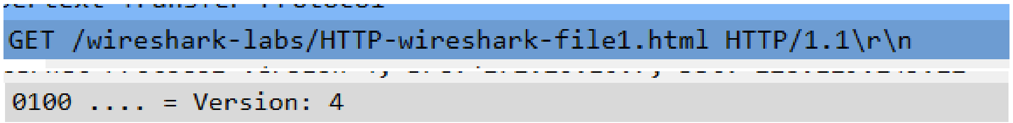
Laboratorinis darbas 3 – Kompiuterių tinklo duomenų srauto analizė

Atliko: Monika Mirbakaitė

HTTP paketų filtravimas

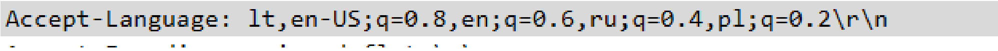
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?



```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
0100 .... = Version: 4
```

Naršyklės versija:	1.1
gaia.cs.umass.edu versija:	4

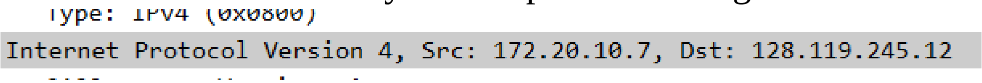
2. What languages (if any) does your browser indicate that it can accept to the server?



```
Accept-Language: lt,en-US;q=0.8,en;q=0.6,ru;q=0.4,pl;q=0.2\r\n
```

Kalbos:	Lietuvių Anglų Rusų Lenkų

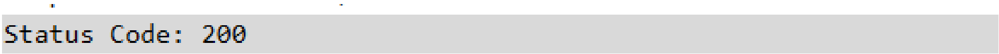
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?



```
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.20.10.7, Dst: 128.119.245.12
```

Src (Kompiurerio adresas):	172.20.10.7
Dst (gaia.cs.umass.edu):	128.119.245.12

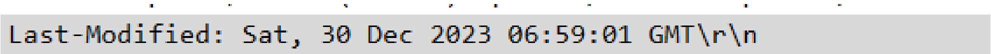
4. What is the status code returned from the server to your browser?



```
Status Code: 200
```

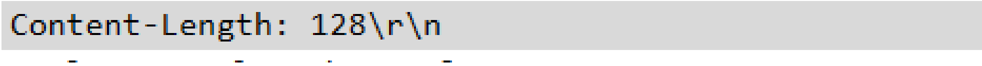
Statuso kodas:	200

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



```
Last-Modified: Sat, 30 Dec 2023 06:59:01 GMT\r\n
```

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



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

Kiek grąžinta?	128 bitai

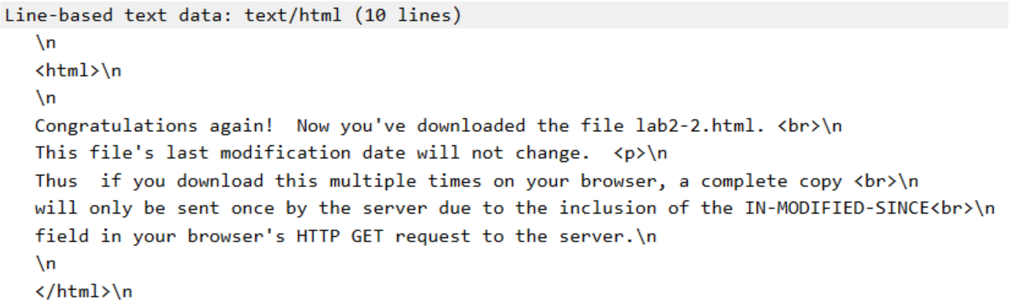
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Atsakymas:	nėra

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

Atsakymas:	nėra

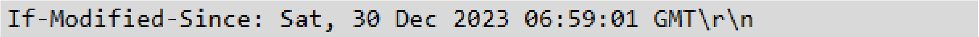
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?



```
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
```

Ar grąžina?	Taip
Iš ko galime nuspręsti?	Faile esanti žinutė sutampa su nuorodoje esančia žinute.

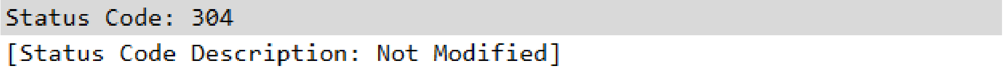
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?



```
If-Modified-Since: Sat, 30 Dec 2023 06:59:01 GMT\r\n
```

Ar yra?	Taip
Kokia informacija seka po?	Data

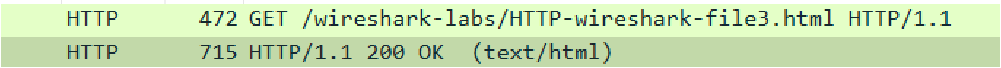
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.



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

Statuso kodas:	304
Response Phrase:	Not Modified
Ar grąžino?	Failo turinys nėra grąžintas

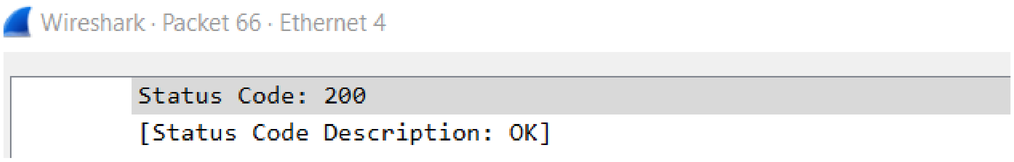
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?



```
    HTTP      472 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
    HTTP      715 HTTP/1.1 200 OK  (text/html)
```

Kiek GET užklausų išsiųsta?	1
Kuris packet numeris turi GET message?	60

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

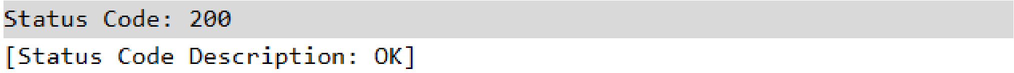


Wireshark · Packet 66 · Ethernet 4

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

Atsakymas:	66

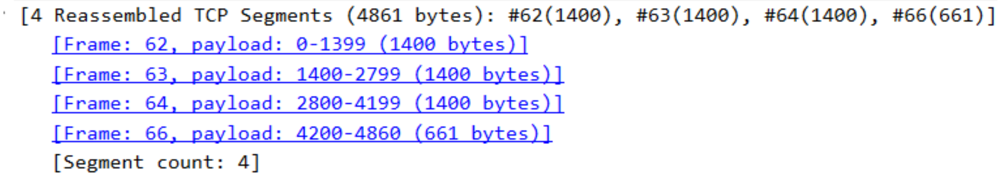
14. What is the status code and phrase in the response?



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

Statuso kodas:	200
Response Phrase:	OK

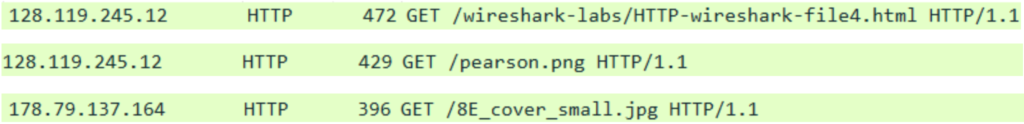
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?



```
[4 Reassembled TCP Segments (4861 bytes): #62(1400), #63(1400), #64(1400), #66(661)]
    [Frame: 62, payload: 0-1399 (1400 bytes)]
    [Frame: 63, payload: 1400-2799 (1400 bytes)]
    [Frame: 64, payload: 2800-4199 (1400 bytes)]
    [Frame: 66, payload: 4200-4860 (661 bytes)]
    [Segment count: 4]
```

TCP segmentų sk:	4

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



```
128.119.245.12    HTTP    472 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
128.119.245.12    HTTP    429 GET /pearson.png HTTP/1.1
178.79.137.164    HTTP    396 GET /8E_cover_small.jpg HTTP/1.1
```

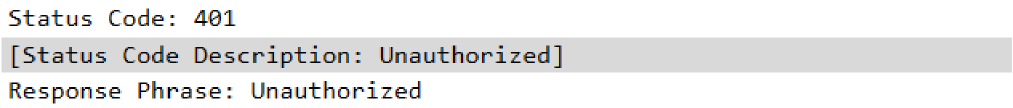
3 GET requests:

Destination	**Info**
128.119.245.12	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
128.119.245.12	GET /pearson.png HTTP/1.1
178.79.137.164	GET /8E_cover_small.jpg HTTP/1.1

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

Kaip buvo atsiųsta?	Lygiagrečiai
Kodėl?	Response gautas tik kai abi nuotraukos atsisiuntė

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

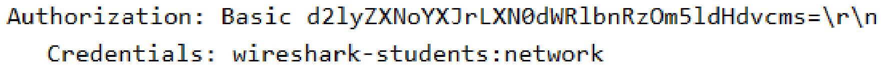


```
Status Code: 401
[Status Code Description: Unauthorized]
Response Phrase: Unauthorized
```

Statuso kodas:	401
Response Phrase:	Unauthorized

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

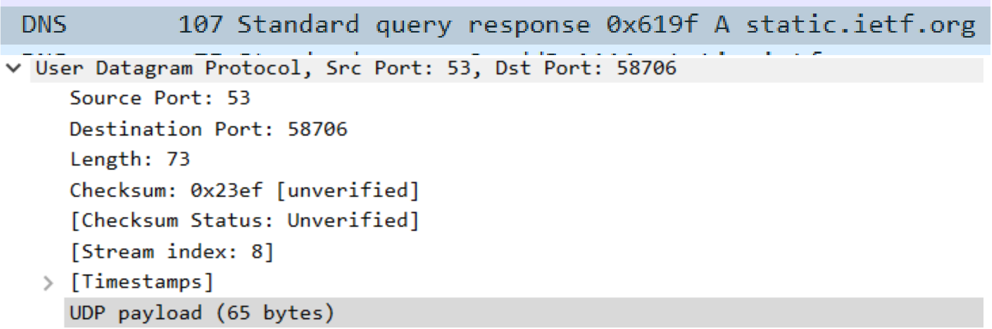
Šis laukas su polaukiu:



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

DNS paketų filtravimas

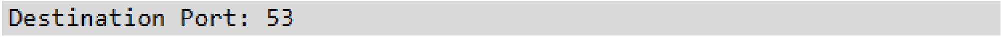
4. Locate the DNS query and response messages. Are then sent over UDP or TCP?



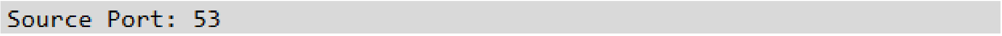
```
DNS        107 Standard query response 0x619f A static.ietf.org
∨ User Datagram Protocol, Src Port: 53, Dst Port: 58706
     Source Port: 53
     Destination Port: 58706
     Length: 73
     Checksum: 0x23ef [unverified]
     [Checksum Status: Unverified]
     [Stream index: 8]
   > [Timestamps]
     UDP payload (65 bytes)
```

DNS response:	UDP

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



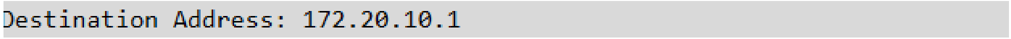
```
Destination Port: 53
```



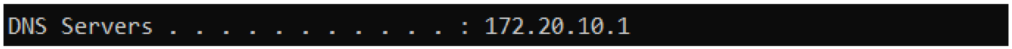
```
Source Port: 53
```

Destination port:	53
Source port:	53

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



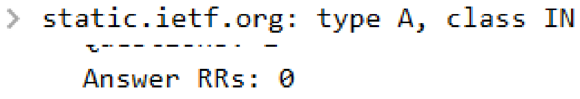
```
Destination Address: 172.20.10.1
```



```
DNS Servers . . . . . . . . . . . : 172.20.10.1
```

Atsakymas:	Taip

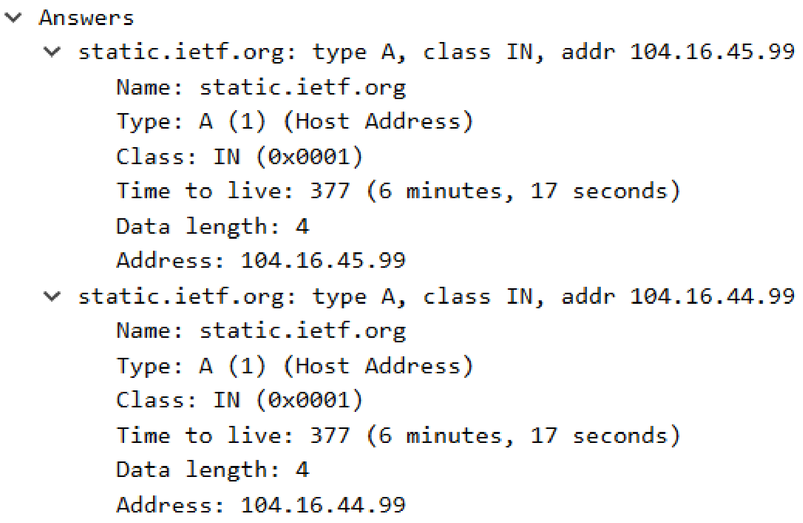
7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?



```
> static.ietf.org: type A, class IN
    Answer RRs: 0
```

Tipas:	A
Atsakymų sk:	0

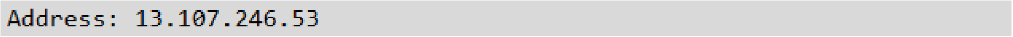
8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?



```
⌄ Answers
  ⌄ static.ietf.org: type A, class IN, addr 104.16.45.99
      Name: static.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 377 (6 minutes, 17 seconds)
      Data length: 4
      Address: 104.16.45.99
  ⌄ static.ietf.org: type A, class IN, addr 104.16.44.99
      Name: static.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 377 (6 minutes, 17 seconds)
      Data length: 4
      Address: 104.16.44.99
```

Atsakymų sk:	2
Turinys:	Name Type Class Time to live Data lengh Address

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



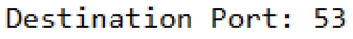
```
Address: 13.107.246.53
```

Atsakymas:	ne

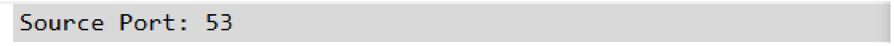
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Atsakymas:	ne

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



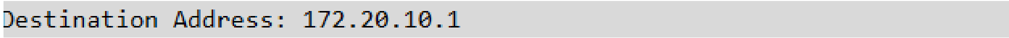
```
Destination Port: 53
```



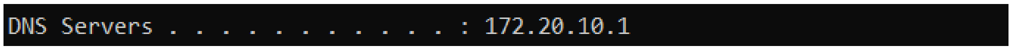
```
Source Port: 53
```

Destination port:	53
Source port:	53

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



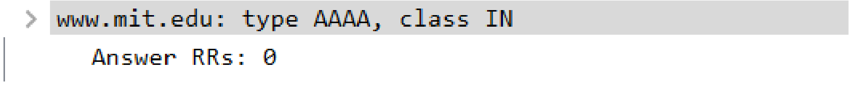
```
Destination Address: 172.20.10.1
```



```
DNS Servers . . . . . . . . . . . : 172.20.10.1
```

Atsakymas:	Taip

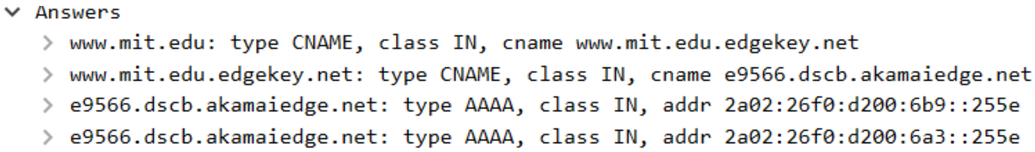
13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



```
> www.mit.edu: type AAAA, class IN
      Answer RRs: 0
```

Tipas:	AAA
Atsakymų sk:	0

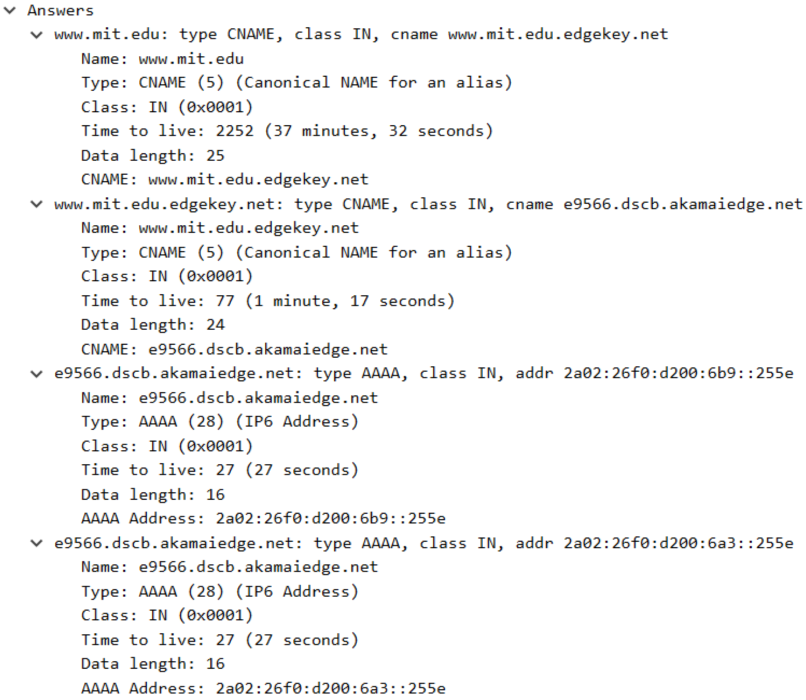
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?



```
v Answers
    > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:6b9::255e
    > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:6a3::255e
```

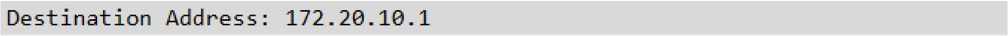
Atsakymų sk:	4
Turinys:	Name Type Class Time to live Data lengh CNAME/Address

15. Provide a screenshot.

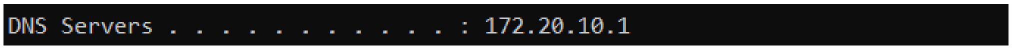


```
v Answers
   v www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 2252 (37 minutes, 32 seconds)
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
   v www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        Name: www.mit.edu.edgekey.net
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 77 (1 minute, 17 seconds)
        Data length: 24
        CNAME: e9566.dscb.akamaiedge.net
   v e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:6b9::255e
        Name: e9566.dscb.akamaiedge.net
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
        Time to live: 27 (27 seconds)
        Data length: 16
        AAAA Address: 2a02:26f0:d200:6b9::255e
   v e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:6a3::255e
        Name: e9566.dscb.akamaiedge.net
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
        Time to live: 27 (27 seconds)
        Data length: 16
        AAAA Address: 2a02:26f0:d200:6a3::255e
```

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



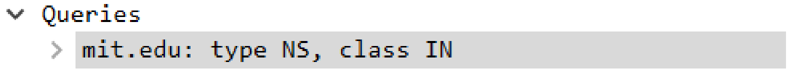
```
Destination Address: 172.20.10.1
```



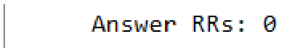
```
DNS Servers . . . . . . . . . . . : 172.20.10.1
```

Atsakymas:	Taip

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



```
⌄ Queries
  › mit.edu: type NS, class IN
```



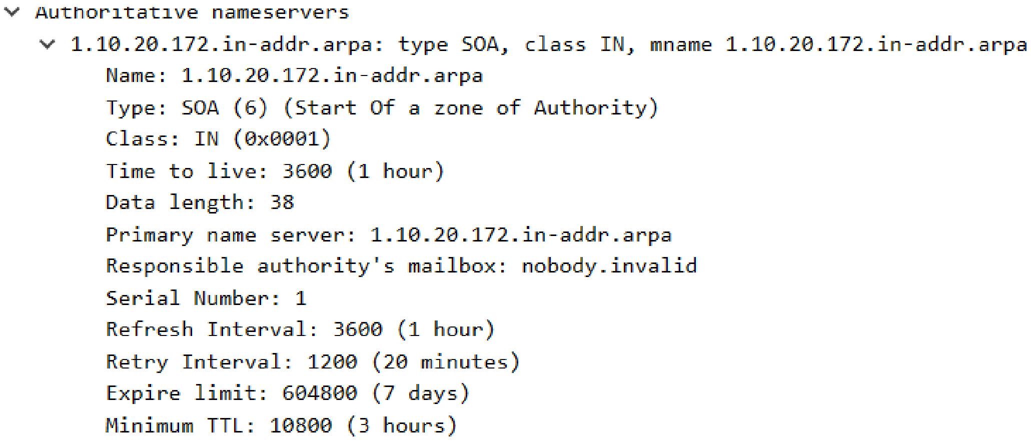
```
      Answer RRs: 0
```

Tipas:	ns
Atsakymų sk:	0

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

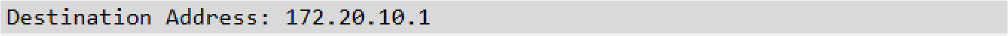
MIT name server:	mname 1.10.20.172.in-addr.arpa
IP:	Taip (1.10.20.172)

19. Provide a screenshot.

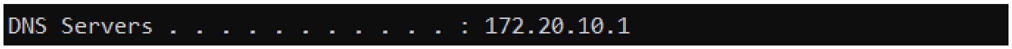


```
⌄ Authoritative nameservers
  ⌄ 1.10.20.172.in-addr.arpa: type SOA, class IN, mname 1.10.20.172.in-addr.arpa
      Name: 1.10.20.172.in-addr.arpa
      Type: SOA (6) (Start Of a zone of Authority)
      Class: IN (0x0001)
      Time to live: 3600 (1 hour)
      Data length: 38
      Primary name server: 1.10.20.172.in-addr.arpa
      Responsible authority's mailbox: nobody.invalid
      Serial Number: 1
      Refresh Interval: 3600 (1 hour)
      Retry Interval: 1200 (20 minutes)
      Expire limit: 604800 (7 days)
      Minimum TTL: 10800 (3 hours)
```

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



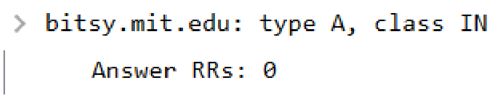
```
Destination Address: 172.20.10.1
```



```
DNS Servers . . . . . . . . . . . : 172.20.10.1
```

Atsakymas:	Taip

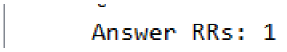
21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



```
> bitsy.mit.edu: type A, class IN
      Answer RRs: 0
```

Tipas:	A
Atsakymų sk:	0

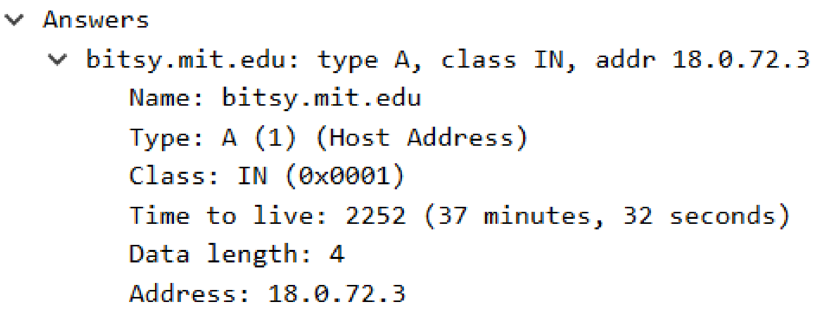
22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?



```
      Answer RRs: 1
```

Atsakymų sk:	1
Turinys:	Name Type Class Time to live Data lengh Address

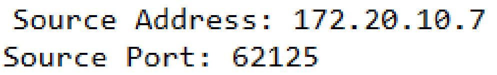
23. Provide a screenshot.



```
v Answers
   v bitsy.mit.edu: type A, class IN, addr 18.0.72.3
        Name: bitsy.mit.edu
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 2252 (37 minutes, 32 seconds)
        Data length: 4
        Address: 18.0.72.3
```

TCP paketų filtravimas

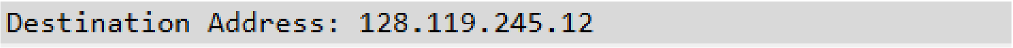
1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?



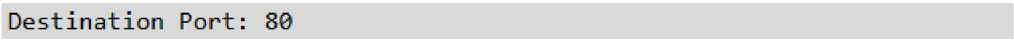
```
 Source Address: 172.20.10.7
Source Port: 62125
```

Šaltinio IP adresas:	172.20.10.7
Šaltinio prievadas:	62125

2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?



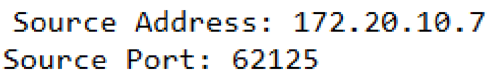
```
Destination Address: 128.119.245.12
```



```
Destination Port: 80
```

gaia.cs.umass.edu IP adresas:	128.119.245.12
gaia.cs.umass.edu prievadas:	80

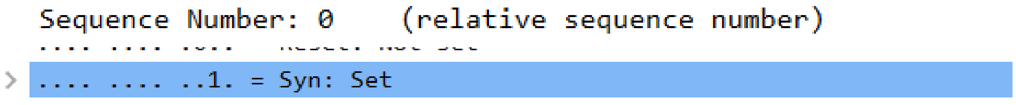
3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?



```
Source Address: 172.20.10.7
Source Port: 62125
```

Šaltinio IP adresas:	172.20.10.7
Šaltinio prievadas:	62125

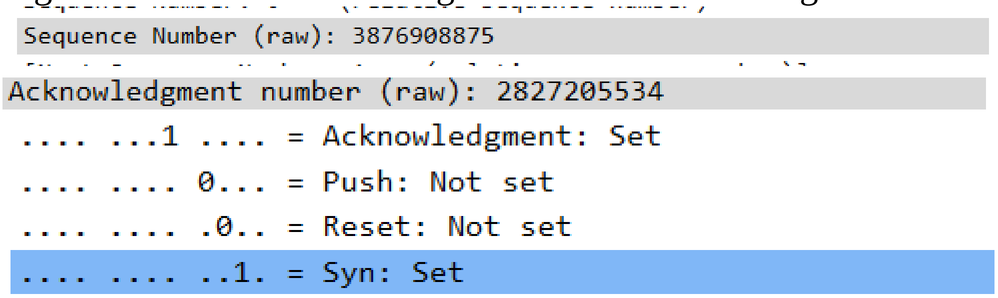
4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?



```
Sequence Number: 0    (relative sequence number)
.... .... ..1. = Syn: Set
```

Sequence numeris:	0
SYN segmento identifikacija:	Syn flag is set

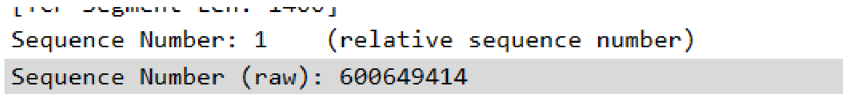
5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?



```
Sequence Number (raw): 3876908875
Acknowledgment number (raw): 2827205534
.... ...1 .... = Acknowledgment: Set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
.... .... ..1. = Syn: Set
```

Sequence numeris:	3876908875
Ack numeris:	2827205534
SYNACK identifikacija:	Syn flag is set Acknowledgement flag is set
How did gaia.cs.umass.edu determine that value?	ACK reikšmė SYNACK yra lygi Sequence numeriui sekančiame ACK.

6. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

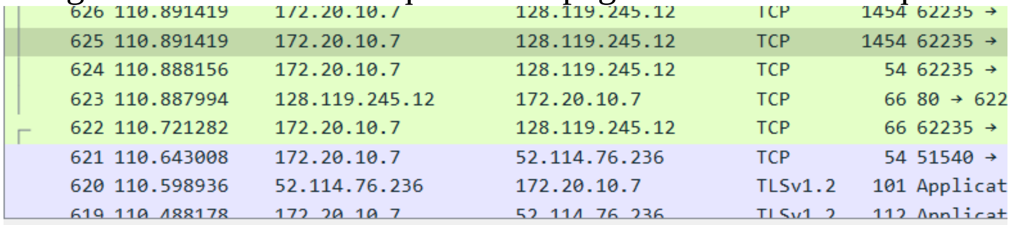


```
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 600649414
```

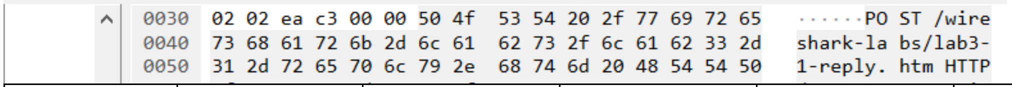
Sequence numeris:	1

7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the sixsegments? What is the EstimatedRTT value (see Section 3.5.3,

page 242 in text) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 242 for all subsequent segments.



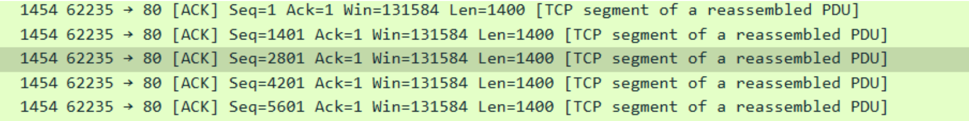
```
626 110.891419    172.20.10.7       128.119.245.12    TCP       1454 62235 →
625 110.891419    172.20.10.7       128.119.245.12    TCP       1454 62235 →
624 110.888156    172.20.10.7       128.119.245.12    TCP         54 62235 →
623 110.887994    128.119.245.12    172.20.10.7       TCP         66 80 → 622
622 110.721282    172.20.10.7       128.119.245.12    TCP         66 62235 →
621 110.643008    172.20.10.7       52.114.76.236     TCP         54 51540 →
620 110.598936    52.114.76.236     172.20.10.7       TLSv1.2    101 Applicat
619 110.488178    172.20.10.7       52.114.76.236     TLSv1.2    112 Applicat
```



```
0030  02 02 ea c3 00 00 50 4f  53 54 20 2f 77 69 72 65   ······PO ST /wire
0040  73 68 61 72 6b 2d 6c 61  62 73 2f 6c 61 62 33 2d   shark-la bs/lab3-
0050  31 2d 72 65 70 6c 79 2e  68 74 6d 20 48 54 54 50   1-reply. htm HTTP
```

Sequence num.	600649414	600650814	600652214	600653614	600655014	600656414
Išsiuntimo laikai	110.891419	110.891419	110.891419	110.891419	110.891419	110.891419
RTT laikai	0.00000000	0.000000000	0.000000000	0.000000000	0.000000000	0.000000000

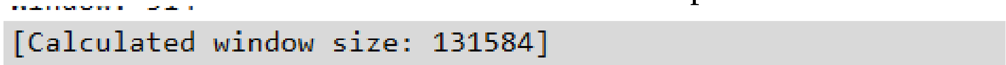
8. What is the length of each of the first six TCP segments?



```
1454 62235 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=1400 [TCP segment of a reassembled PDU]
1454 62235 → 80 [ACK] Seq=1401 Ack=1 Win=131584 Len=1400 [TCP segment of a reassembled PDU]
1454 62235 → 80 [ACK] Seq=2801 Ack=1 Win=131584 Len=1400 [TCP segment of a reassembled PDU]
1454 62235 → 80 [ACK] Seq=4201 Ack=1 Win=131584 Len=1400 [TCP segment of a reassembled PDU]
1454 62235 → 80 [ACK] Seq=5601 Ack=1 Win=131584 Len=1400 [TCP segment of a reassembled PDU]
```

Ilgis (baitais):	visų 1400

9. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?



```
[Calculated window size: 131584]
```

Atsakymas:	ne, nes segmentų ilgiai yra mažesni

10. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

Atsakymas:	ne, nes sequence numeriai didėja

11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 250 in the text).

Atsakymas:	1460
Can you identify cases where the receiver is ACKing every other received segment?	Ne

12. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

Pralaidumas:	30193.030045 MB/s
Apskaičiavimas:	Pirm. segm.: 1 baitas. Pask. segm.: 164091 baitas. Iš viso: 164091 – 1 =164090 baitų

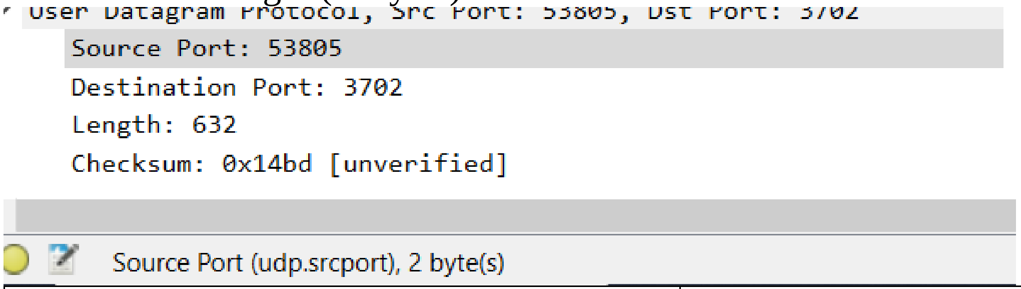
	Pirm. segm. laikas: 0.026477 Pask. segm. laikas: 5.461175 Iš viso: 5.461175 – 0.026477 = 5.434698 Pralaidumas: 164090 / 5.434698 = 30193.030045 MB/S

UDP paketų filtravimas

1. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn’t look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

Kiekis:	4
Pavadinimai:	Source Port: 53805 Destination Port: 3702 Length: 632 Checksum: 0x14bd [unverified]

2. By consulting the displayed information in Wireshark’s packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

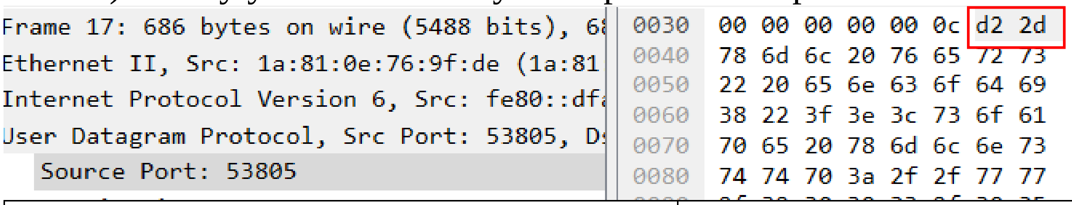


```
User Datagram Protocol, Src Port: 53805, Dst Port: 3702
    Source Port: 53805
    Destination Port: 3702
    Length: 632
    Checksum: 0x14bd [unverified]
```

Source Port (udp.srcport), 2 byte(s)

Atsakymas:	Visi fields turi po 2 bitus

3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.



```
Frame 17: 686 bytes on wire (5488 bits), 68
Ethernet II, Src: 1a:81:0e:76:9f:de (1a:81
Internet Protocol Version 6, Src: fe80::df
User Datagram Protocol, Src Port: 53805, D
   Source Port: 53805
```

```
0030   00 00 00 00 00 0c d2 2d
0040   78 6d 6c 20 76 65 72 73
0050   22 20 65 6e 63 6f 64 69
0060   38 22 3f 3e 3c 73 6f 61
0070   70 65 20 78 6d 6c 6e 73
0080   74 74 70 3a 2f 2f 77 77
```

Atsakymas:	antraštės baitų suma

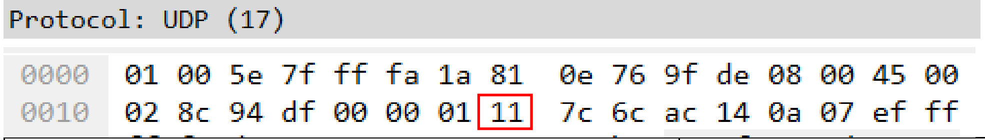
4. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

Didžiausias prievadas:	2^(16) – 1 = 65535
Antraštės baitų suma:	4 * 2 = 8 baitai
Didžiausia UDP apkrova:	65535 – 8 = 65527

5. What is the largest possible source port number? (Hint: see the hint in 4.)

Atsakymas:	2^(16) – 1 = 65535

6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).

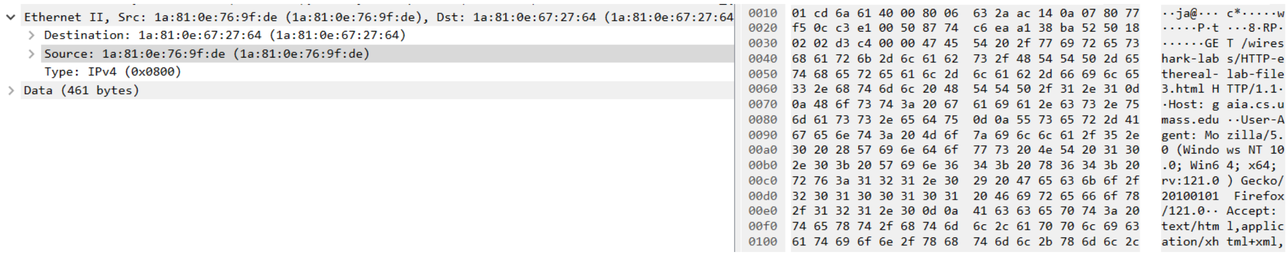


```
Protocol: UDP (17)

0000  01 00 5e 7f ff fa 1a 81  0e 76 9f de 08 00 45 00
0010  02 8c 94 df 00 00 01 11  7c 6c ac 14 0a 07 ef ff
```

UDP numeris:	17
Hex:	11

Ethernet ir ARP paketų filtravimas

1. What is the 48-bit Ethernet address of your computer?

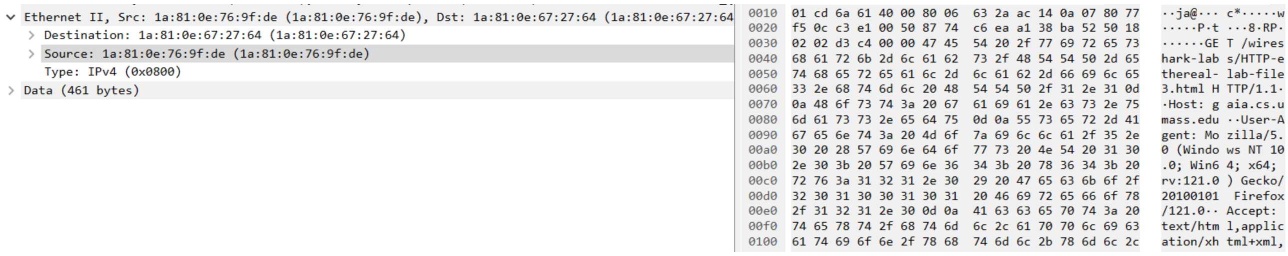


```
v Ethernet II, Src: 1a:81:0e:76:9f:de (1a:81:0e:76:9f:de), Dst: 1a:81:0e:67:27:64 (1a:81:0e:67:27:64
  > Destination: 1a:81:0e:67:27:64 (1a:81:0e:67:27:64)
  > Source: 1a:81:0e:76:9f:de (1a:81:0e:76:9f:de)
    Type: IPv4 (0x0800)
> Data (461 bytes)
```

```
0010  01 cd 6a 61 40 00 80 06  63 2a ac 14 0a 07 80 77   ··ja@··· c*·····w
0020  f5 0c c3 e1 00 50 87 74  c6 ea a1 38 ba 52 50 18   ·····P·t ···8·RP·
0030  02 02 d3 c4 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-lab s/HTTP-e
0050  74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal- lab-file
0060  33 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   3.html H TTP/1.1·
0070  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   ·Host: g aia.cs.u
0080  6d 61 73 73 2e 65 64 75  0d 0a 55 73 65 72 2d 41   mass.edu ··User-A
0090  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
00a0  30 20 28 57 69 6e 64 6f  77 73 20 4e 54 20 31 30   0 (Windo ws NT 10
00b0  2e 30 3b 20 57 69 6e 36  34 3b 20 78 36 34 3b 20   .0; Win6 4; x64;
00c0  72 76 3a 31 32 31 2e 30  29 20 47 65 63 6b 6f 2f   rv:121.0 ) Gecko/
00d0  32 30 31 30 30 31 30 31  20 46 69 72 65 66 6f 78   20100101  Firefox
00e0  2f 31 32 31 2e 30 0d 0a  41 63 63 65 70 74 3a 20   /121.0·· Accept:
00f0  74 65 78 74 2f 68 74 6d  6c 2c 61 70 70 6c 69 63   text/htm l,applic
0100  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
```

Atsakymas:	1a:81:0e:76:9f:de

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is *no*). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]

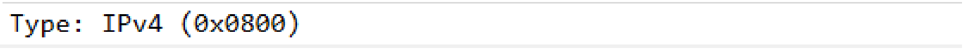


```
v Ethernet II, Src: 1a:81:0e:76:9f:de (1a:81:0e:76:9f:de), Dst: 1a:81:0e:67:27:64 (1a:81:0e:67:27:64
  > Destination: 1a:81:0e:67:27:64 (1a:81:0e:67:27:64)
  > Source: 1a:81:0e:76:9f:de (1a:81:0e:76:9f:de)
    Type: IPv4 (0x0800)
> Data (461 bytes)
```

```
0010  01 cd 6a 61 40 00 80 06  63 2a ac 14 0a 07 80 77   ··ja@··· c*·····w
0020  f5 0c c3 e1 00 50 87 74  c6 ea a1 38 ba 52 50 18   ·····P·t ···8·RP·
0030  02 02 d3 c4 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-lab s/HTTP-e
0050  74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal- lab-file
0060  33 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   3.html H TTP/1.1·
0070  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   ·Host: g aia.cs.u
0080  6d 61 73 73 2e 65 64 75  0d 0a 55 73 65 72 2d 41   mass.edu ··User-A
0090  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
00a0  30 20 28 57 69 6e 64 6f  77 73 20 4e 54 20 31 30   0 (Windo ws NT 10
00b0  2e 30 3b 20 57 69 6e 36  34 3b 20 78 36 34 3b 20   .0; Win6 4; x64;
00c0  72 76 3a 31 32 31 2e 30  29 20 47 65 63 6b 6f 2f   rv:121.0 ) Gecko/
00d0  32 30 31 30 30 31 30 31  20 46 69 72 65 66 6f 78   20100101  Firefox
00e0  2f 31 32 31 2e 30 0d 0a  41 63 63 65 70 74 3a 20   /121.0·· Accept:
00f0  74 65 78 74 2f 68 74 6d  6c 2c 61 70 70 6c 69 63   text/htm l,applic
0100  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
```

Atsakymas:	1a:81:0e:67:27:64
What device has this as its Ethernet address?	Maršrutizatorius

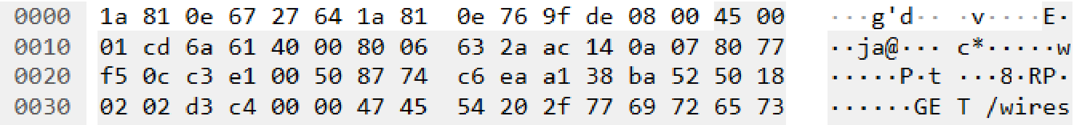
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?



```
Type: IPv4 (0x0800)
```

Hex:	0x0800
Protokolas:	IPv4

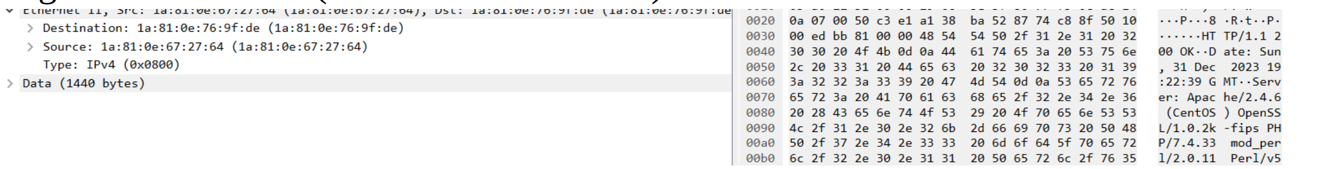
4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?



```
0000  1a 81 0e 67 27 64 1a 81  0e 76 9f de 08 00 45 00   ···g'd·· ·v····E·
0010  01 cd 6a 61 40 00 80 06  63 2a ac 14 0a 07 80 77   ··ja@··· c*·····w
0020  f5 0c c3 e1 00 50 87 74  c6 ea a1 38 ba 52 50 18   ·····P·t ···8·RP·
0030  02 02 d3 c4 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
```

Atsakymas:	54

5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is *no*). What device has this as its Ethernet address?

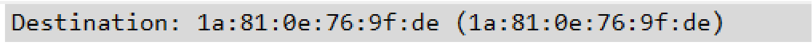


```
⌄ Ethernet II, Src: 1a:81:0e:67:27:64 (1a:81:0e:67:27:64), Dst: 1a:81:0e:76:9f:de (1a:81:0e:76:9f:de
   > Destination: 1a:81:0e:76:9f:de (1a:81:0e:76:9f:de)
   > Source: 1a:81:0e:67:27:64 (1a:81:0e:67:27:64)
     Type: IPv4 (0x0800)
 > Data (1440 bytes)
```

```
0020  0a 07 00 50 c3 e1 a1 38  ba 52 87 74 c8 8f 50 10   ···P···8 ·R·t··P·
0030  00 ed bb 81 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 75 6e   00 OK··D ate: Sun
0050  2c 20 33 31 20 44 65 63  20 32 30 32 33 20 31 39   , 31 Dec  2023 19
0060  3a 32 32 3a 33 39 20 47  4d 54 0d 0a 53 65 72 76   :22:39 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 37 2e 34 2e 33 33  20 6d 6f 64 5f 70 65 72   P/7.4.33  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
```

Atsakymas:	1a:81:0e:67:27:64
What device has this as its Ethernet address?	Maršrutizatorius

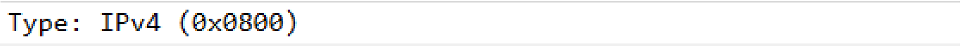
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?



```
Destination: 1a:81:0e:76:9f:de (1a:81:0e:76:9f:de)
```

Destination address:	1a:81:0e:76:9f:de
Atsakymas:	Taip

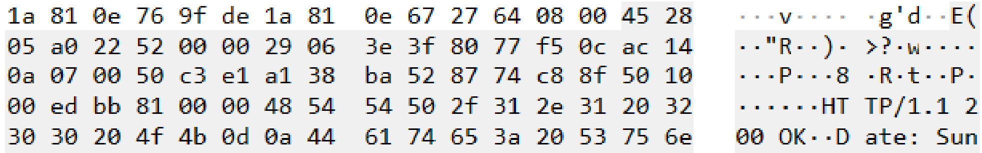
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?



```
Type: IPv4 (0x0800)
```

Hex:	0x0800
Protokolas:	IPv4 (OSI Layer 3)

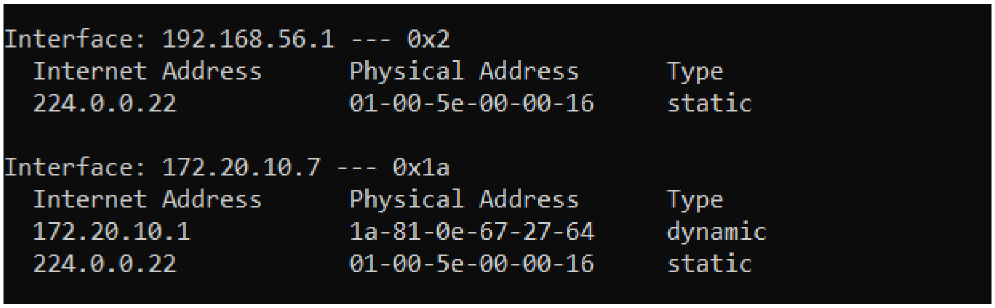
8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?\



```
1a 81 0e 76 9f de 1a 81  0e 67 27 64 08 00 45 28   ···v···· ·g'd··E(
05 a0 22 52 00 00 29 06  3e 3f 80 77 f5 0c ac 14   ··"R··)· >?·w····
0a 07 00 50 c3 e1 a1 38  ba 52 87 74 c8 8f 50 10   ···P···8 ·R·t··P·
00 ed bb 81 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 75 6e   00 OK··D ate: Sun
```

Atsakymas:	54

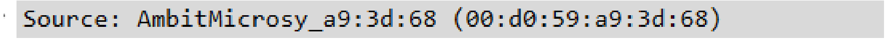
9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?



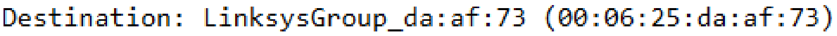
```
Interface: 192.168.56.1 --- 0x2
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 172.20.10.7 --- 0x1a
  Internet Address      Physical Address      Type
  172.20.10.1           1a-81-0e-67-27-64     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
```

Internet Address (IPv4)	Protokolas reguliuojantis duomenų formatą, siunčiamą per internetą arba vietinį tinklą.
Physical Adress (MAC)	Priklauso OSI, kuris įtraukia siuntėjo ir gavėjo MAC adresus į kiekvieno duomenų paketo antraštę, siekiant užtikrinti mazgų tarpusavio ryšį.
Type (static/dynamic)	Kintantis ir nekintantis tipai.

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

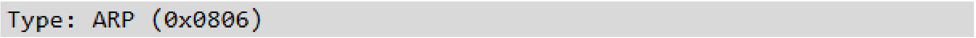


```
Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
```



```
Destination: LinksysGroup_da:af:73 (00:06:25:da:af:73)
```

11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?



```
Type: ARP (0x0806)
```

Hex:	0x0806
Protokolas:	ARP (OSI Layer 3)