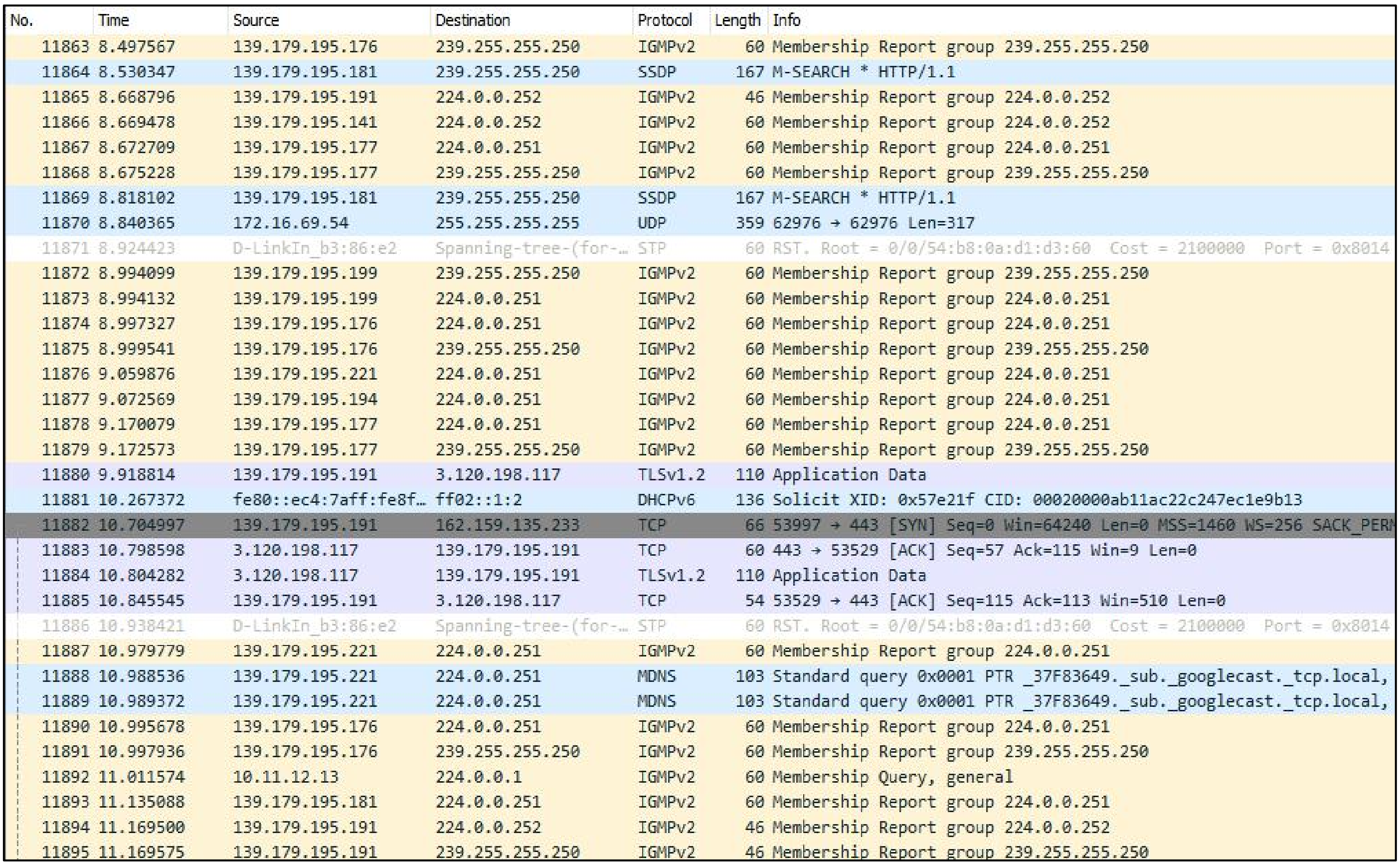
CS 421 COMPUTER ASSIGNMENT

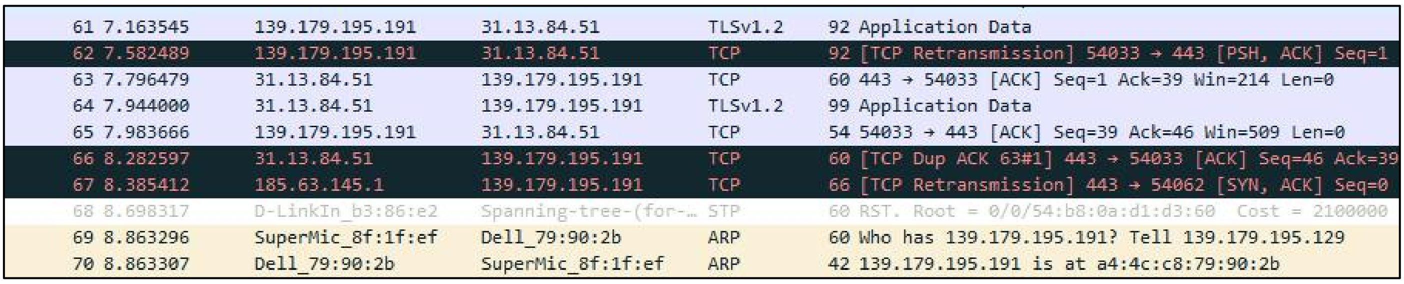
Name: Fatih Sevban Uyanik
Id: 21602486
Department: CS
Section: 1

Taking Wireshark for a Test Run

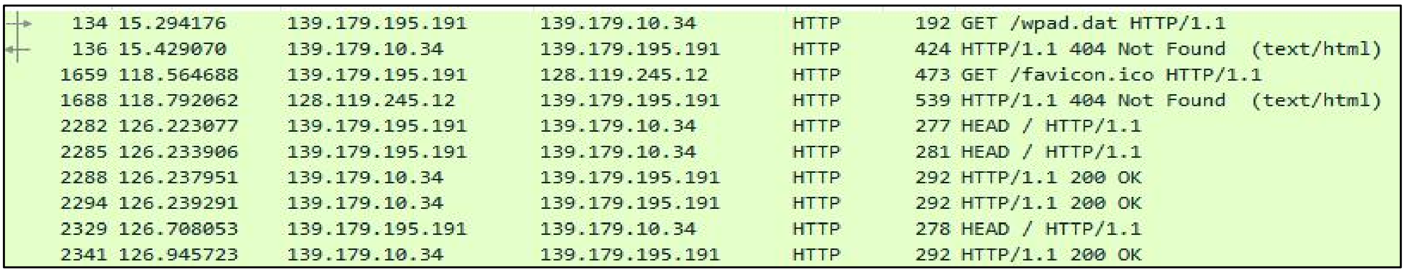
Question1



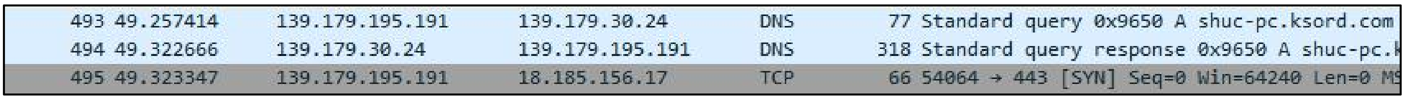
No.	Time	Source	Destination	Protocol	Length	Info
11863	8.497567	139.179.195.176	239.255.255.250	IGMPv2	60	Membership Report group 239.255.255.250
11864	8.530347	139.179.195.181	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
11865	8.668796	139.179.195.191	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
11866	8.669478	139.179.195.141	224.0.0.252	IGMPv2	60	Membership Report group 224.0.0.252
11867	8.672709	139.179.195.177	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
11868	8.675228	139.179.195.177	239.255.255.250	IGMPv2	60	Membership Report group 239.255.255.250
11869	8.818102	139.179.195.181	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
11870	8.840365	172.16.69.54	255.255.255.255	UDP	359	62976 → 62976 Len=317
11871	8.924423	D-LinkIn_b3:86:e2	Spanning-tree-(for-…	STP	60	RST. Root = 0/0/54:b8:0a:d1:d3:60 Cost = 2100000 Port = 0x8014
11872	8.994099	139.179.195.199	239.255.255.250	IGMPv2	60	Membership Report group 239.255.255.250
11873	8.994132	139.179.195.199	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
11874	8.997327	139.179.195.176	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
11875	8.999541	139.179.195.176	239.255.255.250	IGMPv2	60	Membership Report group 239.255.255.250
11876	9.059876	139.179.195.221	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
11877	9.072569	139.179.195.194	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
11878	9.170079	139.179.195.177	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
11879	9.172573	139.179.195.177	239.255.255.250	IGMPv2	60	Membership Report group 239.255.255.250
11880	9.918814	139.179.195.191	3.120.198.117	TLSv1.2	110	Application Data
11881	10.267372	fe80::ec4:7aff:fe8f…	ff02::1:2	DHCPv6	136	Solicit XID: 0x57e21f CID: 00020000ab11ac22c247ec1e9b13
11882	10.704997	139.179.195.191	162.159.135.233	TCP	66	53997 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11883	10.798598	3.120.198.117	139.179.195.191	TCP	60	443 → 53529 [ACK] Seq=57 Ack=115 Win=9 Len=0
11884	10.804282	3.120.198.117	139.179.195.191	TLSv1.2	110	Application Data
11885	10.845545	139.179.195.191	3.120.198.117	TCP	54	53529 → 443 [ACK] Seq=115 Ack=113 Win=510 Len=0
11886	10.938421	D-LinkIn_b3:86:e2	Spanning-tree-(for-…	STP	60	RST. Root = 0/0/54:b8:0a:d1:d3:60 Cost = 2100000 Port = 0x8014
11887	10.979779	139.179.195.221	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
11888	10.988536	139.179.195.221	224.0.0.251	MDNS	103	Standard query 0x0001 PTR _37F83649._sub._googlecast._tcp.local,
11889	10.989372	139.179.195.221	224.0.0.251	MDNS	103	Standard query 0x0001 PTR _37F83649._sub._googlecast._tcp.local,
11890	10.995678	139.179.195.176	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
11891	10.997936	139.179.195.176	239.255.255.250	IGMPv2	60	Membership Report group 239.255.255.250
11892	11.011574	10.11.12.13	224.0.0.1	IGMPv2	60	Membership Query, general
11893	11.135088	139.179.195.181	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
11894	11.169500	139.179.195.191	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
11895	11.169575	139.179.195.191	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250



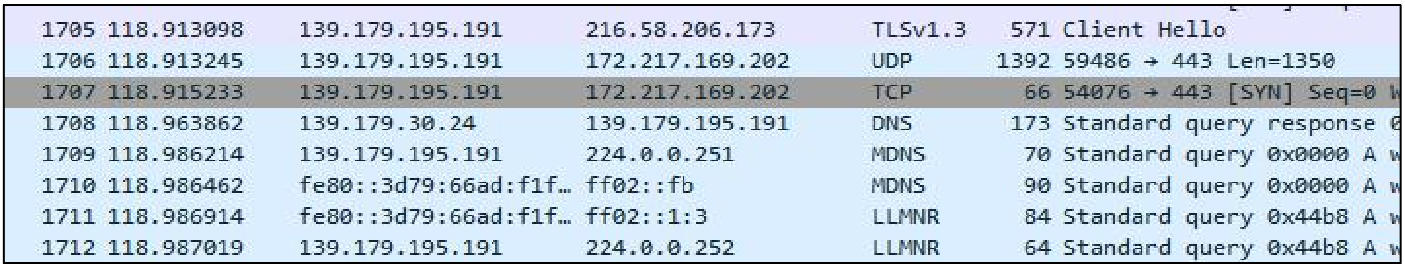
61	7.163545	139.179.195.191	31.13.84.51	TLSv1.2	92	Application Data
62	7.582489	139.179.195.191	31.13.84.51	TCP	92	[TCP Retransmission] 54033 → 443 [PSH, ACK] Seq=1
63	7.796479	31.13.84.51	139.179.195.191	TCP	60	443 → 54033 [ACK] Seq=1 Ack=39 Win=214 Len=0
64	7.944000	31.13.84.51	139.179.195.191	TLSv1.2	99	Application Data
65	7.983666	139.179.195.191	31.13.84.51	TCP	54	54033 → 443 [ACK] Seq=39 Ack=46 Win=509 Len=0
66	8.282597	31.13.84.51	139.179.195.191	TCP	60	[TCP Dup ACK 63#1] 443 → 54033 [ACK] Seq=46 Ack=39
67	8.385412	185.63.145.1	139.179.195.191	TCP	66	[TCP Retransmission] 443 → 54062 [SYN, ACK] Seq=0
68	8.698317	D-LinkIn_b3:86:e2	Spanning-tree-(for-…	STP	60	RST. Root = 0/0/54:b8:0a:d1:d3:60 Cost = 2100000
69	8.863296	SuperMic_8f:1f:ef	Dell_79:90:2b	ARP	60	Who has 139.179.195.191? Tell 139.179.195.129
70	8.863307	Dell_79:90:2b	SuperMic_8f:1f:ef	ARP	42	139.179.195.191 is at a4:4c:c8:79:90:2b



134	15.294176	139.179.195.191	139.179.10.34	HTTP	192	GET /wpad.dat HTTP/1.1
136	15.429070	139.179.10.34	139.179.195.191	HTTP	424	HTTP/1.1 404 Not Found (text/html)
1659	118.564688	139.179.195.191	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
1688	118.792062	128.119.245.12	139.179.195.191	HTTP	539	HTTP/1.1 404 Not Found (text/html)
2282	126.223077	139.179.195.191	139.179.10.34	HTTP	277	HEAD / HTTP/1.1
2285	126.233906	139.179.195.191	139.179.10.34	HTTP	281	HEAD / HTTP/1.1
2288	126.237951	139.179.10.34	139.179.195.191	HTTP	292	HTTP/1.1 200 OK
2294	126.239291	139.179.10.34	139.179.195.191	HTTP	292	HTTP/1.1 200 OK
2329	126.708053	139.179.195.191	139.179.10.34	HTTP	278	HEAD / HTTP/1.1
2341	126.945723	139.179.10.34	139.179.195.191	HTTP	292	HTTP/1.1 200 OK



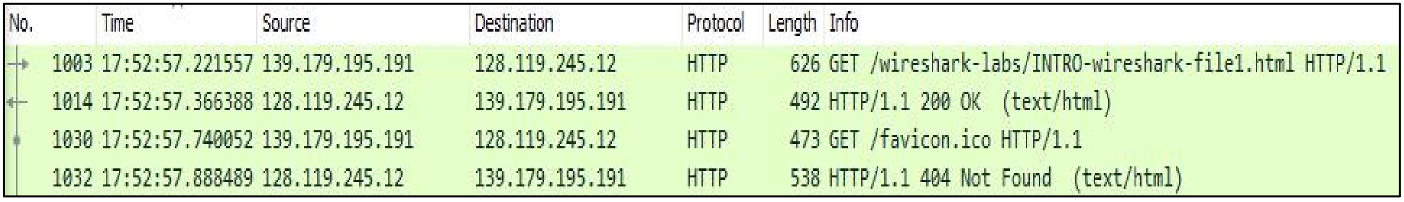
493	49.257414	139.179.195.191	139.179.30.24	DNS	77	Standard query 0x9650 A shuc-pc.ksord.com
494	49.322666	139.179.30.24	139.179.195.191	DNS	318	Standard query response 0x9650 A shuc-pc.k
495	49.323347	139.179.195.191	18.185.156.17	TCP	66	54064 → 443 [SYN] Seq=0 Win=64240 Len=0 MS



1705	118.913098	139.179.195.191	216.58.206.173	TLSv1.3	571	Client Hello
1706	118.913245	139.179.195.191	172.217.169.202	UDP	1392	59486 → 443 Len=1350
1707	118.915233	139.179.195.191	172.217.169.202	TCP	66	54076 → 443 [SYN] Seq=0 W
1708	118.963862	139.179.30.24	139.179.195.191	DNS	173	Standard query response 0
1709	118.986214	139.179.195.191	224.0.0.251	MDNS	70	Standard query 0x0000 A w
1710	118.986462	fe80::3d79:66ad:f1f…	ff02::fb	MDNS	90	Standard query 0x0000 A w
1711	118.986914	fe80::3d79:66ad:f1f…	ff02::1:3	LLMNR	84	Standard query 0x44b8 A w
1712	118.987019	139.179.195.191	224.0.0.252	LLMNR	64	Standard query 0x44b8 A w

10 different protocols --> SSDP, IGMPv2, DHCPv6, MDNS, TLSv1.2, TCP, UDP, ARP, STP, HTTP, DNS, LLMNR, TLSv1.3

Question2



```
No.    Time            Source           Destination      Protocol  Length Info
  1003 17:52:57.221557 139.179.195.191  128.119.245.12   HTTP      626 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  1014 17:52:57.366388 128.119.245.12   139.179.195.191  HTTP      492 HTTP/1.1 200 OK  (text/html)
  1030 17:52:57.740052 139.179.195.191  128.119.245.12   HTTP      473 GET /favicon.ico HTTP/1.1
  1032 17:52:57.888489 128.119.245.12   139.179.195.191  HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

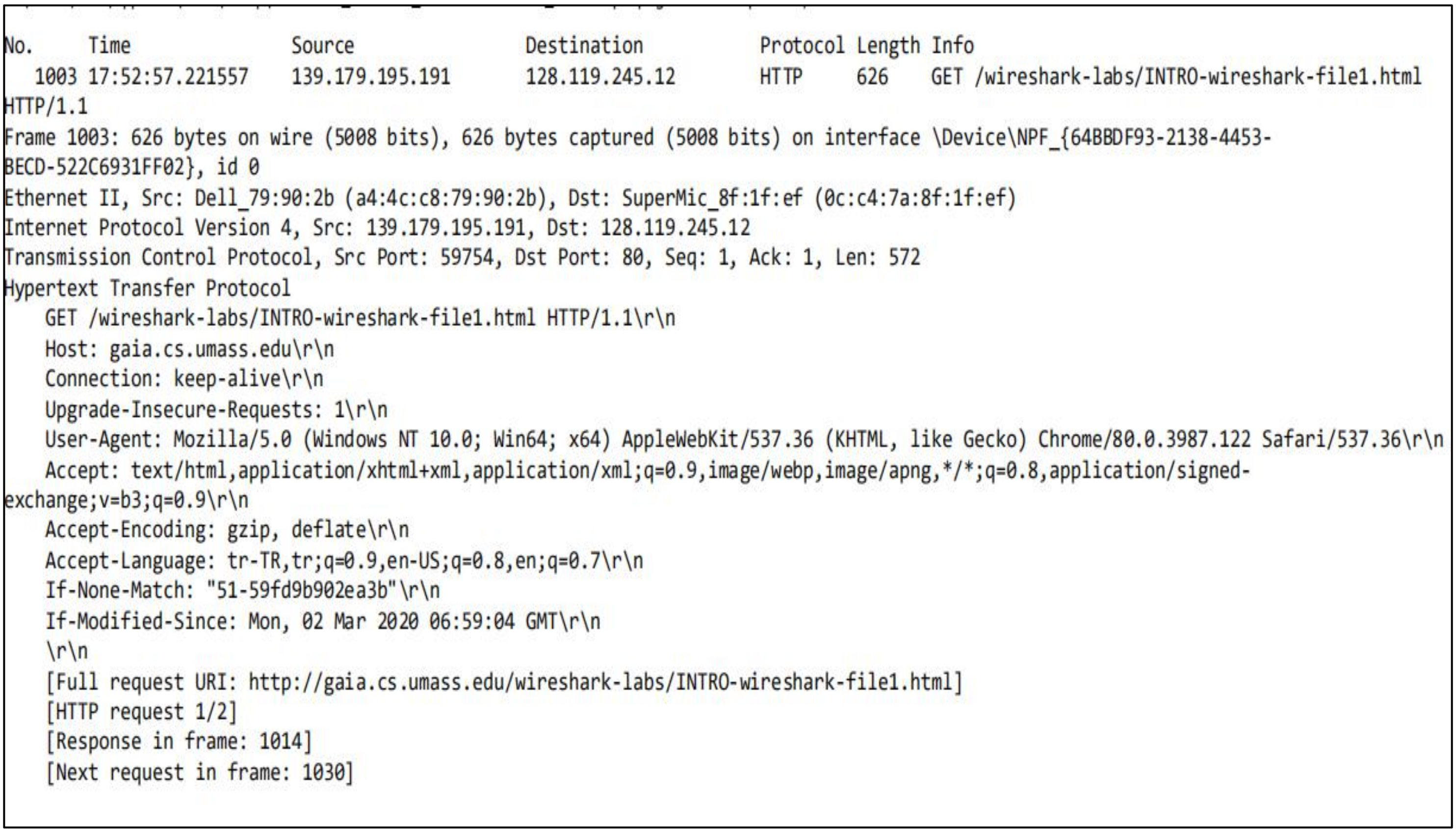
17:52:57.221557 --> HTTP GET message send
17:52:57.366388 --> HTTP OK reply received
Duration Time = (HTTP GET) - (HTTP OK) = 57.366388 - 57.221557 = 0.144831 seconds

Question3

Internet address of gaia.cs.umass.edu = **128.119.245.12**
Internet address of my local computer = **139.179.195.191**

Question4

First print



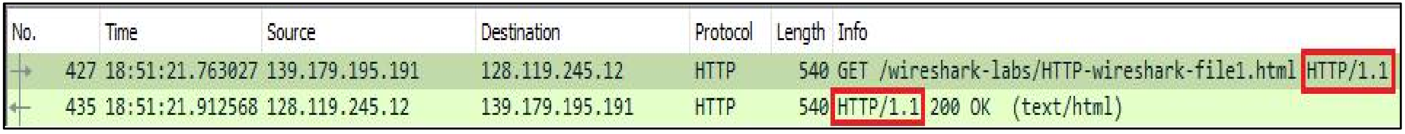
```
No.     Time               Source                Destination           Protocol Length Info
   1003 17:52:57.221557    139.179.195.191       128.119.245.12        HTTP     626    GET /wireshark-labs/INTRO-wireshark-file1.html
HTTP/1.1
Frame 1003: 626 bytes on wire (5008 bits), 626 bytes captured (5008 bits) on interface \Device\NPF_{64BBDF93-2138-4453-
BECD-522C6931FF02}, id 0
Ethernet II, Src: Dell_79:90:2b (a4:4c:c8:79:90:2b), Dst: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef)
Internet Protocol Version 4, Src: 139.179.195.191, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59754, Dst Port: 80, Seq: 1, Ack: 1, Len: 572
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/80.0.3987.122 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    If-None-Match: "51-59fd9b902ea3b"\r\n
    If-Modified-Since: Mon, 02 Mar 2020 06:59:04 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: 1014]
    [Next request in frame: 1030]
```

Second Print

```
No.     Time               Source              Destination          Protocol Length Info
   1014 17:52:57.366388    128.119.245.12      139.179.195.191      HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 1014: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{64BBDF93-2138-4453-
BECD-522C6931FF02}, id 0
Ethernet II, Src: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef), Dst: Dell_79:90:2b (a4:4c:c8:79:90:2b)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.195.191
Transmission Control Protocol, Src Port: 80, Dst Port: 59754, Seq: 1, Ack: 573, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 03 Mar 2020 14:52:57 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 03 Mar 2020 06:59:03 GMT\r\n
    ETag: "51-59fedd6cb932e"\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: 0.144831000 seconds]
    [Request in frame: 1003]
    [Next request in frame: 1030]
    [Next response in frame: 1032]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

The Basic HTTP GET/response interaction

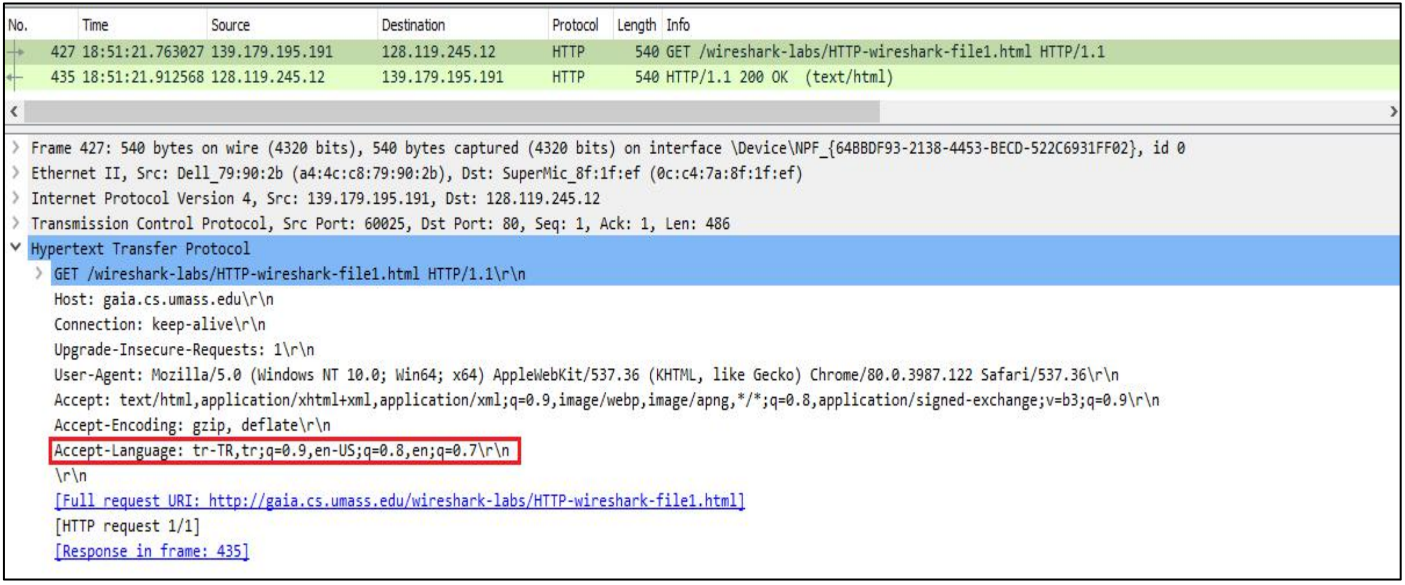
Question1



```
No.  Time               Source           Destination      Protocol Length Info
 427 18:51:21.763027 139.179.195.191  128.119.245.12   HTTP     540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 435 18:51:21.912568 128.119.245.12   139.179.195.191  HTTP     540 HTTP/1.1 200 OK  (text/html)
```

Browser is running HTTP 1.1 and also server is running HTTP 1.1

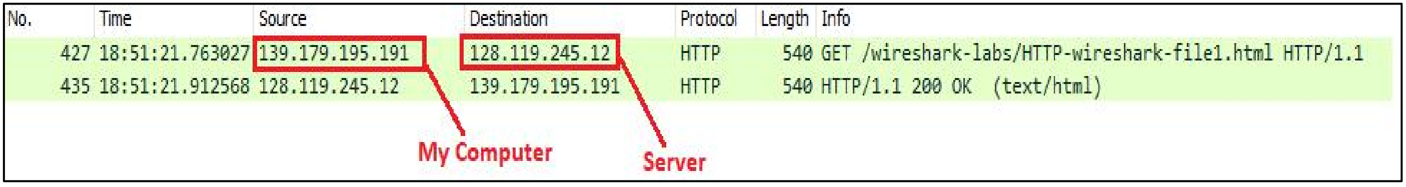
Question2



```
No.  Time               Source           Destination      Protocol Length Info
 427 18:51:21.763027 139.179.195.191  128.119.245.12   HTTP     540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 435 18:51:21.912568 128.119.245.12   139.179.195.191  HTTP     540 HTTP/1.1 200 OK  (text/html)

> Frame 427: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{64BBDF93-2138-4453-BECD-522C6931FF02}, id 0
> Ethernet II, Src: Dell_79:90:2b (a4:4c:c8:79:90:2b), Dst: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef)
> Internet Protocol Version 4, Src: 139.179.195.191, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60025, Dst Port: 80, Seq: 1, Ack: 1, Len: 486
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 435]
```

My browser indicates that it can accept both turkish and english which is indicated by the Accept-Language section.

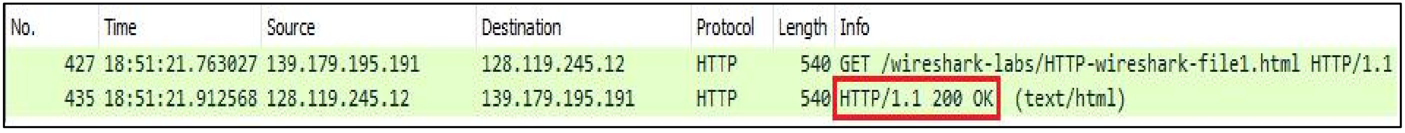
Question3



```
No.   Time             Source           Destination      Protocol  Length  Info
  427 18:51:21.763027 139.179.195.191  128.119.245.12   HTTP        540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  435 18:51:21.912568 128.119.245.12   139.179.195.191  HTTP        540 HTTP/1.1 200 OK  (text/html)
```

IP address of my computer --> 139.179.195.191
IP address of gaia.cs.umass.edu server --> 128.119.245.12

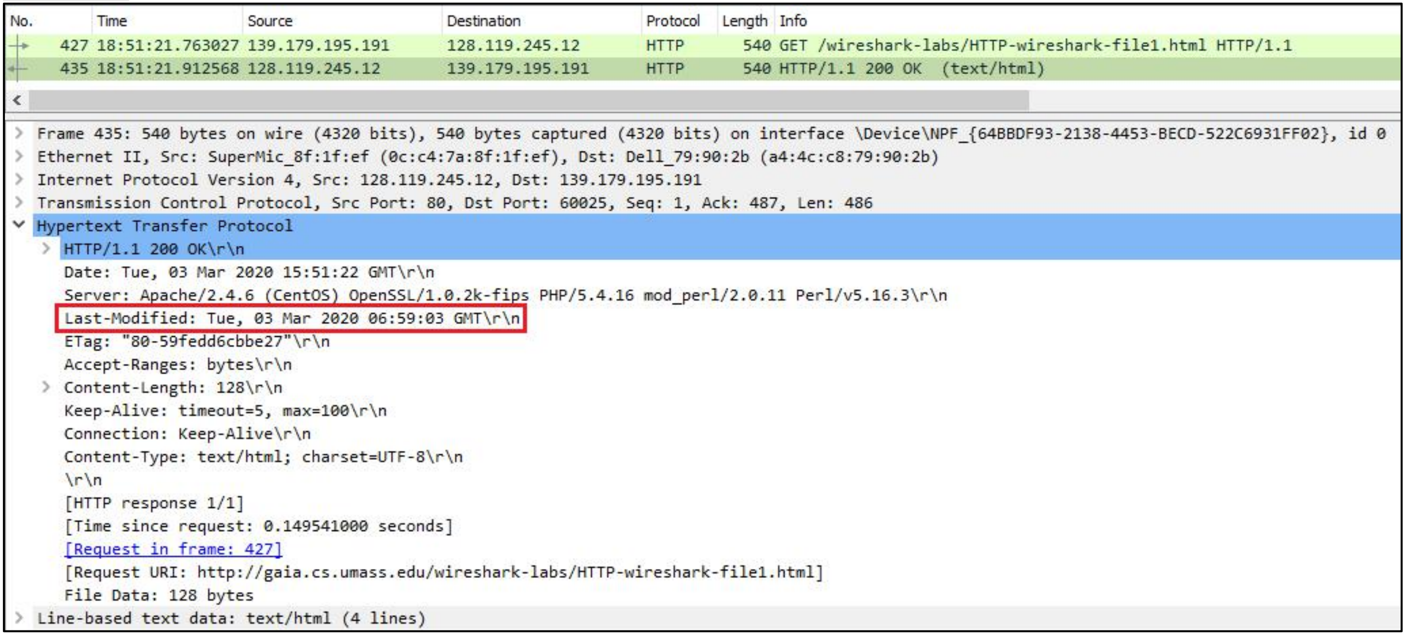
Question4



```
No.   Time             Source           Destination      Protocol  Length  Info
  427 18:51:21.763027 139.179.195.191  128.119.245.12   HTTP        540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  435 18:51:21.912568 128.119.245.12   139.179.195.191  HTTP        540 HTTP/1.1 200 OK  (text/html)
```

HTTP/1.1 200 OK is returned from the server to my browser.

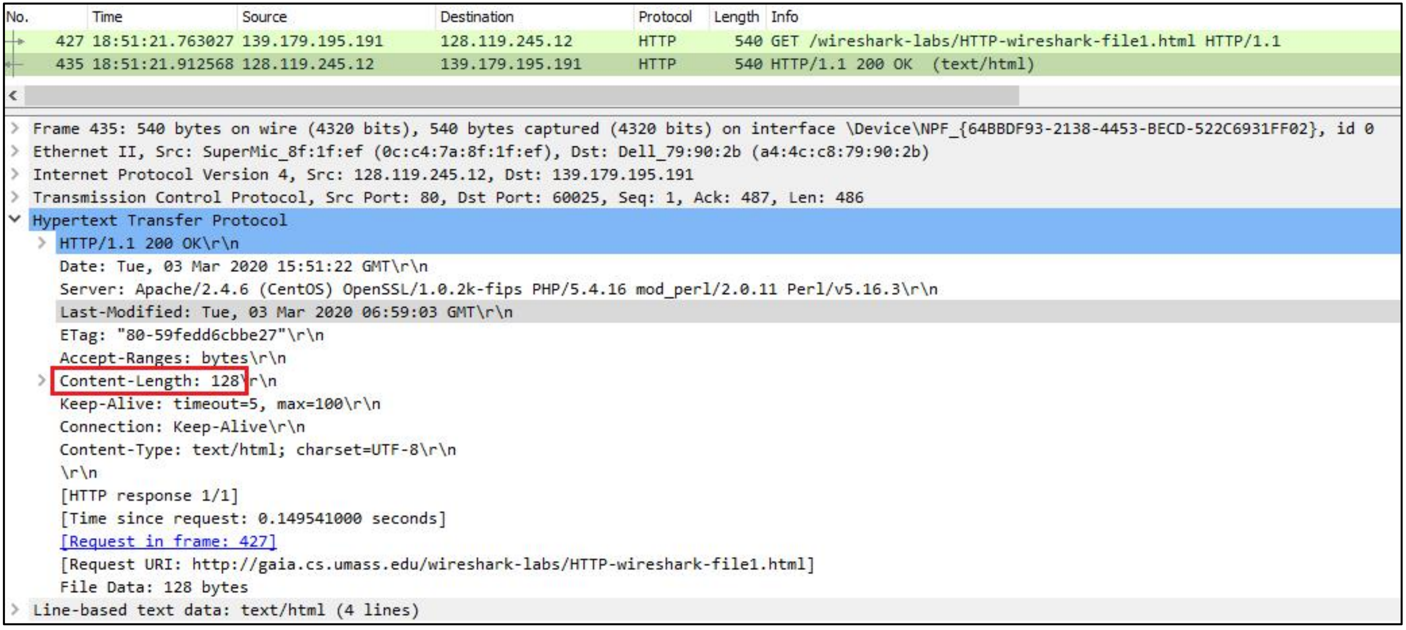
Question5



```
No.   Time             Source           Destination      Protocol  Length  Info
  427 18:51:21.763027 139.179.195.191  128.119.245.12   HTTP        540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  435 18:51:21.912568 128.119.245.12   139.179.195.191  HTTP        540 HTTP/1.1 200 OK  (text/html)

> Frame 435: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{64BBDF93-2138-4453-BECD-522C6931FF02}, id 0
> Ethernet II, Src: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef), Dst: Dell_79:90:2b (a4:4c:c8:79:90:2b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.195.191
> Transmission Control Protocol, Src Port: 80, Dst Port: 60025, Seq: 1, Ack: 487, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 03 Mar 2020 15:51:22 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 03 Mar 2020 06:59:03 GMT\r\n
    ETag: "80-59fedd6cbbe27"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.149541000 seconds]
    [Request in frame: 427]
    [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)
```

The file is lastly modified at the following date and time --> Tue, 03 Mar 2020 06:59:03 GMT

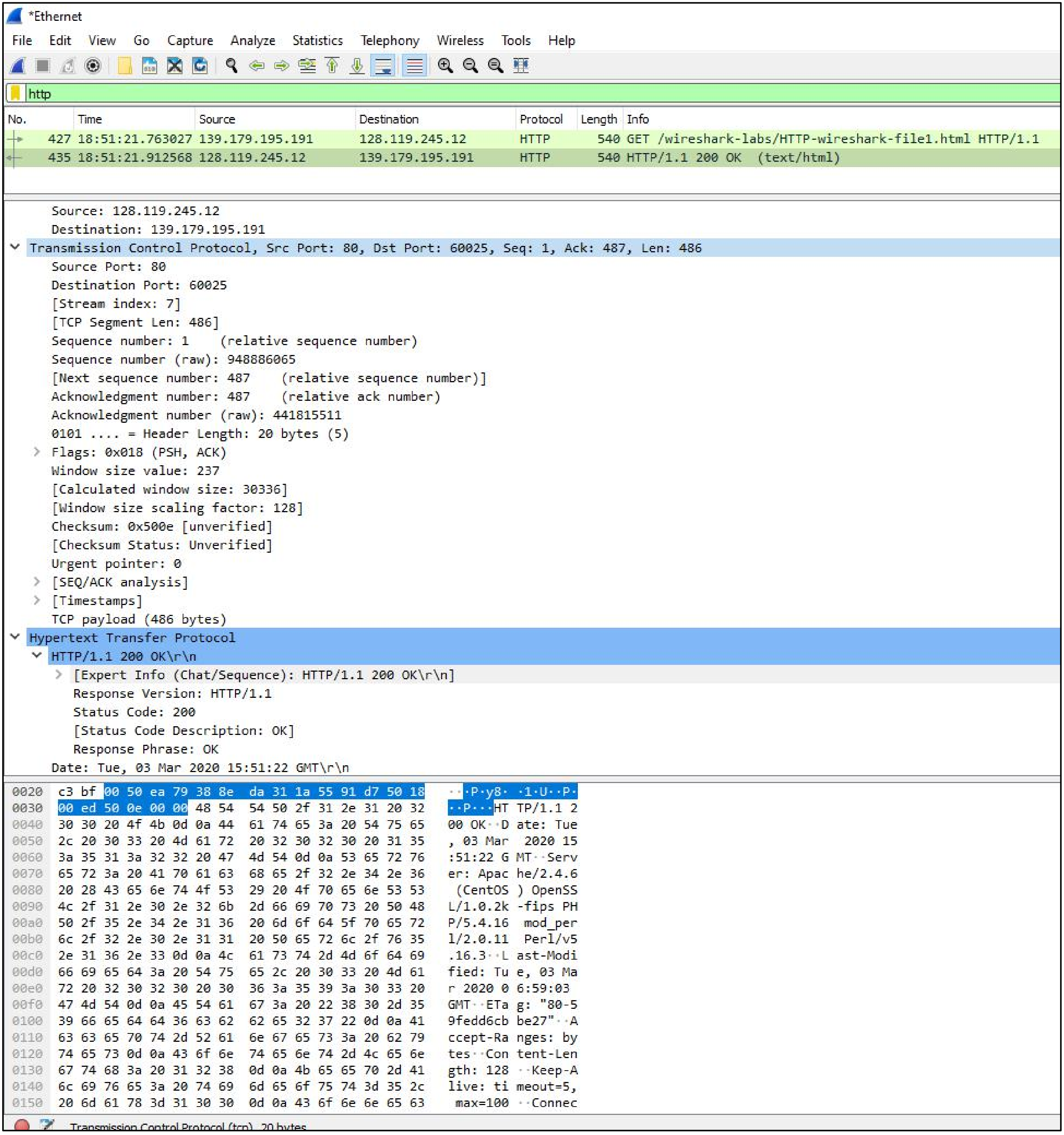
Question6



```
No.   Time             Source           Destination      Protocol  Length  Info
  427 18:51:21.763027 139.179.195.191  128.119.245.12   HTTP        540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  435 18:51:21.912568 128.119.245.12   139.179.195.191  HTTP        540 HTTP/1.1 200 OK  (text/html)

> Frame 435: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{64BBDF93-2138-4453-BECD-522C6931FF02}, id 0
> Ethernet II, Src: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef), Dst: Dell_79:90:2b (a4:4c:c8:79:90:2b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.195.191
> Transmission Control Protocol, Src Port: 80, Dst Port: 60025, Seq: 1, Ack: 487, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 03 Mar 2020 15:51:22 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 03 Mar 2020 06:59:03 GMT\r\n
    ETag: "80-59fedd6cbbe27"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.149541000 seconds]
    [Request in frame: 427]
    [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)
```

128 byte of content has returned to my browser.

Question7



```
http
```

```
No.   Time            Source           Destination      Protocol  Length Info
  427 18:51:21.763027 139.179.195.191  128.119.245.12   HTTP      540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  435 18:51:21.912568 128.119.245.12   139.179.195.191  HTTP      540 HTTP/1.1 200 OK  (text/html)
```

```
    Source: 128.119.245.12
    Destination: 139.179.195.191
v Transmission Control Protocol, Src Port: 80, Dst Port: 60025, Seq: 1, Ack: 487, Len: 486
    Source Port: 80
    Destination Port: 60025
    [Stream index: 7]
    [TCP Segment Len: 486]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 948886065
    [Next sequence number: 487    (relative sequence number)]
    Acknowledgment number: 487    (relative ack number)
    Acknowledgment number (raw): 441815511
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x500e [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (486 bytes)
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: Tue, 03 Mar 2020 15:51:22 GMT\r\n
```

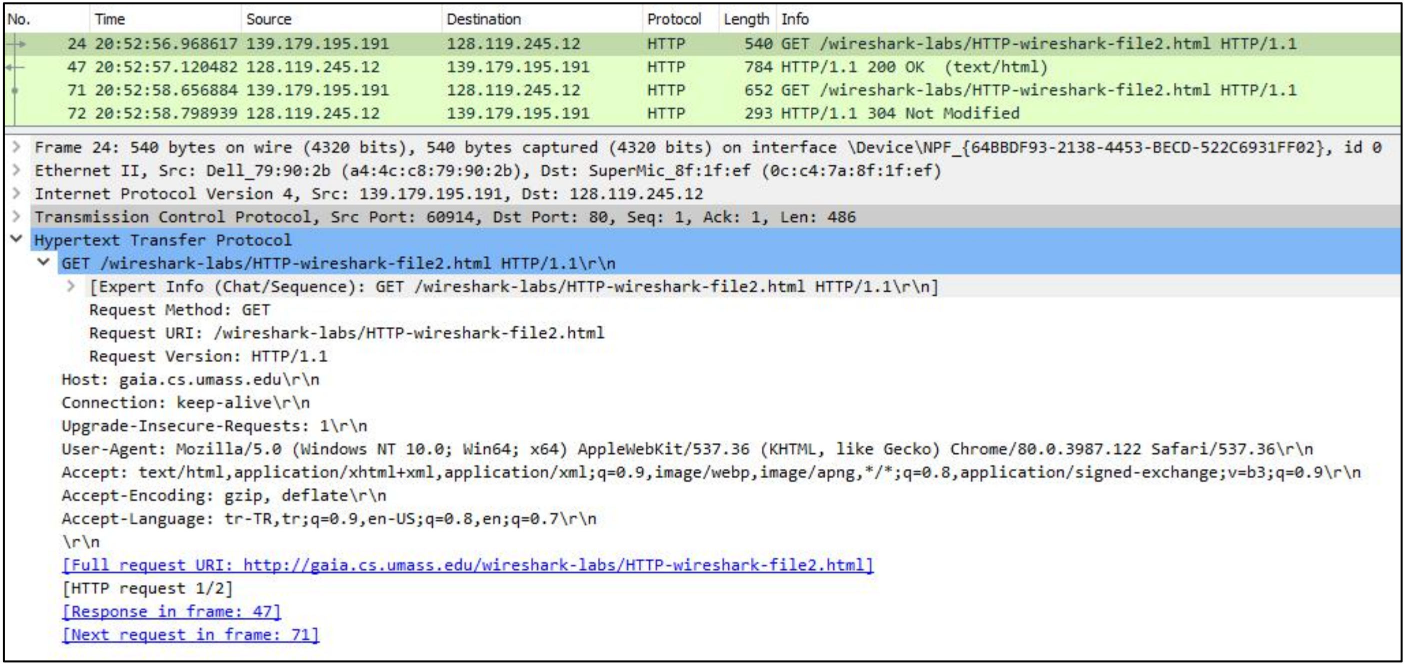
```
0020  c3 bf 00 50 ea 79 38 8e  da 31 1a 55 91 d7 50 18   ···P·y8· ·1·U··P·
0030  00 ed 50 0e 00 00 48 54  54 50 2f 31 2e 31 20 32   ··P···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 75 65   00 OK··D ate: Tue
0050  2c 20 30 33 20 4d 61 72  20 32 30 32 30 20 31 35   , 03 Mar  2020 15
0060  3a 35 31 3a 32 32 20 47  4d 54 0d 0a 53 65 72 76   :51:22 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 35 2e 34 2e 31 36  20 6d 6f 64 5f 70 65 72   P/5.4.16  mod_per
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f 76 35   l/2.0.11  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 54 75  65 2c 20 30 33 20 4d 61   fied: Tu e, 03 Ma
00e0  72 20 32 30 32 30 20 30  36 3a 35 39 3a 30 33 20   r 2020 0 6:59:03 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
0100  39 66 65 64 64 36 63 62  62 65 32 37 22 0d 0a 41   9fedd6cb be27"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
```

Transmission Control Protocol (tcp), 20 bytes

The TCP header is not displayed in the packet listing window.

The HTTP CONDITIONAL GET/response interaction

Question8

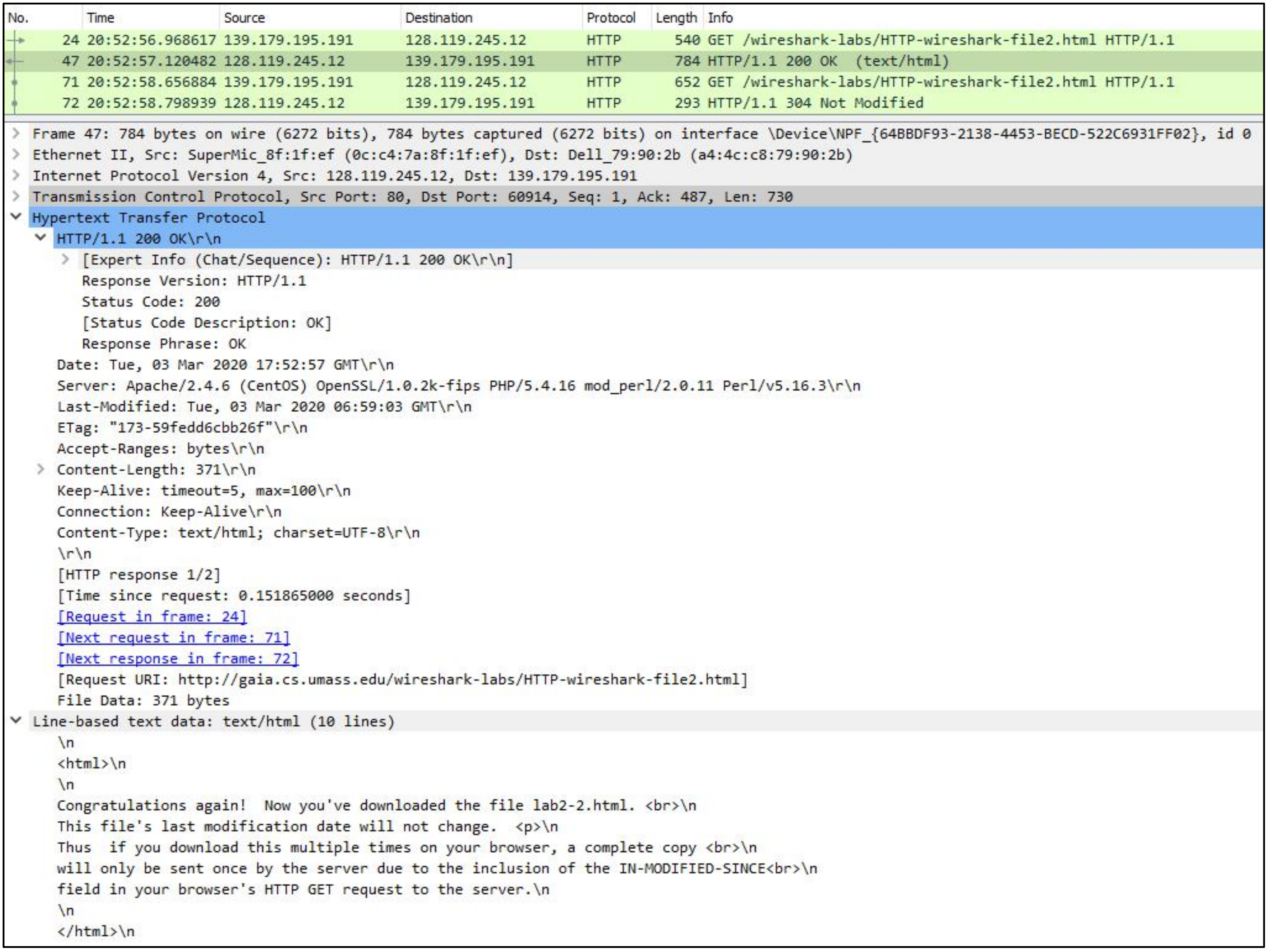


```
No.  Time            Source           Destination      Protocol  Length Info
 24 20:52:56.968617 139.179.195.191  128.119.245.12   HTTP      540 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 47 20:52:57.120482 128.119.245.12   139.179.195.191  HTTP      784 HTTP/1.1 200 OK  (text/html)
 71 20:52:58.656884 139.179.195.191  128.119.245.12   HTTP      652 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 72 20:52:58.798939 128.119.245.12   139.179.195.191  HTTP      293 HTTP/1.1 304 Not Modified
```

```
> Frame 24: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{64BBDF93-2138-4453-BECD-522C6931FF02}, id 0
> Ethernet II, Src: Dell_79:90:2b (a4:4c:c8:79:90:2b), Dst: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef)
> Internet Protocol Version 4, Src: 139.179.195.191, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60914, Dst Port: 80, Seq: 1, Ack: 1, Len: 486
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    > [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
    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/80.0.3987.122 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/2]
    [Response in frame: 47]
    [Next request in frame: 71]
```

There is **NO** “IF-MODIFIED-SINCE” line in the HTTP GET

Question9

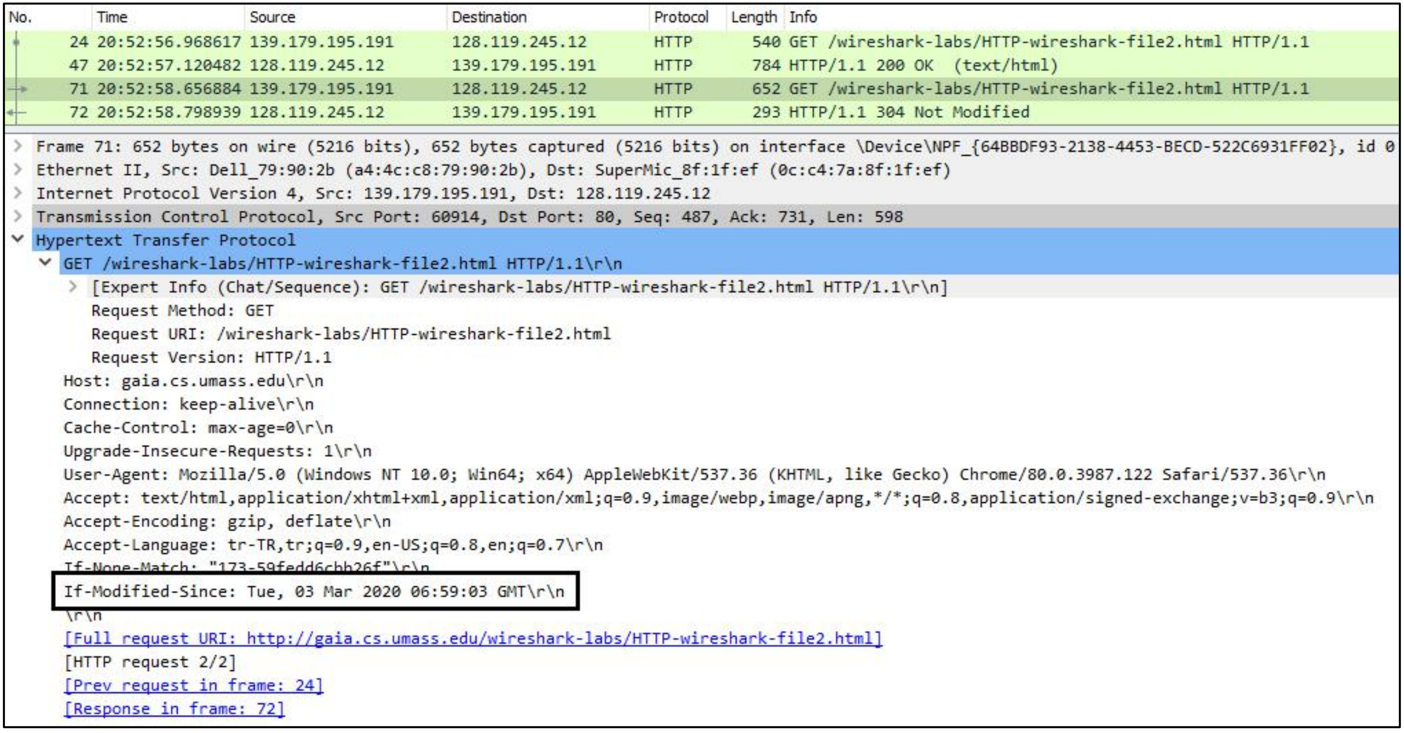


```
No.  Time            Source           Destination      Protocol  Length Info
 24 20:52:56.968617 139.179.195.191  128.119.245.12   HTTP      540 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 47 20:52:57.120482 128.119.245.12   139.179.195.191  HTTP      784 HTTP/1.1 200 OK  (text/html)
 71 20:52:58.656884 139.179.195.191  128.119.245.12   HTTP      652 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 72 20:52:58.798939 128.119.245.12   139.179.195.191  HTTP      293 HTTP/1.1 304 Not Modified
```

```
> Frame 47: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{64BBDF93-2138-4453-BECD-522C6931FF02}, id 0
> Ethernet II, Src: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef), Dst: Dell_79:90:2b (a4:4c:c8:79:90:2b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.195.191
> Transmission Control Protocol, Src Port: 80, Dst Port: 60914, Seq: 1, Ack: 487, Len: 730
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: Tue, 03 Mar 2020 17:52:57 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 03 Mar 2020 06:59:03 GMT\r\n
    ETag: "173-59fedd6cbb26f"\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
    [HTTP response 1/2]
    [Time since request: 0.151865000 seconds]
    [Request in frame: 24]
    [Next request in frame: 71]
    [Next response in frame: 72]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.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
```

Yes, the server explicitly returns the contents of the file. This can be seen in the line based text data section. File data indicates the size of the content data.

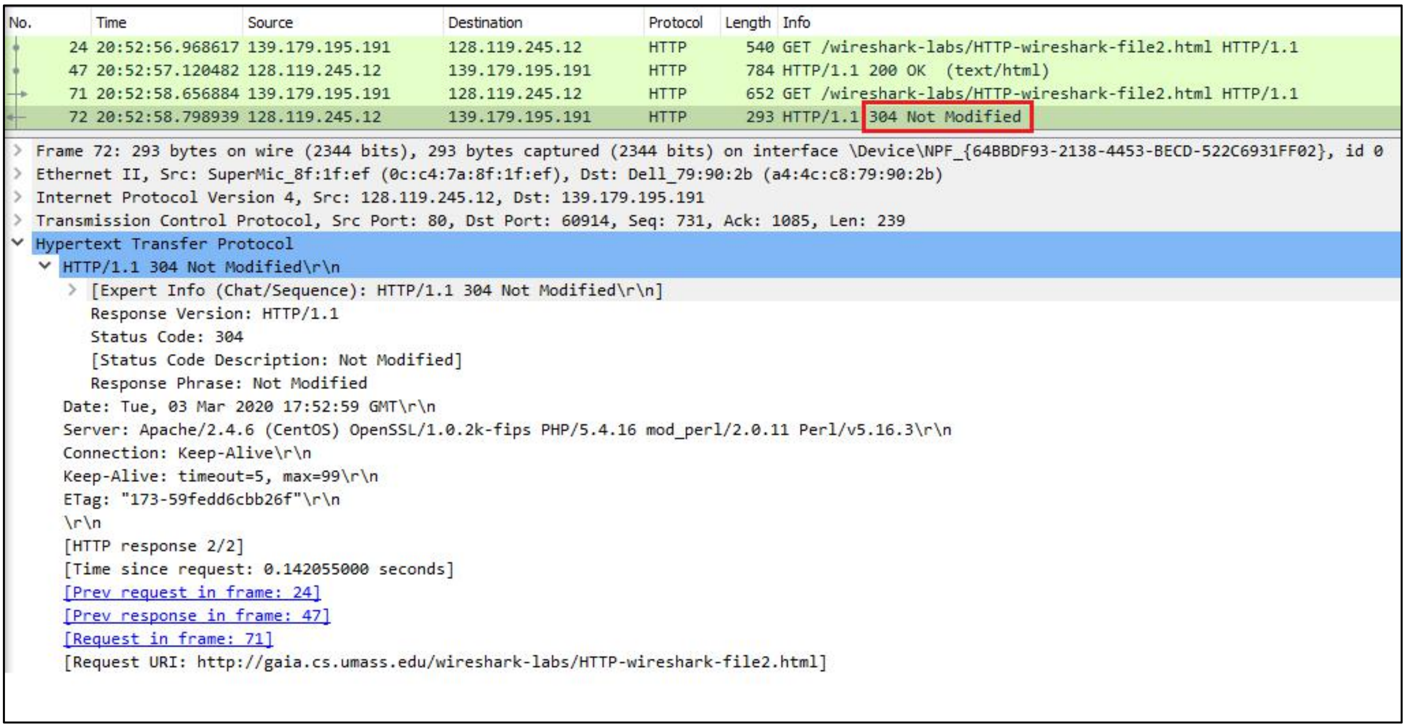
Question10



```
No.  Time             Source           Destination      Protocol  Length Info
  24 20:52:56.968617 139.179.195.191  128.119.245.12   HTTP      540 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  47 20:52:57.120482 128.119.245.12   139.179.195.191  HTTP      784 HTTP/1.1 200 OK  (text/html)
  71 20:52:58.656884 139.179.195.191  128.119.245.12   HTTP      652 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  72 20:52:58.798939 128.119.245.12   139.179.195.191  HTTP      293 HTTP/1.1 304 Not Modified

> Frame 71: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits) on interface \Device\NPF_{64BBDF93-2138-4453-BECD-522C6931FF02}, id 0
> Ethernet II, Src: Dell_79:90:2b (a4:4c:c8:79:90:2b), Dst: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef)
> Internet Protocol Version 4, Src: 139.179.195.191, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60914, Dst Port: 80, Seq: 487, Ack: 731, Len: 598
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    > [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
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    If-None-Match: "173-59fedd6cbb26f"\r\n
    If-Modified-Since: Tue, 03 Mar 2020 06:59:03 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 24]
    [Response in frame: 72]
```

YES, there is which is the indicated line in the figure above.(If-Modified-Since: Tue, 03 Mar 2020 06:59:03 GMT). The server checks whether the file is changed or not since the indicated time.

Question11

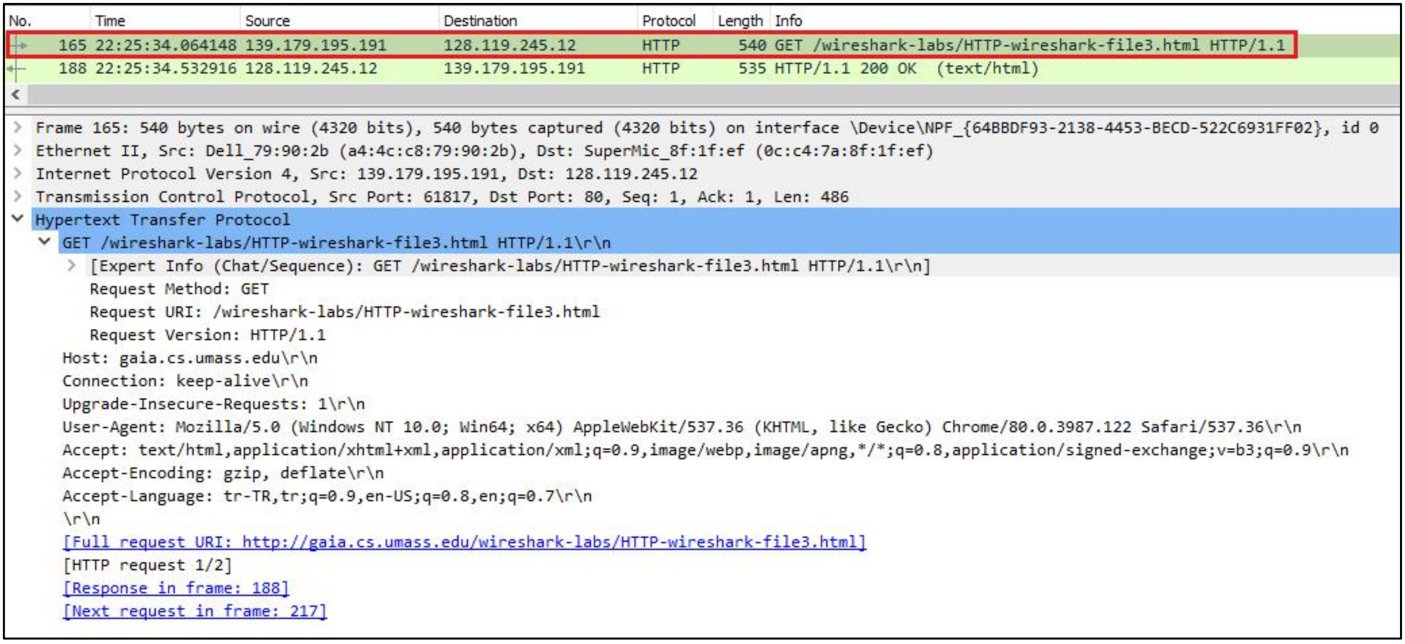


```
No.  Time             Source           Destination      Protocol  Length Info
  24 20:52:56.968617 139.179.195.191  128.119.245.12   HTTP      540 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  47 20:52:57.120482 128.119.245.12   139.179.195.191  HTTP      784 HTTP/1.1 200 OK  (text/html)
  71 20:52:58.656884 139.179.195.191  128.119.245.12   HTTP      652 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  72 20:52:58.798939 128.119.245.12   139.179.195.191  HTTP      293 HTTP/1.1 304 Not Modified

> Frame 72: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{64BBDF93-2138-4453-BECD-522C6931FF02}, id 0
> Ethernet II, Src: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef), Dst: Dell_79:90:2b (a4:4c:c8:79:90:2b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.195.191
> Transmission Control Protocol, Src Port: 80, Dst Port: 60914, Seq: 731, Ack: 1085, Len: 239
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Tue, 03 Mar 2020 17:52:59 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-59fedd6cbb26f"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.142055000 seconds]
    [Prev request in frame: 24]
    [Prev response in frame: 47]
    [Request in frame: 71]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

The HTTP status code and phrase is HTTP/1.1 304 Not Modified. The server did NOT explicitly return the contents of file. The reason why the server does not returns the content file is that the last modification time of the file in the server and the date in the request which is in the "If-Modified-Since" section are compared in server. If the file is not modified since the indicated date in the "If-Modified-Since" section or line, that is to say, the file in the cache of the client computer is up to date. Hence, the server does not returns the entire content. In this case, the web browser of client side obtains the file from the cache and displays it. As a result, efficiency is obtained because there is not always a data transfer between the client and server side.

Retrieving Long Documents

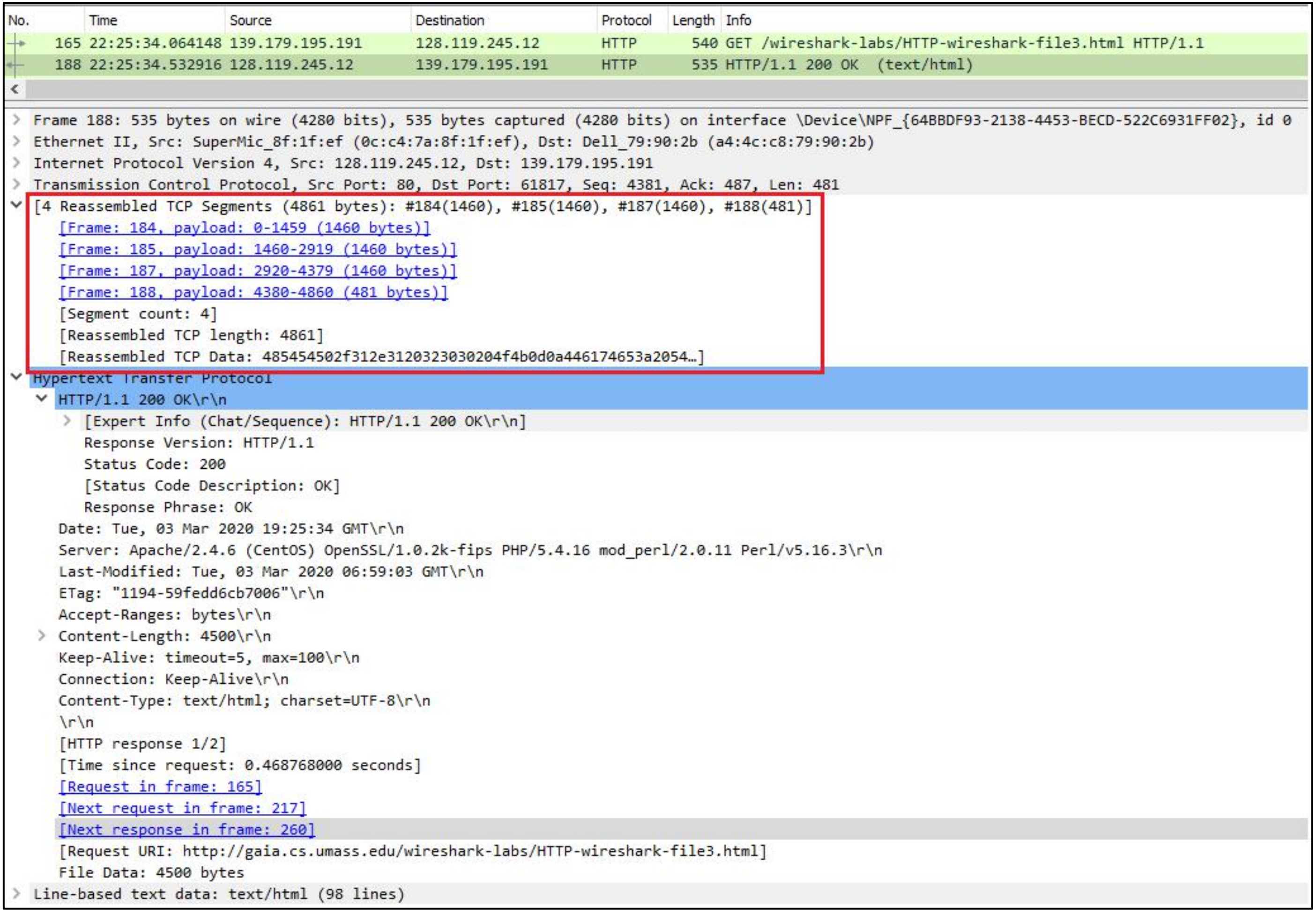
Question12



```
No.   Time               Source            Destination      Protocol  Length  Info
  165 22:25:34.064148 139.179.195.191   128.119.245.12   HTTP         540  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  188 22:25:34.532916 128.119.245.12    139.179.195.191  HTTP         535  HTTP/1.1 200 OK  (text/html)

> Frame 165: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{64BBDF93-2138-4453-BECD-522C6931FF02}, id 0
> Ethernet II, Src: Dell_79:90:2b (a4:4c:c8:79:90:2b), Dst: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef)
> Internet Protocol Version 4, Src: 139.179.195.191, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61817, Dst Port: 80, Seq: 1, Ack: 1, Len: 486
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file3.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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    [HTTP request 1/2]
    [Response in frame: 188]
    [Next request in frame: 217]
```

One HTTP GET request was sent.

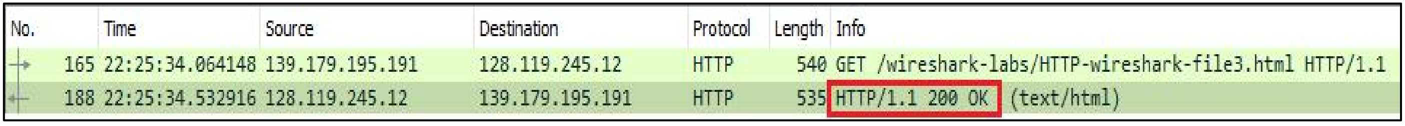
Question13



```
No.   Time               Source            Destination      Protocol  Length  Info
  165 22:25:34.064148 139.179.195.191   128.119.245.12   HTTP         540  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  188 22:25:34.532916 128.119.245.12    139.179.195.191  HTTP         535  HTTP/1.1 200 OK  (text/html)

> Frame 188: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{64BBDF93-2138-4453-BECD-522C6931FF02}, id 0
> Ethernet II, Src: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef), Dst: Dell_79:90:2b (a4:4c:c8:79:90:2b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.195.191
> Transmission Control Protocol, Src Port: 80, Dst Port: 61817, Seq: 4381, Ack: 487, Len: 481
v [4 Reassembled TCP Segments (4861 bytes): #184(1460), #185(1460), #187(1460), #188(481)]
    [Frame: 184, payload: 0-1459 (1460 bytes)]
    [Frame: 185, payload: 1460-2919 (1460 bytes)]
    [Frame: 187, payload: 2920-4379 (1460 bytes)]
    [Frame: 188, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2054…]
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: Tue, 03 Mar 2020 19:25:34 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 03 Mar 2020 06:59:03 GMT\r\n
    ETag: "1194-59fedd6cb7006"\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 1/2]
    [Time since request: 0.468768000 seconds]
    [Request in frame: 165]
    [Next request in frame: 217]
    [Next response in frame: 260]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
> Line-based text data: text/html (98 lines)
```

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

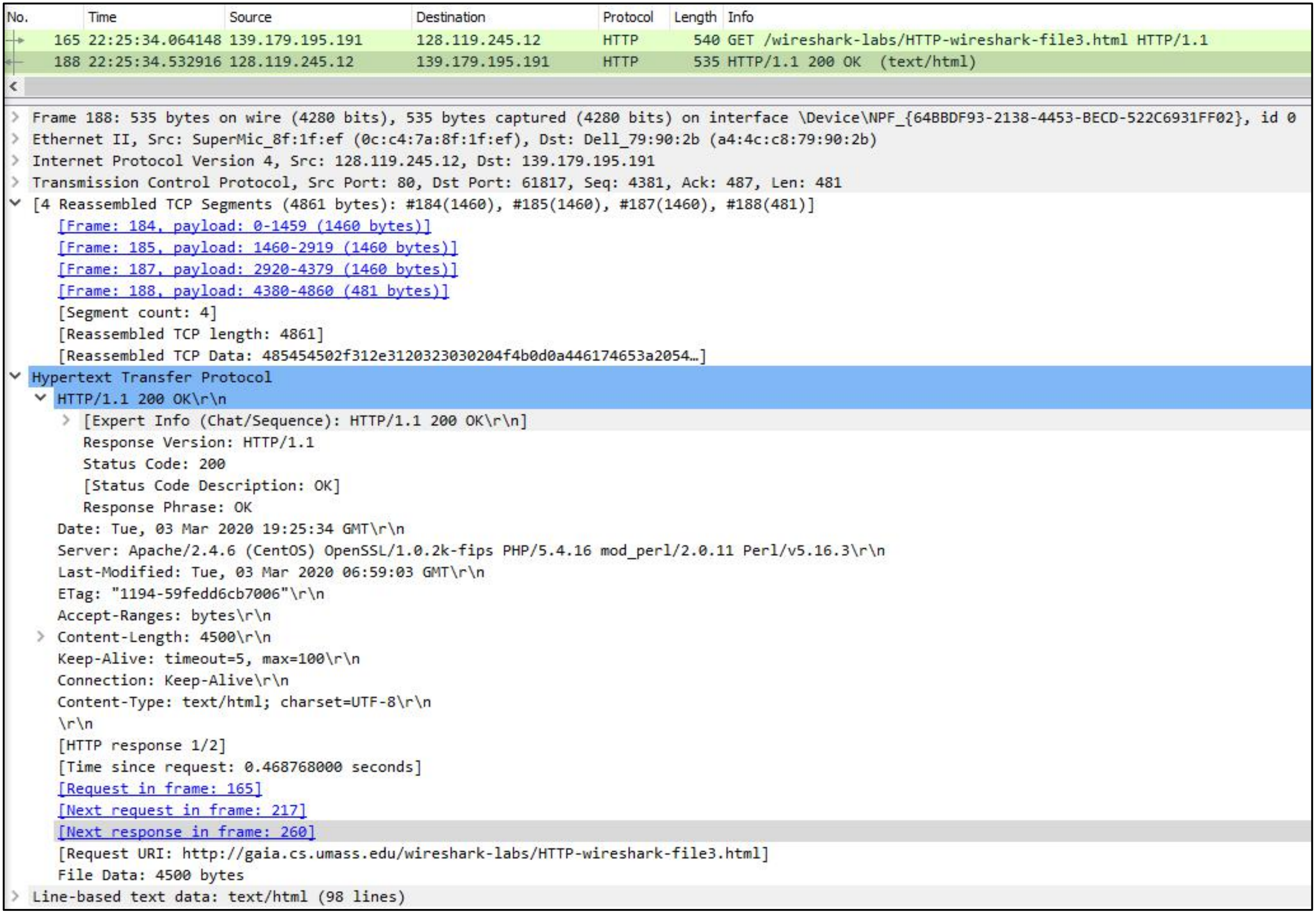
Question14



```
No.   Time             Source           Destination      Protocol  Length Info
  165 22:25:34.064148 139.179.195.191  128.119.245.12   HTTP         540 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  188 22:25:34.532916 128.119.245.12   139.179.195.191  HTTP         535 HTTP/1.1 200 OK  (text/html)
```

The status code phrase is HTTP/1.1 200 OK

Question15

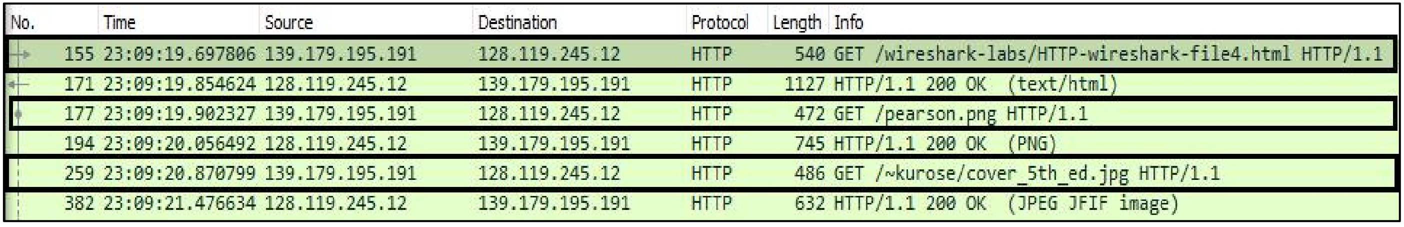


```
No.   Time             Source           Destination      Protocol  Length Info
  165 22:25:34.064148 139.179.195.191  128.119.245.12   HTTP         540 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  188 22:25:34.532916 128.119.245.12   139.179.195.191  HTTP         535 HTTP/1.1 200 OK  (text/html)

> Frame 188: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{64BBDF93-2138-4453-BECD-522C6931FF02}, id 0
> Ethernet II, Src: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef), Dst: Dell_79:90:2b (a4:4c:c8:79:90:2b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.195.191
> Transmission Control Protocol, Src Port: 80, Dst Port: 61817, Seq: 4381, Ack: 487, Len: 481
v [4 Reassembled TCP Segments (4861 bytes): #184(1460), #185(1460), #187(1460), #188(481)]
    [Frame: 184, payload: 0-1459 (1460 bytes)]
    [Frame: 185, payload: 1460-2919 (1460 bytes)]
    [Frame: 187, payload: 2920-4379 (1460 bytes)]
    [Frame: 188, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2054…]
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: Tue, 03 Mar 2020 19:25:34 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 03 Mar 2020 06:59:03 GMT\r\n
    ETag: "1194-59fedd6cb7006"\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 1/2]
    [Time since request: 0.468768000 seconds]
    [Request in frame: 165]
    [Next request in frame: 217]
    [Next response in frame: 260]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
> Line-based text data: text/html (98 lines)
```

There is no HTTP status lines in the transmitted data associated with a TCP-induced "Continuation". Because all segments are sent in the same HTTP response. The four TCP segments are resembled afterwards and sent to the same HTTP.

HTML Documents with Embedded Objects

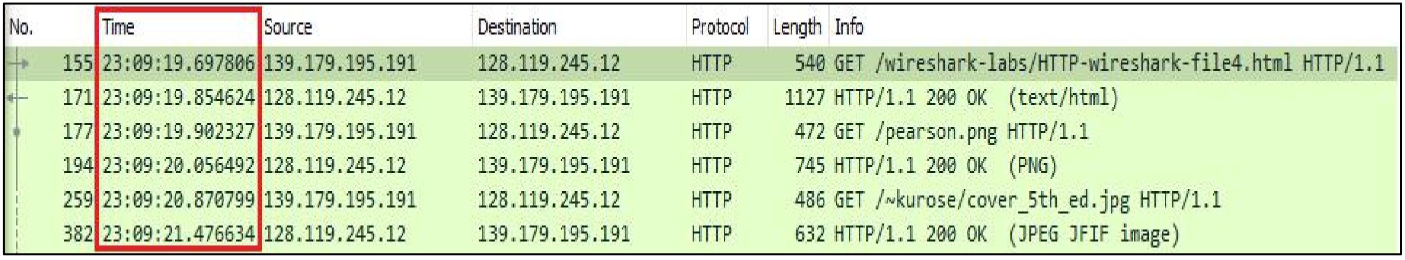
Question16



```
No.   Time             Source           Destination      Protocol  Length Info
  155 23:09:19.697806 139.179.195.191  128.119.245.12   HTTP         540 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  171 23:09:19.854624 128.119.245.12   139.179.195.191  HTTP        1127 HTTP/1.1 200 OK  (text/html)
  177 23:09:19.902327 139.179.195.191  128.119.245.12   HTTP         472 GET /pearson.png HTTP/1.1
  194 23:09:20.056492 128.119.245.12   139.179.195.191  HTTP         745 HTTP/1.1 200 OK  (PNG)
  259 23:09:20.870799 139.179.195.191  128.119.245.12   HTTP         486 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
  382 23:09:21.476634 128.119.245.12   139.179.195.191  HTTP         632 HTTP/1.1 200 OK  (JPEG JFIF image)
```

3 GET request messages were sent by my browser.All of the request messages were sent to the same address. The corresponding IP address is 128.119.245.12.

Question17

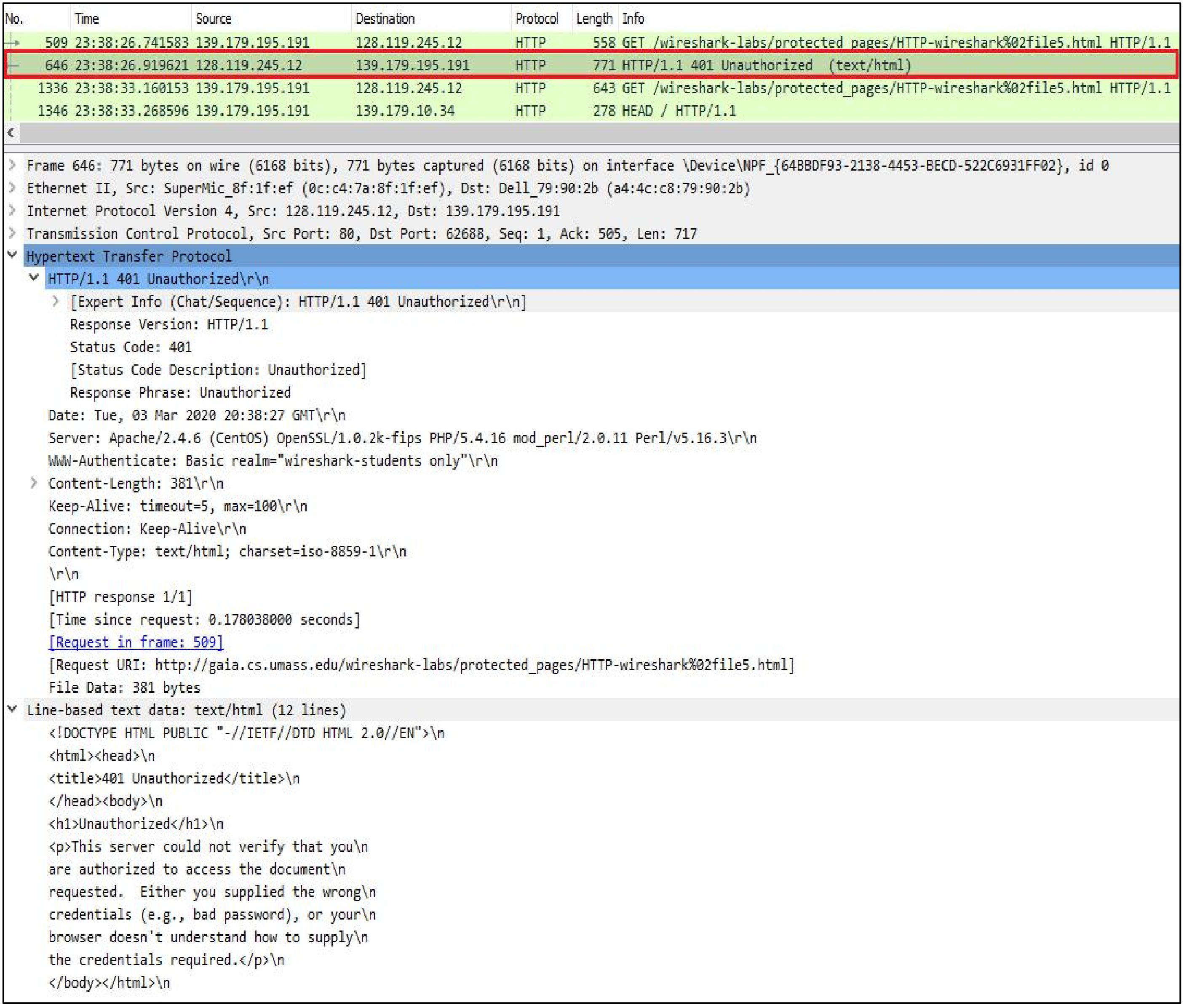


```
No.  Time             Source           Destination      Protocol  Length  Info
155  23:09:19.697806  139.179.195.191  128.119.245.12   HTTP       540  GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
171  23:09:19.854624  128.119.245.12   139.179.195.191  HTTP      1127  HTTP/1.1 200 OK  (text/html)
177  23:09:19.902327  139.179.195.191  128.119.245.12   HTTP       472  GET /pearson.png HTTP/1.1
194  23:09:20.056492  128.119.245.12   139.179.195.191  HTTP       745  HTTP/1.1 200 OK  (PNG)
259  23:09:20.870799  139.179.195.191  128.119.245.12   HTTP       486  GET /~kurose/cover_5th_ed.jpg HTTP/1.1
382  23:09:21.476634  128.119.245.12   139.179.195.191  HTTP       632  HTTP/1.1 200 OK  (JPEG JFIF image)
```

Looking at the times where the operations happened, the download operations are done sequentially and serially. The GET requests are done after retrieving the response messages whose status codes are 200.

HTTP Authentication

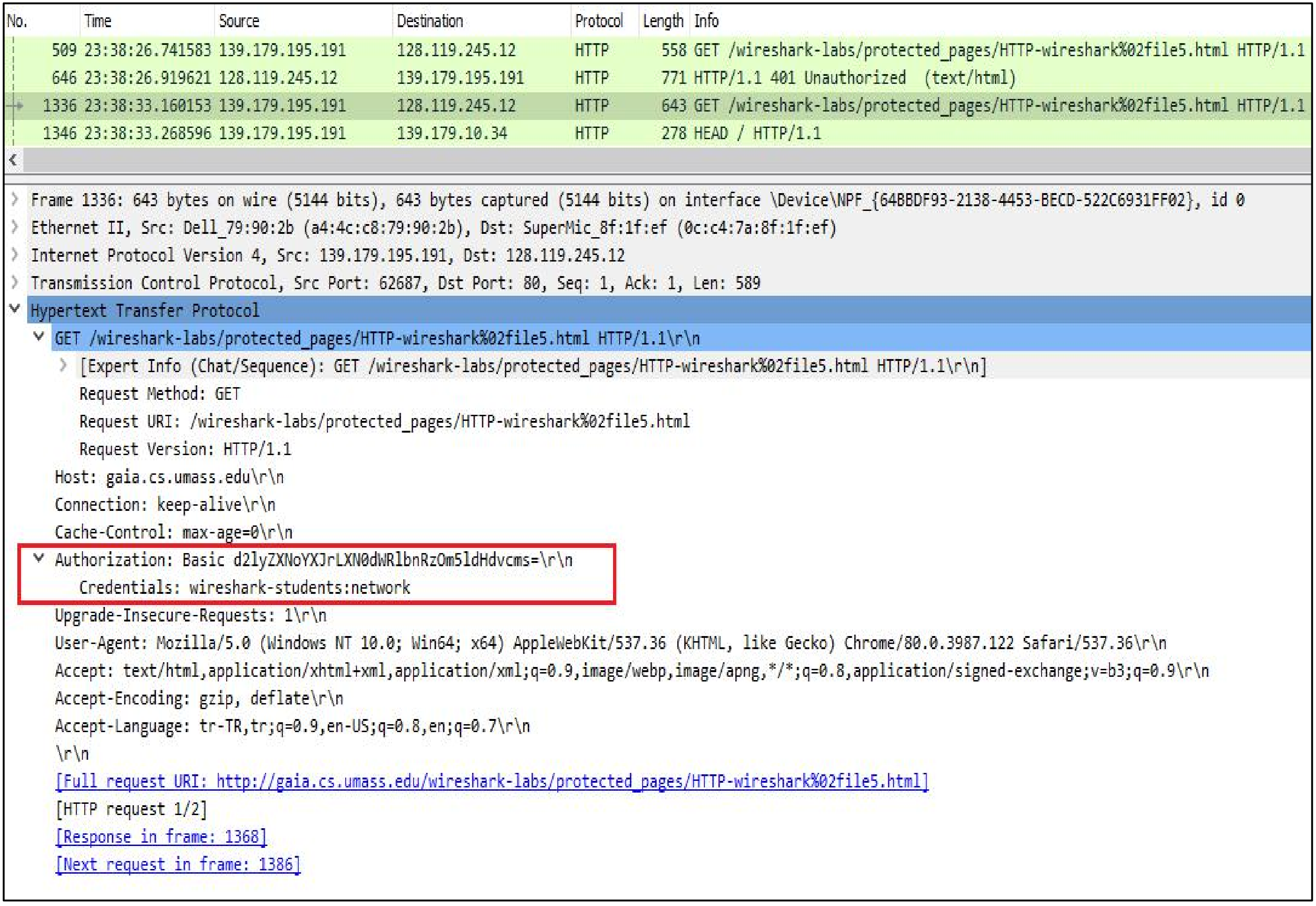
Question18



```
No.   Time             Source           Destination      Protocol  Length  Info
 509  23:38:26.741583  139.179.195.191  128.119.245.12   HTTP      558  GET /wireshark-labs/protected_pages/HTTP-wireshark%02file5.html HTTP/1.1
 646  23:38:26.919621  128.119.245.12   139.179.195.191  HTTP      771  HTTP/1.1 401 Unauthorized  (text/html)
1336  23:38:33.160153  139.179.195.191  128.119.245.12   HTTP      643  GET /wireshark-labs/protected_pages/HTTP-wireshark%02file5.html HTTP/1.1
1346  23:38:33.268596  139.179.195.191  139.179.10.34    HTTP      278  HEAD / HTTP/1.1

> Frame 646: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{64BBDF93-2138-4453-BECD-522C6931FF02}, id 0
> Ethernet II, Src: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef), Dst: Dell_79:90:2b (a4:4c:c8:79:90:2b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.195.191
> Transmission Control Protocol, Src Port: 80, Dst Port: 62688, Seq: 1, Ack: 505, Len: 717
v Hypertext Transfer Protocol
  v HTTP/1.1 401 Unauthorized\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
    Date: Tue, 03 Mar 2020 20:38:27 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  > Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.178038000 seconds]
    [Request in frame: 509]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark%02file5.html]
    File Data: 381 bytes
v Line-based text data: text/html (12 lines)
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>401 Unauthorized</title>\n
    </head><body>\n
    <h1>Unauthorized</h1>\n
    <p>This server could not verify that you\n
    are authorized to access the document\n
    requested.  Either you supplied the wrong\n
    credentials (e.g., bad password), or your\n
    browser doesn't understand how to supply\n
    the credentials required.</p>\n
    </body></html>\n
```

The response of the server to the initial GET message is HTTP/1.1 401 Unauthorized. Server requires authorization.

Question19



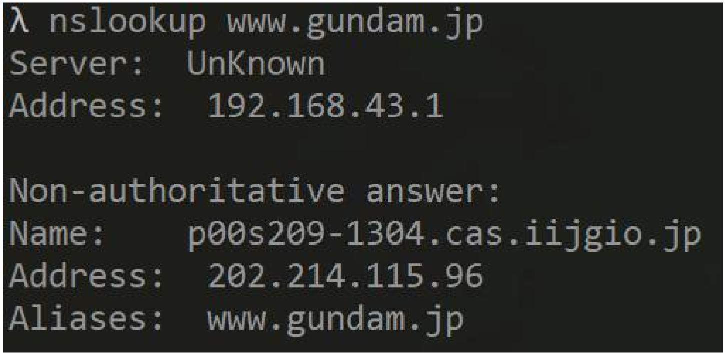
```
No.     Time            Source           Destination      Protocol  Length Info
    509 23:38:26.741583 139.179.195.191  128.119.245.12   HTTP         558 GET /wireshark-labs/protected_pages/HTTP-wireshark%02file5.html HTTP/1.1
    646 23:38:26.919621 128.119.245.12   139.179.195.191  HTTP         771 HTTP/1.1 401 Unauthorized  (text/html)
   1336 23:38:33.160153 139.179.195.191  128.119.245.12   HTTP         643 GET /wireshark-labs/protected_pages/HTTP-wireshark%02file5.html HTTP/1.1
   1346 23:38:33.268596 139.179.195.191  139.179.10.34    HTTP         278 HEAD / HTTP/1.1
```

```
> Frame 1336: 643 bytes on wire (5144 bits), 643 bytes captured (5144 bits) on interface \Device\NPF_{64BBDF93-2138-4453-BECD-522C6931FF02}, id 0
> Ethernet II, Src: Dell_79:90:2b (a4:4c:c8:79:90:2b), Dst: SuperMic_8f:1f:ef (0c:c4:7a:8f:1f:ef)
> Internet Protocol Version 4, Src: 139.179.195.191, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 62687, Dst Port: 80, Seq: 1, Ack: 1, Len: 589
v Hypertext Transfer Protocol
  v GET /wireshark-labs/protected_pages/HTTP-wireshark%02file5.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark%02file5.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark%02file5.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark%02file5.html]
    [HTTP request 1/2]
    [Response in frame: 1368]
    [Next request in frame: 1386]
```

The authorization line is added to the request which is indicated above. This line is required to have an access to the targeted HTML content file.

DNS

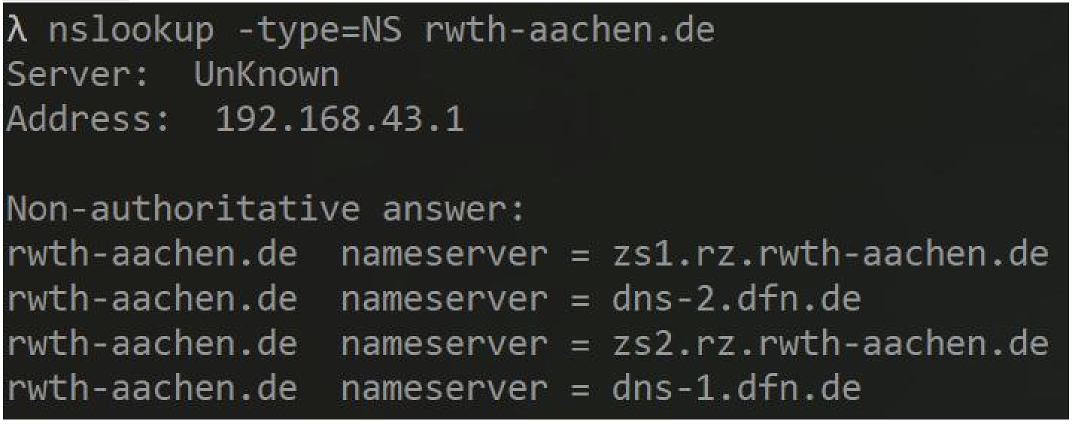
Question1



```
λ nslookup www.gundam.jp
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    p00s209-1304.cas.iijgio.jp
Address:  202.214.115.96
Aliases:  www.gundam.jp
```

I have queried www.gundam.jp. It’s IP address is 202.2014.115.96

Question2

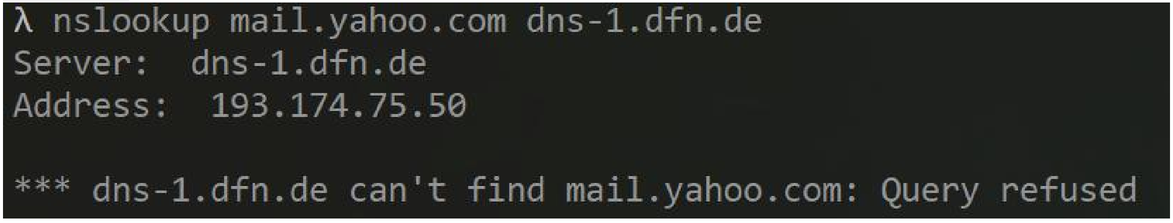


```
λ nslookup -type=NS rwth-aachen.de
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
rwth-aachen.de  nameserver = zs1.rz.rwth-aachen.de
rwth-aachen.de  nameserver = dns-2.dfn.de
rwth-aachen.de  nameserver = zs2.rz.rwth-aachen.de
rwth-aachen.de  nameserver = dns-1.dfn.de
```

I have queried the authoritative DNS servers of RWTH Aachen University. They are:

- zs1.rz.rwth-aachen.de
- dns-2.dfn.de
- zs2.rz.rwth-aachen.de
- dns-1.dfn.de

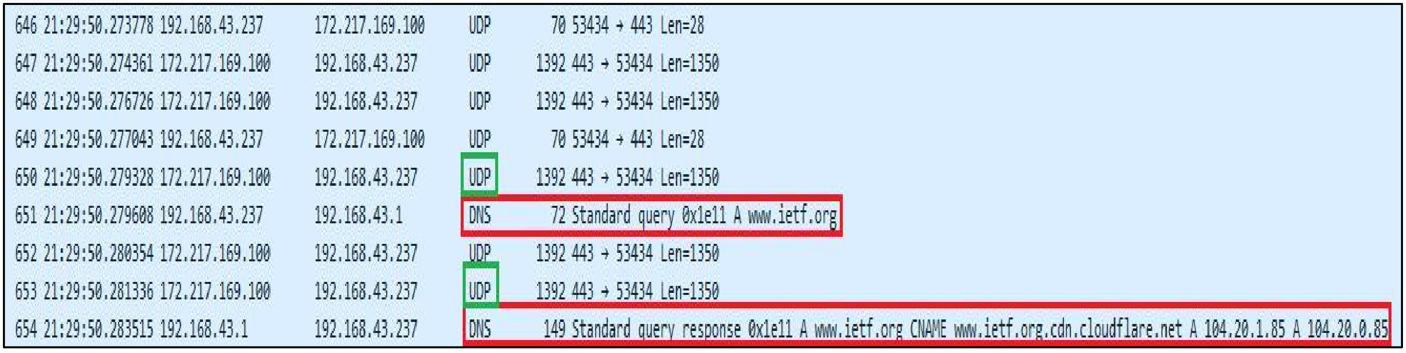
Question3



```
λ nslookup mail.yahoo.com dns-1.dfn.de
Server:  dns-1.dfn.de
Address:  193.174.75.50

*** dns-1.dfn.de can't find mail.yahoo.com: Query refused
```

Unfortunately, the query is refused. mail.yahoo.com could not be found by the dns-1.dfn.de address.

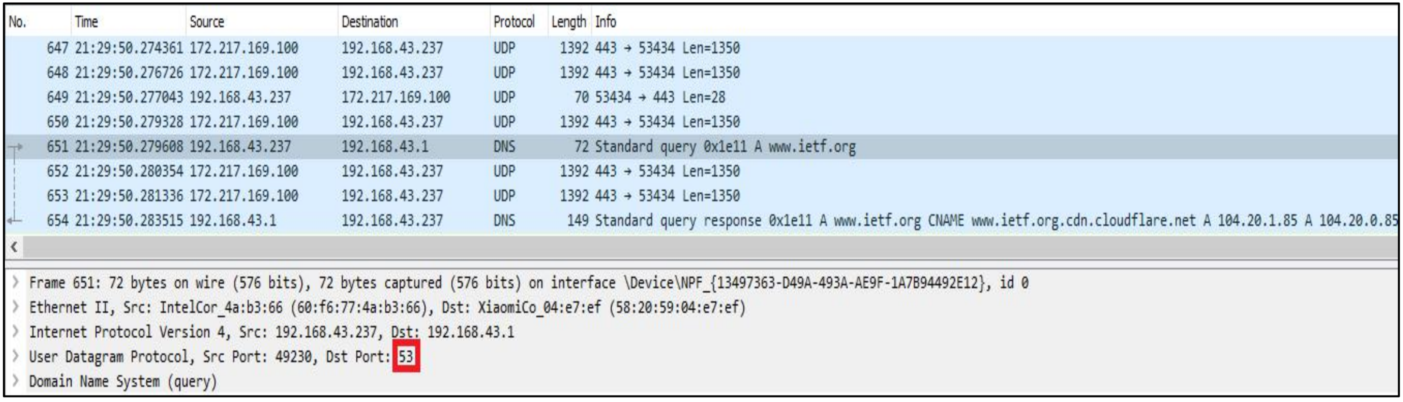
Question4



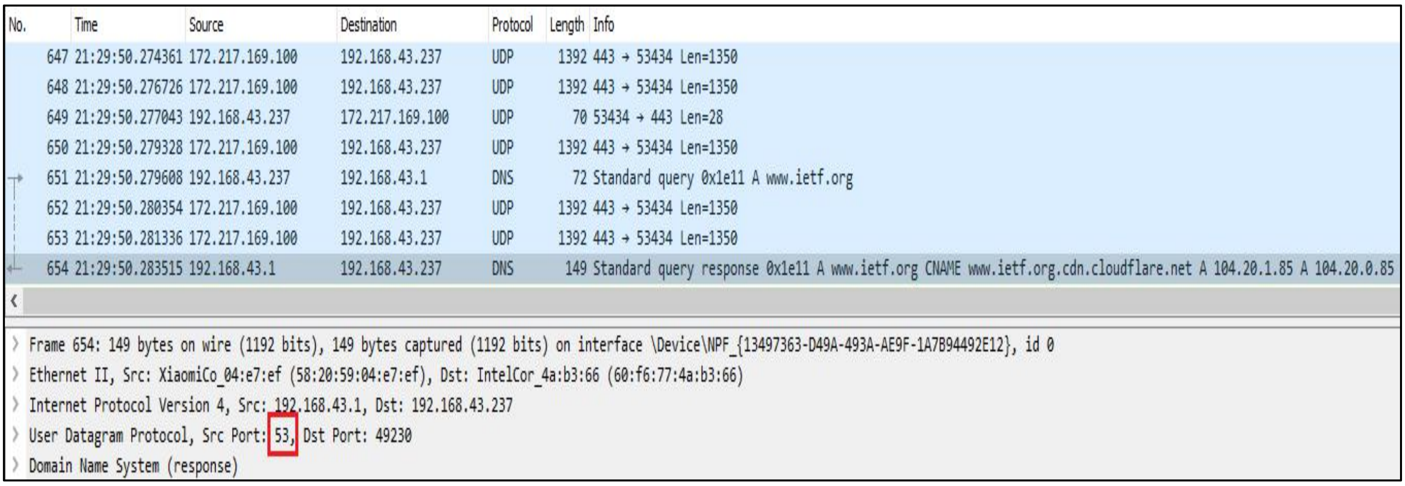
```
646 21:29:50.273778 192.168.43.237   172.217.169.100  UDP     70 53434 → 443 Len=28
647 21:29:50.274361 172.217.169.100  192.168.43.237   UDP   1392 443 → 53434 Len=1350
648 21:29:50.276726 172.217.169.100  192.168.43.237   UDP   1392 443 → 53434 Len=1350
649 21:29:50.277043 192.168.43.237   172.217.169.100  UDP     70 53434 → 443 Len=28
650 21:29:50.279328 172.217.169.100  192.168.43.237   UDP   1392 443 → 53434 Len=1350
651 21:29:50.279608 192.168.43.237   192.168.43.1     DNS     72 Standard query 0x1e11 A www.ietf.org
652 21:29:50.280354 172.217.169.100  192.168.43.237   UDP   1392 443 → 53434 Len=1350
653 21:29:50.281336 172.217.169.100  192.168.43.237   UDP   1392 443 → 53434 Len=1350
654 21:29:50.283515 192.168.43.1     192.168.43.237   DNS    149 Standard query response 0x1e11 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
```

The DNS query and response messages were sent through UDP.

Question5



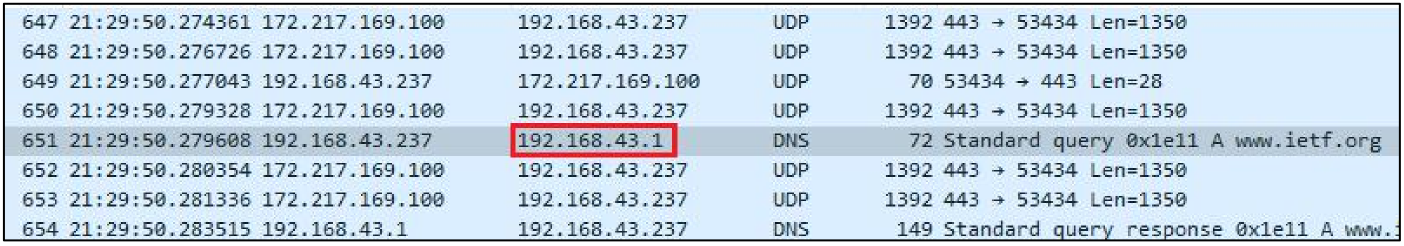
```
No.     Time            Source           Destination      Protocol Length Info
    647 21:29:50.274361 172.217.169.100  192.168.43.237   UDP      1392 443 → 53434 Len=1350
    648 21:29:50.276726 172.217.169.100  192.168.43.237   UDP      1392 443 → 53434 Len=1350
    649 21:29:50.277043 192.168.43.237   172.217.169.100  UDP        70 53434 → 443 Len=28
    650 21:29:50.279328 172.217.169.100  192.168.43.237   UDP      1392 443 → 53434 Len=1350
    651 21:29:50.279608 192.168.43.237   192.168.43.1     DNS        72 Standard query 0x1e11 A www.ietf.org
    652 21:29:50.280354 172.217.169.100  192.168.43.237   UDP      1392 443 → 53434 Len=1350
    653 21:29:50.281336 172.217.169.100  192.168.43.237   UDP      1392 443 → 53434 Len=1350
    654 21:29:50.283515 192.168.43.1     192.168.43.237   DNS       149 Standard query response 0x1e11 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85

> Frame 651: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{13497363-D49A-493A-AE9F-1A7B94492E12}, id 0
> Ethernet II, Src: IntelCor_4a:b3:66 (60:f6:77:4a:b3:66), Dst: XiaomiCo_04:e7:ef (58:20:59:04:e7:ef)
> Internet Protocol Version 4, Src: 192.168.43.237, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 49230, Dst Port: 53
> Domain Name System (query)
```



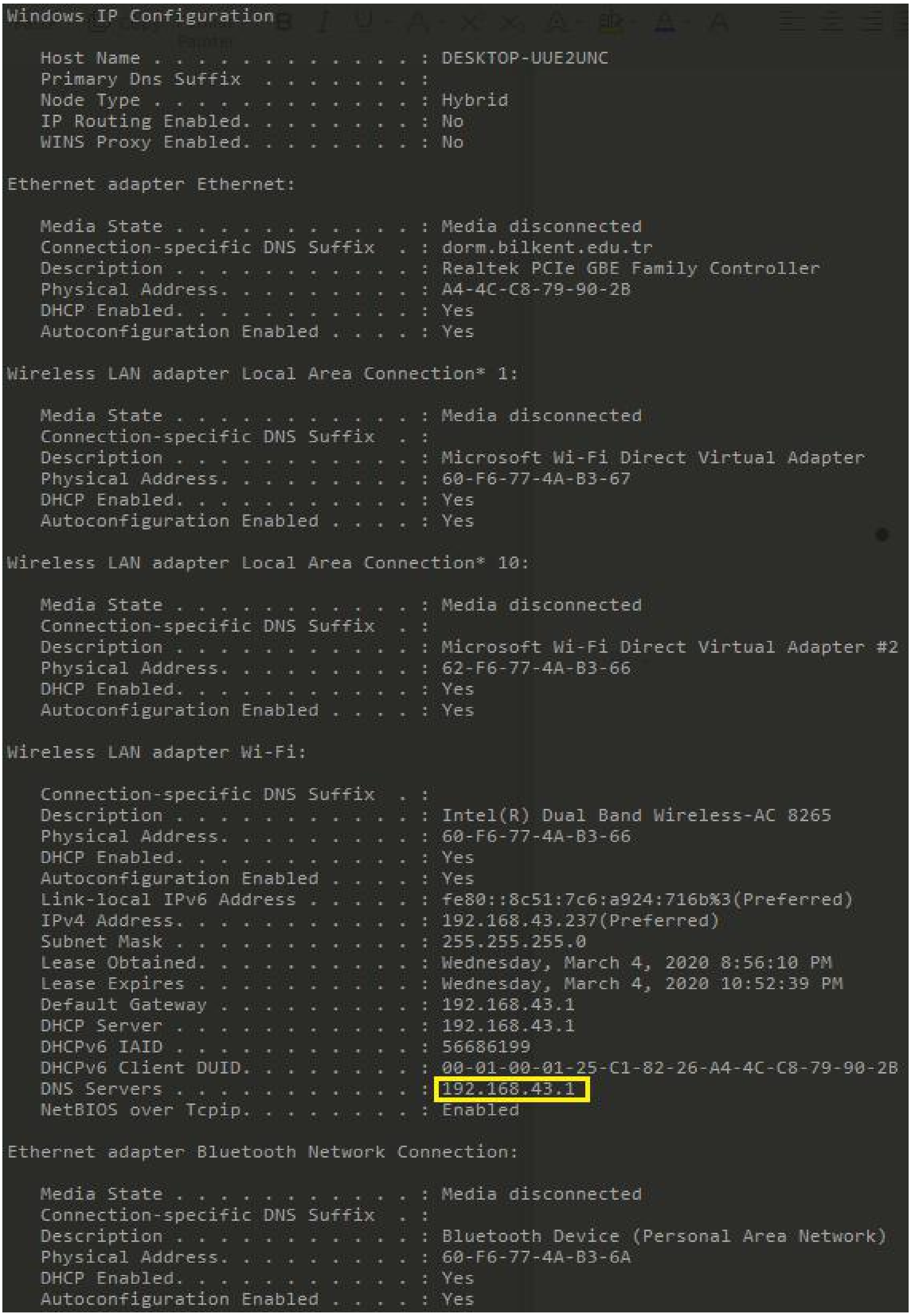
```
No.     Time            Source           Destination      Protocol Length Info
    647 21:29:50.274361 172.217.169.100  192.168.43.237   UDP      1392 443 → 53434 Len=1350
    648 21:29:50.276726 172.217.169.100  192.168.43.237   UDP      1392 443 → 53434 Len=1350
    649 21:29:50.277043 192.168.43.237   172.217.169.100  UDP        70 53434 → 443 Len=28
    650 21:29:50.279328 172.217.169.100  192.168.43.237   UDP      1392 443 → 53434 Len=1350
    651 21:29:50.279608 192.168.43.237   192.168.43.1     DNS        72 Standard query 0x1e11 A www.ietf.org
    652 21:29:50.280354 172.217.169.100  192.168.43.237   UDP      1392 443 → 53434 Len=1350
    653 21:29:50.281336 172.217.169.100  192.168.43.237   UDP      1392 443 → 53434 Len=1350
    654 21:29:50.283515 192.168.43.1     192.168.43.237   DNS       149 Standard query response 0x1e11 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85

> Frame 654: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{13497363-D49A-493A-AE9F-1A7B94492E12}, id 0
> Ethernet II, Src: XiaomiCo_04:e7:ef (58:20:59:04:e7:ef), Dst: IntelCor_4a:b3:66 (60:f6:77:4a:b3:66)
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.237
> User Datagram Protocol, Src Port: 53, Dst Port: 49230
> Domain Name System (response)
```

Both destination port of DNS query message and source port of DNS response messages are 53.

Question6



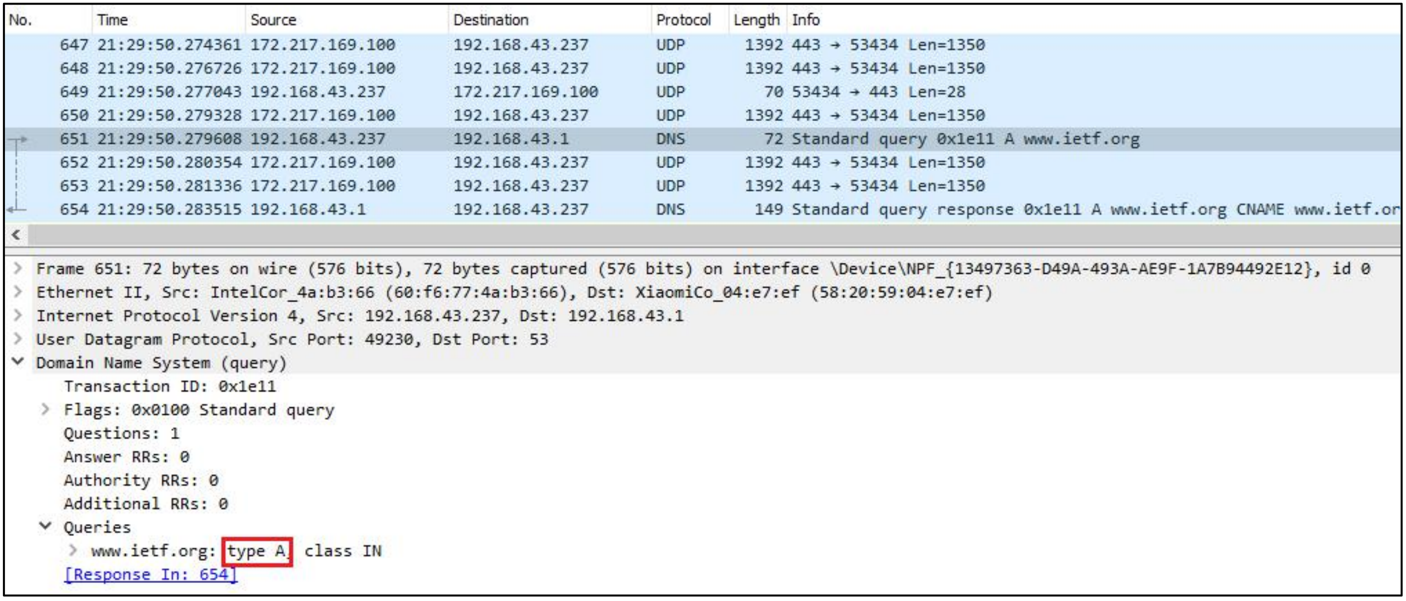
```
647 21:29:50.274361 172.217.169.100    192.168.43.237     UDP     1392 443 → 53434 Len=1350
648 21:29:50.276726 172.217.169.100    192.168.43.237     UDP     1392 443 → 53434 Len=1350
649 21:29:50.277043 192.168.43.237     172.217.169.100    UDP       70 53434 → 443 Len=28
650 21:29:50.279328 172.217.169.100    192.168.43.237     UDP     1392 443 → 53434 Len=1350
651 21:29:50.279608 192.168.43.237     192.168.43.1       DNS       72 Standard query 0x1e11 A www.ietf.org
652 21:29:50.280354 172.217.169.100    192.168.43.237     UDP     1392 443 → 53434 Len=1350
653 21:29:50.281336 172.217.169.100    192.168.43.237     UDP     1392 443 → 53434 Len=1350
654 21:29:50.283515 192.168.43.1       192.168.43.237     DNS      149 Standard query response 0x1e11 A www.i
```



```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-UUE2UNC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : dorm.bilkent.edu.tr
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : A4-4C-C8-79-90-2B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 60-F6-77-4A-B3-67
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 62-F6-77-4A-B3-66
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : 60-F6-77-4A-B3-66
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::8c51:7c6:a924:716b%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.43.237(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, March 4, 2020 8:56:10 PM
   Lease Expires . . . . . . . . . . : Wednesday, March 4, 2020 10:52:39 PM
   Default Gateway . . . . . . . . . : 192.168.43.1
   DHCP Server . . . . . . . . . . . : 192.168.43.1
   DHCPv6 IAID . . . . . . . . . . . : 56686199
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-C1-82-26-A4-4C-C8-79-90-2B
   DNS Servers . . . . . . . . . . . : 192.168.43.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 60-F6-77-4A-B3-6A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

It has been sent to **192.168.43.1.** This is also my local DNS server. This is obtained from ipconfig/all command and indicated above.

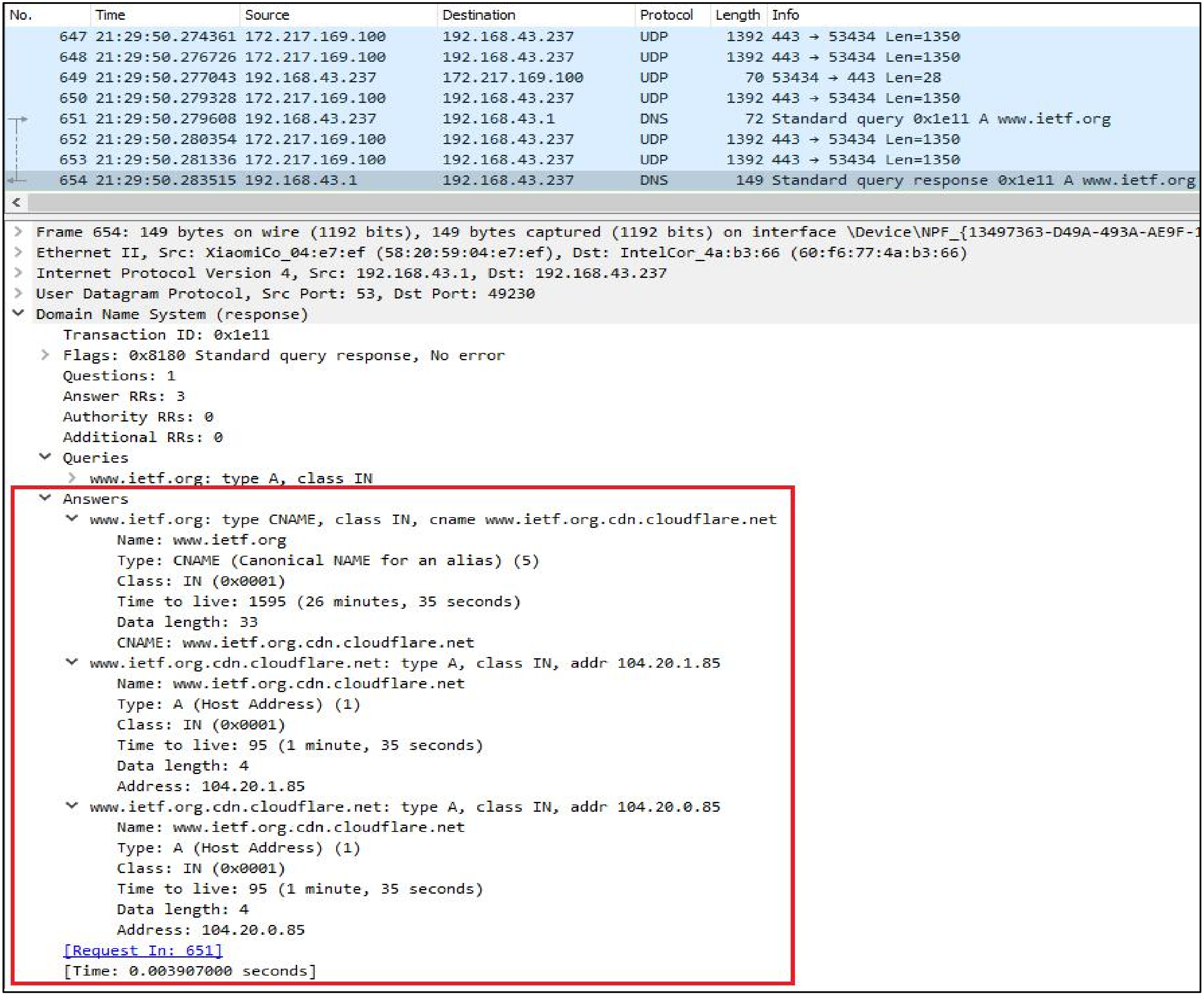
Question7



```
No.   Time             Source          Destination     Protocol Length Info
  647 21:29:50.274361 172.217.169.100 192.168.43.237  UDP      1392 443 → 53434 Len=1350
  648 21:29:50.276726 172.217.169.100 192.168.43.237  UDP      1392 443 → 53434 Len=1350
  649 21:29:50.277043 192.168.43.237  172.217.169.100 UDP        70 53434 → 443 Len=28
  650 21:29:50.279328 172.217.169.100 192.168.43.237  UDP      1392 443 → 53434 Len=1350
  651 21:29:50.279608 192.168.43.237  192.168.43.1    DNS        72 Standard query 0x1e11 A www.ietf.org
  652 21:29:50.280354 172.217.169.100 192.168.43.237  UDP      1392 443 → 53434 Len=1350
  653 21:29:50.281336 172.217.169.100 192.168.43.237  UDP      1392 443 → 53434 Len=1350
  654 21:29:50.283515 192.168.43.1    192.168.43.237  DNS       149 Standard query response 0x1e11 A www.ietf.org CNAME www.ietf.or

> Frame 651: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{13497363-D49A-493A-AE9F-1A7B94492E12}, id 0
> Ethernet II, Src: IntelCor_4a:b3:66 (60:f6:77:4a:b3:66), Dst: XiaomiCo_04:e7:ef (58:20:59:04:e7:ef)
> Internet Protocol Version 4, Src: 192.168.43.237, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 49230, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x1e11
  > 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: 654]
```

Yes, it is a Type A query message.

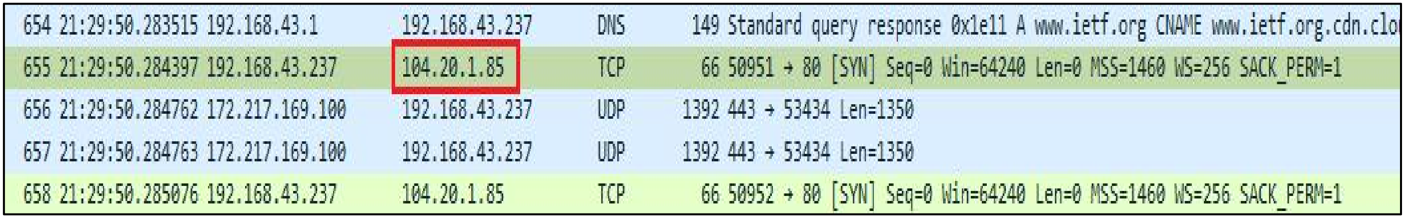
Question8



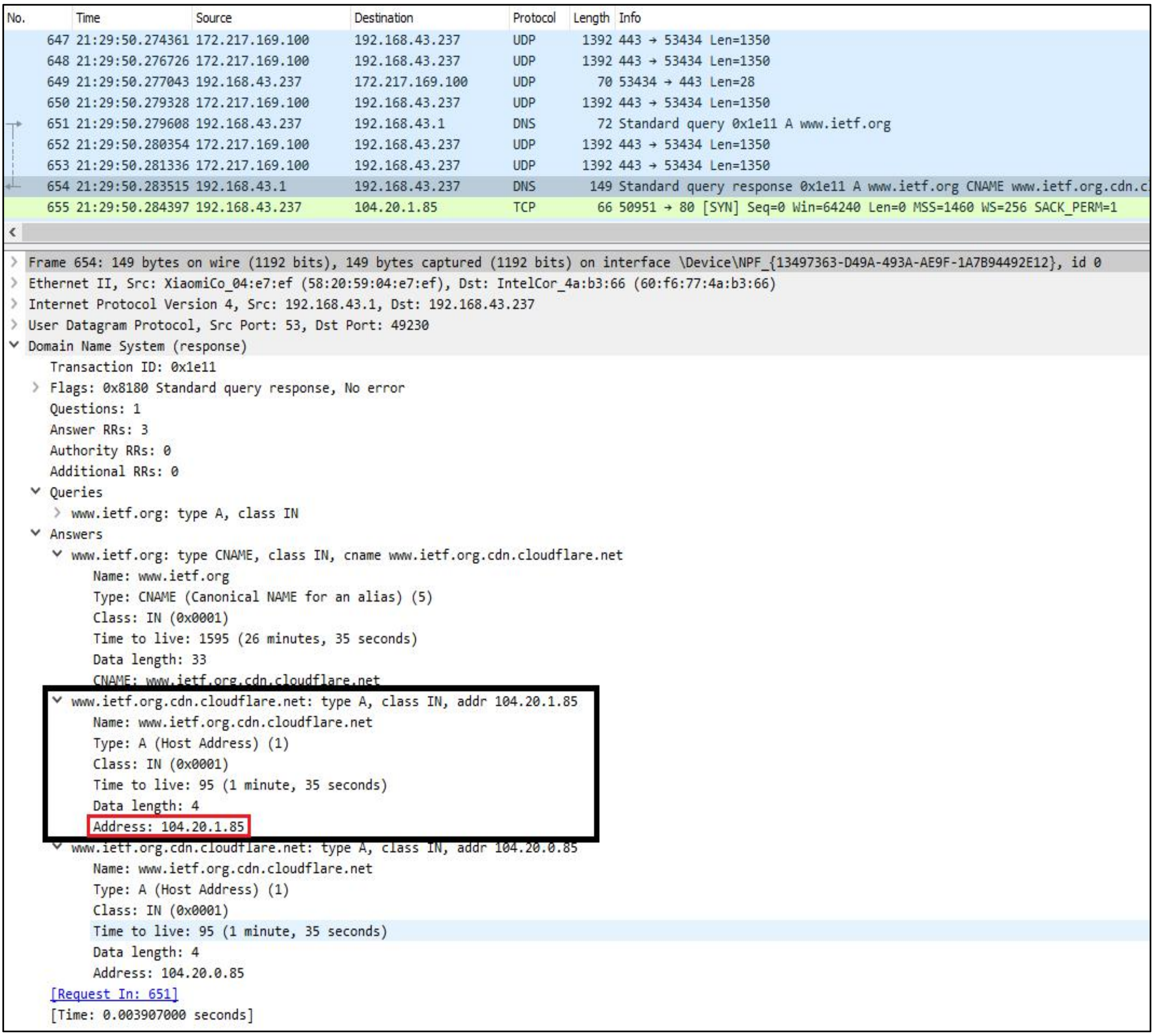
```
No.   Time             Source          Destination     Protocol Length Info
  647 21:29:50.274361 172.217.169.100 192.168.43.237  UDP      1392 443 → 53434 Len=1350
  648 21:29:50.276726 172.217.169.100 192.168.43.237  UDP      1392 443 → 53434 Len=1350
  649 21:29:50.277043 192.168.43.237  172.217.169.100 UDP        70 53434 → 443 Len=28
  650 21:29:50.279328 172.217.169.100 192.168.43.237  UDP      1392 443 → 53434 Len=1350
  651 21:29:50.279608 192.168.43.237  192.168.43.1    DNS        72 Standard query 0x1e11 A www.ietf.org
  652 21:29:50.280354 172.217.169.100 192.168.43.237  UDP      1392 443 → 53434 Len=1350
  653 21:29:50.281336 172.217.169.100 192.168.43.237  UDP      1392 443 → 53434 Len=1350
  654 21:29:50.283515 192.168.43.1    192.168.43.237  DNS       149 Standard query response 0x1e11 A www.ietf.org

> Frame 654: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{13497363-D49A-493A-AE9F-1
> Ethernet II, Src: XiaomiCo_04:e7:ef (58:20:59:04:e7:ef), Dst: IntelCor_4a:b3:66 (60:f6:77:4a:b3:66)
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.237
> User Datagram Protocol, Src Port: 53, Dst Port: 49230
v Domain Name System (response)
    Transaction ID: 0x1e11
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
  v Answers
    v www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
        Name: www.ietf.org
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1595 (26 minutes, 35 seconds)
        Data length: 33
        CNAME: www.ietf.org.cdn.cloudflare.net
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
        Name: www.ietf.org.cdn.cloudflare.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 95 (1 minute, 35 seconds)
        Data length: 4
        Address: 104.20.1.85
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
        Name: www.ietf.org.cdn.cloudflare.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 95 (1 minute, 35 seconds)
        Data length: 4
        Address: 104.20.0.85
    [Request In: 651]
    [Time: 0.003907000 seconds]
```

3 answers are provided. All of them contains name of the host and also the type of address, class, the TTL, data length. Importantly, the first one is a CNAME type record response, whereas the remaining two are A type record responses. That's why, canonical name is presented in the first one and the others contain IP addresses.

Question9



```
654 21:29:50.283515 192.168.43.1     192.168.43.237   DNS    149 Standard query response 0x1e11 A www.ietf.org CNAME www.ietf.org.cdn.clo
655 21:29:50.284397 192.168.43.237   104.20.1.85      TCP     66 50951 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
656 21:29:50.284762 172.217.169.100  192.168.43.237   UDP   1392 443 → 53434 Len=1350
657 21:29:50.284763 172.217.169.100  192.168.43.237   UDP   1392 443 → 53434 Len=1350
658 21:29:50.285076 192.168.43.237   104.20.1.85      TCP     66 50952 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```



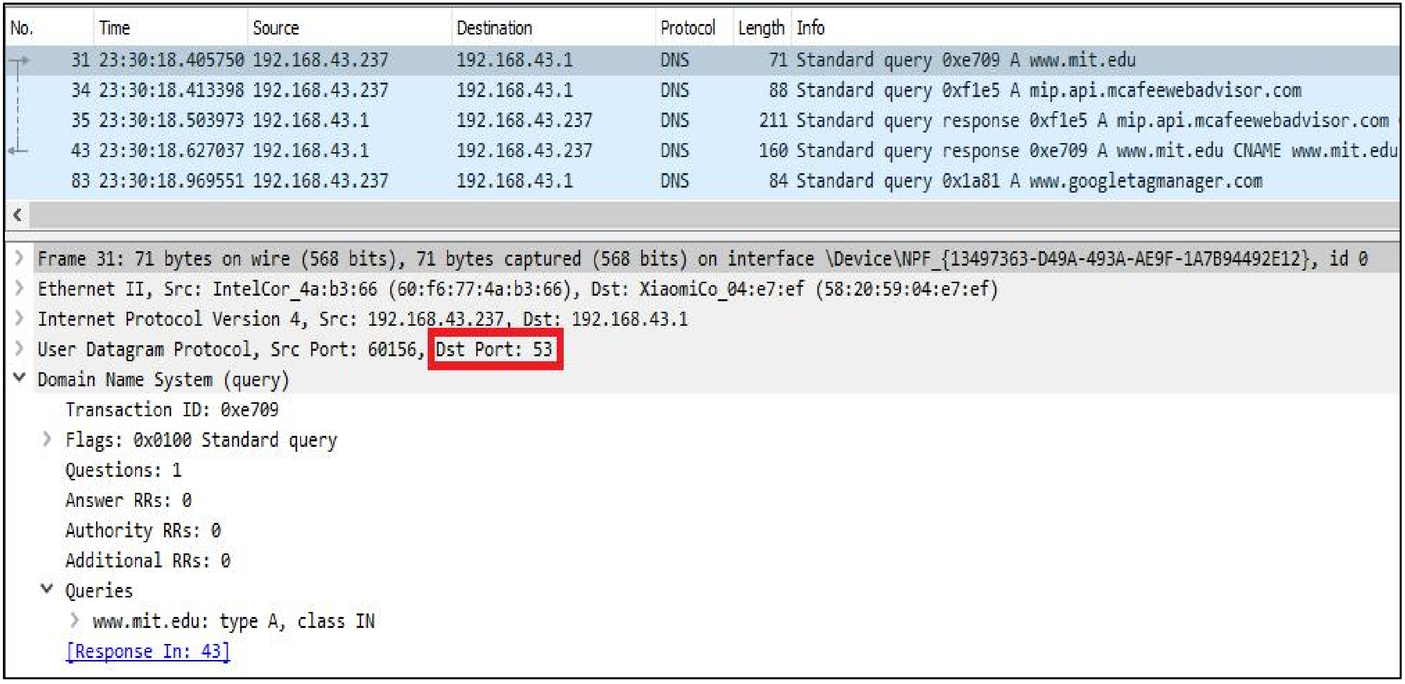
```
No.   Time               Source            Destination       Protocol  Length  Info
  647 21:29:50.274361 172.217.169.100   192.168.43.237    UDP       1392 443 → 53434 Len=1350
  648 21:29:50.276726 172.217.169.100   192.168.43.237    UDP       1392 443 → 53434 Len=1350
  649 21:29:50.277043 192.168.43.237    172.217.169.100   UDP         70 53434 → 443 Len=28
  650 21:29:50.279328 172.217.169.100   192.168.43.237    UDP       1392 443 → 53434 Len=1350
  651 21:29:50.279608 192.168.43.237    192.168.43.1      DNS         72 Standard query 0x1e11 A www.ietf.org
  652 21:29:50.280354 172.217.169.100   192.168.43.237    UDP       1392 443 → 53434 Len=1350
  653 21:29:50.281336 172.217.169.100   192.168.43.237    UDP       1392 443 → 53434 Len=1350
  654 21:29:50.283515 192.168.43.1      192.168.43.237    DNS        149 Standard query response 0x1e11 A www.ietf.org CNAME www.ietf.org.cdn.c
  655 21:29:50.284397 192.168.43.237    104.20.1.85       TCP         66 50951 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 654: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{13497363-D49A-493A-AE9F-1A7B94492E12}, id 0
> Ethernet II, Src: XiaomiCo_04:e7:ef (58:20:59:04:e7:ef), Dst: IntelCor_4a:b3:66 (60:f6:77:4a:b3:66)
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.237
> User Datagram Protocol, Src Port: 53, Dst Port: 49230
v Domain Name System (response)
    Transaction ID: 0x1e11
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
  v Answers
    v www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
        Name: www.ietf.org
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1595 (26 minutes, 35 seconds)
        Data length: 33
        CNAME: www.ietf.org.cdn.cloudflare.net
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
        Name: www.ietf.org.cdn.cloudflare.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 95 (1 minute, 35 seconds)
        Data length: 4
        Address: 104.20.1.85
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
        Name: www.ietf.org.cdn.cloudflare.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 95 (1 minute, 35 seconds)
        Data length: 4
        Address: 104.20.0.85
    [Request In: 651]
    [Time: 0.003907000 seconds]
```

Yes, it does with the one of the answers. It has been indicated in the above figures.

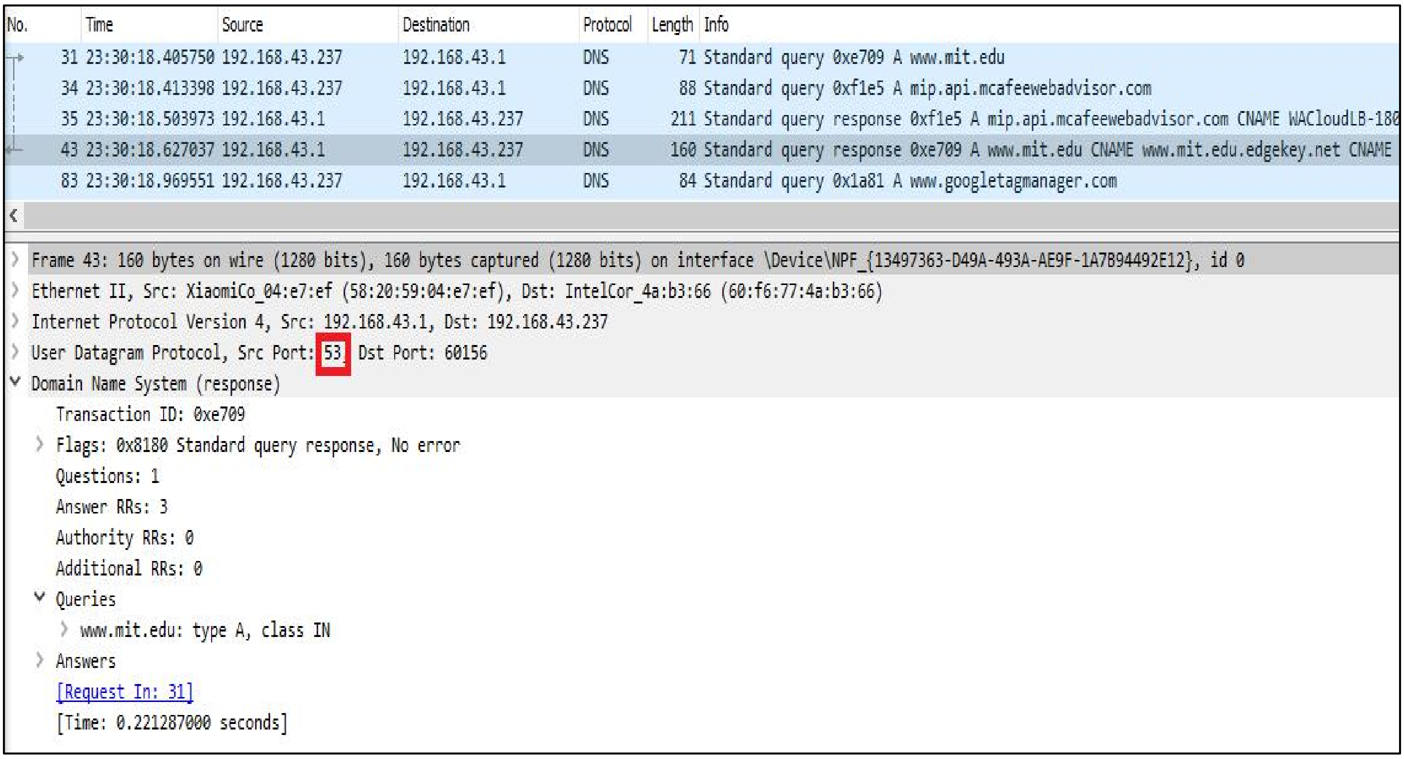
Question10

There is only one DNS query. Hence, there are not any additional DNS queries are done for images.

Question11



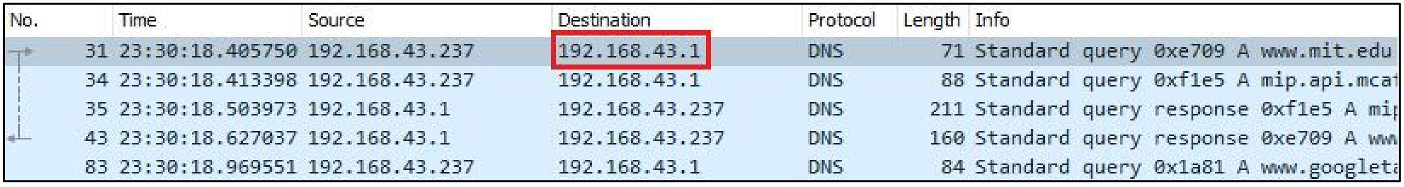
```
No.   Time                Source          Destination     Protocol Length Info
   31 23:30:18.405750 192.168.43.237  192.168.43.1    DNS        71 Standard query 0xe709 A www.mit.edu
   34 23:30:18.413398 192.168.43.237  192.168.43.1    DNS        88 Standard query 0xf1e5 A mip.api.mcafeewebadvisor.com
   35 23:30:18.503973 192.168.43.1    192.168.43.237  DNS       211 Standard query response 0xf1e5 A mip.api.mcafeewebadvisor.com
   43 23:30:18.627037 192.168.43.1    192.168.43.237  DNS       160 Standard query response 0xe709 A www.mit.edu CNAME www.mit.edu
   83 23:30:18.969551 192.168.43.237  192.168.43.1    DNS        84 Standard query 0x1a81 A www.googletagmanager.com

> Frame 31: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{13497363-D49A-493A-AE9F-1A7B94492E12}, id 0
> Ethernet II, Src: IntelCor_4a:b3:66 (60:f6:77:4a:b3:66), Dst: XiaomiCo_04:e7:ef (58:20:59:04:e7:ef)
> Internet Protocol Version 4, Src: 192.168.43.237, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 60156, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xe709
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.mit.edu: type A, class IN
    [Response In: 43]
```



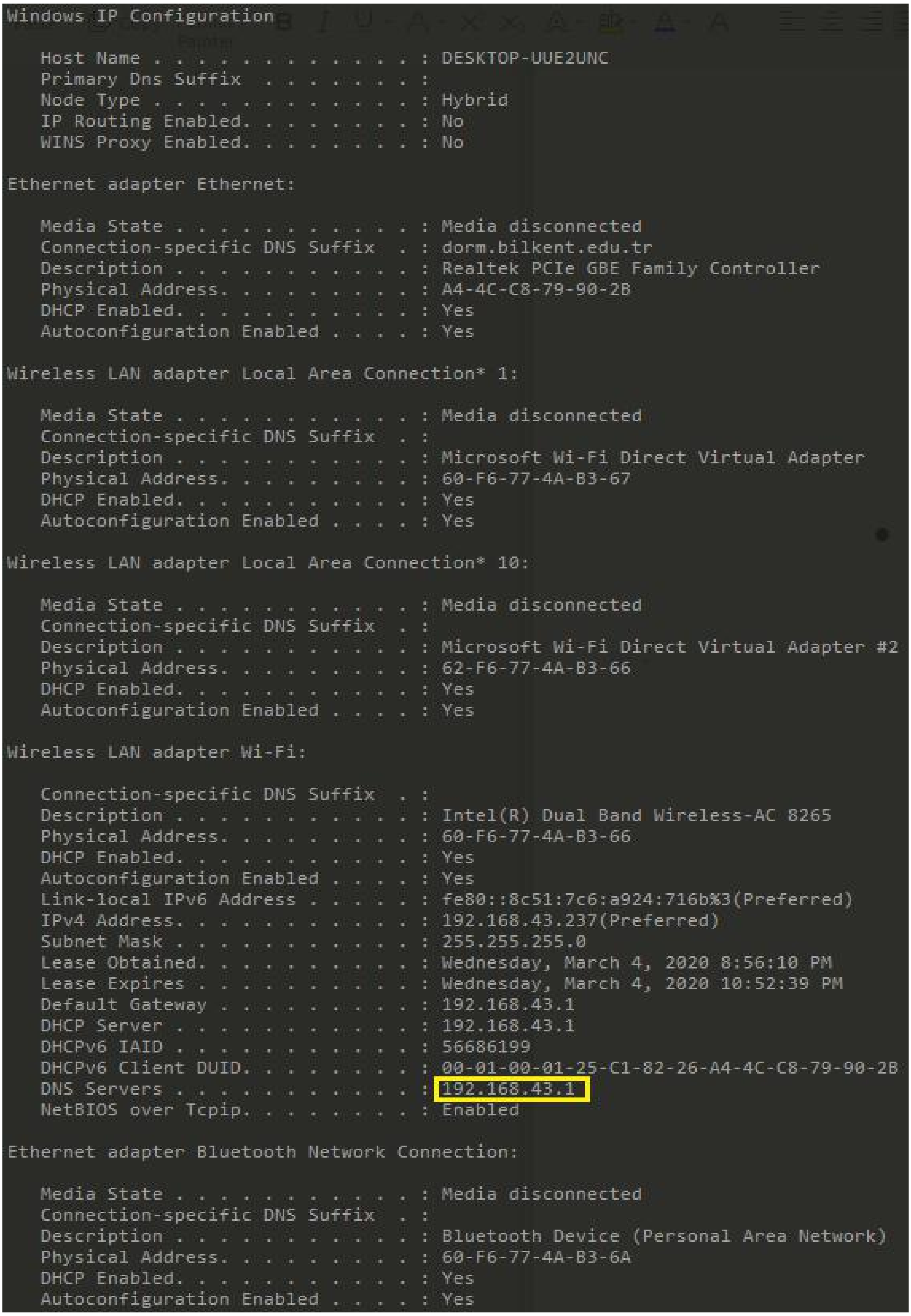
```
No.   Time                Source          Destination     Protocol Length Info
   31 23:30:18.405750 192.168.43.237  192.168.43.1    DNS        71 Standard query 0xe709 A www.mit.edu
   34 23:30:18.413398 192.168.43.237  192.168.43.1    DNS        88 Standard query 0xf1e5 A mip.api.mcafeewebadvisor.com
   35 23:30:18.503973 192.168.43.1    192.168.43.237  DNS       211 Standard query response 0xf1e5 A mip.api.mcafeewebadvisor.com CNAME WACloudLB-180
   43 23:30:18.627037 192.168.43.1    192.168.43.237  DNS       160 Standard query response 0xe709 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME
   83 23:30:18.969551 192.168.43.237  192.168.43.1    DNS        84 Standard query 0x1a81 A www.googletagmanager.com

> Frame 43: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{13497363-D49A-493A-AE9F-1A7B94492E12}, id 0
> Ethernet II, Src: XiaomiCo_04:e7:ef (58:20:59:04:e7:ef), Dst: IntelCor_4a:b3:66 (60:f6:77:4a:b3:66)
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.237
> User Datagram Protocol, Src Port: 53, Dst Port: 60156
v Domain Name System (response)
    Transaction ID: 0xe709
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.mit.edu: type A, class IN
  > Answers
    [Request In: 31]
    [Time: 0.221287000 seconds]
```

Both destination port of DNS query message and source port of DNS response messages are 53.

Question12



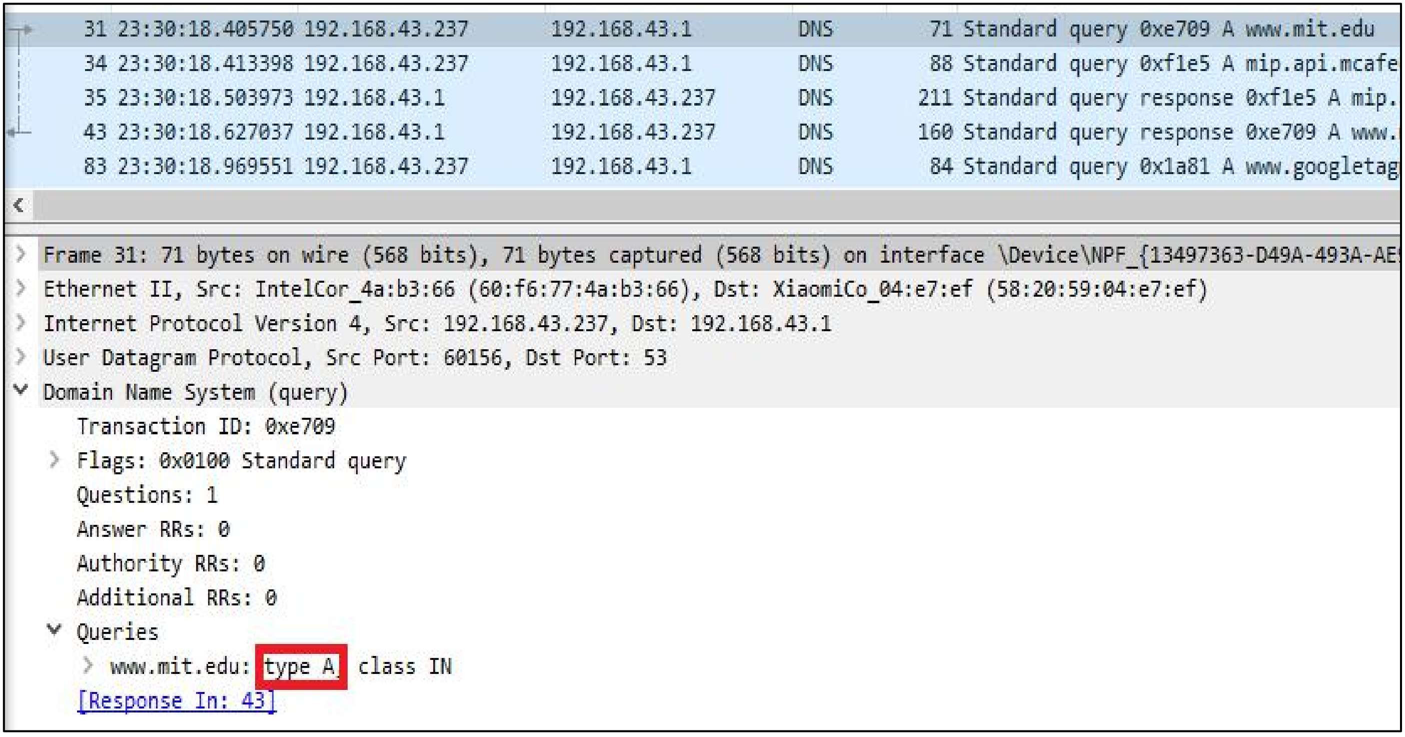
No.	Time	Source	Destination	Protocol	Length	Info
31	23:30:18.405750	192.168.43.237	192.168.43.1	DNS	71	Standard query 0xe709 A www.mit.edu
34	23:30:18.413398	192.168.43.237	192.168.43.1	DNS	88	Standard query 0xf1e5 A mip.api.mcat
35	23:30:18.503973	192.168.43.1	192.168.43.237	DNS	211	Standard query response 0xf1e5 A mip
43	23:30:18.627037	192.168.43.1	192.168.43.237	DNS	160	Standard query response 0xe709 A www
83	23:30:18.969551	192.168.43.237	192.168.43.1	DNS	84	Standard query 0x1a81 A www.googleta



```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-UUE2UNC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : dorm.bilkent.edu.tr
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : A4-4C-C8-79-90-2B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 60-F6-77-4A-B3-67
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 62-F6-77-4A-B3-66
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : 60-F6-77-4A-B3-66
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::8c51:7c6:a924:716b%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.43.237(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, March 4, 2020 8:56:10 PM
   Lease Expires . . . . . . . . . . : Wednesday, March 4, 2020 10:52:39 PM
   Default Gateway . . . . . . . . . : 192.168.43.1
   DHCP Server . . . . . . . . . . . : 192.168.43.1
   DHCPv6 IAID . . . . . . . . . . . : 56686199
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-C1-82-26-A4-4C-C8-79-90-2B
   DNS Servers . . . . . . . . . . . : 192.168.43.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 60-F6-77-4A-B3-6A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

It has been sent to **192.168.43.1.** This is also my local DNS server. This is obtained from ipconfig/all command and indicated above.

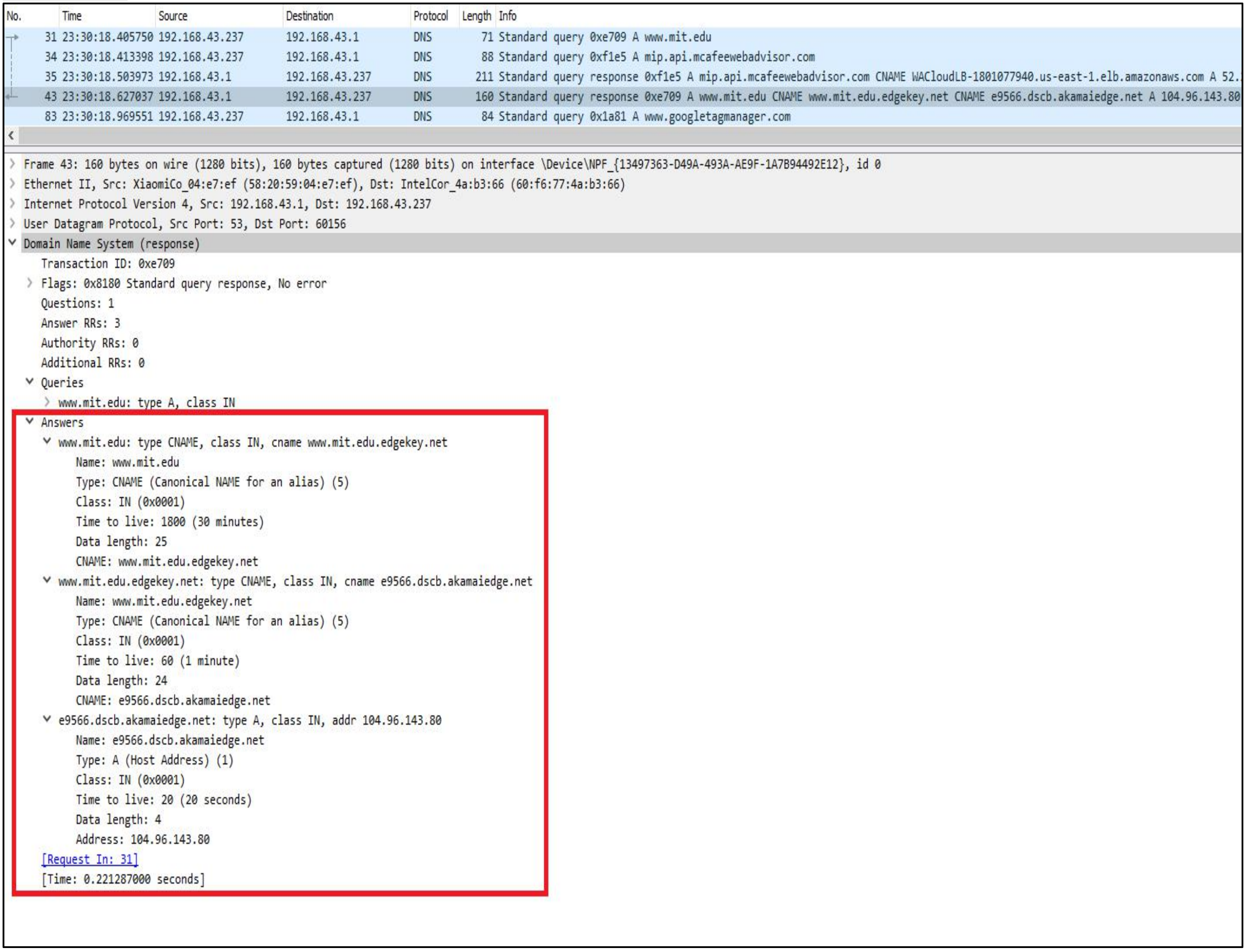
Question13



```
31 23:30:18.405750 192.168.43.237    192.168.43.1      DNS    71 Standard query 0xe709 A www.mit.edu
34 23:30:18.413398 192.168.43.237    192.168.43.1      DNS    88 Standard query 0xf1e5 A mip.api.mcafe
35 23:30:18.503973 192.168.43.1      192.168.43.237    DNS   211 Standard query response 0xf1e5 A mip.
43 23:30:18.627037 192.168.43.1      192.168.43.237    DNS   160 Standard query response 0xe709 A www.
83 23:30:18.969551 192.168.43.237    192.168.43.1      DNS    84 Standard query 0x1a81 A www.googletag

> Frame 31: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{13497363-D49A-493A-AE
> Ethernet II, Src: IntelCor_4a:b3:66 (60:f6:77:4a:b3:66), Dst: XiaomiCo_04:e7:ef (58:20:59:04:e7:ef)
> Internet Protocol Version 4, Src: 192.168.43.237, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 60156, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xe709
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.mit.edu: type A, class IN
    [Response In: 43]
```

It is a Type A query message. There are no answers in query message.

Question14



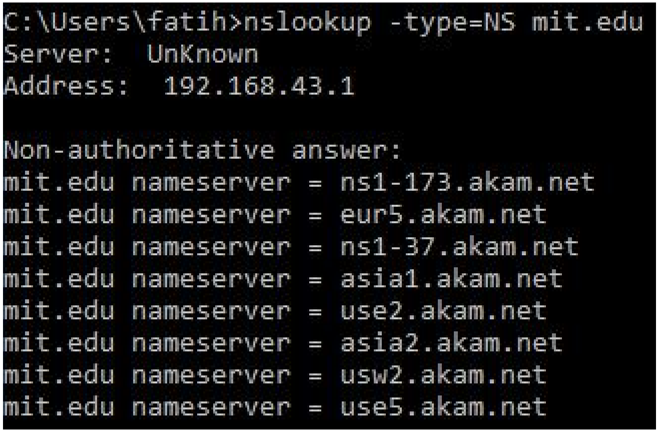
```
No.   Time               Source            Destination       Protocol Length Info
   31 23:30:18.405750 192.168.43.237    192.168.43.1      DNS       71 Standard query 0xe709 A www.mit.edu
   34 23:30:18.413398 192.168.43.237    192.168.43.1      DNS       88 Standard query 0xf1e5 A mip.api.mcafeewebadvisor.com
   35 23:30:18.503973 192.168.43.1      192.168.43.237    DNS      211 Standard query response 0xf1e5 A mip.api.mcafeewebadvisor.com CNAME WACloudLB-1801077940.us-east-1.elb.amazonaws.com A 52.
   43 23:30:18.627037 192.168.43.1      192.168.43.237    DNS      160 Standard query response 0xe709 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.96.143.80
   83 23:30:18.969551 192.168.43.237    192.168.43.1      DNS       84 Standard query 0x1a81 A www.googletagmanager.com

> Frame 43: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{13497363-D49A-493A-AE9F-1A7B94492E12}, id 0
> Ethernet II, Src: XiaomiCo_04:e7:ef (58:20:59:04:e7:ef), Dst: IntelCor_4a:b3:66 (60:f6:77:4a:b3:66)
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.237
> User Datagram Protocol, Src Port: 53, Dst Port: 60156
v Domain Name System (response)
    Transaction ID: 0xe709
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.mit.edu: type A, class IN
  v Answers
    v 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: 1800 (30 minutes)
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
    v 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: 60 (1 minute)
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
    v e9566.dscb.akamaiedge.net: type A, class IN, addr 104.96.143.80
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 4
        Address: 104.96.143.80
    [Request In: 31]
    [Time: 0.221287000 seconds]
```

3 answers are provided. All of them contains name of the host and also the type of address, class, the TTL, data length. Importantly, the first two are CNAME type record responses, whereas the remaining one is an A type record response. That's why, canonical names are presented in the first two answers and the last one contains IP address.

Question15

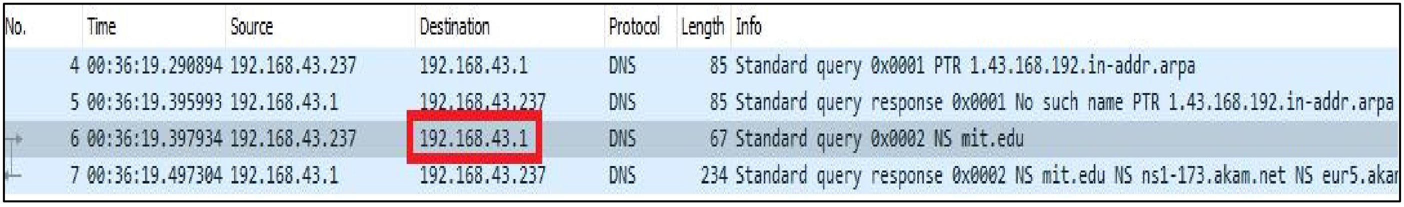
For each question, I have already provided a screenshot.

Typing to command line the command.

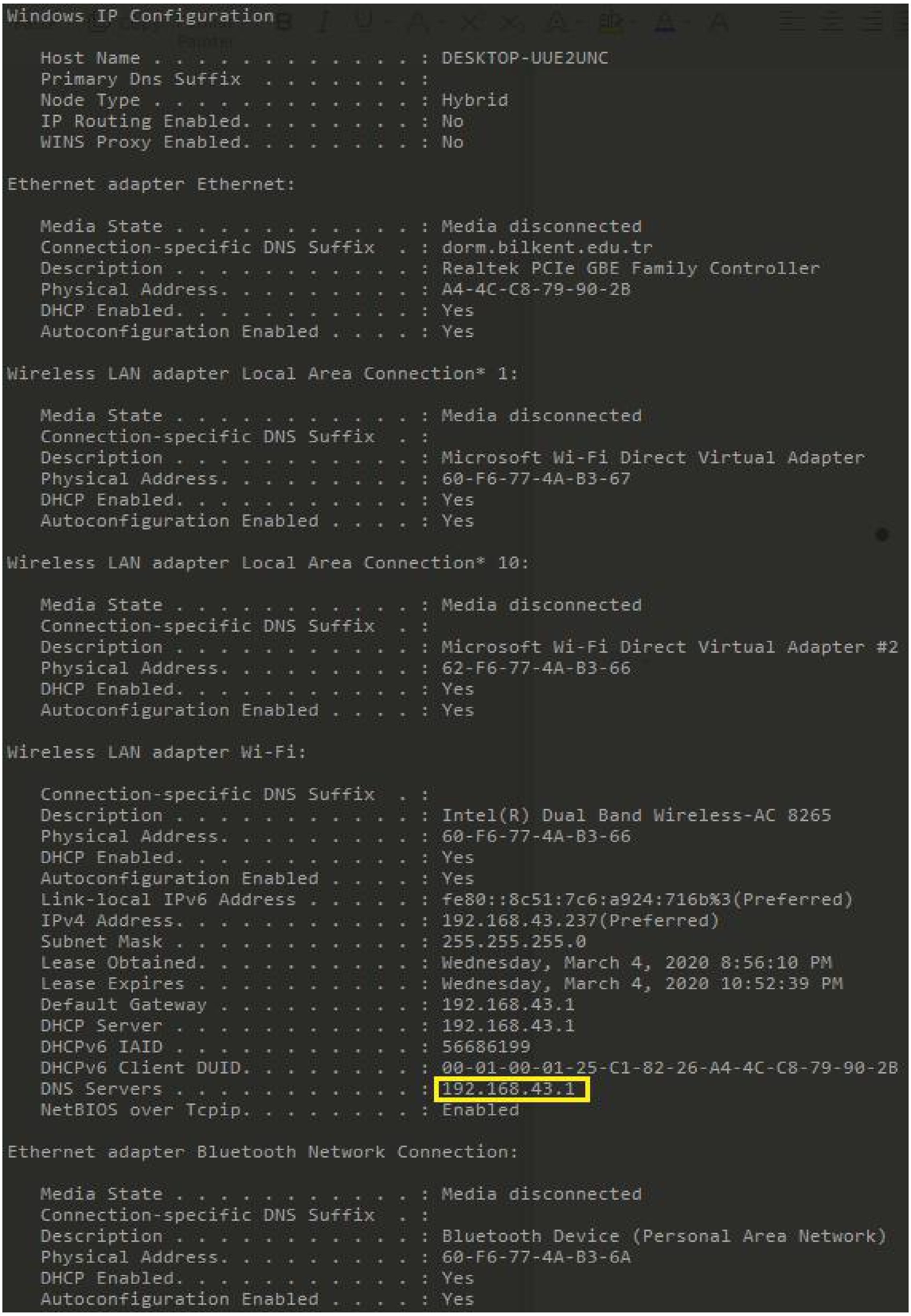


```
C:\Users\fatih>nslookup -type=NS mit.edu
Server:  UnKnown
Address:  192.168.43.1

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

Question16



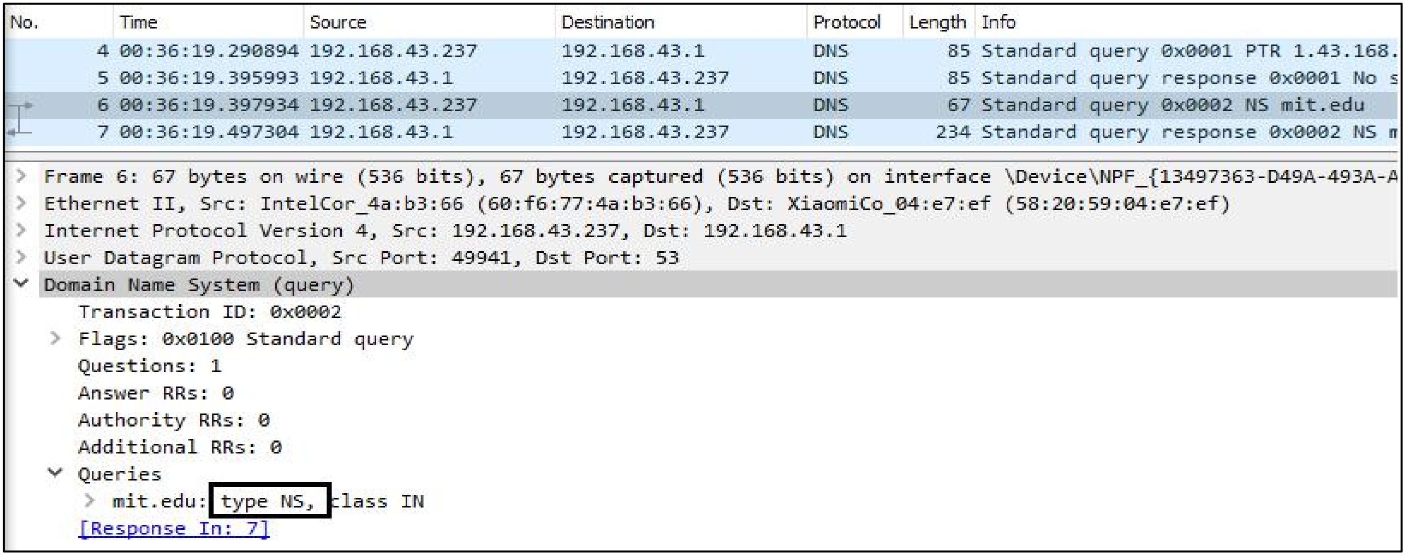
No.	Time	Source	Destination	Protocol	Length	Info
4	00:36:19.290894	192.168.43.237	192.168.43.1	DNS	85	Standard query 0x0001 PTR 1.43.168.192.in-addr.arpa
5	00:36:19.395993	192.168.43.1	192.168.43.237	DNS	85	Standard query response 0x0001 No such name PTR 1.43.168.192.in-addr.arpa
6	00:36:19.397934	192.168.43.237	192.168.43.1	DNS	67	Standard query 0x0002 NS mit.edu
7	00:36:19.497304	192.168.43.1	192.168.43.237	DNS	234	Standard query response 0x0002 NS mit.edu NS ns1-173.akam.net NS eur5.akar



```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-UUE2UNC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : dorm.bilkent.edu.tr
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : A4-4C-C8-79-90-2B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 60-F6-77-4A-B3-67
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 62-F6-77-4A-B3-66
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : 60-F6-77-4A-B3-66
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::8c51:7c6:a924:716b%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.43.237(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, March 4, 2020 8:56:10 PM
   Lease Expires . . . . . . . . . . : Wednesday, March 4, 2020 10:52:39 PM
   Default Gateway . . . . . . . . . : 192.168.43.1
   DHCP Server . . . . . . . . . . . : 192.168.43.1
   DHCPv6 IAID . . . . . . . . . . . : 56686199
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-C1-82-26-A4-4C-C8-79-90-2B
   DNS Servers . . . . . . . . . . . : 192.168.43.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 60-F6-77-4A-B3-6A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

It has been sent to **192.168.43.1.** This is also my local DNS server. This is obtained from ipconfig/all command and indicated above.

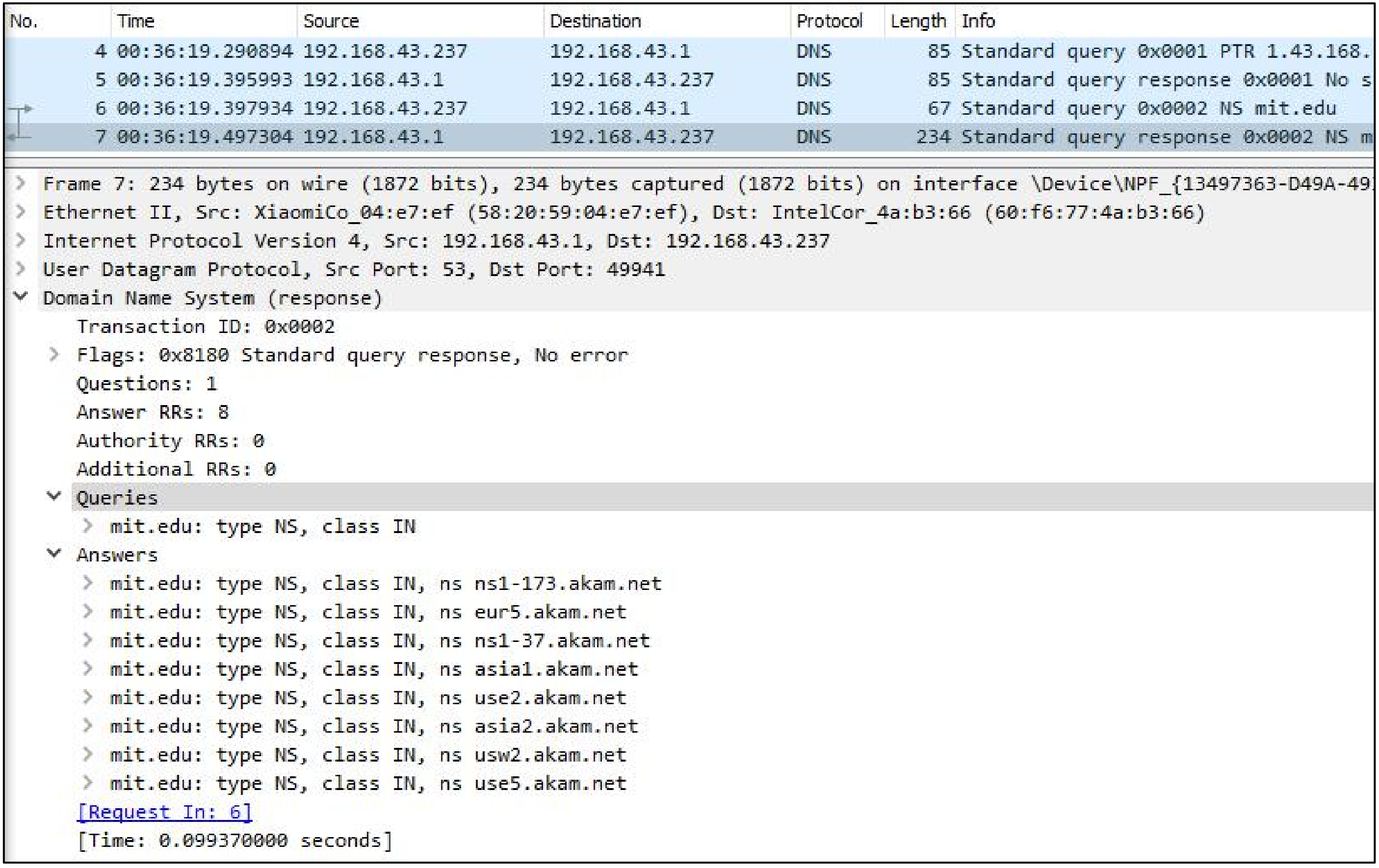
Question17



```
No.         Time            Source            Destination       Protocol  Length Info
      4 00:36:19.290894 192.168.43.237    192.168.43.1      DNS         85 Standard query 0x0001 PTR 1.43.168.
      5 00:36:19.395993 192.168.43.1      192.168.43.237    DNS         85 Standard query response 0x0001 No s
      6 00:36:19.397934 192.168.43.237    192.168.43.1      DNS         67 Standard query 0x0002 NS mit.edu
      7 00:36:19.497304 192.168.43.1      192.168.43.237    DNS        234 Standard query response 0x0002 NS m

> Frame 6: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{13497363-D49A-493A-A
> Ethernet II, Src: IntelCor_4a:b3:66 (60:f6:77:4a:b3:66), Dst: XiaomiCo_04:e7:ef (58:20:59:04:e7:ef)
> Internet Protocol Version 4, Src: 192.168.43.237, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 49941, 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: type NS, class IN
     [Response In: 7]
```

It is a Type NS query message. There are no answers in query message.

Question18



```
No.         Time            Source            Destination       Protocol  Length Info
      4 00:36:19.290894 192.168.43.237    192.168.43.1      DNS         85 Standard query 0x0001 PTR 1.43.168.
      5 00:36:19.395993 192.168.43.1      192.168.43.237    DNS         85 Standard query response 0x0001 No s
      6 00:36:19.397934 192.168.43.237    192.168.43.1      DNS         67 Standard query 0x0002 NS mit.edu
      7 00:36:19.497304 192.168.43.1      192.168.43.237    DNS        234 Standard query response 0x0002 NS m

> Frame 7: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{13497363-D49A-49
> Ethernet II, Src: XiaomiCo_04:e7:ef (58:20:59:04:e7:ef), Dst: IntelCor_4a:b3:66 (60:f6:77:4a:b3:66)
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.237
> User Datagram Protocol, Src Port: 53, Dst Port: 49941
v Domain Name System (response)
     Transaction ID: 0x0002
   > Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 8
     Authority RRs: 0
     Additional RRs: 0
   v Queries
     > mit.edu: type NS, class IN
   v Answers
     > mit.edu: type NS, class IN, ns ns1-173.akam.net
     > mit.edu: type NS, class IN, ns eur5.akam.net
     > mit.edu: type NS, class IN, ns ns1-37.akam.net
     > mit.edu: type NS, class IN, ns asia1.akam.net
     > mit.edu: type NS, class IN, ns use2.akam.net
     > mit.edu: type NS, class IN, ns asia2.akam.net
     > mit.edu: type NS, class IN, ns usw2.akam.net
     > mit.edu: type NS, class IN, ns use5.akam.net
     [Request In: 6]
     [Time: 0.099370000 seconds]
```

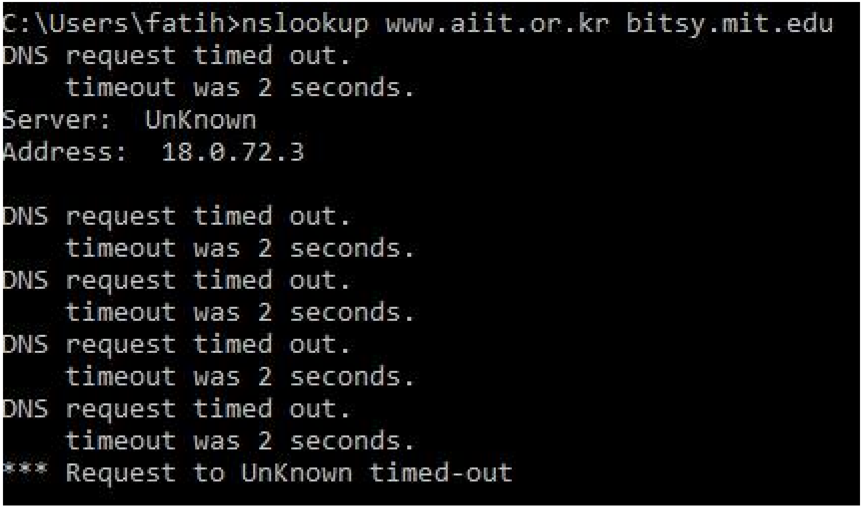
- ns1-173.akam.net
- eur5.akam.net
- ns1-37.akam.net
- asia1.akam.net
- use2.akam.net
- asia2.akam.net
- usw2.akam.net
- use5.akam.net

The message does not provide IP addresses of the name servers.

Question19

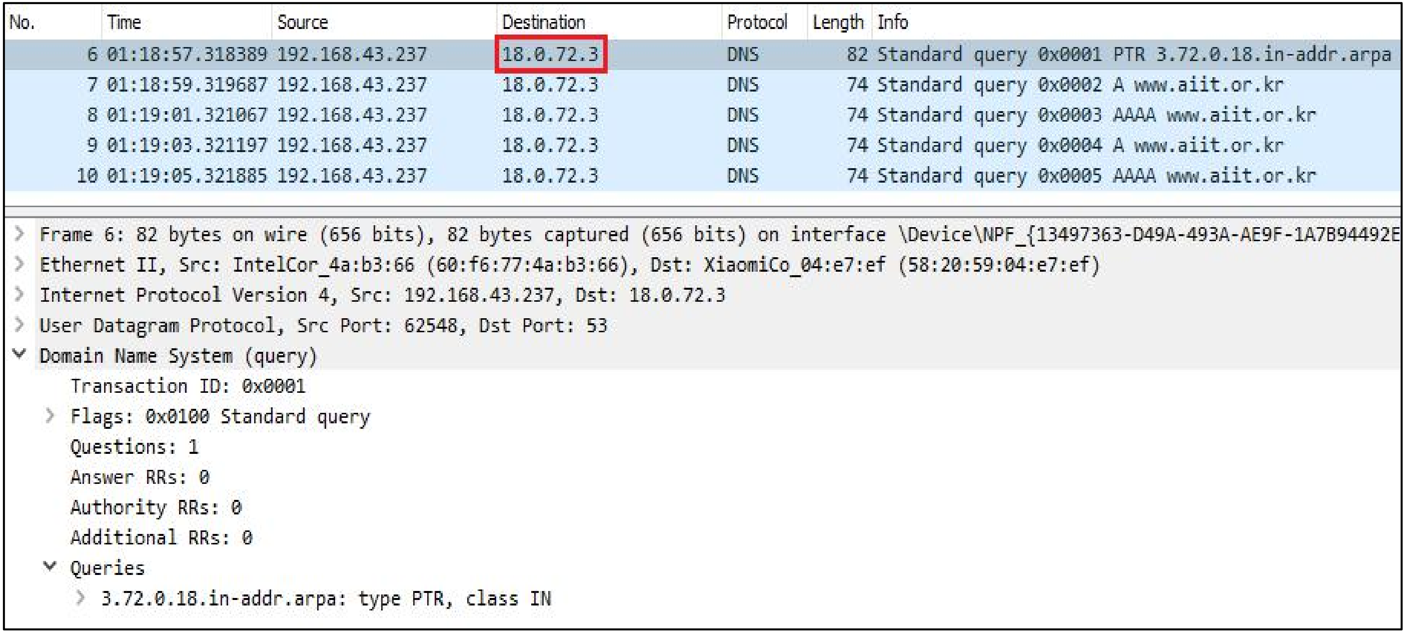
The screen shots are provided in the previous questions.

After typing the command to command line



```
C:\Users\fatih>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
```

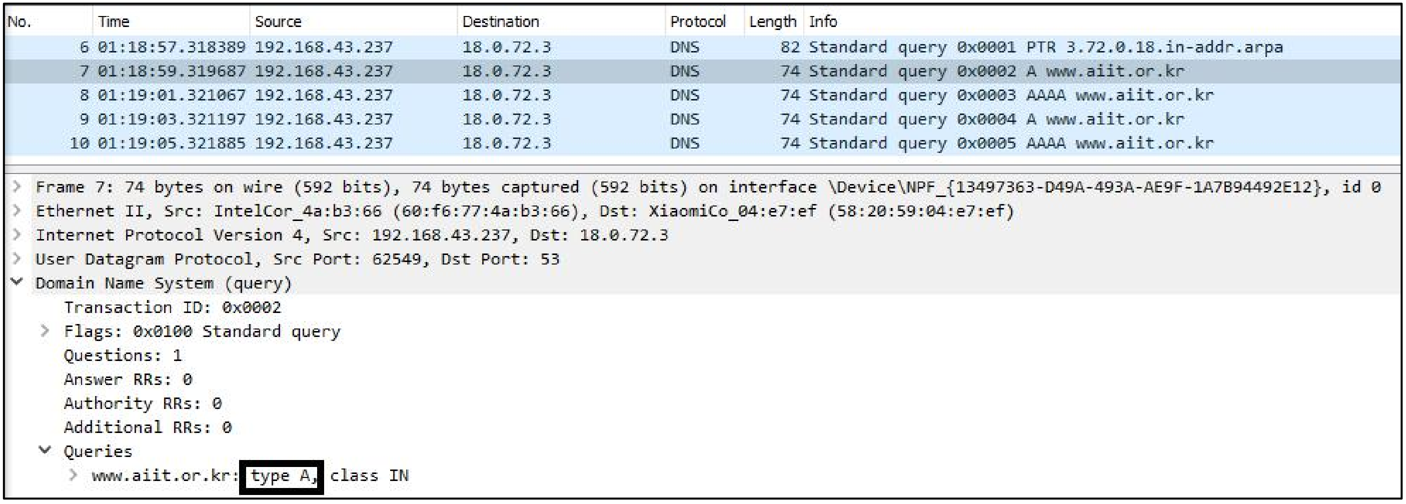
Question20



```
No.   Time             Source          Destination   Protocol  Length Info
    6 01:18:57.318389 192.168.43.237  18.0.72.3     DNS           82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
    7 01:18:59.319687 192.168.43.237  18.0.72.3     DNS           74 Standard query 0x0002 A www.aiit.or.kr
    8 01:19:01.321067 192.168.43.237  18.0.72.3     DNS           74 Standard query 0x0003 AAAA www.aiit.or.kr
    9 01:19:03.321197 192.168.43.237  18.0.72.3     DNS           74 Standard query 0x0004 A www.aiit.or.kr
   10 01:19:05.321885 192.168.43.237  18.0.72.3     DNS           74 Standard query 0x0005 AAAA www.aiit.or.kr

> Frame 6: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{13497363-D49A-493A-AE9F-1A7B94492E
> Ethernet II, Src: IntelCor_4a:b3:66 (60:f6:77:4a:b3:66), Dst: XiaomiCo_04:e7:ef (58:20:59:04:e7:ef)
> Internet Protocol Version 4, Src: 192.168.43.237, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 62548, 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
    > 3.72.0.18.in-addr.arpa: type PTR, class IN
```

In the last part, bitsy.mit.edu was not responding and the request was retried several times. I got a DNS request timed out error. The query message is sent to the IP address of 18.0.72.3 which is not my local IP address. My local IP address is 192.168.43.1 which was found in previous questions.

Question21



```
No.   Time             Source          Destination   Protocol  Length Info
    6 01:18:57.318389 192.168.43.237  18.0.72.3     DNS           82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
    7 01:18:59.319687 192.168.43.237  18.0.72.3     DNS           74 Standard query 0x0002 A www.aiit.or.kr
    8 01:19:01.321067 192.168.43.237  18.0.72.3     DNS           74 Standard query 0x0003 AAAA www.aiit.or.kr
    9 01:19:03.321197 192.168.43.237  18.0.72.3     DNS           74 Standard query 0x0004 A www.aiit.or.kr
   10 01:19:05.321885 192.168.43.237  18.0.72.3     DNS           74 Standard query 0x0005 AAAA www.aiit.or.kr

> Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{13497363-D49A-493A-AE9F-1A7B94492E12}, id 0
> Ethernet II, Src: IntelCor_4a:b3:66 (60:f6:77:4a:b3:66), Dst: XiaomiCo_04:e7:ef (58:20:59:04:e7:ef)
> Internet Protocol Version 4, Src: 192.168.43.237, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 62549, 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
    > www.aiit.or.kr: type A, class IN
```

Its type A query message and does not contain any answers.

Question22

As mentioned, a response message could not be retrieved and request timed error was received. Hence, the response message and response message answers were not available.

Question23

Screenshot was provided in the previous questions.