770863    139.179.210.105   128.119.245.12    HTTP         280  GET /favicon.ico HTTP/1.1
  263  7.924013    128.119.245.12    139.179.210.105   HTTP         538  HTTP/1.1 404 Not Found  (text/html)
```

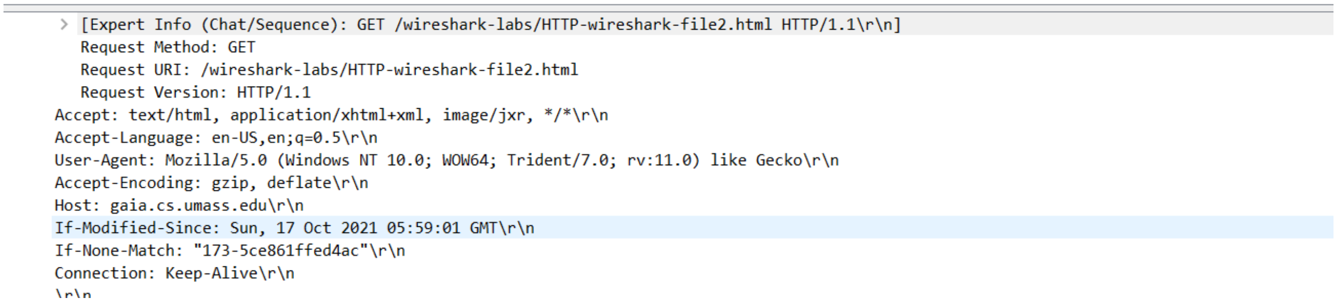


```
    File Data: 371 bytes
v Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, 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
```

Q10. 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?
Answer: Yes, I see an “IF-MODIFIED-SINCE” line. The information is: Sun, 17 Oct 2021, 05:59:01 GMT



```
103 2.638208   139.179.210.105   128.119.245.12    HTTP    367 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
110 2.789302   128.119.245.12    139.179.210.105   HTTP    784 HTTP/1.1 200 OK  (text/html)
120 3.029628   139.179.210.105   128.119.245.12    HTTP    280 GET /favicon.ico HTTP/1.1
131 3.183740   128.119.245.12    139.179.210.105   HTTP    539 HTTP/1.1 404 Not Found  (text/html)
231 7.594948   139.179.210.105   128.119.245.12    HTTP    453 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
233 7.743208   128.119.245.12    139.179.210.105   HTTP    293 HTTP/1.1 304 Not Modified
236 7.770863   139.179.210.105   128.119.245.12    HTTP    280 GET /favicon.ico HTTP/1.1
263 7.924013   128.119.245.12    139.179.210.105   HTTP    538 HTTP/1.1 404 Not Found  (text/html)
```

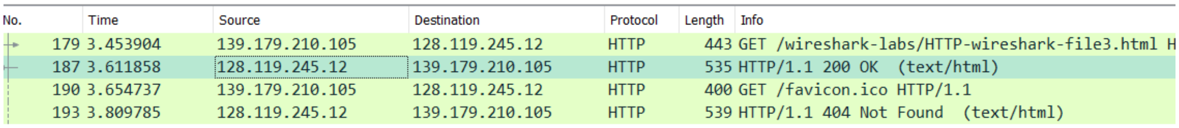


```
  > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.html
    Request Version: HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
Accept-Language: en-US,en;q=0.5\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: gaia.cs.umass.edu\r\n
If-Modified-Since: Sun, 17 Oct 2021 05:59:01 GMT\r\n
If-None-Match: "173-5ce861ffed4ac"\r\n
Connection: Keep-Alive\r\n
\r\n
```

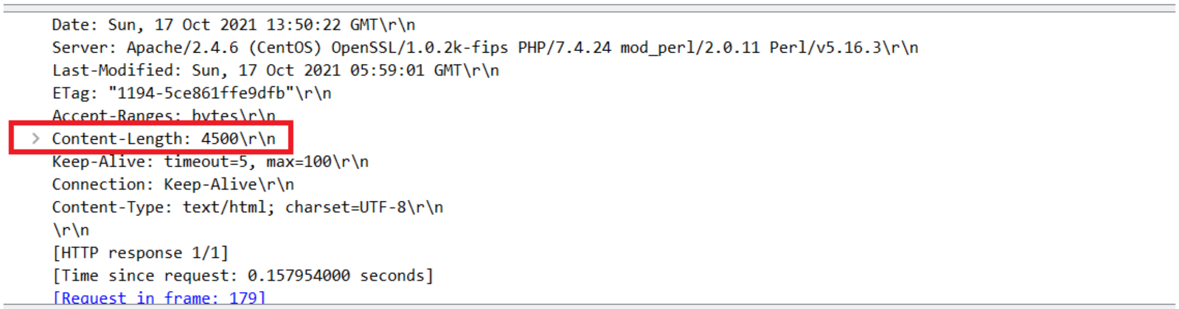
Q11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
Answer: As it can be seen from the screenshots above the status code returned is the “304 Not Modified”. It did not explicitly return the contents of the file since the browser already cached the content.

3. Retrieving Long Document

Although in the question it is said that 4500 bytes is too large to fit in one TCP packet apparently this is not the case anymore as it can be shown from the screenshot belove:



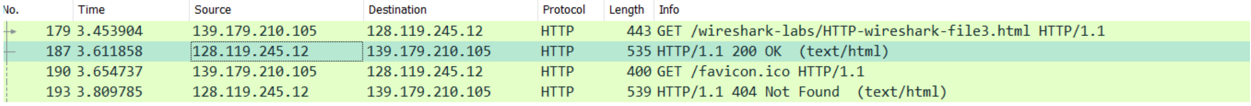
```
No.   Time       Source            Destination       Protocol  Length  Info
179 3.453904   139.179.210.105   128.119.245.12    HTTP        443 GET /wireshark-labs/HTTP-wireshark-file3.html H
187 3.611858   128.119.245.12    139.179.210.105   HTTP        535 HTTP/1.1 200 OK  (text/html)
190 3.654737   139.179.210.105   128.119.245.12    HTTP        400 GET /favicon.ico HTTP/1.1
193 3.809785   128.119.245.12    139.179.210.105   HTTP        539 HTTP/1.1 404 Not Found  (text/html)
```



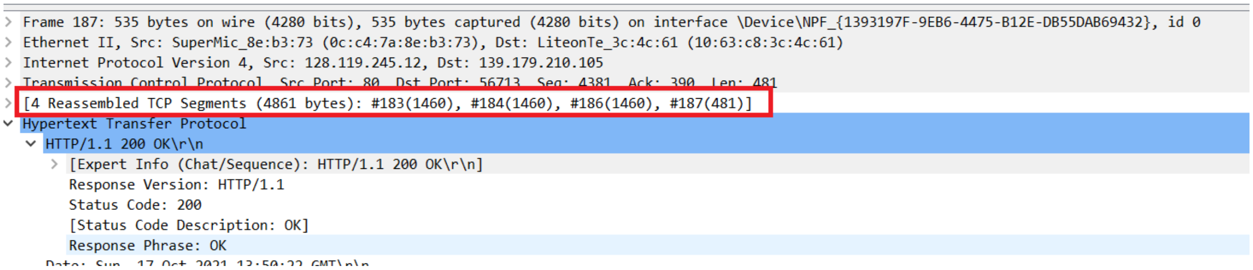
```
Date: Sun, 17 Oct 2021 13:50:22 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sun, 17 Oct 2021 05:59:01 GMT\r\n
ETag: "1194-5ce861ffe9dfb"\r\n
Accept-Ranges: bytes\r\n
> Content-Length: 4500\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.157954000 seconds]
[Request in frame: 179]
```

Q12. How many HTTP GET request messages were sent by your browser?
Answer: Just two. This can be seen from the screenshot above.

Q13. How many data-containing TCP segments were needed to carry the single HTTP response?
Answer: According to the screenshot belove there were 4 Reassembled TCP Segments



No.	Time	Source	Destination	Protocol	Length	Info
179	3.453904	139.179.210.105	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
187	3.611858	128.119.245.12	139.179.210.105	HTTP	535	HTTP/1.1 200 OK (text/html)
190	3.654737	139.179.210.105	128.119.245.12	HTTP	400	GET /favicon.ico HTTP/1.1
193	3.809785	128.119.245.12	139.179.210.105	HTTP	539	HTTP/1.1 404 Not Found (text/html)



```
> Frame 187: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{1393197F-9EB6-4475-B12E-DB55DAB69432}, id 0
> Ethernet II, Src: SuperMic_8e:b3:73 (0c:c4:7a:8e:b3:73), Dst: LiteonTe_3c:4c:61 (10:63:c8:3c:4c:61)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.210.105
> Transmission Control Protocol, Src Port: 80, Dst Port: 56713, Seq: 4381, Ack: 390, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #183(1460), #184(1460), #186(1460), #187(481)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Sun, 17 Oct 2021 13:50:22 GMT\r\n
```

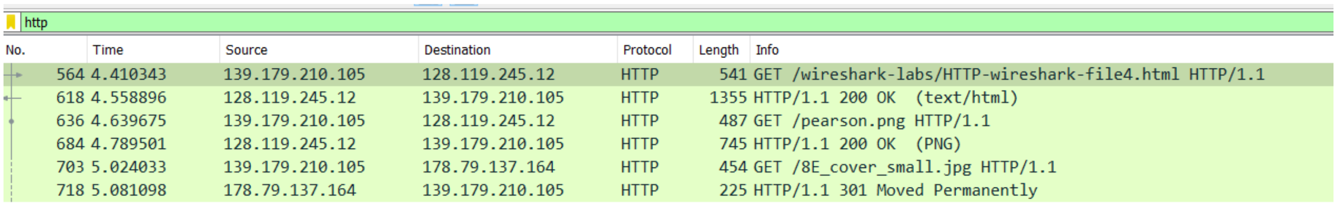
Q14. What is the status code and phrase associated with the response to the HTTP GET request?
Answer: “200 OK” as it can be seen above.

Q15. Are there any HTTP status lines in the transmitted data associated with a TCP induced “Continuation”?
Answer: No.

4. HTML Documents with Embedded Objects

Q16. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?
Answer:

My browser sent 3 HTTP GET requests. Those requests were to either 128.119.245.12 or to 178.79.137.164.



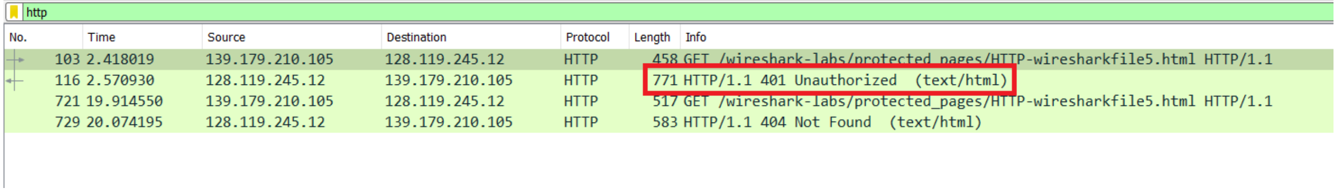
http

No.	Time	Source	Destination	Protocol	Length	Info
564	4.410343	139.179.210.105	128.119.245.12	HTTP	541	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
618	4.558896	128.119.245.12	139.179.210.105	HTTP	1355	HTTP/1.1 200 OK (text/html)
636	4.639675	139.179.210.105	128.119.245.12	HTTP	487	GET /pearson.png HTTP/1.1
684	4.789501	128.119.245.12	139.179.210.105	HTTP	745	HTTP/1.1 200 OK (PNG)
703	5.024033	139.179.210.105	178.79.137.164	HTTP	454	GET /8E_cover_small.jpg HTTP/1.1
718	5.081098	178.79.137.164	139.179.210.105	HTTP	225	HTTP/1.1 301 Moved Permanently

Q17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.
Answer: I think it was serial because before requesting the second image first image is received. If they were parallel the second request would be done before receiving the first request's response.

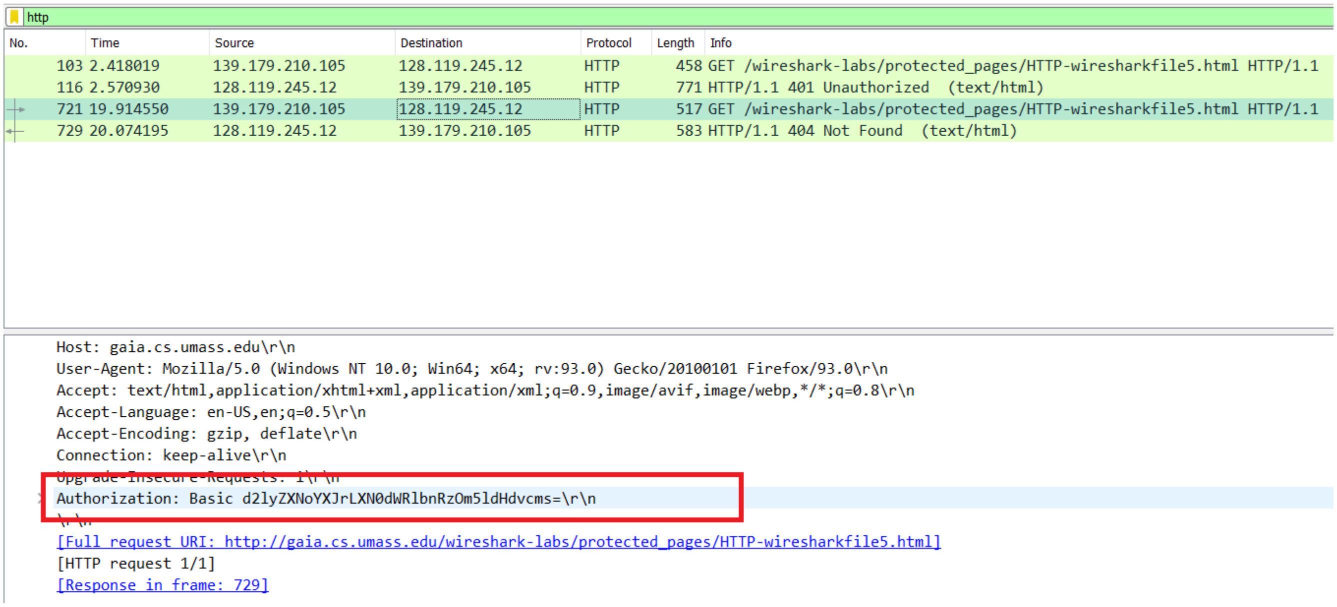
5 HTTP Authentication

Q18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
Answer: The server's response is "401 Unauthorized"



```
http
No.   Time        Source            Destination       Protocol  Length  Info
  103 2.418019    139.179.210.105   128.119.245.12    HTTP       458 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
  116 2.570930    128.119.245.12    139.179.210.105   HTTP       771 HTTP/1.1 401 Unauthorized  (text/html)
  721 19.914550   139.179.210.105   128.119.245.12    HTTP       517 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
  729 20.074195   128.119.245.12    139.179.210.105   HTTP       583 HTTP/1.1 404 Not Found  (text/html)
```

Q19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
Answer: "Authorization" field.

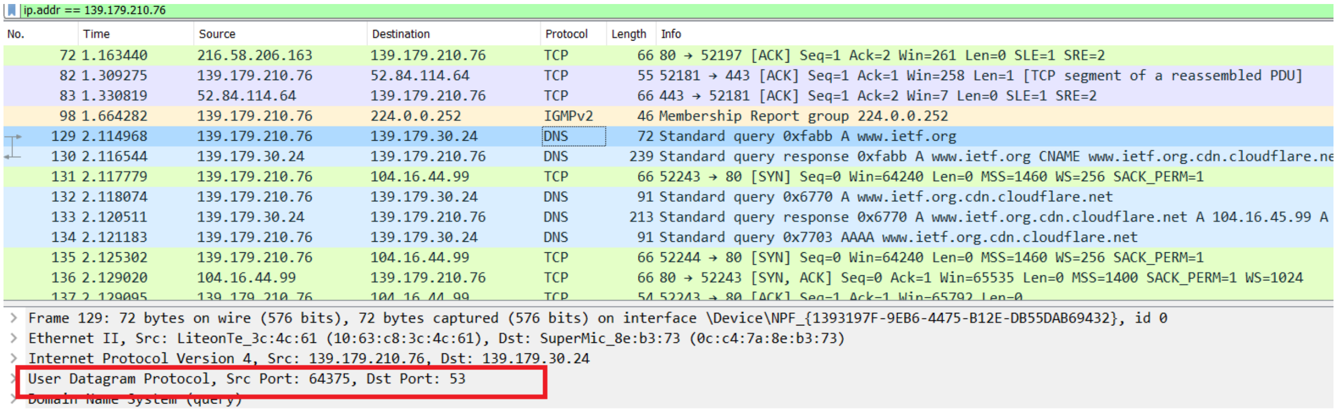


```
http
No.   Time        Source            Destination       Protocol  Length  Info
  103 2.418019    139.179.210.105   128.119.245.12    HTTP       458 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
  116 2.570930    128.119.245.12    139.179.210.105   HTTP       771 HTTP/1.1 401 Unauthorized  (text/html)
  721 19.914550   139.179.210.105   128.119.245.12    HTTP       517 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
  729 20.074195   128.119.245.12    139.179.210.105   HTTP       583 HTTP/1.1 404 Not Found  (text/html)
```

```
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html]
[HTTP request 1/1]
[Response in frame: 729]
```

DNS

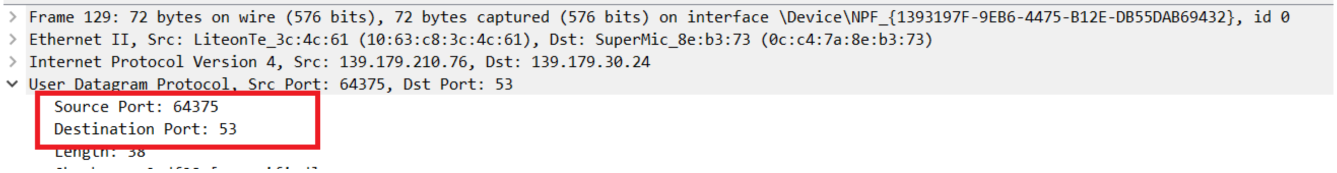
Q4. Locate the DNS query and response messages. Are they sent over UDP or TCP?
Answer: UDP as it can be seen below:



```
ip.addr == 139.179.210.76
No.    Time        Source            Destination       Protocol  Length Info
    72 1.163440    216.58.206.163    139.179.210.76    TCP         66 80 → 52197 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
    82 1.309275    139.179.210.76    52.84.114.64      TCP         55 52181 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]
    83 1.330819    52.84.114.64      139.179.210.76    TCP         66 443 → 52181 [ACK] Seq=1 Ack=2 Win=7 Len=0 SLE=1 SRE=2
    98 1.664282    139.179.210.76    224.0.0.252       IGMPv2      46 Membership Report group 224.0.0.252
   129 2.114968    139.179.210.76    139.179.30.24     DNS         72 Standard query 0xfabb A www.ietf.org
   130 2.116544    139.179.30.24     139.179.210.76    DNS        239 Standard query response 0xfabb A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.ne
   131 2.117779    139.179.210.76    104.16.44.99      TCP         66 52243 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   132 2.118074    139.179.210.76    139.179.30.24     DNS         91 Standard query 0x6770 A www.ietf.org.cdn.cloudflare.net
   133 2.120511    139.179.30.24     139.179.210.76    DNS        213 Standard query response 0x6770 A www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A
   134 2.121183    139.179.210.76    139.179.30.24     DNS         91 Standard query 0x7703 AAAA www.ietf.org.cdn.cloudflare.net
   135 2.125302    139.179.210.76    104.16.44.99      TCP         66 52244 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   136 2.129020    104.16.44.99      139.179.210.76    TCP         66 80 → 52243 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
   137 2.129095    139.179.210.76    104.16.44.99      TCP         54 52243 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0

> Frame 129: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{1393197F-9EB6-4475-B12E-DB55DAB69432}, id 0
> Ethernet II, Src: LiteonTe_3c:4c:61 (10:63:c8:3c:4c:61), Dst: SuperMic_8e:b3:73 (0c:c4:7a:8e:b3:73)
> Internet Protocol Version 4, Src: 139.179.210.76, Dst: 139.179.30.24
> User Datagram Protocol, Src Port: 64375, Dst Port: 53
> Domain Name System (query)
```

Q5. What is the destination port for the DNS query message? What is the source port of DNS response message?
Answer:

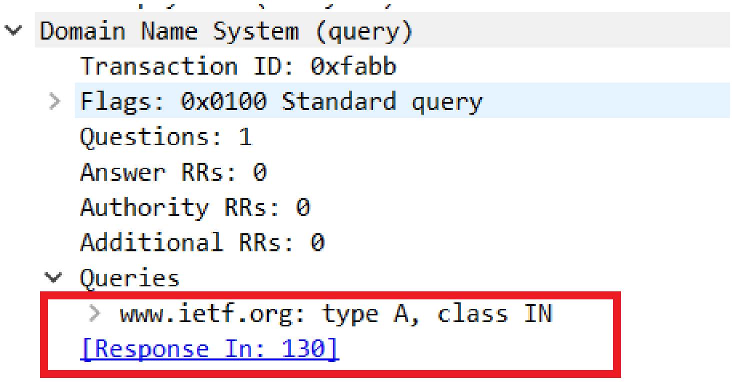
Source port: 64375
Destination: 53



```
> Frame 129: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{1393197F-9EB6-4475-B12E-DB55DAB69432}, id 0
> Ethernet II, Src: LiteonTe_3c:4c:61 (10:63:c8:3c:4c:61), Dst: SuperMic_8e:b3:73 (0c:c4:7a:8e:b3:73)
> Internet Protocol Version 4, Src: 139.179.210.76, Dst: 139.179.30.24
v User Datagram Protocol, Src Port: 64375, Dst Port: 53
      Source Port: 64375
      Destination Port: 53
      Length: 38
```

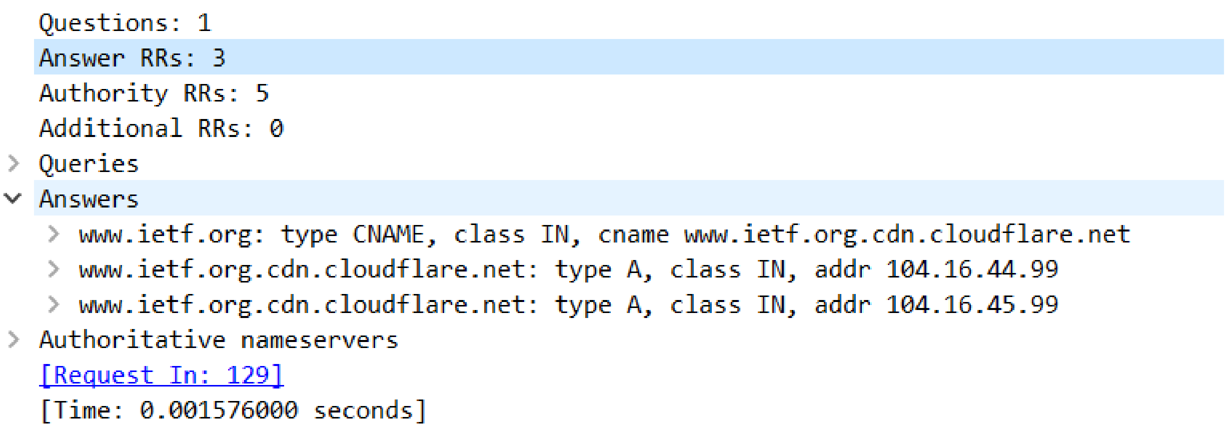
Q6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
Answer: Query was sent to 139.179.30.24. They are the same IP address.

Q7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
Answer: The Type of the DNS query seems to be "A". The message is in another DNS response packet (130th packet).



```
v Domain Name System (query)
    Transaction ID: 0xfabb
  > 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: 130]
```

Q8. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
Answer: It replied 3 answers which contain the site's addresses. It also provided 5 authoritative nameservers.



```
  Questions: 1
  Answer RRs: 3
  Authority RRs: 5
  Additional RRs: 0
> Queries
v Answers
    > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
> Authoritative nameservers
  [Request In: 129]
  [Time: 0.001576000 seconds]
```

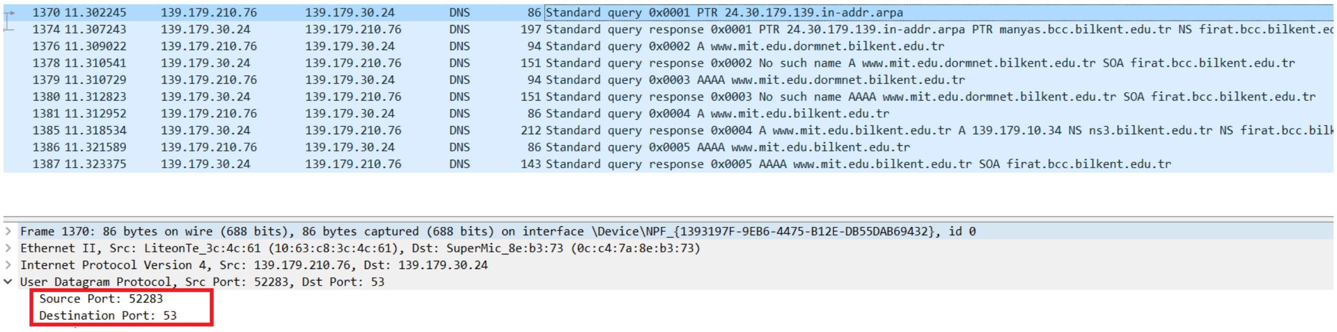
Q9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
Answer: -

Q10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
Answer: No, it seems like there is not any DNS queries regarding the images.

nslookup

Q11. What is the destination port for the DNS query message? What is the source port of DNS response message?
Answer:

Source Port: 52283
Destination Port: 53

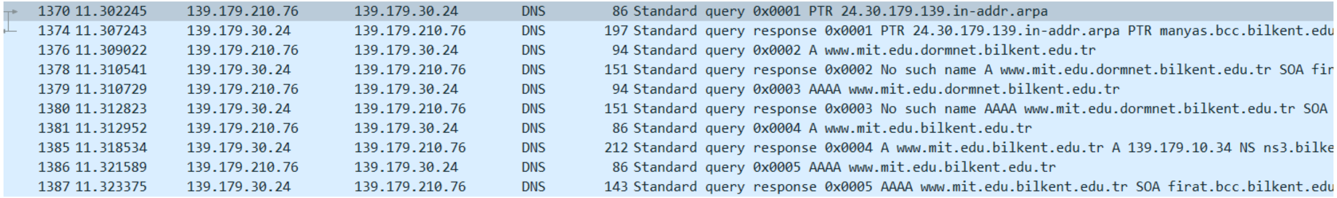


```
1370 11.302245  139.179.210.76  139.179.30.24   DNS   86 Standard query 0x0001 PTR 24.30.179.139.in-addr.arpa
1374 11.307243  139.179.30.24   139.179.210.76  DNS  197 Standard query response 0x0001 PTR 24.30.179.139.in-addr.arpa PTR manyas.bcc.bilkent.edu.tr NS firat.bcc.bilkent.ed
1376 11.309022  139.179.210.76  139.179.30.24   DNS   94 Standard query 0x0002 A www.mit.edu.dormnet.bilkent.edu.tr
1378 11.310541  139.179.30.24   139.179.210.76  DNS  151 Standard query response 0x0002 No such name A www.mit.edu.dormnet.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
1379 11.310729  139.179.210.76  139.179.30.24   DNS   94 Standard query 0x0003 AAAA www.mit.edu.dormnet.bilkent.edu.tr
1380 11.312823  139.179.30.24   139.179.210.76  DNS  151 Standard query response 0x0003 No such name AAAA www.mit.edu.dormnet.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
1381 11.312952  139.179.210.76  139.179.30.24   DNS   86 Standard query 0x0004 A www.mit.edu.bilkent.edu.tr
1385 11.318534  139.179.30.24   139.179.210.76  DNS  212 Standard query response 0x0004 A www.mit.edu.bilkent.edu.tr A 139.179.10.34 NS ns3.bilkent.edu.tr NS firat.bcc.bilk
1386 11.321589  139.179.210.76  139.179.30.24   DNS   86 Standard query 0x0005 AAAA www.mit.edu.bilkent.edu.tr
1387 11.323375  139.179.30.24   139.179.210.76  DNS  143 Standard query response 0x0005 AAAA www.mit.edu.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
```

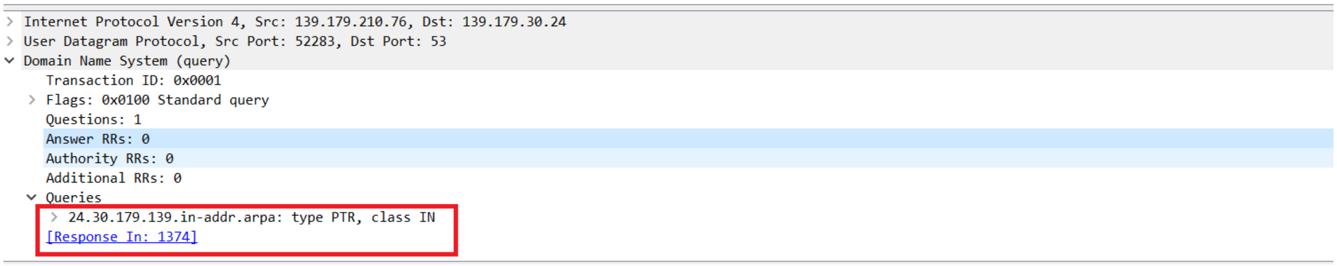
```
> Frame 1370: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{1393197F-9EB6-4475-B12E-DB55DAB69432}, id 0
> Ethernet II, Src: LiteonTe_3c:4c:61 (10:63:c8:3c:4c:61), Dst: SuperMic_8e:b3:73 (0c:c4:7a:8e:b3:73)
> Internet Protocol Version 4, Src: 139.179.210.76, Dst: 139.179.30.24
v User Datagram Protocol, Src Port: 52283, Dst Port: 53
    Source Port: 52283
    Destination Port: 53
```

Q12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
Answer: As it can be seen from the screenshot above, the query was sent to 139.179.30.24. They are the same IP addresses.

Q13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
Answer: Type PTR. There is one question and no answers. Response is in the 1374th packet.

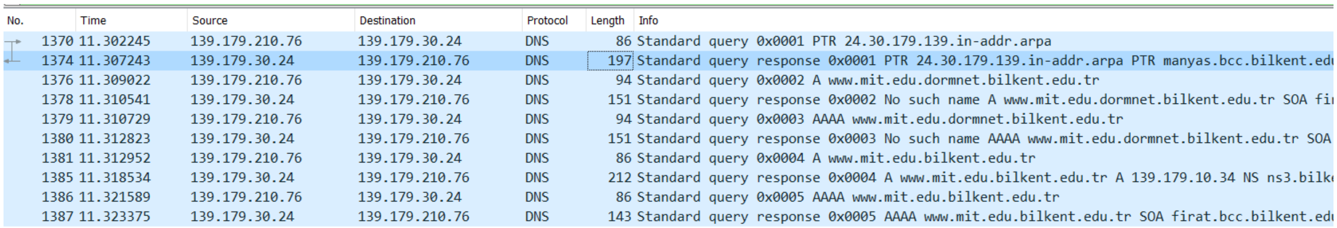


```
1370 11.302245   139.179.210.76   139.179.30.24    DNS    86 Standard query 0x0001 PTR 24.30.179.139.in-addr.arpa
1374 11.307243   139.179.30.24    139.179.210.76   DNS   197 Standard query response 0x0001 PTR 24.30.179.139.in-addr.arpa PTR manyas.bcc.bilkent.edu
1376 11.309022   139.179.210.76   139.179.30.24    DNS    94 Standard query 0x0002 A www.mit.edu.dormnet.bilkent.edu.tr
1378 11.310541   139.179.30.24    139.179.210.76   DNS   151 Standard query response 0x0002 No such name A www.mit.edu.dormnet.bilkent.edu.tr SOA fir
1379 11.310729   139.179.210.76   139.179.30.24    DNS    94 Standard query 0x0003 AAAA www.mit.edu.dormnet.bilkent.edu.tr
1380 11.312823   139.179.30.24    139.179.210.76   DNS   151 Standard query response 0x0003 No such name AAAA www.mit.edu.dormnet.bilkent.edu.tr SOA
1381 11.312952   139.179.210.76   139.179.30.24    DNS    86 Standard query 0x0004 A www.mit.edu.bilkent.edu.tr
1385 11.318534   139.179.30.24    139.179.210.76   DNS   212 Standard query response 0x0004 A www.mit.edu.bilkent.edu.tr A 139.179.10.34 NS ns3.bilke
1386 11.321589   139.179.210.76   139.179.30.24    DNS    86 Standard query 0x0005 AAAA www.mit.edu.bilkent.edu.tr
1387 11.323375   139.179.30.24    139.179.210.76   DNS   143 Standard query response 0x0005 AAAA www.mit.edu.bilkent.edu.tr SOA firat.bcc.bilkent.edu
```

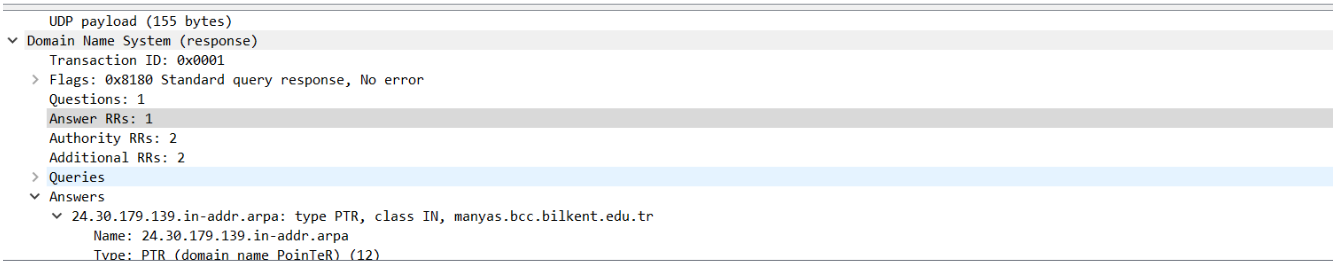


```
> Internet Protocol Version 4, Src: 139.179.210.76, Dst: 139.179.30.24
> User Datagram Protocol, Src Port: 52283, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > 24.30.179.139.in-addr.arpa: type PTR, class IN
    [Response In: 1374]
```

Q14. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
Answer: It contained 1 answers, 2 authoritative responses and 2 additional responses.

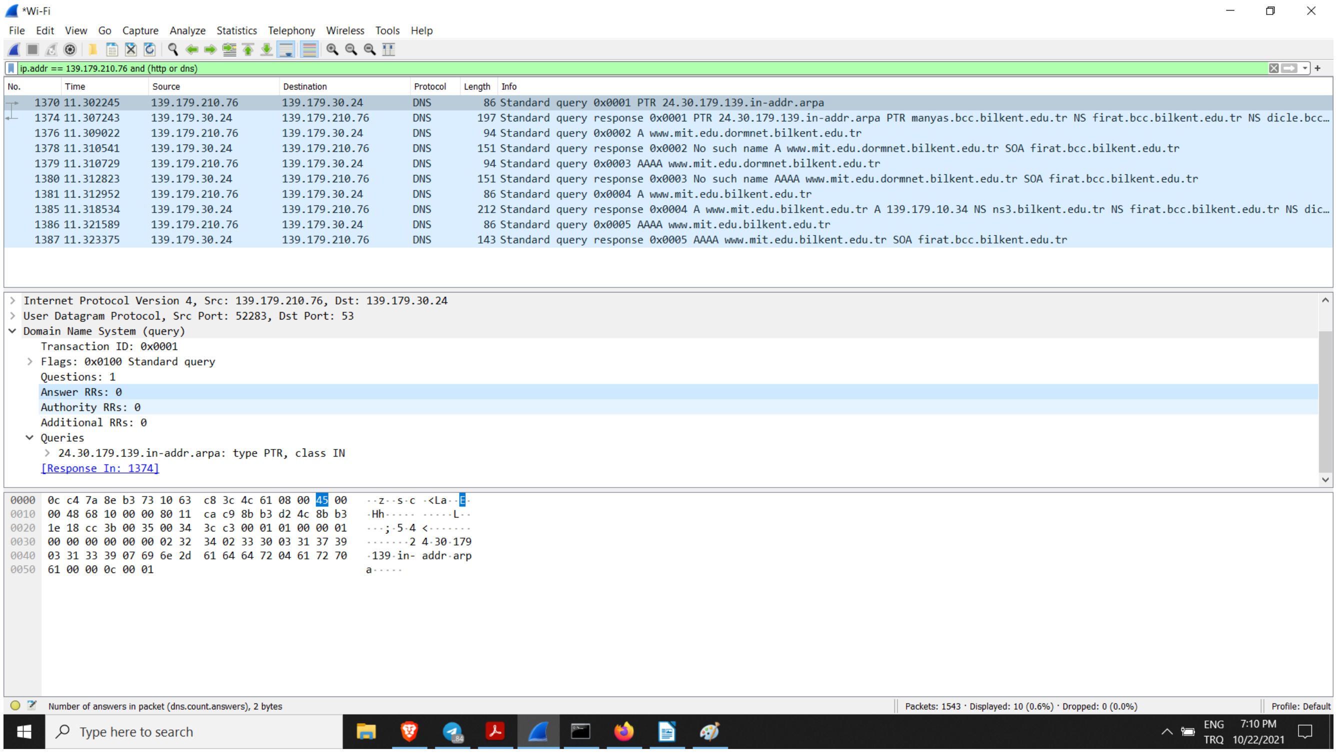


```
No.  Time        Source           Destination      Protocol Length Info
1370 11.302245   139.179.210.76   139.179.30.24    DNS    86 Standard query 0x0001 PTR 24.30.179.139.in-addr.arpa
1374 11.307243   139.179.30.24    139.179.210.76   DNS   197 Standard query response 0x0001 PTR 24.30.179.139.in-addr.arpa PTR manyas.bcc.bilkent.edu
1376 11.309022   139.179.210.76   139.179.30.24    DNS    94 Standard query 0x0002 A www.mit.edu.dormnet.bilkent.edu.tr
1378 11.310541   139.179.30.24    139.179.210.76   DNS   151 Standard query response 0x0002 No such name A www.mit.edu.dormnet.bilkent.edu.tr SOA fi
1379 11.310729   139.179.210.76   139.179.30.24    DNS    94 Standard query 0x0003 AAAA www.mit.edu.dormnet.bilkent.edu.tr
1380 11.312823   139.179.30.24    139.179.210.76   DNS   151 Standard query response 0x0003 No such name AAAA www.mit.edu.dormnet.bilkent.edu.tr SOA
1381 11.312952   139.179.210.76   139.179.30.24    DNS    86 Standard query 0x0004 A www.mit.edu.bilkent.edu.tr
1385 11.318534   139.179.30.24    139.179.210.76   DNS   212 Standard query response 0x0004 A www.mit.edu.bilkent.edu.tr A 139.179.10.34 NS ns3.bilk
1386 11.321589   139.179.210.76   139.179.30.24    DNS    86 Standard query 0x0005 AAAA www.mit.edu.bilkent.edu.tr
1387 11.323375   139.179.30.24    139.179.210.76   DNS   143 Standard query response 0x0005 AAAA www.mit.edu.bilkent.edu.tr SOA firat.bcc.bilkent.edu
```



```
    UDP payload (155 bytes)
v Domain Name System (response)
    Transaction ID: 0x0001
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  > Queries
  v Answers
    v 24.30.179.139.in-addr.arpa: type PTR, class IN, manyas.bcc.bilkent.edu.tr
        Name: 24.30.179.139.in-addr.arpa
        Type: PTR (domain name PointeR) (12)
```

Q15. Provide a screenshot.
Answer:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search
ENG
TRQ
7:10 PM
10/22/2021

```
ip.addr == 139.179.210.76 and (http or dns)

No.  Time       Source          Destination     Protocol Length Info
1370 11.302245  139.179.210.76  139.179.30.24   DNS       86 Standard query 0x0001 PTR 24.30.179.139.in-addr.arpa
1374 11.307243  139.179.30.24   139.179.210.76  DNS      197 Standard query response 0x0001 PTR 24.30.179.139.in-addr.arpa PTR manyas.bcc.bilkent.edu.tr NS firat.bcc.bilkent.edu.tr NS dicle.bcc…
1376 11.309022  139.179.210.76  139.179.30.24   DNS       94 Standard query 0x0002 A www.mit.edu.dormnet.bilkent.edu.tr
1378 11.310541  139.179.30.24   139.179.210.76  DNS      151 Standard query response 0x0002 No such name A www.mit.edu.dormnet.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
1379 11.310729  139.179.210.76  139.179.30.24   DNS       94 Standard query 0x0003 AAAA www.mit.edu.dormnet.bilkent.edu.tr
1380 11.312823  139.179.30.24   139.179.210.76  DNS      151 Standard query response 0x0003 No such name AAAA www.mit.edu.dormnet.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
1381 11.312952  139.179.210.76  139.179.30.24   DNS       86 Standard query 0x0004 A www.mit.edu.bilkent.edu.tr
1385 11.318534  139.179.30.24   139.179.210.76  DNS      212 Standard query response 0x0004 A www.mit.edu.bilkent.edu.tr A 139.179.10.34 NS ns3.bilkent.edu.tr NS firat.bcc.bilkent.edu.tr NS dic…
1386 11.321589  139.179.210.76  139.179.30.24   DNS       86 Standard query 0x0005 AAAA www.mit.edu.bilkent.edu.tr
1387 11.323375  139.179.30.24   139.179.210.76  DNS      143 Standard query response 0x0005 AAAA www.mit.edu.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
```

```
> Internet Protocol Version 4, Src: 139.179.210.76, Dst: 139.179.30.24
> User Datagram Protocol, Src Port: 52283, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > 24.30.179.139.in-addr.arpa: type PTR, class IN
    [Response In: 1374]
```

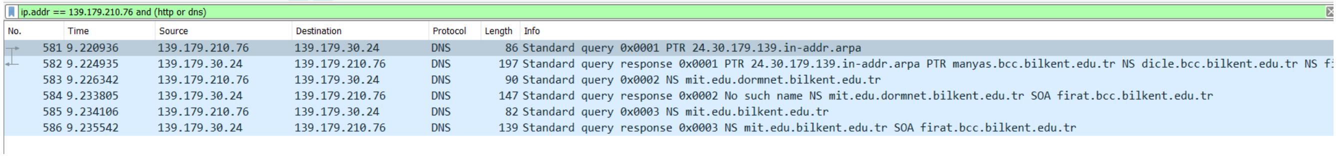
```
0000  0c c4 7a 8e b3 73 10 63  c8 3c 4c 61 08 00 45 00   ··z··s·c ·<La··E·
0010  00 48 68 10 00 00 80 11  ca c9 8b b3 d2 4c 8b b3   ·Hh····· ·····L··
0020  1e 18 cc 3b 00 35 00 34  3c c3 00 01 01 00 00 01   ···;·5·4 <·······
0030  00 00 00 00 00 00 02 32  34 02 33 30 03 31 37 39   ·······2 4·30·179
0040  03 31 33 39 07 69 6e 2d  61 64 64 72 04 61 72 70   ·139·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

Number of answers in packet (dns.count.answers), 2 bytes | Packets: 1543 · Displayed: 10 (0.6%) · Dropped: 0 (0.0%) | Profile: Default

```
nslookup –type=NS mit.edu
```

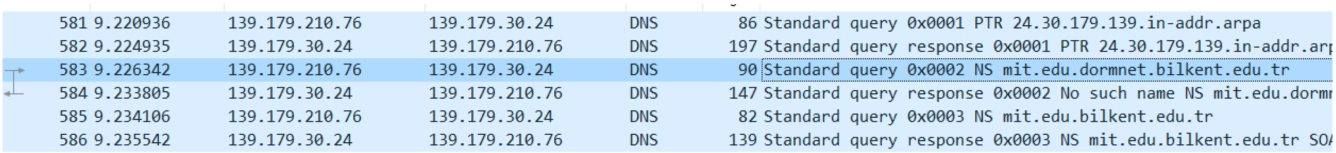
Q16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
Answer:

As it can be seen from the screenshot below, the query was sent to 139.179.30.24. They are the same IP addresses.

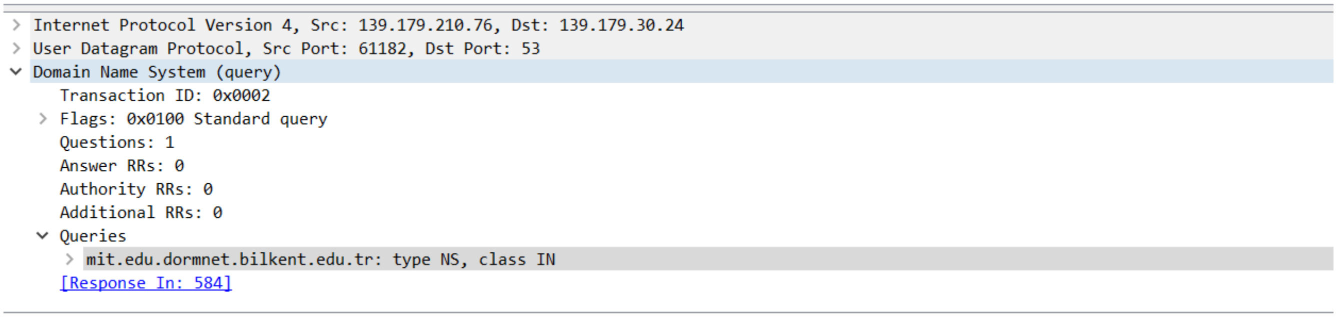


```
ip.addr == 139.179.210.76 and (http or dns)

No. Time      Source          Destination     Protocol Length Info
581 9.220936  139.179.210.76  139.179.30.24   DNS       86 Standard query 0x0001 PTR 24.30.179.139.in-addr.arpa
582 9.224935  139.179.30.24   139.179.210.76  DNS      197 Standard query response 0x0001 PTR 24.30.179.139.in-addr.arpa PTR manyas.bcc.bilkent.edu.tr NS dicle.bcc.bilkent.edu.tr NS fi
583 9.226342  139.179.210.76  139.179.30.24   DNS       90 Standard query 0x0002 NS mit.edu.dormnet.bilkent.edu.tr
584 9.233805  139.179.30.24   139.179.210.76  DNS      147 Standard query response 0x0002 No such name NS mit.edu.dormnet.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
585 9.234106  139.179.210.76  139.179.30.24   DNS       82 Standard query 0x0003 NS mit.edu.bilkent.edu.tr
586 9.235542  139.179.30.24   139.179.210.76  DNS      139 Standard query response 0x0003 NS mit.edu.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
```

Q17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
Answer: The type is NS. There is one question but no answers.



```
581 9.220936   139.179.210.76   139.179.30.24    DNS    86 Standard query 0x0001 PTR 24.30.179.139.in-addr.arpa
582 9.224935   139.179.30.24    139.179.210.76   DNS   197 Standard query response 0x0001 PTR 24.30.179.139.in-addr.arp
583 9.226342   139.179.210.76   139.179.30.24    DNS    90 Standard query 0x0002 NS mit.edu.dormnet.bilkent.edu.tr
584 9.233805   139.179.30.24    139.179.210.76   DNS   147 Standard query response 0x0002 No such name NS mit.edu.dormn
585 9.234106   139.179.210.76   139.179.30.24    DNS    82 Standard query 0x0003 NS mit.edu.bilkent.edu.tr
586 9.235542   139.179.30.24    139.179.210.76   DNS   139 Standard query response 0x0003 NS mit.edu.bilkent.edu.tr SOA
```

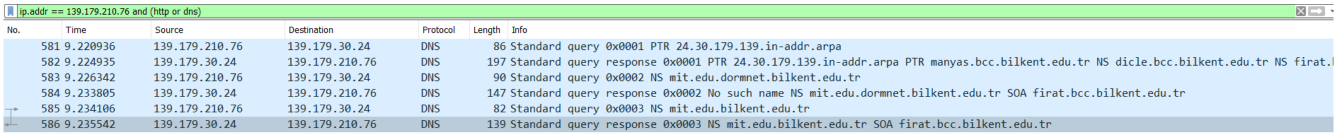


```
> Internet Protocol Version 4, Src: 139.179.210.76, Dst: 139.179.30.24
> User Datagram Protocol, Src Port: 61182, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > mit.edu.dormnet.bilkent.edu.tr: type NS, class IN
    [Response In: 584]
```

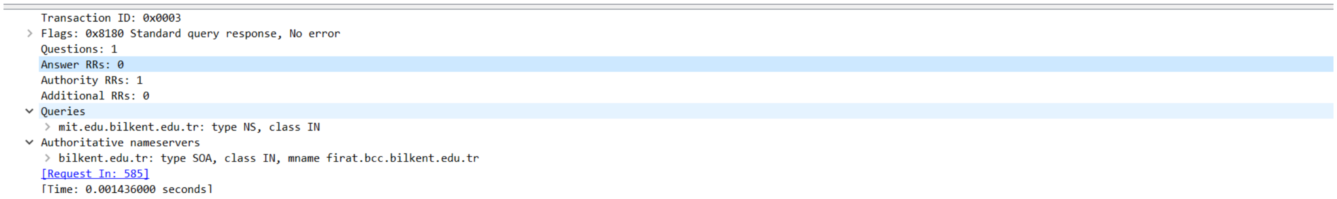
Q18. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?

Answer:

It provided one authoritative NS which is www.firat.bcc.bilkent.edu.tr. It did not provide other answers though.



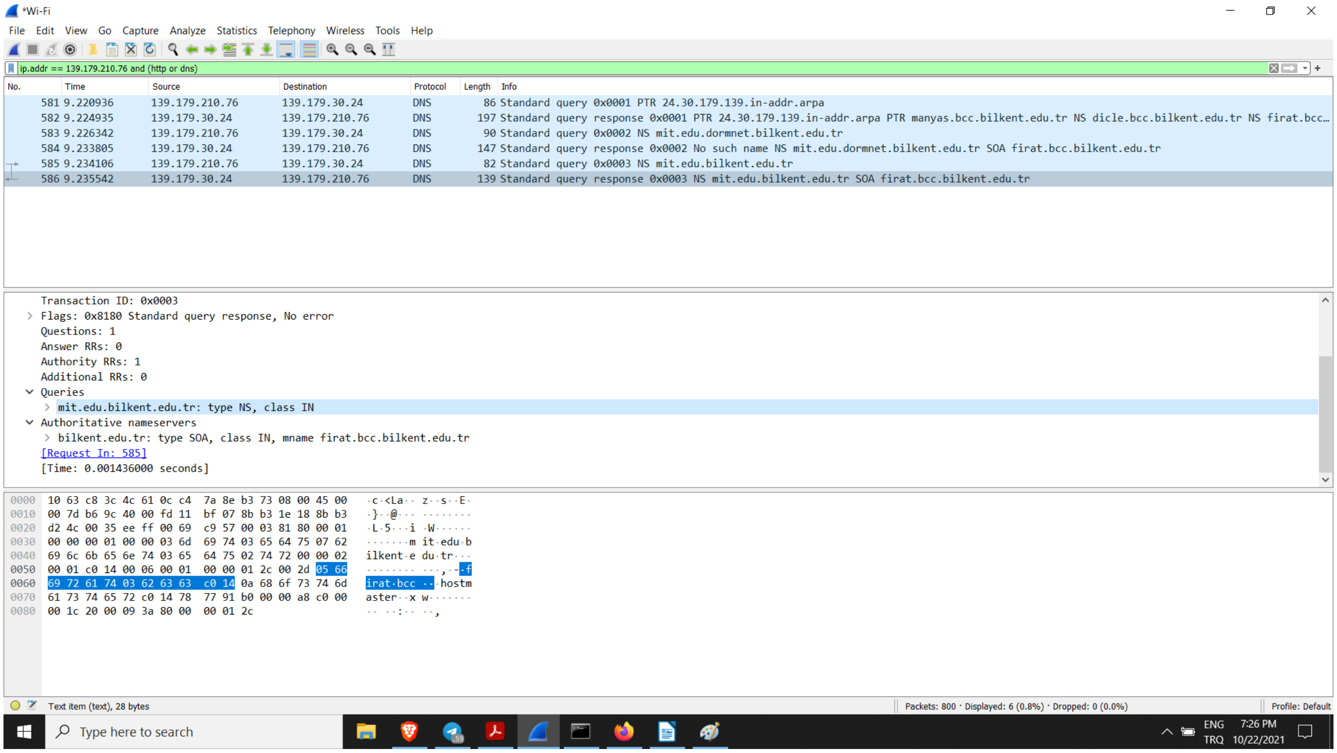
```
ip.addr == 139.179.210.76 and (http or dns)

No.  Time        Source           Destination      Protocol  Length Info
581 9.220936   139.179.210.76   139.179.30.24    DNS    86 Standard query 0x0001 PTR 24.30.179.139.in-addr.arpa
582 9.224935   139.179.30.24    139.179.210.76   DNS   197 Standard query response 0x0001 PTR 24.30.179.139.in-addr.arpa PTR manyas.bcc.bilkent.edu.tr NS dicle.bcc.bilkent.edu.tr NS firat.
583 9.226342   139.179.210.76   139.179.30.24    DNS    90 Standard query 0x0002 NS mit.edu.dormnet.bilkent.edu.tr
584 9.233805   139.179.30.24    139.179.210.76   DNS   147 Standard query response 0x0002 No such name NS mit.edu.dormnet.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
585 9.234106   139.179.210.76   139.179.30.24    DNS    82 Standard query 0x0003 NS mit.edu.bilkent.edu.tr
586 9.235542   139.179.30.24    139.179.210.76   DNS   139 Standard query response 0x0003 NS mit.edu.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
```



```
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  v Queries
    > mit.edu.bilkent.edu.tr: type NS, class IN
  v Authoritative nameservers
    > bilkent.edu.tr: type SOA, class IN, mname firat.bcc.bilkent.edu.tr
    [Request In: 585]
    [Time: 0.001436000 seconds]
```

Q19. Provide a screenshot.

Answer:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search
ENG
TRQ

```
ip.addr == 139.179.210.76 and (http or dns)
```

```
No.   Time      Source          Destination     Protocol Length Info
  581 9.220936  139.179.210.76  139.179.30.24   DNS       86 Standard query 0x0001 PTR 24.30.179.139.in-addr.arpa
  582 9.224935  139.179.30.24   139.179.210.76  DNS      197 Standard query response 0x0001 PTR 24.30.179.139.in-addr.arpa PTR manyas.bcc.bilkent.edu.tr NS dicle.bcc.bilkent.edu.tr NS firat.bcc…
  583 9.226342  139.179.210.76  139.179.30.24   DNS       90 Standard query 0x0002 NS mit.edu.dormnet.bilkent.edu.tr
  584 9.233805  139.179.30.24   139.179.210.76  DNS      147 Standard query response 0x0002 No such name NS mit.edu.dormnet.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
  585 9.234106  139.179.210.76  139.179.30.24   DNS       82 Standard query 0x0003 NS mit.edu.bilkent.edu.tr
  586 9.235542  139.179.30.24   139.179.210.76  DNS      139 Standard query response 0x0003 NS mit.edu.bilkent.edu.tr SOA firat.bcc.bilkent.edu.tr
```

```
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  v Queries
    > mit.edu.bilkent.edu.tr: type NS, class IN
  v Authoritative nameservers
    > bilkent.edu.tr: type SOA, class IN, mname firat.bcc.bilkent.edu.tr
    [Request In: 585]
    [Time: 0.001436000 seconds]
```

```
0000  10 63 c8 3c 4c 61 0c c4  7a 8e b3 73 08 00 45 00   ·c·<La·· z··s··E·
0010  00 7d b6 9c 40 00 fd 11  bf 07 8b b3 1e 18 8b b3   ·}··@··· ········
0020  d2 4c 00 35 ee ff 00 69  c9 57 00 03 81 80 00 01   ·L·5···i ·W······
0030  00 00 00 01 00 00 03 6d  69 74 03 65 64 75 07 62   ·······m it·edu·b
0040  69 6c 6b 65 6e 74 03 65  64 75 02 74 72 00 00 02   ilkent·e du·tr···
0050  00 01 c0 14 00 06 00 01  00 00 01 2c 00 2d 05 66   ········ ···,·-·f
0060  69 72 61 74 03 62 63 63  c0 14 0a 68 6f 73 74 6d   irat·bcc ···hostm
0070  61 73 74 65 72 c0 14 78  77 91 b0 00 00 a8 c0 00   aster··x w·······
0080  00 1c 20 00 09 3a 80 00  00 01 2c                  ·· ··:·· ··,
```

Text item (text), 28 bytes

Packets: 800 · Displayed: 6 (0.8%) · Dropped: 0 (0.0%)

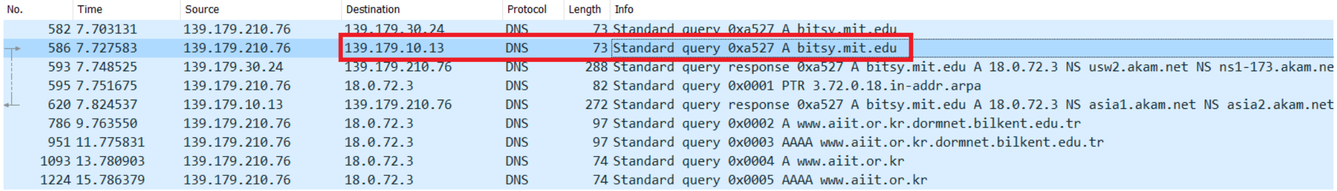
Profile: Default

7:26 PM
10/22/2021

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

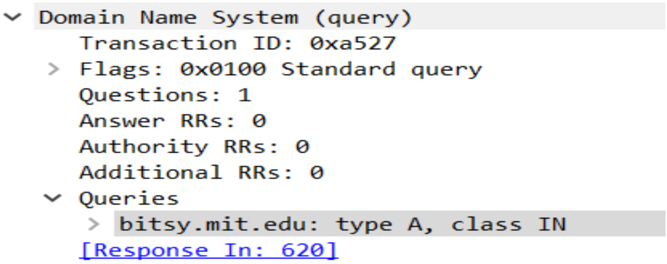
Q20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
Answer:

No this is not the IP address of my default local DNS server. I think this is the address for MIT's DNS response sender.



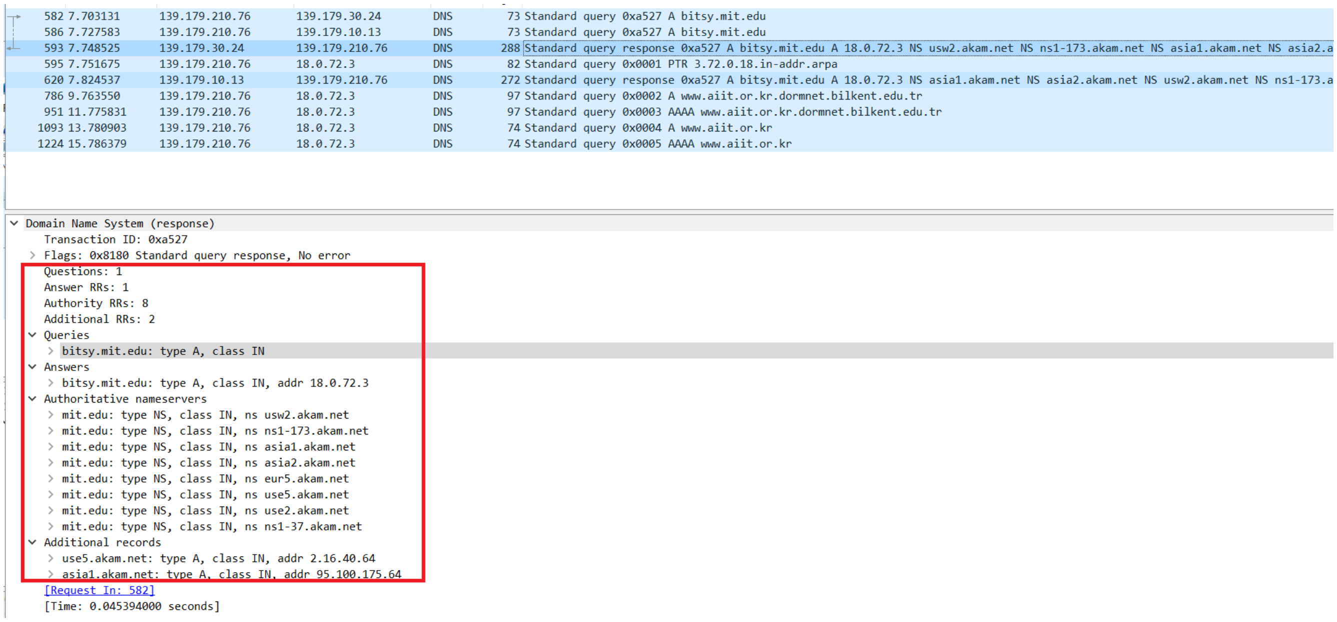
```
No.   Time       Source          Destination     Protocol Length Info
  582 7.703131   139.179.210.76  139.179.30.24   DNS       73 Standard query 0xa527 A bitsy.mit.edu
  586 7.727583   139.179.210.76  139.179.10.13   DNS       73 Standard query 0xa527 A bitsy.mit.edu
  593 7.748525   139.179.30.24   139.179.210.76  DNS      288 Standard query response 0xa527 A bitsy.mit.edu A 18.0.72.3 NS usw2.akam.net NS ns1-173.akam.ne
  595 7.751675   139.179.210.76  18.0.72.3       DNS       82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
  620 7.824537   139.179.10.13   139.179.210.76  DNS      272 Standard query response 0xa527 A bitsy.mit.edu A 18.0.72.3 NS asia1.akam.net NS asia2.akam.net
  786 9.763550   139.179.210.76  18.0.72.3       DNS       97 Standard query 0x0002 A www.aiit.or.kr.dormnet.bilkent.edu.tr
  951 11.775831  139.179.210.76  18.0.72.3       DNS       97 Standard query 0x0003 AAAA www.aiit.or.kr.dormnet.bilkent.edu.tr
 1093 13.780903  139.179.210.76  18.0.72.3       DNS       74 Standard query 0x0004 A www.aiit.or.kr
 1224 15.786379  139.179.210.76  18.0.72.3       DNS       74 Standard query 0x0005 AAAA www.aiit.or.kr
```

Q21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
Answer: Type A. One question but no answers.



```
v Domain Name System (query)
    Transaction ID: 0xa527
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > bitsy.mit.edu: type A, class IN
    [Response In: 620]
```

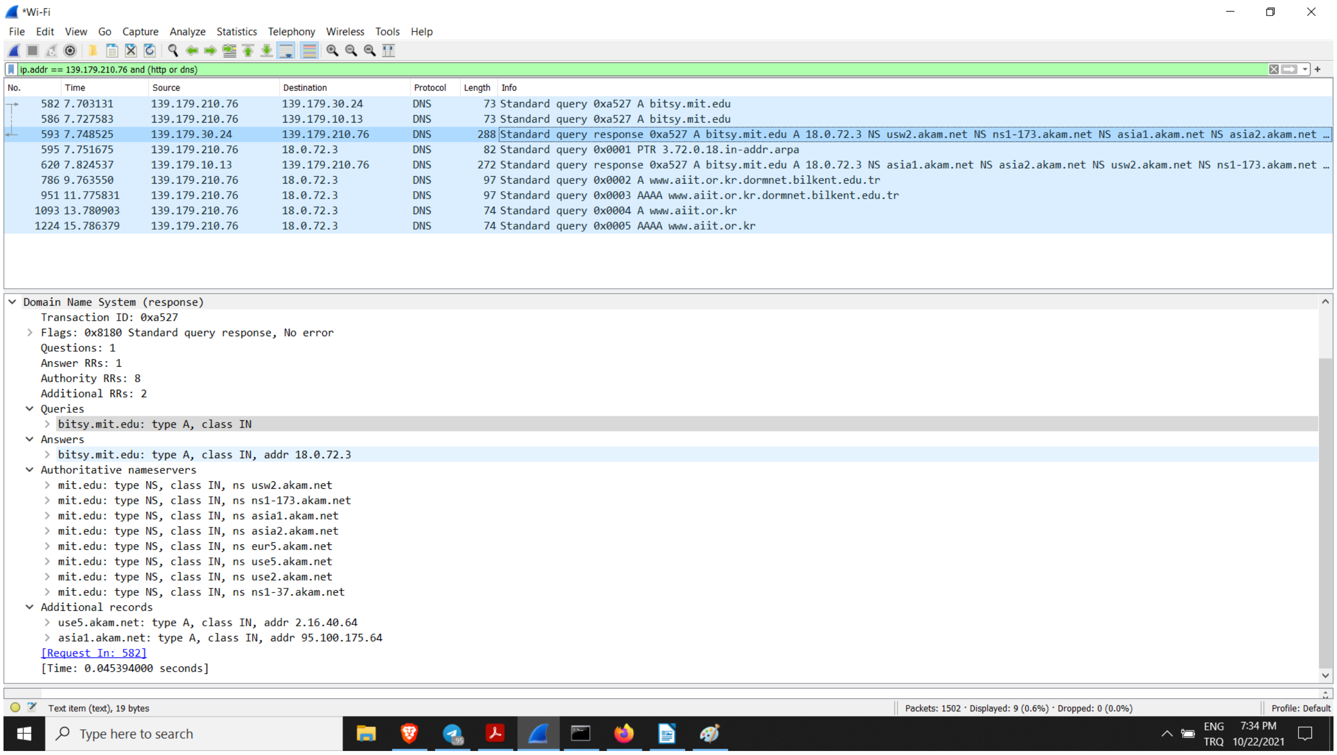
Q22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
Answer: One answer RRs, 8 authority RRs, 2 additional records.



```
  582 7.703131    139.179.210.76    139.179.30.24     DNS     73 Standard query 0xa527 A bitsy.mit.edu
  586 7.727583    139.179.210.76    139.179.10.13     DNS     73 Standard query 0xa527 A bitsy.mit.edu
  593 7.748525    139.179.30.24     139.179.210.76    DNS    288 Standard query response 0xa527 A bitsy.mit.edu A 18.0.72.3 NS usw2.akam.net NS ns1-173.akam.net NS asia1.akam.net NS asia2.a
  595 7.751675    139.179.210.76    18.0.72.3         DNS     82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
  620 7.824537    139.179.10.13     139.179.210.76    DNS    272 Standard query response 0xa527 A bitsy.mit.edu A 18.0.72.3 NS asia1.akam.net NS asia2.akam.net NS usw2.akam.net NS ns1-173.a
  786 9.763550    139.179.210.76    18.0.72.3         DNS     97 Standard query 0x0002 A www.aiit.or.kr.dormnet.bilkent.edu.tr
  951 11.775831   139.179.210.76    18.0.72.3         DNS     97 Standard query 0x0003 AAAA www.aiit.or.kr.dormnet.bilkent.edu.tr
 1093 13.780903   139.179.210.76    18.0.72.3         DNS     74 Standard query 0x0004 A www.aiit.or.kr
 1224 15.786379   139.179.210.76    18.0.72.3         DNS     74 Standard query 0x0005 AAAA www.aiit.or.kr
```

```
v Domain Name System (response)
    Transaction ID: 0xa527
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 8
    Additional RRs: 2
  v Queries
    > bitsy.mit.edu: type A, class IN
  v Answers
    > bitsy.mit.edu: type A, class IN, addr 18.0.72.3
  v Authoritative nameservers
    > mit.edu: type NS, class IN, ns usw2.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    > mit.edu: type NS, class IN, ns asia2.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
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
  v Additional records
    > use5.akam.net: type A, class IN, addr 2.16.40.64
    > asia1.akam.net: type A, class IN, addr 95.100.175.64
    [Request In: 582]
    [Time: 0.045394000 seconds]
```

Q23. Provide a screenshot.
Answer:



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search
ENG
TRQ
7:34 PM
10/22/2021

```
ip.addr == 139.179.210.76 and (http or dns)
```

```
No.   Time        Source            Destination       Protocol Length Info
  582 7.703131    139.179.210.76    139.179.30.24     DNS     73 Standard query 0xa527 A bitsy.mit.edu
  586 7.727583    139.179.210.76    139.179.10.13     DNS     73 Standard query 0xa527 A bitsy.mit.edu
  593 7.748525    139.179.30.24     139.179.210.76    DNS    288 Standard query response 0xa527 A bitsy.mit.edu A 18.0.72.3 NS usw2.akam.net NS ns1-173.akam.net NS asia1.akam.net NS asia2.akam.net …
  595 7.751675    139.179.210.76    18.0.72.3         DNS     82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
  620 7.824537    139.179.10.13     139.179.210.76    DNS    272 Standard query response 0xa527 A bitsy.mit.edu A 18.0.72.3 NS asia1.akam.net NS asia2.akam.net NS usw2.akam.net NS ns1-173.akam.net …
  786 9.763550    139.179.210.76    18.0.72.3         DNS     97 Standard query 0x0002 A www.aiit.or.kr.dormnet.bilkent.edu.tr
  951 11.775831   139.179.210.76    18.0.72.3         DNS     97 Standard query 0x0003 AAAA www.aiit.or.kr.dormnet.bilkent.edu.tr
 1093 13.780903   139.179.210.76    18.0.72.3         DNS     74 Standard query 0x0004 A www.aiit.or.kr
 1224 15.786379   139.179.210.76    18.0.72.3         DNS     74 Standard query 0x0005 AAAA www.aiit.or.kr
```

```
v Domain Name System (response)
    Transaction ID: 0xa527
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 8
    Additional RRs: 2
  v Queries
    > bitsy.mit.edu: type A, class IN
  v Answers
    > bitsy.mit.edu: type A, class IN, addr 18.0.72.3
  v Authoritative nameservers
    > mit.edu: type NS, class IN, ns usw2.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    > mit.edu: type NS, class IN, ns asia2.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
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
  v Additional records
    > use5.akam.net: type A, class IN, addr 2.16.40.64
    > asia1.akam.net: type A, class IN, addr 95.100.175.64
    [Request In: 582]
    [Time: 0.045394000 seconds]
```

```
Text item (text), 19 bytes        Packets: 1502 · Displayed: 9 (0.6%) · Dropped: 0 (0.0%)        Profile: Default
```