

## **Laboratorinio darbo ataskaita**



VILNIAUS UNIVERSITETAS  
MATEMATIKOS IR INFORMATIKOS FAKULTETAS  
INFORMACINIŲ SISTEMŲ INŽINERIJA, 3 KURSAS

### **Laboratorinis darbas 3 – Kompiuterių tinklo duomenų srauto analizė KOMPIUTERIŲ TINKLAI**

Atliko: Martynas Jašinskas

VU el. p: [martynas.jasinskas@mif.stud.vu.lt](mailto:martynas.jasinskas@mif.stud.vu.lt)

Vilnius, 2022

## HTTP paketu filtravimas

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

My browser:

Wireshark screenshot showing a network capture. The top pane displays two rows of traffic: a GET request from the browser to the server (Frame 770) and a response from the server back to the browser (Frame 792). The bottom pane shows the detailed structure of the selected GET request (Frame 770), specifically the Hypertext Transfer Protocol section. The 'Request Version' field is highlighted with a red box and shows the value 'HTTP/1.1'. The right side of the bottom pane shows the raw hex and ASCII data for the selected frame.

Server:

Wireshark screenshot showing a network capture. The top pane displays a single row of traffic: a response from the server back to the browser (Frame 792). The bottom pane shows the detailed structure of this response, specifically the Hypertext Transfer Protocol section. The 'HTTP/1.1 404 Not Found\r\n' line is highlighted with a red box. The right side of the bottom pane shows the raw hex and ASCII data for the selected frame.

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

The Wireshark interface is shown with the 'http' protocol selected in the top bar. The main pane displays two rows of network traffic. The first row (Frame 770) shows a GET request from 192.168.0.54 to 128.119.245.12. The second row (Frame 792) shows a 404 Not Found response from 128.119.245.12 back to 192.168.0.54.

The detailed information pane below the traffic list shows the structure of the GET request. It highlights the 'GET /favicon.ico HTTP/1.1\r\n' line, which is expanded to show the full request message. The 'Accept-Language' header is highlighted with a red box and contains the value 'en-GB,en-US;q=0.9,en;q=0.8,lt;q=0.7\r\n'.

No.	Time	Source	Destination	Protocol	Length	Info
770	3.544952	192.168.0.54	128.119.245.12	HTTP	511	GET /favicon.ico HTTP/1.1
792	3.658394	128.119.245.12	192.168.0.54	HTTP	551	HTTP/1.1 404 Not Found (text/html)

```

> Frame 770: 511 bytes on wire (4088 bits), 511 bytes captured (4088 bits) on interface en0, id 0
> Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe)
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58313, Dst Port: 80, Seq: 1, Ack: 1, Len: 445
< Hypertext Transfer Protocol
  > GET /favicon.ico HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /favicon.ico
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
      Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
      Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-GB,en-US;q=0.9,en;q=0.8,lt;q=0.7\r\n

```

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

The Wireshark interface is shown with the 'http' protocol selected in the top bar. The main pane displays two rows of network traffic. The first row (Frame 770) shows a GET request from 192.168.0.54 to 128.119.245.12. The second row (Frame 792) shows a 404 Not Found response from 128.119.245.12 back to 192.168.0.54.

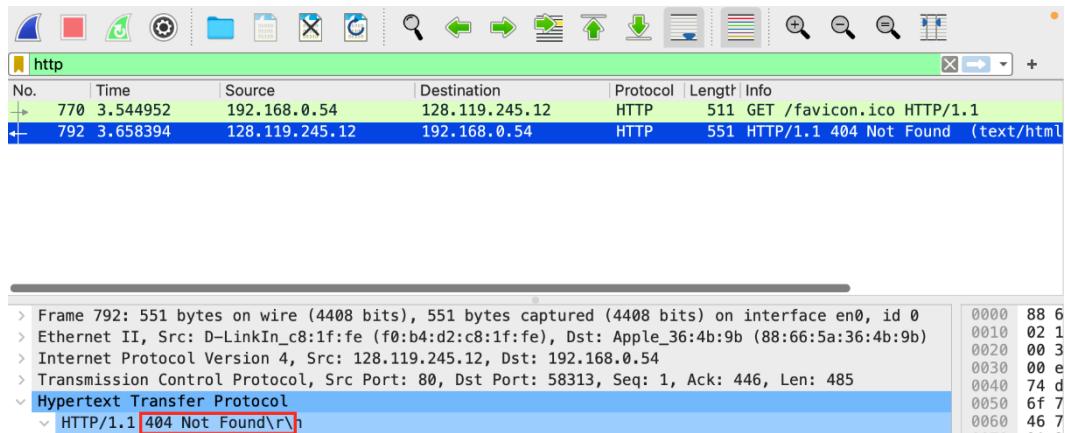
The detailed information pane below the traffic list shows the structure of the GET request. It highlights the 'Source' field in the first row, which contains the IP address '192.168.0.54'. The 'Destination' field in the same row also contains the IP address '128.119.245.12'.

No.	Time	Source	Destination	Protocol	Length	Info
770	3.544952	192.168.0.54	128.119.245.12	HTTP	511	GET /favicon.ico HTTP/1.1
792	3.658394	128.119.245.12	192.168.0.54	HTTP	551	HTTP/1.1 404 Not Found (text/html)

192.168.0.54 – Mano kompiuterio adresas.

128.119.245.12 – Gaia.cs.umass.edu adresas.

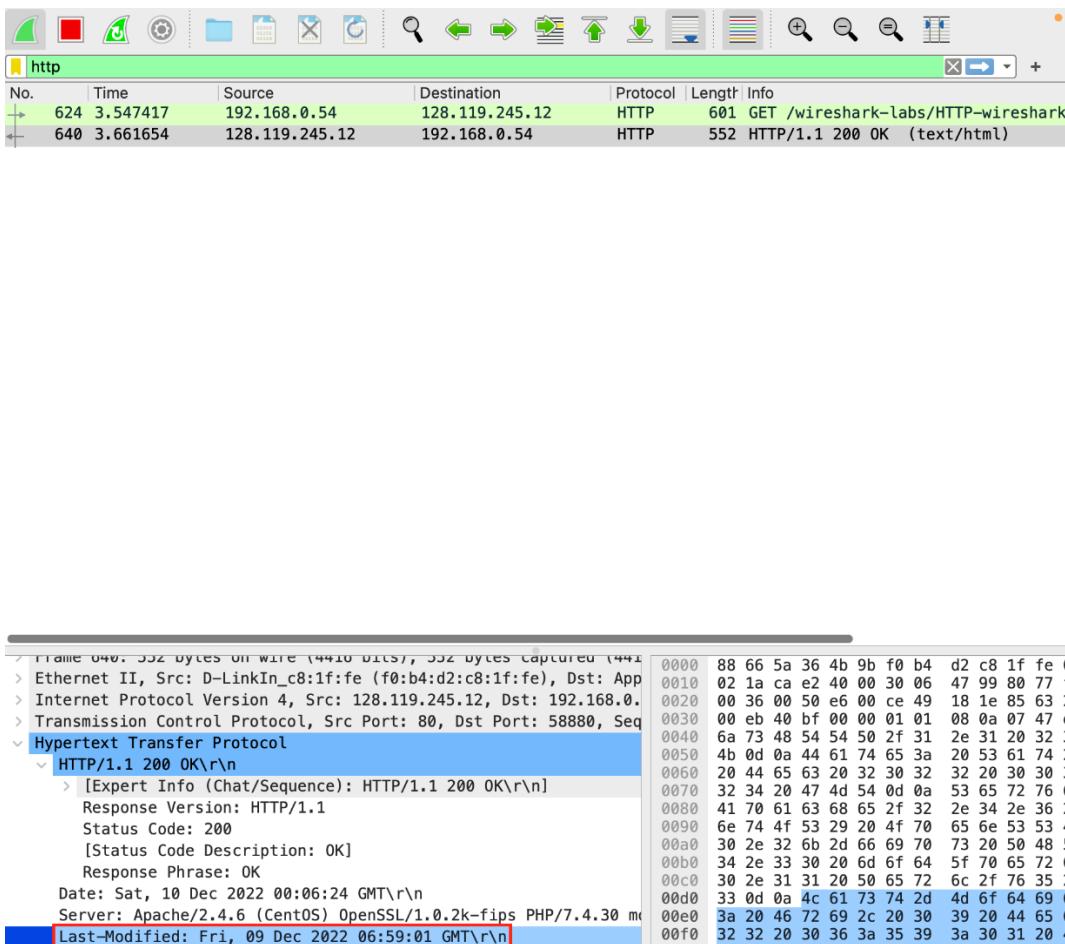
4. What is the status code returned from the server to your browser?



Čia buvo gautas 404 kodas, kuris rodo, kad toks resursas nebuvu rastas. Iš requesito galime matyti, kad mano browseris bandė prašyti kažkokios ikonėlės, vietoje reikiamao html failo. Galiausiai pasisekė surasti tuos paketus, todėl tolimesnėse užduotyse matytis paketai su reikiama resursu.

Kadangi norimas resursas paskiausiai buvo rastas, galime sakyti kad status kode buvo 200 OK.

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



Data sutampa maždaug su puslapio atidarymo data (čia taip specialiai buvo padaryta).

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

The screenshot shows a Wireshark interface with a single selected packet (Frame 640). The packet details pane shows:

No.	Time	Source	Destination	Protocol	Length	Info
624	3.547417	192.168.0.54	128.119.245.12	HTTP	601	GET /wireshark-labs/HTTP-wireshark
640	3.661654	128.119.245.12	192.168.0.54	HTTP	552	HTTP/1.1 200 OK (text/html)

The packet bytes pane shows the raw content of the selected packet. The content starts with:

```

> Frame 640: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits)
> Ethernet II, Src: D-LinkIn_c8:1f:fe (08:b4:d2:c8:1f:fe), Dst: App
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.
> Transmission Control Protocol, Src Port: 80, Dst Port: 58880, Seq
  Hypertext Transfer Protocol
    < 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: Sat, 10 Dec 2022 00:06:24 GMT\r\n
        Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 m
        Last-Modified: Fri, 09 Dec 2022 06:59:01 GMT\r\n
        ETag: "80-5ef5fb042acd1"\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: 0.114237000 seconds]
        [Request in frame: 624]
        [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wi
        File Data: 128 bytes
  
```

The content ends with:

```

</html>
<body data-new-gr-c-s-check-loaded="14.1088.6" data-gr-ext-installed=">
  Congratulations. You've downloaded the file http://gaia.cs.umass.edu/wireshark-
  labs/HTTP-wireshark-file1.html!
</body>
</grammatically-desktop-integration data-grammatically-shadow-root="true"></grammatically-
  desktop-integration>
</html>

```

## 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.

The screenshot shows a browser developer tools Network tab and a Wireshark interface. The browser tab shows a file download confirmation message:

```

<html>
<body>
  Congratulations. You've downloaded the file \n
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
</body>

```

The Wireshark interface shows the raw content of the selected packet (Frame 640) in the bytes pane:

```

> Frame 640: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits)
> Ethernet II, Src: D-LinkIn_c8:1f:fe (08:b4:d2:c8:1f:fe), Dst: App
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.
> Transmission Control Protocol, Src Port: 80, Dst Port: 58880, Seq
  Hypertext Transfer Protocol
    < 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: Sat, 10 Dec 2022 00:06:24 GMT\r\n
        Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 m
        Last-Modified: Fri, 09 Dec 2022 06:59:01 GMT\r\n
        ETag: "80-5ef5fb042acd1"\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: 0.114237000 seconds]
        [Request in frame: 624]
        [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wi
        File Data: 128 bytes
  
```

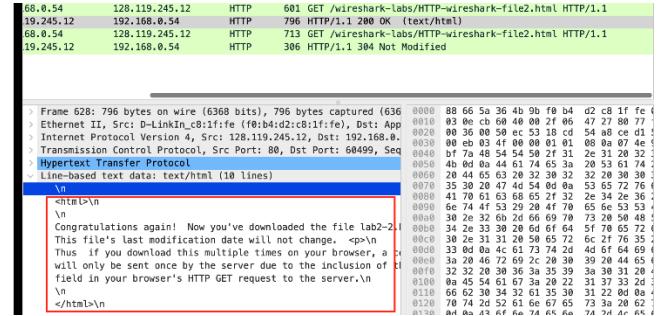
Galime pastebeti, kad originaliame HTML faile yra papildomos `<body>` ir `<head>` žymės.

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?

Pirmame GET requeste nieko nematome, kadangi mūsų cache buvo išvalytas ir naršyklė „pirmą“ kartą atsiisiuntė šitą HTML dokumentą.

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

Congratulations again! Now you've downloaded the file lab2-2.html.  
This file's last modification date will not change.  
Thus if you download this multiple times on your browser, a complete copy  
will only be sent once by the server due to the inclusion of the IF-MODIFIED-SINCE  
field in your browser's HTTP GET request to the server.



Taip, serveris atgal gražino visą informaciją, kuri sutampa su naršyklėje rodomu tekstu.

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?

68.0.54	128.119.245.12	HTTP	601 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
19.245.12	192.168.0.54	HTTP	796 HTTP/1.1 200 OK (text/html)
68.0.54	128.119.245.12	HTTP	713 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
19.245.12	192.168.0.54	HTTP	306 HTTP/1.1 304 Not Modified

```

> Frame 2113: 713 bytes on wire (5704 bits), 713 bytes captured (57
> Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-Link
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 128.119.245.
> Transmission Control Protocol, Src Port: 60498, Dst Port: 80, Seq
< Hypertext Transfer Protocol
  < GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wires
      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 (Macintosh; Intel Mac OS X 10_15_7) Ap
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
      Referer: http://staff.ustc.edu.cn/\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-GB,en-US;q=0.9,en;q=0.8,lt;q=0.7\r\n
      If-None-Match: "173-5ef5fb042a501"\r\n
      If-Modified-Since: Fri, 09 Dec 2022 06:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTT
    [HTTP request 1/1]
    [Response in frame: 2142]
  
```

0000	f0 b4 d2 c8 1f fe 88 66	5a 36 4b 9b	0
0010	02 bb 00 00 40 00 40 06	01 db c0 a8	0
0020	f5 0c ec 52 00 50 f9 ab	30 39 36 0a	0
0030	08 0a 8b c7 00 00 01 01	08 0a ab bb	0
0040	9f 88 47 45 54 20 2f 77	69 72 65 73	0
0050	2d 6c 61 62 73 2f 48 54	54 50 2d 77	0
0060	68 61 72 6b 2d 66 69 6c	65 32 2e 68	0
0070	48 54 54 50 2f 31 2e 31	0d 0a 48 6f	0
0080	67 61 69 61 2e 63 73 2e	75 6d 61 73	0
0090	75 0d 0a 43 6f 6e 66 65	63 74 69 6f	0
00a0	65 65 70 2d 61 6c 69 76	65 0d 0a 43	0
00b0	2d 43 6f 6e 74 72 6f 6c	3a 20 6d 61	0
00c0	65 3d 30 0d 0a 55 70 67	72 61 64 65	0
00d0	65 63 75 72 65 2d 52 65	71 75 65 73	0
00e0	31 0d 0a 55 73 65 72 2d	41 67 65 6e	0
00f0	6f 7a 69 6c 6c 61 2f 35	2e 30 20 28	0
0100	6e 74 6f 73 68 3b 20 49	6e 74 65 6c	0
0110	20 4f 53 20 58 20 31 30	5f 31 35 5f	0
0120	70 70 6c 65 57 65 62 4b	69 74 2f 35	0
0130	36 20 28 4b 48 54 4d 4c	2c 20 6c 69	0
0140	65 63 6b 6f 29 20 43 68	72 6f 6d 65	0
0150	2e 30 2e 30 2e 30 20 53	61 66 61 72	0
0160	37 2e 33 36 0d 0a 41 63	63 65 70 74	0
0170	78 74 2f 68 74 6d 6c 2c	61 70 70 6c	0
0180	69 6f 6e 2f 78 68 74 6d	6c 2b 78 6d	0
0190	70 6c 69 63 61 74 69 6f	6e 2f 78 6d	0
01a0	30 2e 39 2c 69 6d 61 67	65 2f 61 76	0
01b0	6d 61 67 65 2f 77 65 62	70 2c 69 6d	0
01c0	61 70 6e 67 2c 2a 2f 2a	3b 71 3d 30	0
01d0	70 70 6c 69 63 61 74 69	6f 6e 2f 73	0

Antrą karta siunčiant GET requeštą jau yra matomas „IF-MODIFIED-SINCE“ header’is. Juo yra pateikiamas laikas kuomet paskutinį kartą buvo atsiųstas HTML dokumentas. Jeigu dokumentas nepakitęs nuo to laiko, serveris nesiūs nieko atgal.

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.

68.0.54	128.119.245.12	HTTP	601 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
19.245.12	192.168.0.54	HTTP	796 HTTP/1.1 200 OK (text/html)
68.0.54	128.119.245.12	HTTP	713 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
19.245.12	192.168.0.54	HTTP	306 HTTP/1.1 304 Not Modified

Kadangi failas nepakito, tai serveris mum duomenų pilnų negražino ir todėl naršyklė pasižmė šį resursą iš cache.

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?

→	445 2.895914	192.168.0.54	128.119.245.12	HTTP	601 GET /wireshark-labs/HTTP-wireshark
←	462 3.010260	128.119.245.12	192.168.0.54	HTTP	583 HTTP/1.1 200 OK (text/html)

Buvo išsiųstas 1 HTTP GET requestas, jo numeris yra 445.

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

→	445 2.895914	192.168.0.54	128.119.245.12	HTTP	601 GET /wireshark-labs/HTTP-wireshark
←	462 3.010260	128.119.245.12	192.168.0.54	HTTP	583 HTTP/1.1 200 OK (text/html)

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

→	445 2.895914	192.168.0.54	128.119.245.12	HTTP	601 GET /wireshark-labs/HTTP-wireshark
←	462 3.010260	128.119.245.12	192.168.0.54	HTTP	583 HTTP/1.1 200 OK (text/html)

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

→	445 2.895914	192.168.0.54	128.119.245.12	HTTP	601 GET /wireshark-labs/HTTP-wireshark
←	462 3.010260	128.119.245.12	192.168.0.54	HTTP	583 HTTP/1.1 200 OK (text/html)
> Frame 462: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) at 00:00:00:00:00:00 [ethernet] on "D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe)", Src: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe), Dst: App [00:00:00:00:00:00] on interface 1 > Ethernet II, Src: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe), Dst: App [00:00:00:00:00:00] on interface 1 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.54 [00:00:00:00:00:00] on interface 1 > Transmission Control Protocol, Src Port: 80, Dst Port: 60708, Seq: 0, Ack: 0, Len: 583 [00:00:00:00:00:00] on interface 1 > [4 Reassembled TCP Segments] (4861 bytes): #458(1448), #460(1448), #461(1448), #462(1448) ↳ Hypertext Transfer Protocol ↳ HTTP/1.1 200 OK\r\n					
0000 48 54 54 50 2f 31 2e 31 20 32 30 30 0010 0a 44 61 74 65 3a 20 53 61 74 2c 20 0020 65 63 20 32 30 32 32 20 30 30 3a 33 0030 20 47 4d 54 0d 0a 53 65 72 76 65 72 0040 61 63 68 65 2f 32 2e 34 2e 36 20 28 0050 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 0060 32 6b 2d 66 69 70 73 20 50 48 50 2f 0070 33 30 20 6d 6f 64 5f 70 65 72 6c 2f 0080 21 21 20 50 65 72 6c 2f 76 75 21 21					

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

786	5.180865	192.168.0.54	128.119.245.12	HTTP	601 GET /wireshark-labs/HTTP-wireshark
799	5.291643	128.119.245.12	192.168.0.54	HTTP	1367 HTTP/1.1 200 OK (text/html)
804	5.306670	192.168.0.54	128.119.245.12	HTTP	511 GET /pearson.png HTTP/1.1
826	5.416891	128.119.245.12	192.168.0.54	HTTP	781 HTTP/1.1 200 OK (PNG)
841	5.558632	192.168.0.54	178.79.137.164	HTTP	478 GET /8E_cover_small.jpg HTTP/1.1
851	5.605735	178.79.137.164	192.168.0.54	HTTP	237 HTTP/1.1 301 Moved Permanently

Buvo siūsti 3 GET request'ai. Pirmi du kreipėsi į tą patį puslapio adresą (128.119.245.12), kol paskutinis į 178.79.137.164

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.

Kadangi šiu paketu laikas yra skirtinas ir didėja monotoniškai, tai darau prielaida kad juos atsiisiuntė vieną po kito.

786	5.180865	192.168.0.54	128.119.245.12	HTTP	601 GET /wireshark-labs/HTTP-wireshark
799	5.291643	128.119.245.12	192.168.0.54	HTTP	1367 HTTP/1.1 200 OK (text/html)
804	5.306670	192.168.0.54	128.119.245.12	HTTP	511 GET /pearson.png HTTP/1.1
826	5.416891	128.119.245.12	192.168.0.54	HTTP	781 HTTP/1.1 200 OK (PNG)
841	5.558632	192.168.0.54	178.79.137.164	HTTP	478 GET /8E_cover_small.jpg HTTP/1.1
851	5.605735	178.79.137.164	192.168.0.54	HTTP	237 HTTP/1.1 301 Moved Permanently

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

68.0.54	128.119.245.12	HTTP	617 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.htm...
19.245.12	192.168.0.54	HTTP	783 HTTP/1.1 401 Unauthorized (text/html)
68.0.54	128.119.245.12	HTTP	702 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.htm...
19.245.12	192.168.0.54	HTTP	556 HTTP/1.1 200 OK (text/html)

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

68.0.54	128.119.245.12	HTTP	617	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.htm...
19.245.12	192.168.0.54	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
68.0.54	128.119.245.12	HTTP	702	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.htm...
19.245.12	192.168.0.54	HTTP	556	HTTP/1.1 200 OK (text/html)

```

> Frame 5076: 702 bytes on wire (5616 bits), 702 bytes captured (5616 bits)
> Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-Link (08:00:22:00:00:00)
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60944, Dst Port: 80, Seq 1, Ack 1, Len 5616
< Hypertext Transfer Protocol
  < GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.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
    < Authorization: Basic d2lyZXNoYXJrLXN0dWRlbz0m5ldHdvcmss=\r\n
      Credentials: wireshark-students:network
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.122 Safari/537.36
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,application/xml;q=0.9,*/*;q=0.8
      Referer: http://staff.ustc.edu.cn/\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-GB,en-US;q=0.9,en;q=0.8,lt;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protection/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
    [Response in frame: 5110]
  
```

0000	f0 b4 d2 c8 1f fe 88 66 5a 36 4b 9b 00
0010	02 b0 00 00 40 00 40 06 01 e6 c0 a8 00
0020	f5 0c ee 10 00 50 15 25 2c 47 db 30 00
0030	08 0a 97 64 00 00 01 01 08 0a 08 08 00
0040	80 c4 47 45 54 20 2f 77 69 72 65 73 00
0050	2d 6c 61 62 73 2f 70 72 6f 74 65 63 00
0060	70 61 67 65 73 2f 48 54 54 50 2d 77 00
0070	68 61 72 6b 2d 66 69 6c 65 35 2e 68 00
0080	48 54 54 50 2f 31 2e 31 0d 0a 48 6f 00
0090	67 61 69 61 2e 63 73 2e 75 6d 61 73 00
00a0	75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 00
00b0	65 65 70 2d 61 6c 69 76 65 0d 0a 43 00
00c0	2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 00
00d0	65 3d 30 0d 0a 41 75 74 68 6f 72 69 00
00e0	6f 6e 3a 20 42 61 73 69 63 20 64 32 00
00f0	4e 6f 59 58 4a 72 4c 58 4e 30 64 57 00
0100	52 7a 4f 6d 35 6c 64 48 64 76 63 6d 00
0110	55 70 67 72 61 64 65 2d 49 6e 73 65 00
0120	2d 52 65 71 75 65 73 74 73 3a 20 31 00
0130	65 72 2d 41 67 65 6e 74 3a 20 4d 6f 00
0140	61 2f 35 2e 30 20 28 4d 61 63 69 6e 00
0150	3b 20 49 6e 74 65 6c 20 4d 61 63 20 00
0160	20 31 30 5f 31 35 5f 37 29 20 41 70 00
0170	65 62 4b 69 74 2f 35 33 37 2e 33 36 00
0180	54 4d 4c 2c 20 6c 69 6b 65 20 47 65 00
0190	20 43 68 72 6f 6d 65 2f 31 30 38 2e 00
01a0	30 20 53 61 66 61 72 69 2f 35 33 37 00
01b0	0a 41 63 63 65 70 74 3a 20 74 65 78 00
01c0	6d 6c 2c 61 70 70 6c 69 63 61 74 69 00
01d0	68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 00

## DNS paketu filtravimas

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

<table border="1"> <thead> <tr><th></th><th>6</th><th>2.466045</th><th>192.168.0.54</th><th>5.20.0.10</th><th>DNS</th><th>72</th><th>Standard query 0x80bf A www.ietf.org</th></tr> </thead> <tbody> <tr><td>-</td><td>7</td><td>2.468977</td><td>5.20.0.10</td><td>192.168.0.54</td><td>DNS</td><td>459</td><td>Standard query response 0x80bf A www.ietf.org</td></tr> <tr><td>-</td><td>618</td><td>2.901472</td><td>192.168.0.54</td><td>5.20.0.10</td><td>DNS</td><td>78</td><td>Standard query 0xc94a A analytics.ietf.org</td></tr> <tr><td>&gt;</td><td colspan="7">Frame 6: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface</td></tr> <tr><td>&gt;</td><td colspan="7">Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn_c8:1f:01 (00:0c:29:00:00:01)</td></tr> <tr><td>&gt;</td><td colspan="7">Internet Protocol Version 4, Src: 192.168.0.54, Dst: 5.20.0.10</td></tr> <tr><td>    0100 .... = Version: 4</td><td colspan="7"></td></tr> <tr><td>    .... 0101 = Header Length: 20 bytes (5)</td><td colspan="7"></td></tr> <tr><td>&gt; Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</td><td colspan="7"></td></tr> <tr><td>    Total Length: 58</td><td colspan="7"></td></tr> <tr><td>    Identification: 0xb733 (46899)</td><td colspan="7"></td></tr> <tr><td>&gt; 000. .... = Flags: 0x0</td><td colspan="7"></td></tr> <tr><td>    ..0 0000 0000 0000 = Fragment Offset: 0</td><td colspan="7"></td></tr> <tr><td>    Time to Live: 64</td><td colspan="7"></td></tr> <tr><td>Protocol: UDP (17)</td><td colspan="7"></td></tr> <tr><td>    Header Checksum: 0xfd83 [validation disabled]</td><td colspan="7"></td></tr> <tr><td>        [Header checksum status: Unverified]</td><td colspan="7"></td></tr> <tr><td>    Source Address: 192.168.0.54</td><td colspan="7"></td></tr> <tr><td>    Destination Address: 5.20.0.10</td><td colspan="7"></td></tr> <tr><td>&gt; User Datagram Protocol, Src Port: 62246, Dst Port: 53</td><td colspan="7"></td></tr> <tr><td>&gt; Domain Name System (query)</td><td colspan="7"></td></tr> </tbody> </table>		6	2.466045	192.168.0.54	5.20.0.10	DNS	72	Standard query 0x80bf A www.ietf.org	-	7	2.468977	5.20.0.10	192.168.0.54	DNS	459	Standard query response 0x80bf A www.ietf.org	-	618	2.901472	192.168.0.54	5.20.0.10	DNS	78	Standard query 0xc94a A analytics.ietf.org	>	Frame 6: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface							>	Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn_c8:1f:01 (00:0c:29:00:00:01)							>	Internet Protocol Version 4, Src: 192.168.0.54, Dst: 5.20.0.10							0100 .... = Version: 4								.... 0101 = Header Length: 20 bytes (5)								> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)								Total Length: 58								Identification: 0xb733 (46899)								> 000. .... = Flags: 0x0								..0 0000 0000 0000 = Fragment Offset: 0								Time to Live: 64								Protocol: UDP (17)								Header Checksum: 0xfd83 [validation disabled]								[Header checksum status: Unverified]								Source Address: 192.168.0.54								Destination Address: 5.20.0.10								> User Datagram Protocol, Src Port: 62246, Dst Port: 53								> Domain Name System (query)								<table border="1"> <tbody> <tr><td>0000</td><td>f0</td><td>b4</td><td>d2</td><td>c8</td><td>1f</td><td>fe</td><td>88</td><td>66</td><td>5a</td><td>36</td><td>4b</td><td>9b</td><td>08</td><td>00</td></tr> <tr><td>0010</td><td>00</td><td>3a</td><td>b7</td><td>33</td><td>00</td><td>00</td><td>40</td><td>11</td><td>fd</td><td>83</td><td>c0</td><td>a8</td><td>00</td><td>36</td></tr> <tr><td>0020</td><td>00</td><td>0a</td><td>f3</td><td>26</td><td>00</td><td>35</td><td>00</td><td>26</td><td>a3</td><td>45</td><td>80</td><td>bf</td><td>01</td><td>00</td></tr> <tr><td>0030</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>03</td><td>77</td><td>77</td><td>77</td><td>04</td><td>69</td><td>65</td><td>74</td></tr> <tr><td>0040</td><td>6f</td><td>72</td><td>67</td><td>00</td><td>00</td><td>01</td><td>00</td><td>01</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>01</td></tr> </tbody> </table>	0000	f0	b4	d2	c8	1f	fe	88	66	5a	36	4b	9b	08	00	0010	00	3a	b7	33	00	00	40	11	fd	83	c0	a8	00	36	0020	00	0a	f3	26	00	35	00	26	a3	45	80	bf	01	00	0030	00	00	00	00	00	00	03	77	77	77	04	69	65	74	0040	6f	72	67	00	00	01	00	01	00	00	00	00	00	01
	6	2.466045	192.168.0.54	5.20.0.10	DNS	72	Standard query 0x80bf A www.ietf.org																																																																																																																																																																																																																																													
-	7	2.468977	5.20.0.10	192.168.0.54	DNS	459	Standard query response 0x80bf A www.ietf.org																																																																																																																																																																																																																																													
-	618	2.901472	192.168.0.54	5.20.0.10	DNS	78	Standard query 0xc94a A analytics.ietf.org																																																																																																																																																																																																																																													
>	Frame 6: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface																																																																																																																																																																																																																																																			
>	Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn_c8:1f:01 (00:0c:29:00:00:01)																																																																																																																																																																																																																																																			
>	Internet Protocol Version 4, Src: 192.168.0.54, Dst: 5.20.0.10																																																																																																																																																																																																																																																			
0100 .... = Version: 4																																																																																																																																																																																																																																																				
.... 0101 = Header Length: 20 bytes (5)																																																																																																																																																																																																																																																				
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)																																																																																																																																																																																																																																																				
Total Length: 58																																																																																																																																																																																																																																																				
Identification: 0xb733 (46899)																																																																																																																																																																																																																																																				
> 000. .... = Flags: 0x0																																																																																																																																																																																																																																																				
..0 0000 0000 0000 = Fragment Offset: 0																																																																																																																																																																																																																																																				
Time to Live: 64																																																																																																																																																																																																																																																				
Protocol: UDP (17)																																																																																																																																																																																																																																																				
Header Checksum: 0xfd83 [validation disabled]																																																																																																																																																																																																																																																				
[Header checksum status: Unverified]																																																																																																																																																																																																																																																				
Source Address: 192.168.0.54																																																																																																																																																																																																																																																				
Destination Address: 5.20.0.10																																																																																																																																																																																																																																																				
> User Datagram Protocol, Src Port: 62246, Dst Port: 53																																																																																																																																																																																																																																																				
> Domain Name System (query)																																																																																																																																																																																																																																																				
0000	f0	b4	d2	c8	1f	fe	88	66	5a	36	4b	9b	08	00																																																																																																																																																																																																																																						
0010	00	3a	b7	33	00	00	40	11	fd	83	c0	a8	00	36																																																																																																																																																																																																																																						
0020	00	0a	f3	26	00	35	00	26	a3	45	80	bf	01	00																																																																																																																																																																																																																																						
0030	00	00	00	00	00	00	03	77	77	77	04	69	65	74																																																																																																																																																																																																																																						
0040	6f	72	67	00	00	01	00	01	00	00	00	00	00	01																																																																																																																																																																																																																																						

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

<table border="1"> <thead> <tr><th></th><th>6</th><th>2.466045</th><th>192.168.0.54</th><th>5.20.0.10</th><th>DNS</th><th>72</th><th>Standard query 0x80bf A www.ietf.org</th></tr> </thead> <tbody> <tr><td>-</td><td>7</td><td>2.468977</td><td>5.20.0.10</td><td>192.168.0.54</td><td>DNS</td><td>459</td><td>Standard query response 0x80bf A www.ietf.org</td></tr> <tr><td>-</td><td>618</td><td>2.901472</td><td>192.168.0.54</td><td>5.20.0.10</td><td>DNS</td><td>78</td><td>Standard query 0xc94a A analytics.ietf.org</td></tr> <tr><td>-</td><td>668</td><td>2.904173</td><td>5.20.0.10</td><td>192.168.0.54</td><td>DNS</td><td>496</td><td>Standard query response 0xc94a A analytics.ietf.org</td></tr> <tr><td>&gt;</td><td colspan="7">Frame 6: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface</td></tr> <tr><td>&gt;</td><td colspan="7">Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn_c8:1f:01 (00:0c:29:00:00:01)</td></tr> <tr><td>&gt;</td><td colspan="7">Internet Protocol Version 4, Src: 192.168.0.54, Dst: 5.20.0.10</td></tr> <tr><td>&gt;</td><td colspan="7">User Datagram Protocol, Src Port: 53, Dst Port: 62246</td></tr> <tr><td>    Source Port: 53</td><td colspan="7"></td></tr> <tr><td>    Destination Port: 62246</td><td colspan="7"></td></tr> <tr><td>    Length: 425</td><td colspan="7"></td></tr> <tr><td>    Checksum: 0x8b54 [unverified]</td><td colspan="7"></td></tr> <tr><td>        [Checksum Status: Unverified]</td><td colspan="7"></td></tr> <tr><td>        [Stream index: 0]</td><td colspan="7"></td></tr> <tr><td>&gt; [Timestamps]</td><td colspan="7"></td></tr> <tr><td>    UDP payload (417 bytes)</td><td colspan="7"></td></tr> <tr><td>&gt; Domain Name System (response)</td><td colspan="7"></td></tr> </tbody> </table>		6	2.466045	192.168.0.54	5.20.0.10	DNS	72	Standard query 0x80bf A www.ietf.org	-	7	2.468977	5.20.0.10	192.168.0.54	DNS	459	Standard query response 0x80bf A www.ietf.org	-	618	2.901472	192.168.0.54	5.20.0.10	DNS	78	Standard query 0xc94a A analytics.ietf.org	-	668	2.904173	5.20.0.10	192.168.0.54	DNS	496	Standard query response 0xc94a A analytics.ietf.org	>	Frame 6: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface							>	Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn_c8:1f:01 (00:0c:29:00:00:01)							>	Internet Protocol Version 4, Src: 192.168.0.54, Dst: 5.20.0.10							>	User Datagram Protocol, Src Port: 53, Dst Port: 62246							Source Port: 53								Destination Port: 62246								Length: 425								Checksum: 0x8b54 [unverified]								[Checksum Status: Unverified]								[Stream index: 0]								> [Timestamps]								UDP payload (417 bytes)								> Domain Name System (response)								<table border="1"> <tbody> <tr><td>0000</td><td>88</td><td>66</td><td>5a</td><td>36</td><td>4b</td><td>9b</td><td>f0</td><td>b4</td><td>d2</td><td>c8</td><td>1f</td><td>fe</td><td>08</td><td>00</td></tr> <tr><td>0010</td><td>01</td><td>bd</td><td>57</td><td>7e</td><td>00</td><td>3e</td><td>11</td><td>5d</td><td>b6</td><td>05</td><td>14</td><td>00</td><td>0a</td><td></td></tr> <tr><td>0020</td><td>00</td><td>36</td><td>00</td><td>35</td><td>f3</td><td>26</td><td>01</td><td>a9</td><td>8b</td><td>54</td><td>80</td><td>bf</td><td>81</td><td>80</td></tr> <tr><td>0030</td><td>00</td><td>03</td><td>00</td><td>05</td><td>00</td><td>0a</td><td>03</td><td>77</td><td>77</td><td>77</td><td>04</td><td>69</td><td>65</td><td>74</td></tr> <tr><td>0040</td><td>6f</td><td>72</td><td>67</td><td>00</td><td>00</td><td>01</td><td>00</td><td>01</td><td>c0</td><td>0c</td><td>00</td><td>05</td><td>00</td><td>01</td></tr> <tr><td>0050</td><td>06</td><td>11</td><td>00</td><td>21</td><td>03</td><td>77</td><td>77</td><td>77</td><td>04</td><td>69</td><td>65</td><td>74</td><td>66</td><td>03</td></tr> <tr><td>0060</td><td>67</td><td>03</td><td>63</td><td>64</td><td>6e</td><td>0a</td><td>63</td><td>6c</td><td>6f</td><td>75</td><td>64</td><td>66</td><td>6c</td><td>61</td></tr> <tr><td>0070</td><td>03</td><td>6e</td><td>65</td><td>74</td><td>00</td><td>c0</td><td>2a</td><td>00</td><td>01</td><td>00</td><td>01</td><td>00</td><td>00</td><td>00</td></tr> <tr><td>0080</td><td>04</td><td>68</td><td>10</td><td>2c</td><td>63</td><td>c0</td><td>2a</td><td>00</td><td>01</td><td>00</td><td>01</td><td>00</td><td>00</td><td>00</td></tr> <tr><td>0090</td><td>04</td><td>68</td><td>10</td><td>2d</td><td>63</td><td>c0</td><td>3b</td><td>00</td><td>02</td><td>00</td><td>01</td><td>00</td><td>00</td><td>89</td></tr> <tr><td>00a0</td><td>06</td><td>03</td><td>6e</td><td>73</td><td>32</td><td>c0</td><td>3b</td><td>c0</td><td>3b</td><td>00</td><td>02</td><td>00</td><td>01</td><td>00</td></tr> <tr><td>00b0</td><td>14</td><td>00</td><td>06</td><td>03</td><td>6e</td><td>73</td><td>35</td><td>c0</td><td>3b</td><td>c0</td><td>3b</td><td>00</td><td>02</td><td>00</td></tr> <tr><td>00c0</td><td>00</td><td>89</td><td>14</td><td>00</td><td>06</td><td>03</td><td>6e</td><td>73</td><td>33</td><td>c0</td><td>3b</td><td>c0</td><td>3b</td><td>00</td></tr> <tr><td>00d0</td><td>01</td><td>00</td><td>00</td><td>89</td><td>14</td><td>00</td><td>06</td><td>03</td><td>6e</td><td>73</td><td>31</td><td>c0</td><td>3b</td><td>c0</td></tr> <tr><td>00e0</td><td>02</td><td>00</td><td>01</td><td>00</td><td>00</td><td>89</td><td>14</td><td>00</td><td>06</td><td>03</td><td>6e</td><td>73</td><td>34</td><td>c0</td></tr> <tr><td>00f0</td><td>77</td><td>00</td><td>01</td><td>00</td><td>01</td><td>00</td><td>02</td><td>6d</td><td>00</td><td>04</td><td>c6</td><td>29</td><td>2d</td><td>00</td></tr> </tbody> </table>	0000	88	66	5a	36	4b	9b	f0	b4	d2	c8	1f	fe	08	00	0010	01	bd	57	7e	00	3e	11	5d	b6	05	14	00	0a		0020	00	36	00	35	f3	26	01	a9	8b	54	80	bf	81	80	0030	00	03	00	05	00	0a	03	77	77	77	04	69	65	74	0040	6f	72	67	00	00	01	00	01	c0	0c	00	05	00	01	0050	06	11	00	21	03	77	77	77	04	69	65	74	66	03	0060	67	03	63	64	6e	0a	63	6c	6f	75	64	66	6c	61	0070	03	6e	65	74	00	c0	2a	00	01	00	01	00	00	00	0080	04	68	10	2c	63	c0	2a	00	01	00	01	00	00	00	0090	04	68	10	2d	63	c0	3b	00	02	00	01	00	00	89	00a0	06	03	6e	73	32	c0	3b	c0	3b	00	02	00	01	00	00b0	14	00	06	03	6e	73	35	c0	3b	c0	3b	00	02	00	00c0	00	89	14	00	06	03	6e	73	33	c0	3b	c0	3b	00	00d0	01	00	00	89	14	00	06	03	6e	73	31	c0	3b	c0	00e0	02	00	01	00	00	89	14	00	06	03	6e	73	34	c0	00f0	77	00	01	00	01	00	02	6d	00	04	c6	29	2d	00
	6	2.466045	192.168.0.54	5.20.0.10	DNS	72	Standard query 0x80bf A www.ietf.org																																																																																																																																																																																																																																																																																																																																																																																		
-	7	2.468977	5.20.0.10	192.168.0.54	DNS	459	Standard query response 0x80bf A www.ietf.org																																																																																																																																																																																																																																																																																																																																																																																		
-	618	2.901472	192.168.0.54	5.20.0.10	DNS	78	Standard query 0xc94a A analytics.ietf.org																																																																																																																																																																																																																																																																																																																																																																																		
-	668	2.904173	5.20.0.10	192.168.0.54	DNS	496	Standard query response 0xc94a A analytics.ietf.org																																																																																																																																																																																																																																																																																																																																																																																		
>	Frame 6: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface																																																																																																																																																																																																																																																																																																																																																																																								
>	Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn_c8:1f:01 (00:0c:29:00:00:01)																																																																																																																																																																																																																																																																																																																																																																																								
>	Internet Protocol Version 4, Src: 192.168.0.54, Dst: 5.20.0.10																																																																																																																																																																																																																																																																																																																																																																																								
>	User Datagram Protocol, Src Port: 53, Dst Port: 62246																																																																																																																																																																																																																																																																																																																																																																																								
Source Port: 53																																																																																																																																																																																																																																																																																																																																																																																									
Destination Port: 62246																																																																																																																																																																																																																																																																																																																																																																																									
Length: 425																																																																																																																																																																																																																																																																																																																																																																																									
Checksum: 0x8b54 [unverified]																																																																																																																																																																																																																																																																																																																																																																																									
[Checksum Status: Unverified]																																																																																																																																																																																																																																																																																																																																																																																									
[Stream index: 0]																																																																																																																																																																																																																																																																																																																																																																																									
> [Timestamps]																																																																																																																																																																																																																																																																																																																																																																																									
UDP payload (417 bytes)																																																																																																																																																																																																																																																																																																																																																																																									
> Domain Name System (response)																																																																																																																																																																																																																																																																																																																																																																																									
0000	88	66	5a	36	4b	9b	f0	b4	d2	c8	1f	fe	08	00																																																																																																																																																																																																																																																																																																																																																																											
0010	01	bd	57	7e	00	3e	11	5d	b6	05	14	00	0a																																																																																																																																																																																																																																																																																																																																																																												
0020	00	36	00	35	f3	26	01	a9	8b	54	80	bf	81	80																																																																																																																																																																																																																																																																																																																																																																											
0030	00	03	00	05	00	0a	03	77	77	77	04	69	65	74																																																																																																																																																																																																																																																																																																																																																																											
0040	6f	72	67	00	00	01	00	01	c0	0c	00	05	00	01																																																																																																																																																																																																																																																																																																																																																																											
0050	06	11	00	21	03	77	77	77	04	69	65	74	66	03																																																																																																																																																																																																																																																																																																																																																																											
0060	67	03	63	64	6e	0a	63	6c	6f	75	64	66	6c	61																																																																																																																																																																																																																																																																																																																																																																											
0070	03	6e	65	74	00	c0	2a	00	01	00	01	00	00	00																																																																																																																																																																																																																																																																																																																																																																											
0080	04	68	10	2c	63	c0	2a	00	01	00	01	00	00	00																																																																																																																																																																																																																																																																																																																																																																											
0090	04	68	10	2d	63	c0	3b	00	02	00	01	00	00	89																																																																																																																																																																																																																																																																																																																																																																											
00a0	06	03	6e	73	32	c0	3b	c0	3b	00	02	00	01	00																																																																																																																																																																																																																																																																																																																																																																											
00b0	14	00	06	03	6e	73	35	c0	3b	c0	3b	00	02	00																																																																																																																																																																																																																																																																																																																																																																											
00c0	00	89	14	00	06	03	6e	73	33	c0	3b	c0	3b	00																																																																																																																																																																																																																																																																																																																																																																											
00d0	01	00	00	89	14	00	06	03	6e	73	31	c0	3b	c0																																																																																																																																																																																																																																																																																																																																																																											
00e0	02	00	01	00	00	89	14	00	06	03	6e	73	34	c0																																																																																																																																																																																																																																																																																																																																																																											
00f0	77	00	01	00	01	00	02	6d	00	04	c6	29	2d	00																																																																																																																																																																																																																																																																																																																																																																											

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?

```
~ $ cat /etc/resolv.conf
#
# macOS Notice
#
# This file is not consulted for DNS hostname resolution, address
# resolution, or the DNS query routing mechanism used by most
# processes on this system.
#
# To view the DNS configuration used by this system, use:
# scutil --dns
#
# SEE ALSO
# dns-sd(1), scutil(8)
#
# This file is automatically generated.
#
search Dlink
nameserver 5.20.0.10
nameserver 5.20.0.11
~ $
```

No.	Time	Source	Destination	Protocol	Length	Info
6	2.466045	192.168.0.54	5.20.0.10	DNS	72	Standard query 0x80bf A www.ietf.org
7	2.468977	5.20.0.10	192.168.0.54	DNS	459	Standard query response 0x80bf A www.ietf.org
618	2.901472	192.168.0.54	5.20.0.10	DNS	78	Standard query 0xc94a A analytics.ietf.org
668	2.904173	5.20.0.10	192.168.0.54	DNS	496	Standard query response 0xc94a A analytics.ietf.org
12	2.475491	192.168.0.54	104.16.44.99	HTTP	556	GET / HTTP/1.1
17	2.499896	104.16.44.99	192.168.0.54	HTTP	369	HTTP/1.1 301 Moved Permanently
4	2.457537	192.168.0.54	3.121.238.86	TCP	1514	61034 -> 443 [ACK] Seq=1 Ack=1 Win=2048

Frame 6: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eth0  
> Ethernet II, Src: Apple\_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-Link\_c8:1f:fe (00:0c:29:c8:1f:fe)  
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 5.20.0.10  
 0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 58  
Identification: 0xb733 (46899)  
.... 0000 .... = Flags: 0xA

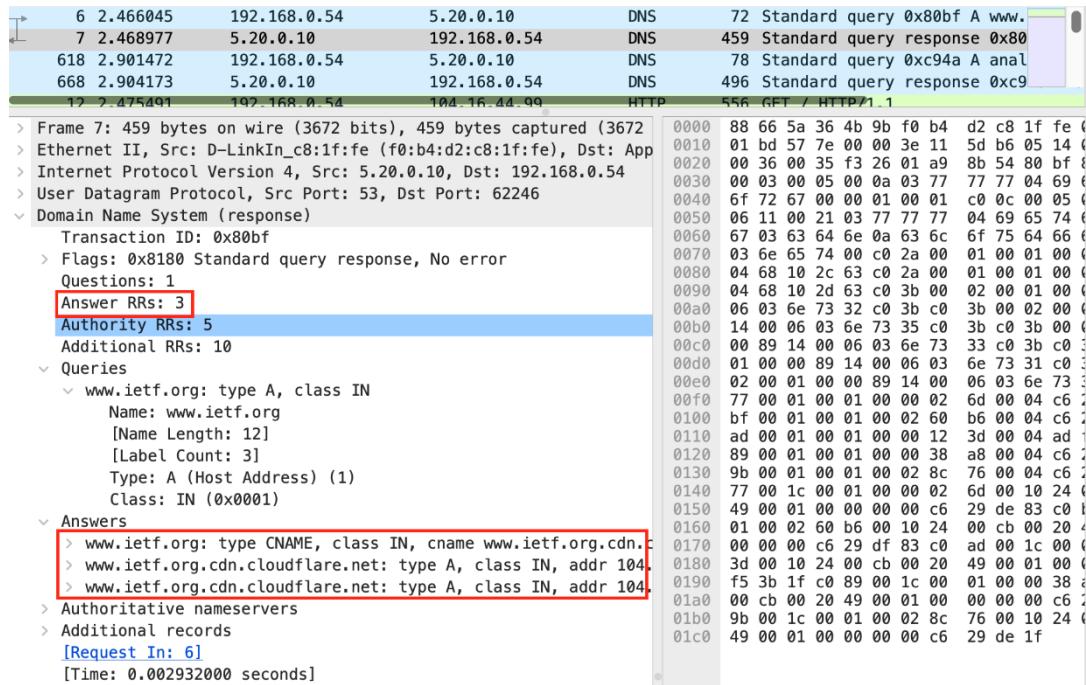
7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

No.	Time	Source	Destination	Protocol	Length	Info
6	2.466045	192.168.0.54	5.20.0.10	DNS	72	Standard query 0x80bf A www.ietf.org
7	2.468977	5.20.0.10	192.168.0.54	DNS	459	Standard query response 0x80bf A www.ietf.org
618	2.901472	192.168.0.54	5.20.0.10	DNS	78	Standard query 0xc94a A analytics.ietf.org
668	2.904173	5.20.0.10	192.168.0.54	DNS	496	Standard query response 0xc94a A analytics.ietf.org
12	2.475491	192.168.0.54	104.16.44.99	HTTP	556	GET / HTTP/1.1

> Frame 6: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)  
> Ethernet II, Src: Apple\_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-Link\_c8:1f:fe (00:0c:29:c8:1f:fe)  
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 5.20.0.10  
> User Datagram Protocol, Src Port: 62246, Dst Port: 53  
> Domain Name System (query)  
 Transaction ID: 0x80bf  
> Flags: 0x0100 Standard query  
 Questions: 1  
 Answer RRs: 0  
 Authority RRs: 0  
 Additional RRs: 0  
 > Queries  
 > www.ietf.org: type A, class IN  
 Name: www.ietf.org  
 [Name Length: 12]  
 [Label Count: 3]  
 Type: A (Host Address) (1)  
 Class: IN (0x0001)

Čia yra „A“ tipo užklausa. Negražintas nei vienas „answer“

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



Kiekviename atsakyme yra gražinama:

- Vardas, pagal kurių yra kuriamas DNS užklausa
- DNS įrašo tipas
- TTL – time to live
- Duomenų ilgis
- IP adresas (jeigu tankamas DNS įrašo tipas)

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?

b 2.466045	192.168.0.54	5.20.0.10	DNS	/z Standard query 0x8001 A www.
7 2.468977	5.20.0.10	192.168.0.54	DNS	459 Standard query response 0x80
8 2.472360	192.168.0.54	104.16.44.99	TCP	78 62098 → 80 [SYN] Seq=0 Win=6
9 2.472806	192.168.0.54	104.16.44.99	TCP	78 62099 → 80 [SYN] Seq=0 Win=6
10 2.474969	104.16.44.99	192.168.0.54	TCP	74 80 → 62098 [SYN, ACK] Seq=0
11 2.475032	192.168.0.54	104.16.44.99	TCP	66 62098 → 80 [ACK] Seq=1 Ack=1
12 2.475491	192.168.0.54	104.16.44.99	HTTP	556 GET / HTTP/1.1
13 2.475818	104.16.44.99	192.168.0.54	TCP	74 80 → 62099 [SYN, ACK] Seq=0
14 2.475858	192.168.0.54	104.16.44.99	TCP	66 62099 → 80 [ACK] Seq=1 Ack=1
15 2.479350	104.16.44.99	192.168.0.54	TCP	66 80 → 62098 [ACK] Seq=1 Ack=4
16 2.489666	3.121.238.86	192.168.0.54	TCP	66 443 → 61934 [ACK] Seq=1 Ack=
17 2.499896	104.16.44.99	192.168.0.54	HTTP	369 HTTP/1.1 301 Moved Permanent
18 2.499961	192.168.0.54	104.16.44.99	TCP	66 62098 → 80 [ACK] Seq=491 Ack
19 2.504136	192.168.0.54	104.16.44.99	TCP	78 62100 → 443 [SYN] Seq=0 Win=
20 2.506763	104.16.44.99	192.168.0.54	TCP	74 443 → 62100 [SYN, ACK] Seq=0
21 2.506823	192.168.0.54	104.16.44.99	TCP	66 62100 → 443 [ACK] Seq=1 Ack=
22 2.507002	192.168.0.54	104.16.44.99	TLSv1...	615 Client Hello
23 2.509961	104.16.44.99	192.168.0.54	TCP	66 443 → 62100 [ACK] Seq=1 Ack=
24 2.512073	104.16.44.99	192.168.0.54	TLSv1...	278 Server Hello, Change Cipher
25 2.512108	192.168.0.54	104.16.44.99	TCP	66 62100 → 443 [ACK] Seq=550 Ac
26 2.512407	192.168.0.54	104.16.44.99	TLSv1...	130 Change Cipher Spec, Applicat
27 2.512528	192.168.0.54	104.16.44.99	TLSv1...	164 Application Data
28 2.512635	192.168.0.54	104.16.44.99	TLSv1...	574 Application Data
29 2.515106	104.16.44.99	192.168.0.54	TLSv1...	578 Application Data, Applicatio
30 2.515106	104.16.44.99	192.168.0.54	TLSv1...	97 Application Data
Name: www.ietf.org [Name Length: 12] [Label Count: 3] Type: A (Host Address) (1) Class: IN (0x0001)				
Answers				
www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net				
Name: www.ietf.org Type: CNAME (Canonical NAME for an alias) (5) Class: IN (0x0001) Time to live: 1553 (25 minutes, 53 seconds) Data length: 33 CNAME: www.ietf.org.cdn.cloudflare.net				
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99				
Name: www.ietf.org.cdn.cloudflare.net Type: A (Host Address) (1) Class: IN (0x0001) Time to live: 53 (53 seconds) Data length: 4 Address: 104.16.44.99				

0000	88 66 5a 36 4b 9b f0 b4 d2 c8 1
0010	01 bd 57 7e 00 00 3e 11 5d b6 0
0020	00 36 00 35 f3 26 01 a9 8b 54 8
0030	00 03 00 05 00 0a 03 77 77 77 0
0040	6f 72 67 00 00 01 00 01 c0 0c 0
0050	06 11 00 21 03 77 77 77 04 69 6
0060	67 03 63 64 6e 0a 63 6c 6f 75 6
0070	03 6e 65 74 00 c0 2a 00 01 00 0
0080	04 68 10 2c 63 c0 2a 00 01 00 0
0090	04 68 10 2d 63 c0 3b 00 02 00 0
00a0	06 03 6e 73 32 c0 3b c0 3b 00 0
00b0	14 00 06 03 6e 73 35 c0 3b c0 3
00c0	00 89 14 00 06 03 6e 73 33 c0 3
00d0	01 00 00 89 14 00 06 03 6e 73 33
00e0	02 00 01 00 00 89 14 00 06 03 6e 73 3
00f0	77 00 01 00 01 00 00 02 6d 00 0
0100	bf 00 01 00 01 00 02 60 b6 00 0
0110	ad 00 01 00 01 00 00 12 3d 00 0
0120	89 00 01 00 01 00 00 38 a8 00 0
0130	9b 00 01 00 01 00 02 8c 76 00 0
0140	77 00 1c 00 01 00 00 02 6d 00 1
0150	49 00 01 00 00 00 00 c6 29 de 0
0160	01 00 02 60 b6 00 10 24 00 cb 0
0170	00 00 00 c6 29 df 83 c0 ad 00 1

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

6	2.466045	192.168.0.54	5.20.0.10	DNS	72	Standard query 0x80bf A www.
7	2.468977	5.20.0.10	192.168.0.54	DNS	459	Standard query response 0x80
8	2.472360	192.168.0.54	104.16.44.99	TCP	78	62098 → 80 [SYN] Seq=0 Win=6
9	2.472806	192.168.0.54	104.16.44.99	TCP	78	62099 → 80 [SYN] Seq=0 Win=6
10	2.474969	104.16.44.99	192.168.0.54	TCP	74	80 → 62098 [SYN, ACK] Seq=0
11	2.475032	192.168.0.54	104.16.44.99	TCP	66	62098 → 80 [ACK] Seq=1 Ack=1
12	2.475491	192.168.0.54	104.16.44.99	HTTP	556	GET / HTTP/1.1
13	2.475818	104.16.44.99	192.168.0.54	TCP	74	80 → 62099 [SYN, ACK] Seq=0
14	2.475858	192.168.0.54	104.16.44.99	TCP	66	62099 → 80 [ACK] Seq=1 Ack=1
15	2.479350	104.16.44.99	192.168.0.54	TCP	66	80 → 62098 [ACK] Seq=1 Ack=4
16	2.489666	3.121.238.86	192.168.0.54	TCP	66	443 → 61934 [ACK] Seq=1 Ack=
17	2.499896	104.16.44.99	192.168.0.54	HTTP	369	HTTP/1.1 301 Moved Permanent
18	2.499961	192.168.0.54	104.16.44.99	TCP	66	62098 → 80 [ACK] Seq=491 Ack
19	2.504136	192.168.0.54	104.16.44.99	TCP	78	62100 → 443 [SYN] Seq=0 Win=
20	2.506763	104.16.44.99	192.168.0.54	TCP	74	443 → 62100 [SYN, ACK] Seq=0
21	2.506823	192.168.0.54	104.16.44.99	TCP	66	62100 → 443 [ACK] Seq=1 Ack=
22	2.507002	192.168.0.54	104.16.44.99	TLSv1...	615	Client Hello
23	2.509961	104.16.44.99	192.168.0.54	TCP	66	443 → 62100 [ACK] Seq=1 Ack=
24	2.512073	104.16.44.99	192.168.0.54	TLSv1...	278	Server Hello, Change Cipher
25	2.512108	192.168.0.54	104.16.44.99	TCP	66	62100 → 443 [ACK] Seq=550 Ac
26	2.512407	192.168.0.54	104.16.44.99	TLSv1...	130	Change Cipher Spec, Applicat
27	2.512528	192.168.0.54	104.16.44.99	TLSv1...	164	Application Data
28	2.512635	192.168.0.54	104.16.44.99	TLSv1...	574	Application Data
29	2.515106	104.16.44.99	192.168.0.54	TLSv1...	578	Application Data, Applicatio
30	2.515106	104.16.44.99	192.168.0.54	TLSv1...	97	Application Data
31	2.515154	192.168.0.54	104.16.44.99		66	62100 → 443 [ACK] Seq=1020 Ack

Iš paviršutiniško paketų vaizdo tas nebuvo pastebėta.

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

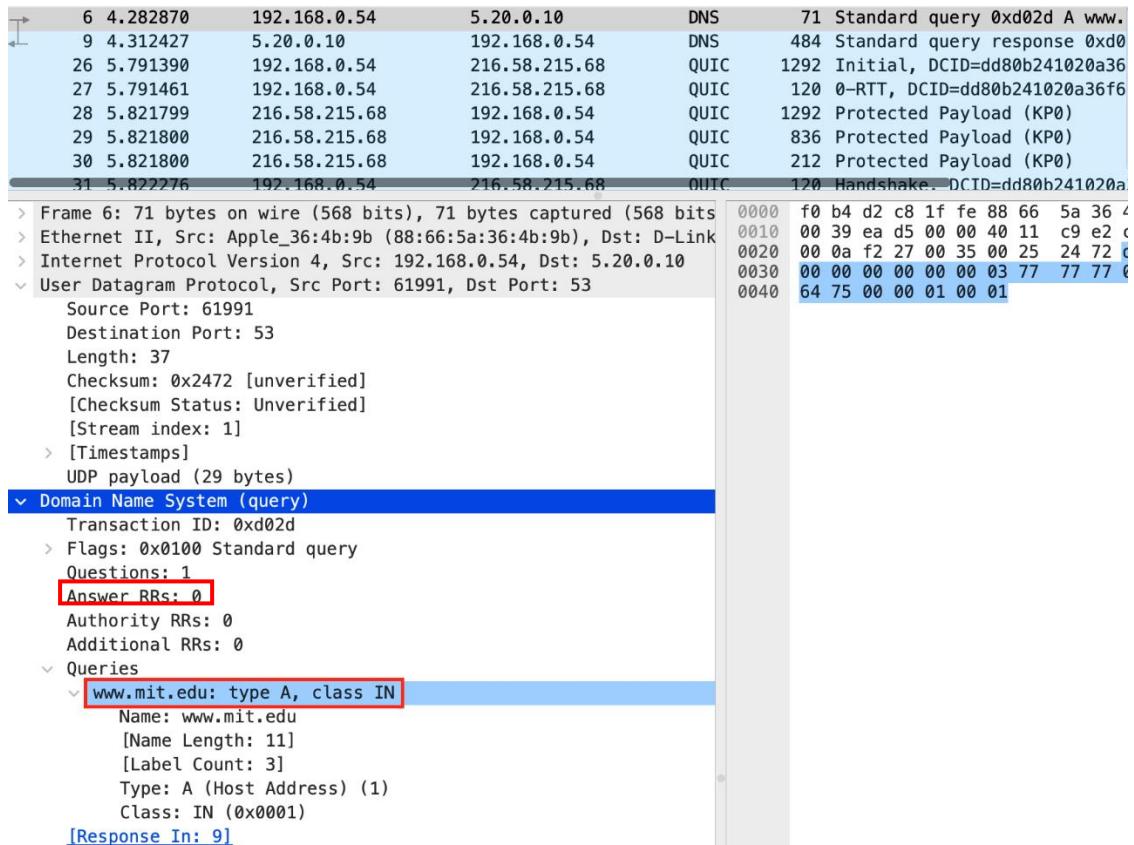
68.0.54	5.20.0.10	DNS	71 Standard query 0xd02d A www.mit.edu
0.10	192.168.0.54	DNS	484 Standard query response 0xd02d A www.mit.edu CNAME www.m.
68.0.54	216.58.215.68	QUIC	1292 Initial, DCID=dd80b241020a36f6, PKN: 1, PADDING, PING, P
68.0.54	216.58.215.68	QUIC	120 0-RTT, DCID=dd80b241020a36f6
8 215 68	192.168.0.54	QUIC	1292 Protected Payload (KPA)
> Frame 6: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)			
> Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-Link			
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 5.20.0.10			
> User Datagram Protocol, Src Port: 61991, Dst Port: 53			
Source Port: 61991			
Destination Port: 53			
Length: 37			
Checksum: 0x2472 [unverified]			
[Checksum Status: Unverified]			
[Stream index: 1]			
> [Timestamps]			
UDP payload (29 bytes)			
68.0.54	5.20.0.10	DNS	71 Standard query 0xd02d A www.mit.edu
0.10	192.168.0.54	DNS	484 Standard query response 0xd02d A www.mit.edu CNAME www.m.
68.0.54	216.58.215.68	QUIC	1292 Initial, DCID=dd80b241020a36f6, PKN: 1, PADDING, PING, P
68.0.54	216.58.215.68	QUIC	120 0-RTT, DCID=dd80b241020a36f6
8 215 68	192.168.0.54	QUIC	1292 Protected Payload (KPA)
> Frame 9: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits)			
> Ethernet II, Src: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe), Dst: App			
> Internet Protocol Version 4, Src: 5.20.0.10, Dst: 192.168.0.54			
> User Datagram Protocol, Src Port: 53, Dst Port: 61991			
Source Port: 53			
Destination Port: 61991			
Length: 450			
Checksum: 0xaef9 [unverified]			
[Checksum Status: Unverified]			
[Stream index: 1]			
> [Timestamps]			
UDP payload (442 bytes)			

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

6 4.282870	192.168.0.54	5.20.0.10	DNS	71 Standard query 0xd02d A www.
9 4.312427	5.20.0.10	192.168.0.54	DNS	484 Standard query response 0xd0
26 5.791390	192.168.0.54	216.58.215.68	QUIC	1292 Initial, DCID=dd80b241020a36
27 5.791461	192.168.0.54	216.58.215.68	QUIC	120 0-RTT, DCID=dd80b241020a36f6
28 5.821700	216.58.215.68	192.168.0.54	QUIC	1292 Protected Payload (KPA)
> Frame 6: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)				
> Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-Link				
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 5.20.0.10				
> User Datagram Protocol, Src Port: 61991, Dst Port: 53				
Source Port: 61991				
Destination Port: 53				
Length: 37				
Checksum: 0x2472 [unverified]				
[Checksum Status: Unverified]				
[Stream index: 1]				
> [Timestamps]				
UDP payload (29 bytes)				

Taip, čia yra mano lokalus DNS serverio adresas (žiūrėti 6 užduotį)

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



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

6	4.282870	192.168.0.54	5.20.0.10	DNS	71	Standard query 0xd02d A www.
9	4.312427	5.20.0.10	192.168.0.54	DNS	484	Standard query response 0xd0
26	5.791390	192.168.0.54	216.58.215.68	QUIC	1292	Initial, DCID=dd80b241020a36
27	5.791461	192.168.0.54	216.58.215.68	QUIC	120	0-RTT, DCID=dd80b241020a36f6
28	5.821799	216.58.215.68	192.168.0.54	QUIC	1292	Protected Payload (KPO)
29	5.821800	216.58.215.68	192.168.0.54	QUIC	836	Protected Payload (KPO)
30	5.821800	216.58.215.68	192.168.0.54	QUIC	212	Protected Payload (KPO)
31	5.822276	192.168.0.54	216.58.215.68	QUIC	120	Handshake. DCID=dd80b241020a
> Frame 9: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits)						
> Ethernet II, Src: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe), Dst: App						
> Internet Protocol Version 4, Src: 5.20.0.10, Dst: 192.168.0.54						
< User Datagram Protocol, Src Port: 53, Dst Port: 61991						
Source Port: 53						
Destination Port: 61991						
Length: 450						
Checksum: 0xaef9 [unverified]						
[Checksum Status: Unverified]						
[Stream index: 1]						
[Timestamps]						
UDP payload (442 bytes)						
< Domain Name System (response)						
Transaction ID: 0xd02d						
> Flags: 0x8100 Standard query response, No error						
Questions: 1						
Answer RRs: 3						
Authority RRs: 8						
Additional RRs: 9						
< Queries						
< www.mit.edu: type A, class IN						
Name: www.mit.edu						
[Name Length: 11]						
[Label Count: 3]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
< Answers						
> www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey						
> www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.c						
Name: www.mit.edu.edgekey.net						
Type: CNAME (Canonical NAME for an alias) (5)						
Class: IN (0x0001)						
Time to live: 37 (37 seconds)						
Data length: 24						
CNAME: e9566.dscb.akamaiedge.net						
> e9566.dscb.akamaiedge.net: type A, class IN, addr 104.81.118						
< Authoritative nameservers						
< Additional records						
[Request In: 6]						
[Time: 0.029557000 seconds]						

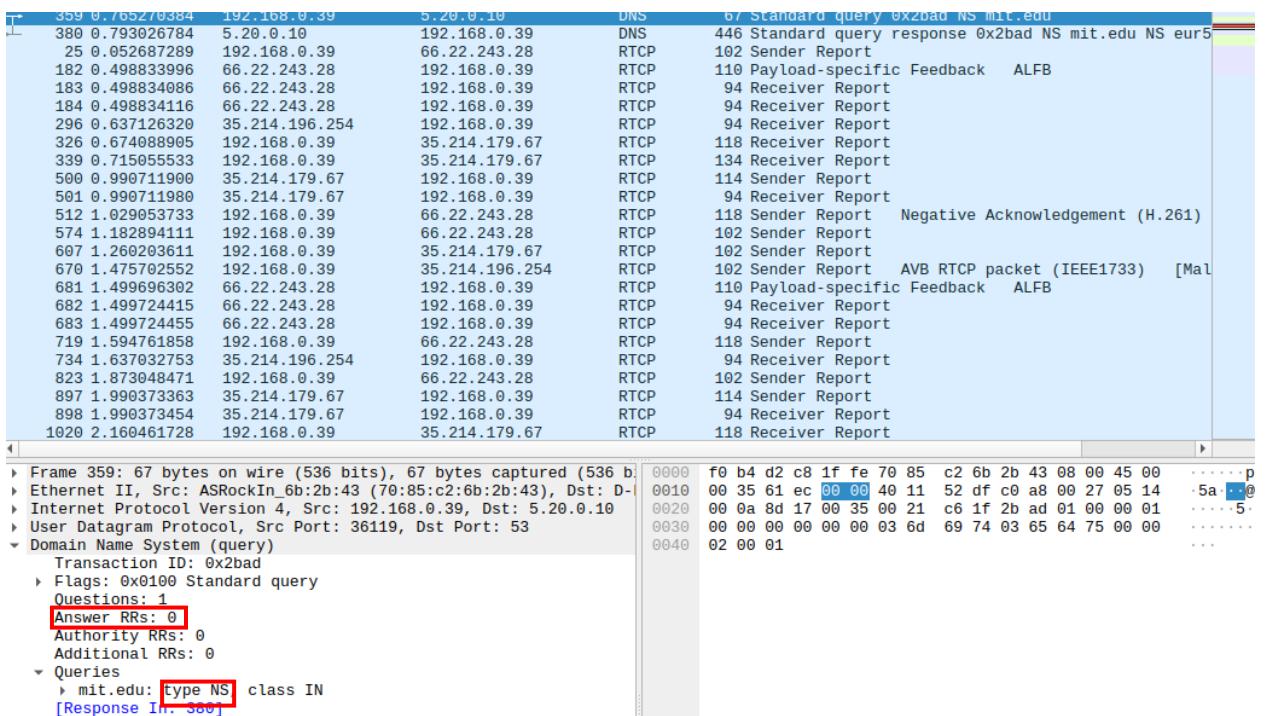
Gauti 3 atsakymai. Žiūrėti 8 užduotį, nes joje pateikiama informacija yra identiška šiam atasakymui.

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

192.168.0.39	5.20.0.10	DNS	67 Standard query 0x2bad NS mit.edu
5.20.0.10	192.168.0.39	DNS	446 Standard query response 0x2bad NS mit.edu

Taip, čia yra mano lokalaus DNS serverio adresas (žiūrėti 6 užduotį)

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



Ši kartą tai yra Name Server DNS užklausa. Tačiau ir vėl gražinama 0 atsakymų.

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

Internet Protocol Version 4, Src: 5.20.0.10, Dst: 192.168.0.39  
User Datagram Protocol, Src Port: 53, Dst Port: 36119  
Domain Name System (response)  
Transaction ID: 0x2bad  
Flags: 0x8180 Standard query response, No error  
Questions: 1  
Answer RRs: 8  
Authority RRs: 0  
Additional RRs: 11  
Queries  
Answers  
Additional records

- ▶ use5.akam.net: type A, class IN, addr 2.16.40.64
- ▶ ns1-173.akam.net: type A, class IN, addr 193.108.91.173
- ▶ use2.akam.net: type A, class IN, addr 96.7.49.64
- ▶ usw2.akam.net: type A, class IN, addr 184.26.161.64
- ▶ ns1-37.akam.net: type A, class IN, addr 193.108.91.37
- ▶ eur5.akam.net: type A, class IN, addr 23.74.25.64
- ▶ asia1.akam.net: type A, class IN, addr 95.100.175.64
- ▶ asia2.akam.net: type A, class IN, addr 95.101.36.64
- ▶ use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
- ▶ ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
- ▶ ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25

[Request In: 359]  
[Time: 0.027756460 seconds]

Pateikiami 8 „A“ tipo DNS įrašai. Šalia jų yra pateikiami ir jų adresai.

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?

5769552	192.168.0.39	<b>5.20.0.10</b>	DNS	73 Standard query 0x56d4 A bitsy.mit.edu
5777717	192.168.0.39	<b>5.20.0.10</b>	DNS	73 Standard query 0x00d0 AAAA bitsy.mit.edu
2046232	5.20.0.10	192.168.0.39	DNS	138 Standard query response 0x00d0 AAAA bitsy.mit.edu SOA use2.ak...
2437717	5.20.0.10	192.168.0.39	DNS	468 Standard query response 0x56d4 A bitsy.mit.edu A 18.0.72.3 NS..

Taip, čia yra mano lokalus DNS serverio adresas (žiūrėti 6 užduotį).

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

6769552	192.168.0.39	5.20.0.10	DNS	73 Standard query 0x56d4 A bitsy.mit.edu
5777717	192.168.0.39	5.20.0.10	DNS	73 Standard query 0x00d0 AAAA bitsy.mit.edu
2046232	5.20.0.10	192.168.0.39	DNS	138 Standard query response 0x00d0 AAAA bitsy.mit.edu SOA use2.ak...
2437717	5.20.0.10	192.168.0.39	DNS	468 Standard query response 0x56d4 A bitsy.mit.edu A 18.0.72.3 NS...

Tipas – A, 0 „atsakymų“.

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

6769552	192.168.0.39	5.20.0.10	DNS	73 Standard query 0x56d4 A bitsy.mit.edu
5777717	192.168.0.39	5.20.0.10	DNS	73 Standard query 0x00d0 AAAA bitsy.mit.edu
2046232	5.20.0.10	192.168.0.39	DNS	138 Standard query response 0x00d0 AAAA bitsy.mit.edu SOA use2.ak...
2437717	5.20.0.10	192.168.0.39	DNS	468 Standard query response 0x56d4 A bitsy.mit.edu A 18.0.72.3 NS...
3287071	192.168.0.39	18.0.72.3	DNS	74 Standard query 0x0375 A www.aiit.or.kr
3953913	192.168.0.39	18.0.72.3	DNS	74 Standard query 0x0375 A www.aiit.or.kr
28048998	192.168.0.39	5.20.0.10	DNS	71 Standard query 0x8643 A discord.com
28057764	192.168.0.39	5.20.0.10	DNS	71 Standard query 0x0345 AAAA discord.com
29151026	5.20.0.10	192.168.0.39	DNS	467 Standard query response 0x8643 A discord.com A 162.159.135.23...
29194086	5.20.0.10	192.168.0.39	DNS	130 Standard query response 0x0345 AAAA discord.com SOA gabe.ns.c...
50293541	192.168.0.39	18.0.72.3	DNS	74 Standard query 0x0375 A www.aiit.or.kr
32633198	192.168.0.39	5.20.0.10	DNS	85 Standard query 0xbf56 A ade.googlesyndication.com
32636645	192.168.0.39	5.20.0.10	DNS	85 Standard query 0x6350 AAAA ade.googlesyndication.com A ...
33687707	5.20.0.10	192.168.0.39	DNS	356 Standard query response 0xbf56 A ade.googlesyndication.com A ...
37312453	5.20.0.10	192.168.0.39	DNS	142 Standard query response 0x6350 AAAA ade.googlesyndication.com ...
73836326	192.168.0.39	5.20.0.10	DNS	78 Standard query 0xecd9 A ping.archlinux.org
73848148	192.168.0.39	5.20.0.10	DNS	78 Standard query 0x90d8 AAAA ping.archlinux.org
74810554	5.20.0.10	192.168.0.39	DNS	519 Standard query response 0xecd9 A ping.archlinux.org CNAME red...
74971146	5.20.0.10	192.168.0.39	DNS	531 Standard query response 0x90d8 AAAA ping.archlinux.org CNAME ...
29535056	192.168.0.39	162.159.135.232	QUIC	1392 Initial, DCID=2fa740a5b25efccf, PKN: 1, CRYPTO, PADDING
29637739	192.168.0.39	162.159.135.232	QUIC	116 0-RTT, DCID=2fa740a5b25efccf
29743197	192.168.0.39	162.159.135.232	QUIC	310 0-RTT, DCID=2fa740a5b25efccf
31253270	162.159.135.232	192.168.0.39	QUIC	1242 Protected Payload (KP0)
31498450	192.168.0.39	162.159.135.232	QUIC	132 Handshake, DCID=01e2e26f6e0d8f4539e2766f700dbf72131bd185
31703194	162.159.135.232	192.168.0.39	QUIC	94 Protected Payload (KP0)
31731067	162.159.135.232	192.168.0.39	QUIC	66 Protected Payload (KP0)
31731107	162.159.135.232	192.168.0.39	QUIC	66 Protected Payload (KP0)
31759591	192.168.0.39	162.159.135.232	QUIC	87 Protected Payload (KP0), DCID=01e2e26f6e0d8f4539e2766f700dbf7...
31773627	162.159.135.232	192.168.0.39	QUIC	91 Protected Payload (KP0)
31797371	192.168.0.39	162.159.135.232	QUIC	87 Protected Payload (KP0), DCID=01e2e26f6e0d8f4539e2766f700dbf7...
31837196	192.168.0.39	162.159.135.232	QUIC	89 Protected Payload (KP0), DCID=01e2e26f6e0d8f4539e2766f700dbf7...

Frame 275: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits) ▶ Ethernet II, Src: D-LinkIn\_C8:1f:fe (00:b4:d2:c8:1f:fe), Dst: ASI [ether] ▶ Internet Protocol Version 4, Src: 5.20.0.10, Dst: 192.168.0.39 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 48773 ▶ Domain Name System (response)  
 Transaction ID: 0x56d4  
 Flags: 0x0100 Standard query response, No error  
 Questions: 1  
 Answer RRs: 1  
 Authority RRs: 8  
 Additional RRs: 11  
 ▶ Queries  
 ▶ Answers  
 ▶ bitsy.mit.edu: type A, class IN, addr 18.0.72.3  
 ▶ Authoritative nameservers  
 ▶ Additional records  
 [Request In: 267]  
 [Time: 0.005668165 seconds]

Pateikiamas 1 atsakymas. Informacija identiškai kaip ir 8 uždavinyje.

## TCP paketu 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?

1	0.000000	192.168.0.54	3.121.187.176	TCP	1514	49640
2	0.000134	192.168.0.54	3.121.187.176	TLSv1...	192	Appli
3	0.031413	3.121.187.176	192.168.0.54	TCP	66	443 →
4	0.344259	3.121.187.176	192.168.0.54	TLSv1...	111	Appli
5	0.344334	192.168.0.54	3.121.187.176	TCP	66	49640

```
Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface
Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn_c8:1f:fe (f0:1
Internet Protocol Version 4, Src: 192.168.0.54, Dst: 3.121.187.176
Transmission Control Protocol, Src Port: 49640, Dst Port: 443, Seq: 1, Ack: 1, Len:
Source Port: 49640
Destination Port: 443
```

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?

2	0.000134	192.168.0.54	3.121.187.176	TLSv1...	192	Application Data
3	0.031413	3.121.187.176	192.168.0.54	TCP	66	443 → 49640 [ACK] Seq=1 Ack=1575 Win=
4	0.344259	3.121.187.176	192.168.0.54	TLSv1...	111	Application Data
5	0.344334	192.168.0.54	3.121.187.176	TCP	66	49640 → 443 [ACK] Seq=1575 Ack=46 Win
6	1.223568	192.168.0.54	128.119.245.12	TCP	66	49824 → 80 [FIN, ACK] Seq=1 Ack=1 Win
7	1.223748	192.168.0.54	128.119.245.12	TCP	66	49821 → 80 [FIN, ACK] Seq=1 Ack=1 Win
8	1.223901	192.168.0.54	128.119.245.12	TCP	78	49840 → 80 [SYN] Seq=0 Win=65535 Len=

```
> Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
> Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe)
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49824, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
Source Port: 49824
Destination Port: 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?

160	1.681312	192.168.0.54	128.119.245.12	HTTP	347	POST /wireshark-labs/lab3-1-reply.htm
175	1.792808	128.119.245.12	192.168.0.54	HTTP	843	HTTP/1.1 200 OK (text/html)
	1	0.000000	192.168.0.54	3.121.187.176	TCP	1514 49640 → 443 [ACK] Seq=1 Ack=1 Win=204
	3	0.031413	3.121.187.176	192.168.0.54	TCP	66 443 → 49640 [ACK] Seq=1 Ack=1575 Win=
	5	0.344334	192.168.0.54	3.121.187.176	TCP	66 49640 → 443 [ACK] Seq=1575 Ack=46 Win

```
> Frame 160: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface en0, id 0
> Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe)
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49841, Dst Port: 80, Seq: 152775, Ack: 1, Len: 281
Source Port: 49841
Destination Port: 80
```

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?

5 1.223568	192.168.0.54	128.119.245.12	TCP	66 49824 → 80 [FIN, ACK] Seq=1 Ack=1 Win=
7 1.223748	192.168.0.54	128.119.245.12	TCP	66 49821 → 80 [FIN, ACK] Seq=1 Ack=1 Win=
8 1.223901	192.168.0.54	128.119.245.12	TCP	78 49840 → 80 [SYN] Seq=0 Win=65535 Len=
9 1.224000	192.168.0.54	128.119.245.12	TCP	78 49841 → 80 [SYN] Seq=0 Win=65535 Len=
10 1.341314	128.119.245.12	192.168.0.54	TCP	74 80 → 49841 [SYN, ACK] Seq=0 Ack=1 Win=
11 1.341315	128.119.245.12	192.168.0.54	TCP	66 80 → 49824 [ACK] Seq=1 Ack=2 Win=227

> Frame 8: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id 0  
 > Ethernet II, Src: Apple\_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn\_c8:1f:fe (f0:b4:d2:c8:1f:fe)  
 > Internet Protocol Version 4, Src: 192.168.0.54, Dst: 128.119.245.12  
 > Transmission Control Protocol, Src Port: 49840, Dst Port: 80, Seq: 0, Len: 0

Source Port: 49840  
 Destination Port: 80  
 [Stream index: 3]  
 [Conversation completeness: Incomplete, ESTABLISHED (7)]  
 [TCP Segment Len: 0]  
 Sequence Number: 0 (relative sequence number)  
 Sequence Number (raw): 3710385467  
 [Next Sequence Number: 1 (relative sequence number)]  
 Acknowledgment Number: 0  
 Acknowledgment number (raw): 0  
 1011 .... = Header Length: 44 bytes (11)  
 > Flags: 0x002 (SYN)

Kad čia yra SYN segmentas galime pagal Flag'us, kuriose yra matoma ši žymė.

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?

0 1.223568	192.168.0.54	128.119.245.12	TCP	66 49824 → 80 [FIN, ACK] Seq=1 Ack=1 Win=
7 1.223748	192.168.0.54	128.119.245.12	TCP	66 49821 → 80 [FIN, ACK] Seq=1 Ack=1 Win=
8 1.223901	192.168.0.54	128.119.245.12	TCP	78 49840 → 80 [SYN] Seq=0 Win=65535 Len=
9 1.224000	192.168.0.54	128.119.245.12	TCP	78 49841 → 80 [SYN] Seq=0 Win=65535 Len=
10 1.341314	128.119.245.12	192.168.0.54	TCP	74 80 → 49841 [SYN, ACK] Seq=0 Ack=1 Win=
11 1.341315	128.119.245.12	192.168.0.54	TCP	66 80 → 49824 [ACK] Seq=1 Ack=2 Win=227
12 1.341453	192.168.0.54	128.119.245.12	TCP	66 49841 → 80 [ACK] Seq=1 Ack=1 Win=1317

> Frame 10: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface en0, id 0  
 > Ethernet II, Src: D-LinkIn\_c8:1f:fe (f0:b4:d2:c8:1f:fe), Dst: Apple\_36:4b:9b (88:66:5a:36:4b:9b)  
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.54  
 > Transmission Control Protocol, Src Port: 80, Dst Port: 49841, Seq: 0, Ack: 1, Len: 0

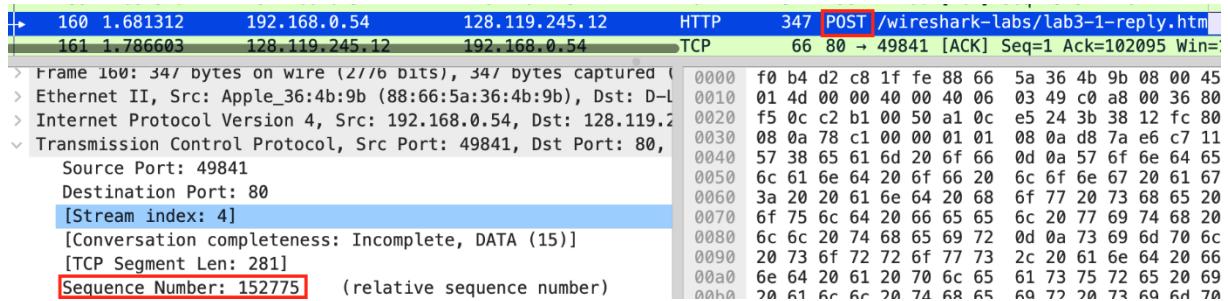
Source Port: 80  
 Destination Port: 49841  
 [Stream index: 4]  
 [Conversation completeness: Incomplete, DATA (15)]  
 [TCP Segment Len: 0]  
 Sequence Number: 0 (relative sequence number)  
 Sequence Number (raw): 993530619  
 [Next Sequence Number: 1 (relative ack number)]  
 Acknowledgment Number: 1 (relative ack number)  
 Acknowledgment number (raw): 2701824094  
 1010 .... = Header Length: 40 bytes (10)  
 > Flags: 0x012 (SYN, ACK)

„Acknowledgement“ skaičius pasako iki kokio baito gavėjas yra gavęs informaciją. Jeigu tikėtinas sequence skaičius iš siuntėjo ir acknowledgement skaičius ant gavėjo nesutampa po vieno paketu exchange, tai gali signalizuoti informacijos neatitikimą.

Kad šis segmentas yra SYN ACK, galime matyti vėl gi iš flag'ų.

6. What is the sequence number of the TCP segment containing the HTTP POST command?

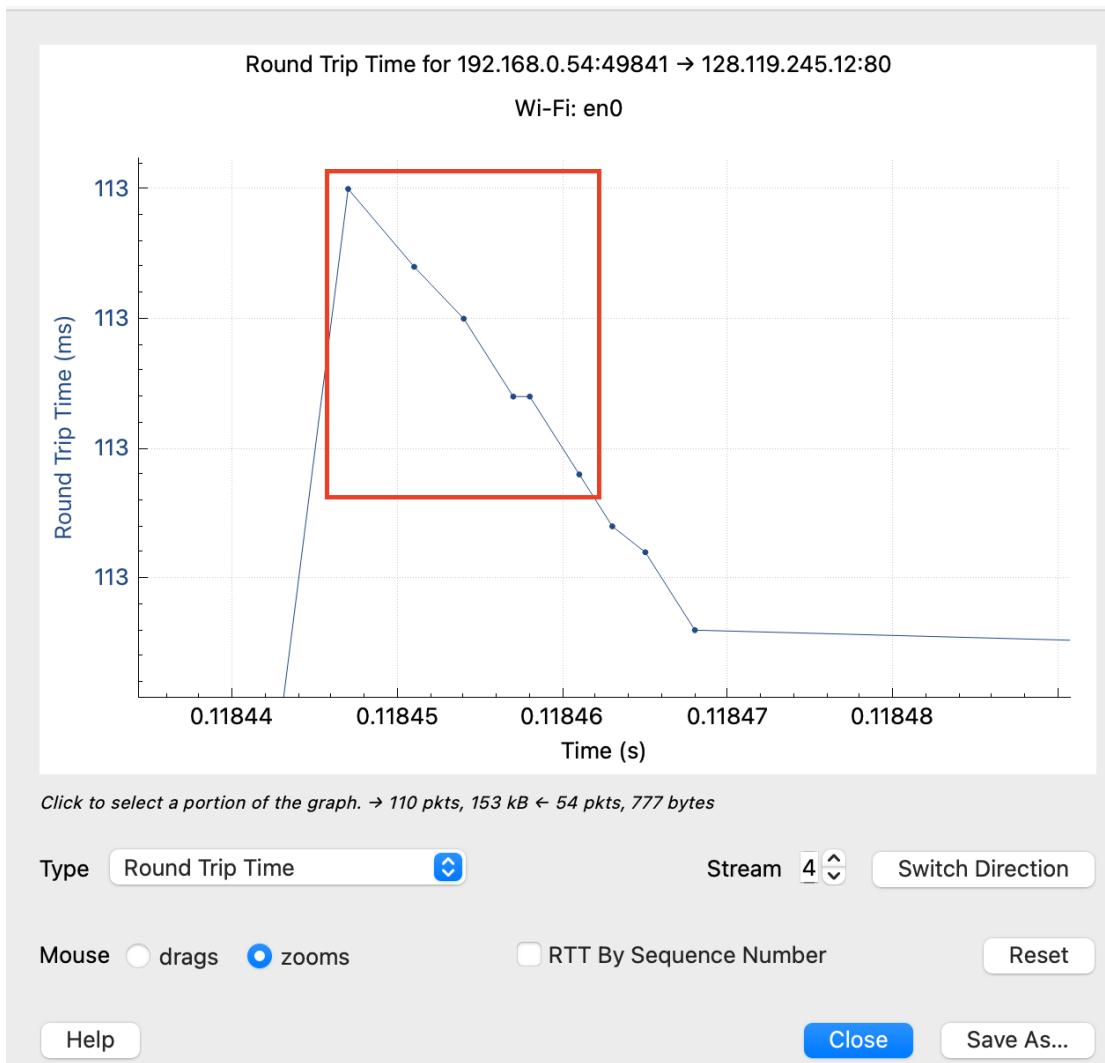
Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.



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 six segments? What is the EstimatedRTT value (see Section 3.5.3, page 242 in text) after the receipt of each ACK?

tcp.reassembled_in == 160						
No.	Time	Source	Destination	Protocol	Length	Info
13	1.342069	192.168.0.54	128.119.245.12	TCP	800	49841 → 80 [PSH, ACK] Seq=1 Ack=1 Win=1
17	1.342447	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=735 Ack=1 Win=13
18	1.342451	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=2183 Ack=1 Win=1
19	1.342454	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=3631 Ack=1 Win=1
20	1.342457	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=5079 Ack=1 Win=1
21	1.342458	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=6527 Ack=1 Win=1
22	1.342461	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=7975 Ack=1 Win=1
23	1.342463	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=9423 Ack=1 Win=1
24	1.342465	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=10871 Ack=1 Win=1
25	1.342468	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=12210 Ack=1 Win=1

Sequence number	Sent Time	Received time
1	1.342090	1.453099
735	1.342447	1.455372
2183	1.342451	1.455373
3631	1.342454	1.455374
5079	1.342457	1.455374
6527	1.342458	1.455375



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

13	1.342069	192.168.0.54	128.119.245.12	TCP	800	49841 → 80 [PSH, ACK] Seq=1 Ack=1 Win=13
17	1.342447	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=735 Ack=1 Win=13
18	1.342451	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=2183 Ack=1 Win=1
19	1.342454	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=3631 Ack=1 Win=1
20	1.342457	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=5079 Ack=1 Win=1
21	1.342458	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=6527 Ack=1 Win=1
22	1.342461	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=7975 Ack=1 Win=1
23	1.342463	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=9423 Ack=1 Win=1
24	1.342465	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=10871 Ack=1 Win=
25	1.342468	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=12319 Ack=1 Win=
27	1.453210	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=13767 Ack=1 Win=
37	1.455499	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=15215 Ack=1 Win=
38	1.455504	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=16663 Ack=1 Win=
39	1.455577	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=18111 Ack=1 Win=
40	1.455579	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=19559 Ack=1 Win=
41	1.455677	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=21007 Ack=1 Win=
42	1.455683	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=22455 Ack=1 Win=
43	1.455739	192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=23903 Ack=1 Win=1317

1514, išskyrus pradinį segmentą - 800.

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?

Source	Destination	Protocol	Length	Info
192.168.0.54	128.119.245.12	TCP	800	49841 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131712 Len=734 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=735 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=2183 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=3631 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=5079 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=6527 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=7975 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=9423 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=10871 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=12319 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=13767 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=15215 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=16663 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=18111 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=19559 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=21007 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=22455 Ack=1 Win=131712 Len=1448 TSval=363193
192.168.0.54	128.119.245.12	TCP	1514	49841 → 80 [ACK] Seq=23903 Ack=1 Win=131712 Len=1448 TSval=363193

Window size – 131712, ir jis tikrai nelimituoja siuntimo, žinant, kad vidutinis segmentas buvo vos apie 1514 baitų.

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

Kadangi iš atsakų „acknowledgement“ skaičiai nesikartodavo, tai galime sakyti, kad segmentai nebuvu persiūsti iš naujo.

(tcp.stream == 4 ) && !(tcp.reassembled_in == 160)				
Source	Destination	Protocol	Length	Info
192.168.0.54	128.119.245.12	TCP	78	49841 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 TSval=297358
192.168.0.54	128.119.245.12	TCP	66	49841 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=363193
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=735 Win=30464 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=2183 Win=33408 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=3631 Win=36224 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=5079 Win=39168 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=6527 Win=42112 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=7975 Win=44928 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=9423 Win=47872 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=10871 Win=50816 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=12319 Win=53632 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=13767 Win=56576 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=15215 Win=59392 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=18111 Win=65280 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=21007 Win=71040 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=23903 Win=76800 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=26799 Win=82560 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=29695 Win=88448 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=31143 Win=91264 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=32591 Win=94208 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=35487 Win=99968 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=38383 Win=105728 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=41279 Win=111616 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=44175 Win=117376 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=49967 Win=128896 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=51415 Win=131840 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=55759 Win=140544 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=61551 Win=152064 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=62999 Win=155008 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=67343 Win=163712 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=70239 Win=169472 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=73135 Win=175232 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=76031 Win=180608 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=77479 Win=179584 Len=0 TSval=297358

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).

Source	Destination	Protocol	Length	Info
192.168.0.54	128.119.245.12	TCP	78	49841 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=131712 Len=0 TSval=363193
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
192.168.0.54	128.119.245.12	TCP	66	49841 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=363193
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=735 Win=30464 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=2183 Win=33408 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=3631 Win=36224 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=5079 Win=39168 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=6527 Win=42112 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=7975 Win=44928 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=9423 Win=47872 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=10871 Win=50816 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=12319 Win=53632 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=13767 Win=56576 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=15215 Win=59392 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=18111 Win=65280 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=21007 Win=71040 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=23903 Win=76800 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=26799 Win=82560 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=29695 Win=88448 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=31143 Win=91264 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=32591 Win=94208 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=35487 Win=99968 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=38383 Win=105728 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=41279 Win=111616 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=44175 Win=117376 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=49967 Win=128896 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=51415 Win=131840 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=55759 Win=140544 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=61551 Win=152064 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=62999 Win=155008 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=67343 Win=163712 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=70239 Win=169472 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=73135 Win=175232 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	74	80 → 49841 [ACK] Seq=1 Ack=76031 Win=180608 Len=0 TSval=297358
128.119.245.12	192.168.0.54	TCP	66	80 → 49841 [ACK] Seq=1 Ack=77479 Win=179584 Len=0 TSval=297358

Vidutiniškai aknolege 'ina apie 1448 baitų. (inkrementas tarp ACK segmentų).

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

163 1.788854	128.119.245.12	192.168.0.54	TCP	66 80 → 49841 [ACK] Seq=1 Ack=113679 Win
164 1.789300	128.119.245.12	192.168.0.54	TCP	66 80 → 49841 [ACK] Seq=1 Ack=116575 Win
165 1.789301	128.119.245.12	192.168.0.54	TCP	66 80 → 49841 [ACK] Seq=1 Ack=123815 Win
166 1.789783	128.119.245.12	192.168.0.54	TCP	66 80 → 49841 [ACK] Seq=1 Ack=125263 Win
167 1.791269	128.119.245.12	192.168.0.54	TCP	66 80 → 49841 [ACK] Seq=1 Ack=132503 Win
168 1.791270	128.119.245.12	192.168.0.54	TCP	66 80 → 49841 [ACK] Seq=1 Ack=136847 Win
169 1.791911	128.119.245.12	192.168.0.54	TCP	66 80 → 49841 [ACK] Seq=1 Ack=139743 Win
170 1.791912	128.119.245.12	192.168.0.54	TCP	66 80 → 49841 [ACK] Seq=1 Ack=144087 Win
171 1.791912	128.119.245.12	192.168.0.54	TCP	66 80 → 49841 [ACK] Seq=1 Ack=145535 Win
172 1.792346	128.119.245.12	192.168.0.54	TCP	66 80 → 49841 [ACK] Seq=1 Ack=148431 Win
173 1.792346	128.119.245.12	192.168.0.54	TCP	66 80 → 49841 [ACK] Seq=1 Ack=152775 Win
174 1.792808	128.119.245.12	192.168.0.54	TCP	66 80 → 49841 [ACK] Seq=1 Ack=153056 Win
175 1.792808	128.119.245.12	192.168.0.54	HTTP	843 HTTP/1.1 200 OK (text/html)
176 1.792888	192.168.0.54	128.119.245.12	TCP	66 49841 → 80 [ACK] Seq=153056 Ack=778 Win=1

[Conversation completeness: Incomplete, DATA (15)]	0000 88 66 5a 36 4b 9b f0 b4 d2 c8 1f fe 08 00 45 0f
[TCP Segment Len: 0]	0010 00 34 44 dc 40 00 2f 06 d0 85 80 77 f5 0c c0 a5
Sequence Number: 1 (relative sequence number)	0020 00 36 00 50 c2 b1 3b 38 12 fc a1 0c e6 3d 80 1e
Sequence Number (raw): 993530620	0030 07 5c 77 da 00 00 01 01 08 0a 11 b9 57 a8 d8 7e
[Next Sequence Number: 1 (relative sequence number)]	0040 e6 c7
Acknowledgment Number: 153056 (relative ack number)	
Acknowledgment number (raw): 2701977149	
1000 .... = Header Length: 32 bytes (8)	
> Flags: 0x010 (ACK)	
Window: 1884	
[Calculated window size: 241152]	
[Window size scaling factor: 128]	
Checksum: 0x77da [unverified]	
[Checksum Status: Unverified]	
Urgent Pointer: 0	
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP)	
< [Timestamps]	
[Time since first frame in this TCP stream: 0.568808000]	

154056 / 0.568 ≈ 269085 Bps

## UDP paketu filtravimas

- 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.

5	0.000045	192.168.0.54	35.217.26.44	UDP	1158	65054 → 50002	Len=1116
6	0.000058	192.168.0.54	35.217.26.44	UDP	1158	65054 → 50002	Len=1116
7	0.005592	192.168.0.54	35.217.26.44	UDP	1158	65054 → 50002	Len=1116
8	0.005659	192.168.0.54	35.217.26.44	UDP	1158	65054 → 50002	Len=1116
9	0.005666	192.168.0.54	35.217.26.44	UDP	1158	65054 → 50002	Len=1116
10	0.005691	192.168.0.54	35.217.26.44	UDP	1159	65054 → 50002	Len=1117
12	0.011514	192.168.0.54	35.217.19.209	UDP	224	52483 → 50003	Len=182
> Frame 5: 1158 bytes on wire (9264 bits), 1158 bytes captured (9264 bits) on interface en0 > Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn_c8:1f:fe (f0:b4:d2:c1) > Internet Protocol Version 4, Src: 192.168.0.54, Dst: 35.217.26.44 ▼ User Datagram Protocol, Src Port: 65054, Dst Port: 50002							
Source Port: 65054 Destination Port: 50002 Length: 1124 Checksum: 0xafed [unverified]							

- source port
- destination port
- length
- checksum.

- 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.

5	0.000045	192.168.0.54	35.217.26.44	UDP	1158	65054 → 50002	Len=1116
6	0.000058	192.168.0.54	35.217.26.44	UDP	1158	65054 → 50002	Len=1116
7	0.005592	192.168.0.54	35.217.26.44	UDP	1158	65054 → 50002	Len=1116
8	0.005659	192.168.0.54	35.217.26.44	UDP	1158	65054 → 50002	Len=1116
9	0.005666	192.168.0.54	35.217.26.44	UDP	1158	65054 → 50002	Len=1116
10	0.005691	192.168.0.54	35.217.26.44	UDP	1159	65054 → 50002	Len=1117
12	0.011514	192.168.0.54	35.217.19.209	UDP	224	52483 → 50003	Len=182
> Frame 5: 1158 bytes on wire (9264 bits), 1158 bytes captured (9264 bits) on interface en0 > Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn_c8:1f:fe (f0:b4:d2:c1) > Internet Protocol Version 4, Src: 192.168.0.54, Dst: 35.217.26.44 ▼ User Datagram Protocol, Src Port: 65054, Dst Port: 50002							
Source Port: 65054 Destination Port: 50002 Length: 1124 Checksum: 0xafed [unverified]							
0020 1a 2c fe 1e c3 52 04 64 af ed 90 65 68 19 69 53 0030 2e 36 00 05 83 3b be de 00 03 01 ab 50 14 05 fa 0040 60 bd 13 45 99 14 9d fb 89 d0 0f f1 5f 6e 71 75 0050 60 64 1e 2a 7f a5 f3 db 83 84 75 33 12 58 cd 7d 0060 b5 6b 9b 04 65 35 25 e9 11 45 50 4c 3f b5 3b 47 0070 30 80 16 da 1b 84 98 c8 1d 6f c1 15 4e f9 58 3e 0080 67 f2 77 48 e0 3d b2 13 d0 ba d2 06 0b 4e c4 64 0090 5a 80 a4 ca fe 7f 45 be fd d7 da 8a b1 95 63 c5 00a0 18 d2 05 3c 59 62 2e a7 54 91 3c 73 7d 7d 49 a2 00b0 a1 r7 7a r4 a1 r6 r2 r7 76 73 77 f0 26 h2 r3							

2 baitai, nes čia yra „hexadecimal characters“, kurie kiekvienas užima 4 bitus, tai jų pora yra oktetas, arba vienas baitas.

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.

Paketo dydis (ar ilgis) susideda iš antraštės (*header*) ir siunčiamų duomenų. Taigi, imant tą patį pavyzdį:

5 0.000045	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
6 0.000058	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
7 0.005592	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
8 0.005659	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
9 0.005666	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
10 0.005691	192.168.0.54	35.217.26.44	UDP	1159 65054 → 50002 Len=1117
12 0.011514	192.168.0.54	35.217.19.209	UDP	224 52483 → 50003 Len=182

> Frame 5: 1158 bytes on wire (9264 bits), 1158 bytes captured (9264 bits)  
> Ethernet II, Src: Apple\_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn\_c8:1  
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 35.217.26.44  
< User Datagram Protocol, Src Port: 65054, Dst Port: 50002  
  Source Port: 65054  
  Destination Port: 50002  
**Length: 1124**  
  Checksum: 0xafed [unverified]  
  [Checksum Status: Unverified]  
  [Stream index: 0]  
  > [Timestamps]  
    **UDP payload (1116 bytes)**

**1116 + 2\*4 = 1124**

0020	1a 2c fe 1e c3 52 04 64 af ed 90 65 68 19 69 53
0030	2e 36 00 05 83 3b be de 00 03 01 ab 50 14 05 fa
0040	60 bd 13 45 99 14 9d fb 89 d0 0f f1 5f 6e 71 75
0050	60 64 1e 2a 7f a5 f3 db 83 84 75 33 12 58 cd 7d
0060	b5 6b 9b 04 65 35 25 e9 11 45 50 4c 3f b5 3b 47
0070	30 80 16 da 1b 84 98 c8 1d 6f c1 15 4e f9 58 3e
0080	67 f2 77 48 e0 3d b2 13 d0 ba d2 06 0b 4e c4 64
0090	5a 80 a4 ca fe 7f 45 be fd d7 da 8a b1 95 63 c5
00a0	18 d2 05 3c 59 62 2e a7 54 91 3c 73 7d 7d 49 a2
00b0	a1 c7 7e c4 04 8f d6 32 2c 76 73 77 f0 26 b2 c3
00c0	fb b2 f1 7e 49 8b d0 fa ab 6f 65 83 c2 06 79 cc
00d0	c4 a7 59 3b d9 58 66 ae 1b 03 8e 87 9c f9 d5 ba
00e0	e1 90 8f 92 13 cd 5b 38 2b 33 e0 91 2d 51 c0 ba
00f0	35 87 26 d1 51 00 8a ba d7 d4 a7 82 82 1b c9 2c
0100	52 48 76 f4 h1 90 57 21 98 4e 43 e5 34 81 7b a4

Kadangi headeryje yra 4 laukai, ir kiekvienas užima po 2 baitus, pats headeris sudaro 8 baitus. Likę baitai yra skirti payload'ui. O „length“ rodo visą segmento dydį (i.e. headerio ir payload sumą)

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)

5 0.000045	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
6 0.000058	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
7 0.005592	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
8 0.005659	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
9 0.005666	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
10 0.005691	192.168.0.54	35.217.26.44	UDP	1159 65054 → 50002 Len=1117
12 0.011514	192.168.0.54	35.217.19.209	UDP	224 52483 → 50003 Len=182

> Frame 5: 1158 bytes on wire (9264 bits), 1158 bytes captured (9264 bits)  
> Ethernet II, Src: Apple\_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn\_c8:1  
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 35.217.26.44  
< User Datagram Protocol, Src Port: 65054, Dst Port: 50002  
  Source Port: 65054  
  Destination Port: 50002  
**Length: 1124**  
  Checksum: 0xafed [unverified]  
  [Checksum Status: Unverified]  
  [Stream index: 0]  
  > [Timestamps]  
    **UDP payload (1116 bytes)**

**2 Bytes = 16 bits**

**max payload =  $(2^{16} - 1) - (2^4) = 35535 - 8 = 35527$**

0020	1a 2c fe 1e c3 52 04 64 af ed 90 65 68 19 69 53
0030	2e 36 00 05 83 3b be de 00 03 01 ab 50 14 05 fa
0040	60 bd 13 45 99 14 9d fb 89 d0 0f f1 5f 6e 71 75
0050	60 64 1e 2a 7f a5 f3 db 83 84 75 33 12 58 cd 7d
0060	b5 6b 9b 04 65 35 25 e9 11 45 50 4c 3f b5 3b 47
0070	30 80 16 da 1b 84 98 c8 1d 6f c1 15 4e f9 58 3e
0080	67 f2 77 48 e0 3d b2 13 d0 ba d2 06 0b 4e c4 64
0090	5a 80 a4 ca fe 7f 45 be fd d7 da 8a b1 95 63 c5
00a0	18 d2 05 3c 59 62 2e a7 54 91 3c 73 7d 7d 49 a2
00b0	a1 c7 7e c4 04 8f d6 32 2c 76 73 77 f0 26 b2 c3
00c0	fb b2 f1 7e 49 8b d0 fa ab 6f 65 83 c2 06 79 cc
00d0	c4 a7 59 3b d9 58 66 ae 1b 03 8e 87 9c f9 d5 ba
00e0	e1 90 8f 92 13 cd 5b 38 2b 33 e0 91 2d 51 c0 ba
00f0	35 87 26 d1 51 00 8a ba d7 d4 a7 82 82 1b c9 2c
0100	52 48 76 f4 h1 90 57 21 98 4e 43 e5 34 81 7b a4
0110	b8 2c 04 5a b1 aa 50 0c ca e8 d5 db 13 00 14 6f
0120	d7 a6 79 6a ed 89 27 9e d8 18 79 8a d5 75 a5 59
0130	c7 1a a1 72 e2 2d 38 9f ba c5 6b 0a c5 d4 74 cd
0140	f2 a9 1a fb 38 ae bc cf 62 6a 7d 61 6e 48 58 ca

Pirma, suskaičiuojame kokį didžiausią skaičių gali laikyti „length“ field –  $2^{16} - 1$  (nes 0 išskaičiuojame). Tuomet iš gauto skaičiaus atimame headerio dydį – 8 baitus, ir gauname max payload dydį.

P.S. Čia yra skaičiavimo klaida, vietoj 3, turėtų būti 6. Teisingas atsakymas 65527 baitai.

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

5 0.000045	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
6 0.000058	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
7 0.005592	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
8 0.005659	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
9 0.005666	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
10 0.005691	192.168.0.54	35.217.26.44	UDP	1159 65054 → 50002 Len=1117
12 0.011514	192.168.0.54	35.217.19.209	UDP	224 52483 → 50003 Len=182 2 Bytes = 16 bits

> Frame 5: 1158 bytes on wire (9264 bits), 1158 bytes captured (9264 bits) 0020 1a 2c fe 1e c3 52 04 64 af ed 90 65 68 19 69 53  
> Ethernet II, Src: Apple\_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn\_c8:1 0030 2e 36 00 05 83 3b be de 00 03 01 ab 50 14 05 fa  
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 35.217.26.44 0040 60 bd 13 45 99 14 9d fb 89 d0 0f f1 5f 6e 71 75  
> User Datagram Protocol, Src Port: 65054, Dst Port: 50002

Source Port: 65054  
Destination Port: 50002  
Length: 1124  
Checksum: 0xafe0 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 0]  
> [Timestamps]  
UDP payload (1116 bytes)  
Data (1116 bytes)  
Data: 0965681969532e360005833bbebe000301ab501405fa60bd134599149dfb89d  
[Length: 1116]

max port =  $2^{16} - 1 = 65535$

00a0	18 a2 05 3c 59 b2 2e a/	54 91 3c /3 /d /d 49 a2
00b0	a1 c7 7e c4 04 8f d6 32	2c 76 73 77 f0 26 b2 c3
00c0	fb b2 f1 7e 49 8b d0 fa	ab 6f 65 83 c2 06 79 cc
00d0	c4 a7 59 3b d9 58 66 ae	1b 03 8e 87 9c f9 d5 ba
00e0	e1 90 8f 92 13 cd 5b 38	2b 33 e0 91 2d 51 c0 ba
00f0	35 87 26 d1 51 00 8a ba	d7 d4 a7 82 82 1b c9 2c
0100	52 48 76 f4 b1 90 57 21	98 4e 43 e5 34 81 7b a4
0110	b8 2c 04 5a b1 aa 50 0c	ca e8 d5 db 13 00 14 6f
0120	7d a6 79 6a ed 89 27 9e	d8 18 79 8a d5 75 a5 59
0130	c7 1a a1 72 ef 2d 38 9f	ba c5 6b 0a c5 da 74 cd
0140	f2 a9 1a fb 38 ae bc cf	62 6a 7d 61 6e 48 58 ca

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).

5 0.000045	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
6 0.000058	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
7 0.005592	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
8 0.005659	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
9 0.005666	192.168.0.54	35.217.26.44	UDP	1158 65054 → 50002 Len=1116
10 0.005691	192.168.0.54	35.217.26.44	UDP	1159 65054 → 50002 Len=1117
12 0.011514	192.168.0.54	35.217.19.209	UDP	224 52483 → 50003 Len=182

> Frame 5: 1158 bytes on wire (9264 bits), 1158 bytes captured (9264 bits) 0010 04 78 ef 7a 00 00 40 11 88 17 c0 a8 00 36 23 d9  
> Ethernet II, Src: Apple\_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn\_c8:1 0020 1a 2c fe 1e c3 52 04 64 af ed 90 65 68 19 69 53  
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 35.217.26.\*\* 0030 2e 36 00 05 83 3b be de 00 03 01 ab 50 14 05 fa  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 1144  
Identification: 0xeffa (61306)  
> 000. .... = Flags: 0x0  
...0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 64  
Protocol: UDP (17)

Header Checksum: 0x8817 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 192.168.0.54  
Destination Address: 35.217.26.44

Decimal: 17  
Hexadecimal: 0x11

00e0	e1 90 8f 92 13 cd 5b 38	2b 33 e0 91 2d 51 c0 ba
00f0	35 87 26 d1 51 00 8a ba	d7 d4 a7 82 82 1b c9 2c
0100	52 48 76 f4 b1 90 57 21	98 4e 43 e5 34 81 7b a4
0110	b8 2c 04 5a b1 aa 50 0c	ca e8 d5 db 13 00 14 6f
0120	7d a6 79 6a ed 89 27 9e	d8 18 79 8a d5 75 a5 59
0130	c7 1a a1 72 ef 2d 38 9f	ba c5 6b 0a c5 da 74 cd

## Ethernet ir ARP paketu filtravimas

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

Wireshark screenshot showing network traffic. The packet list shows two entries:

- Frame 1970: 604 bytes on wire (4832 bits), 604 bytes captured (4832 bits) [id=1]
  - Ethernet II, Src: Apple\_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn\_c8:1f:fe (f0:b4:d2:c8:1f:fe)
    - Address: D-LinkIn\_c8:1f:fe (f0:b4:d2:c8:1f:fe)
    - .... .0. .... .... .... = LG bit: Globally unique address (fa)
    - .... .0. .... .... .... = IG bit: Individual address (unicast)
  - Source: Apple\_36:4b:9b (88:66:5a:36:4b:9b)
    - Address: Apple\_36:4b:9b (88:66:5a:36:4b:9b)
    - .... .0. .... .... .... = LG bit: Globally unique address (fa)
    - .... .0. .... .... .... = IG bit: Individual address (unicast)
- Frame 2043: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) [id=2]
  - HTTP 583 HTTP/1.1 200 OK (text/html)

The details pane shows the raw hex and ASCII data for the selected frame (Frame 1970). A red box highlights the source MAC address: Apple\_36:4b:9b (88:66:5a:36:4b:9b).

- 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.]

Wireshark screenshot showing network traffic. The packet list shows two entries:

- Frame 1970: 604 bytes on wire (4832 bits), 604 bytes captured (4832 bits) [id=1]
  - Ethernet II, Src: Apple\_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn\_c8:1f:fe (f0:b4:d2:c8:1f:fe)
    - Address: D-LinkIn\_c8:1f:fe (f0:b4:d2:c8:1f:fe)
    - .... .0. .... .... .... = LG bit: Globally unique address (fa)
    - .... .0. .... .... .... = IG bit: Individual address (unicast)
  - Source: Apple\_36:4b:9b (88:66:5a:36:4b:9b)
    - Address: Apple\_36:4b:9b (88:66:5a:36:4b:9b)
    - .... .0. .... .... .... = LG bit: Globally unique address (fa)
    - .... .0. .... .... .... = IG bit: Individual address (unicast)
- Frame 2043: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) [id=2]
  - HTTP 583 HTTP/1.1 200 OK (text/html)

The details pane shows the raw hex and ASCII data for the selected frame (Frame 1970). A red box highlights the destination MAC address: D-LinkIn\_c8:1f:fe (f0:b4:d2:c8:1f:fe). A red arrow points from the question text to this highlighted address.

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

Wireshark screenshot showing network traffic. The packet list shows two entries:

- Frame 1970: 604 bytes on wire (4832 bits), 604 bytes captured (4832 bits) [id=1]
  - Ethernet II, Src: Apple\_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-LinkIn\_c8:1f:fe (f0:b4:d2:c8:1f:fe)
    - Address: D-LinkIn\_c8:1f:fe (f0:b4:d2:c8:1f:fe)
    - .... .0. .... .... .... = LG bit: Globally unique address (fa)
    - .... .0. .... .... .... = IG bit: Individual address (unicast)
  - Source: Apple\_36:4b:9b (88:66:5a:36:4b:9b)
    - Address: Apple\_36:4b:9b (88:66:5a:36:4b:9b)
    - .... .0. .... .... .... = LG bit: Globally unique address (fa)
    - .... .0. .... .... .... = IG bit: Individual address (unicast)
- Frame 2043: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) [id=2]
  - HTTP 583 HTTP/1.1 200 OK (text/html)

The details pane shows the raw hex and ASCII data for the selected frame (Frame 1970). A red box highlights the type field: IPv4 (0x0800). A red arrow points from the question text to this highlighted field. The word "IPv4 packet" is written above the type field in red.

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

1970 3.861631	192.168.0.54	128.119.245.12	HTTP	604 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
2043 3.993716	128.119.245.12	192.168.0.54	HTTP	583 HTTP/1.1 200 OK (text/html)
66 Bytes				
<ul style="list-style-type: none"> <li>✓ Ethernet II, Src: Apple_36:4b:9b (88:66:5a:36:4b:9b), Dst: D-Li...</li> <li>Destination: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe)           <ul style="list-style-type: none"> <li>Address: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe)</li> <li>.... .0. .... .... .... = LG bit: Globally unique address</li> <li>.... .0. .... .... .... = IG bit: Individual address</li> </ul> </li> <li>Source: Apple_36:4b:9b (88:66:5a:36:4b:9b)           <ul style="list-style-type: none"> <li>Address: Apple_36:4b:9b (88:66:5a:36:4b:9b)</li> <li>.... .0. .... .... .... = LG bit: Globally unique address</li> <li>.... .0. .... .... .... = IG bit: Individual address</li> </ul> </li> <li>Type: IPv4 (0x0800)</li> </ul>				
> Internet Protocol Version 4, Src: 192.168.0.54, Dst: 128.119.245.12				

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?

1957 3.755110	192.168.0.54	128.119.245.12	TCP	74 80 → 54039 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TS
1968 3.861464	128.119.245.12	192.168.0.54	TCP	74 80 → 54039 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TS
1969 3.861526	192.168.0.54	128.119.245.12	TCP	66 54039 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=47970826 TSecr=3640
1970 3.861631	192.168.0.54	128.119.245.12	HTTP	604 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
2039 3.993714	128.119.245.12	192.168.0.54	TCP	66 80 → 54039 [ACK] Seq=1 Ack=539 Win=30080 Len=0 TSval=364081780 TSecr=47
2040 3.993714	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=1 Ack=539 Win=30080 Len=1448 TSval=364081780 TSecr=47
2041 3.993715	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=1449 Ack=539 Win=30080 Len=1448 TSval=364081780 TS
2042 3.993715	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=2897 Ack=539 Win=30080 Len=1448 TSval=364081780 TS
2043 3.993716	128.119.245.12	192.168.0.54	HTTP	583 HTTP/1.1 200 OK (text/html)
2044 3.993783	192.168.0.54	128.119.245.12	TCP	66 54039 → 80 [ACK] Seq=539 Ack=4862 Win=126848 Len=0 TSval=47970958 TSecr=47
2045 3.994931	192.168.0.54	128.119.245.12	TCP	66 [TCP Window Update] 54039 → 80 [ACK] Seq=539 Ack=4862 Win=131072 Len=0

My Router				
<ul style="list-style-type: none"> <li>&gt; Frame 2039: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0           <ul style="list-style-type: none"> <li>Ethernet II, Src: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe), Dst: Apple_36:4b:9b (88:66:5a:36:4b:9b)               <ul style="list-style-type: none"> <li>Destination: Apple_36:4b:9b (88:66:5a:36:4b:9b)                   <ul style="list-style-type: none"> <li>Address: Apple_36:4b:9b (88:66:5a:36:4b:9b)</li> <li>.... .0. .... .... .... = LG bit: Globally unique address</li> <li>.... .0. .... .... .... = IG bit: Individual address</li> </ul> </li> <li>Source: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe)</li> </ul> </li> </ul> </li> </ul>				
<ul style="list-style-type: none"> <li>0000 88 66 5a 36 4b 9b f0 b4 d2 c8 1f fe 08 00 45 00 :fZ6K... .E...</li> <li>0010 00 34 94 64 40 00 2d 06 82 fd 80 77 f5 0c c0 a8 :4-d@-- ...w...</li> <li>0020 00 36 00 50 d3 17 ac 18 e6 10 d3 09 10 2a 80 10 :6-P... . .*</li> <li>0030 00 eb 71 9d 00 00 01 01 08 0a 15 b3 72 74 02 db :q..... .rt...</li> <li>0040 fa 0a .....</li> </ul>				
1957 3.755110	192.168.0.54	128.119.245.12	TCP	74 80 → 54039 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TS
1968 3.861464	128.119.245.12	192.168.0.54	TCP	74 80 → 54039 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TS
1969 3.861526	192.168.0.54	128.119.245.12	TCP	66 54039 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=47970826 TSecr=3640
1970 3.861631	192.168.0.54	128.119.245.12	HTTP	604 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
2039 3.993714	128.119.245.12	192.168.0.54	TCP	66 80 → 54039 [ACK] Seq=1 Ack=539 Win=30080 Len=0 TSval=364081780 TSecr=47
2040 3.993714	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=1 Ack=539 Win=30080 Len=1448 TSval=364081780 TSecr=47
2041 3.993715	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=1449 Ack=539 Win=30080 Len=1448 TSval=364081780 TS
2042 3.993715	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=2897 Ack=539 Win=30080 Len=1448 TSval=364081780 TS
2043 3.993716	128.119.245.12	192.168.0.54	HTTP	583 HTTP/1.1 200 OK (text/html)
2044 3.993783	192.168.0.54	128.119.245.12	TCP	66 54039 → 80 [ACK] Seq=539 Ack=4862 Win=126848 Len=0 TSval=47970958 TSecr=47
2045 3.994931	192.168.0.54	128.119.245.12	TCP	66 [TCP Window Update] 54039 → 80 [ACK] Seq=539 Ack=4862 Win=131072 Len=0

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

My PC MAC				
<ul style="list-style-type: none"> <li>&gt; Frame 2039: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0           <ul style="list-style-type: none"> <li>Ethernet II, Src: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe), Dst: Apple_36:4b:9b (88:66:5a:36:4b:9b)               <ul style="list-style-type: none"> <li>Destination: Apple_36:4b:9b (88:66:5a:36:4b:9b)                   <ul style="list-style-type: none"> <li>Address: Apple_36:4b:9b (88:66:5a:36:4b:9b)</li> <li>.... .0. .... .... .... = LG bit: Globally unique address</li> <li>.... .0. .... .... .... = IG bit: Individual address</li> </ul> </li> <li>Source: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe)</li> </ul> </li> </ul> </li> </ul>				
<ul style="list-style-type: none"> <li>0000 88 66 5a 36 4b 9b f0 b4 d2 c8 1f fe 08 00 45 00 :fZ6K... .E...</li> <li>0010 00 34 94 64 40 00 2d 06 82 fd 80 77 f5 0c c0 a8 :4-d@-- ...w...</li> <li>0020 00 36 00 50 d3 17 ac 18 e6 10 d3 09 10 2a 80 10 :6-P... . .*</li> <li>0030 00 eb 71 9d 00 00 01 01 08 0a 15 b3 72 74 02 db :q..... .rt...</li> <li>0040 fa 0a .....</li> </ul>				
1957 3.755110	192.168.0.54	128.119.245.12	TCP	74 80 → 54039 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TS
1968 3.861464	128.119.245.12	192.168.0.54	TCP	74 80 → 54039 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TS
1969 3.861526	192.168.0.54	128.119.245.12	TCP	66 54039 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=47970826 TSecr=3640
1970 3.861631	192.168.0.54	128.119.245.12	HTTP	604 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
2039 3.993714	128.119.245.12	192.168.0.54	TCP	66 80 → 54039 [ACK] Seq=1 Ack=539 Win=30080 Len=0 TSval=364081780 TSecr=47
2040 3.993714	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=1 Ack=539 Win=30080 Len=1448 TSval=364081780 TSecr=47
2041 3.993715	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=1449 Ack=539 Win=30080 Len=1448 TSval=364081780 TS
2042 3.993715	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=2897 Ack=539 Win=30080 Len=1448 TSval=364081780 TS
2043 3.993716	128.119.245.12	192.168.0.54	HTTP	583 HTTP/1.1 200 OK (text/html)
2044 3.993783	192.168.0.54	128.119.245.12	TCP	66 54039 → 80 [ACK] Seq=539 Ack=4862 Win=126848 Len=0 TSval=47970958 TSecr=47
2045 3.994931	192.168.0.54	128.119.245.12	TCP	66 [TCP Window Update] 54039 → 80 [ACK] Seq=539 Ack=4862 Win=131072 Len=0

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

1957 3.735110	128.108.0.54	128.119.245.12	TCP	70 34039 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 TSval=47970097 TSecr=47
1968 3.861464	128.119.245.12	192.168.0.54	TCP	74 80 → 54039 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TS
1969 3.861526	192.168.0.54	128.119.245.12	TCP	66 54039 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=47970826 TSecr=3640
1970 3.861631	192.168.0.54	128.119.245.12	HTTP	604 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
2039 3.993714	128.119.245.12	192.168.0.54	TCP	66 80 → 54039 [ACK] Seq=1 Ack=539 Win=30080 Len=0 TSval=364081780 TSecr=47
2040 3.993714	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=1 Ack=539 Win=30080 Len=1448 TSval=364081780 TSecr
2041 3.993715	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=1449 Ack=539 Win=30080 Len=1448 TSval=364081780 TS
2042 3.993715	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=2897 Ack=539 Win=30080 Len=1448 TSval=364081780 TS
2043 3.993716	128.119.245.12	192.168.0.54	HTTP	583 HTTP/1.1 200 OK (text/html)
2044 3.993783	192.168.0.54	128.119.245.12	TCP	66 54039 → 80 [ACK] Seq=539 Ack=4862 Win=126848 Len=0 TSval=47970958 TSecr
2045 3.994931	192.168.0.54	128.119.245.12	TCP	66 [TCP Window Update] 54039 → 80 [ACK] Seq=539 Ack=4862 Win=131072 Len=0

> Frame 2039: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, duration 0.000000 seconds, transmit rate 0 bits/sec, capture rate 0 bits/sec	0000 88 66 5a 36 4b 9b f0 b4 d2 c8 1f fe 08 00 45 00 ·fZ6K... ···· ··E·
> Ethernet II, Src: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe), Dst: Apple_36:4b:9b (88:66:5a:36:4b:9b)	0010 00 34 94 64 40 00 2d 06 82 fd 80 77 f5 0c c0 a8 ·4-d@- ···· ··W···
Destination: Apple_36:4b:9b (88:66:5a:36:4b:9b)	0020 00 36 00 50 d3 17 ac 18 e6 10 d3 09 10 2a 80 10 ·6-P··· ···· ··*···
Address: Apple_36:4b:9b (88:66:5a:36:4b:9b)	0030 00 eb 71 9d 00 00 01 01 08 0a 15 b3 72 74 02 db ·q ···· ··rt···
Source: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe)	0040 fa 0a 48 54 54 50 2f 31 28 31 20 32 30 30 20 4f ·fZ6K... ···· ··E·
Address: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe)	0050 4b 0d 0a 44 61 74 65 3e 20 4d 6f 6e 2c 20 31 32 ·e@- ···· ·T·w···
Type: IPv4 (0x0800)	0060 20 44 65 63 20 32 30 32 20 31 39 3a 31 38 3a ·6 P··· ···· ··*···

Vél IPv4 protokolo kodas

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?

1957 3.735110	128.108.0.54	128.119.245.12	TCP	70 34039 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 TSval=47970097 TSecr=47
1968 3.861464	128.119.245.12	192.168.0.54	TCP	74 80 → 54039 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TS
1969 3.861526	192.168.0.54	128.119.245.12	TCP	66 54039 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=47970826 TSecr=3640
1970 3.861631	192.168.0.54	128.119.245.12	HTTP	604 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
2039 3.993714	128.119.245.12	192.168.0.54	TCP	66 80 → 54039 [ACK] Seq=1 Ack=539 Win=30080 Len=0 TSval=364081780 TSecr=47
2040 3.993714	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=1 Ack=539 Win=30080 Len=1448 TSval=364081780 TSecr
2041 3.993715	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=1449 Ack=539 Win=30080 Len=1448 TSval=364081780 TS
2042 3.993715	128.119.245.12	192.168.0.54	TCP	1514 80 → 54039 [ACK] Seq=2897 Ack=539 Win=30080 Len=1448 TSval=364081780 TS
2043 3.993716	128.119.245.12	192.168.0.54	HTTP	583 HTTP/1.1 200 OK (text/html)
2044 3.993783	192.168.0.54	128.119.245.12	TCP	66 54039 → 80 [ACK] Seq=539 Ack=4862 Win=126848 Len=0 TSval=47970958 TSecr
2045 3.994931	192.168.0.54	128.119.245.12	TCP	66 [TCP Window Update] 54039 → 80 [ACK] Seq=539 Ack=4862 Win=131072 Len=0

79 bytes				
> Frame 2040: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface eth0, duration 0.000000 seconds, transmit rate 0 bits/sec, capture rate 0 bits/sec				0000 88 66 5a 36 4b 9b f0 b4 d2 c8 1f fe 08 00 45 00 ·fZ6K... ···· ··E·
> Ethernet II, Src: D-LinkIn_c8:1f:fe (f0:b4:d2:c8:1f:fe), Dst: Apple_36:4b:9b (88:66:5a:36:4b:9b)				0010 05 dc 94 65 40 00 2d 06 7d 54 80 77 f5 0c c0 a8 ·e@- ···· ·T·w···
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.54				0020 00 36 00 50 d3 17 ac 18 e6 10 d3 09 10 2a 80 10 ·6 P··· ···· ··*···
> Transmission Control Protocol, Src Port: 80, Dst Port: 54039, Seq: 1, Ack: 539, Len: 79				0030 00 eb 6d cd 00 00 01 01 08 0a 15 b3 72 74 02 db ·m ···· ··rt···
> HTTP/1.1 200 OK (text/html)				0040 fa 0a 48 54 54 50 2f 31 28 31 20 32 30 30 20 4f ·HTTP/1.1 200 0
>				0050 4b 0d 0a 44 61 74 65 3e 20 4d 6f 6e 2c 20 31 32 K-Date: Mon, 12 Dec 202 2 19:18:
>				0060 20 44 65 63 20 32 30 32 20 31 39 3a 31 38 3a 39 GMT: Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2 PHP/7.0.2 mod_perl/2.4.3 4.30 Per l/v5.16.
>				0070 33 39 20 47 4d 54 0d 02 53 65 72 76 65 72 3a 20 0.2K-fip s PHP/7.0.2.4.30 mod_perl/2.4.3 0.11 Per l/v5.16.
>				0080 41 70 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 0.2K-fip s PHP/7.0.2.4.30 mod_perl/2.4.3 0.11 Per l/v5.16.
>				0090 6e 74 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 0.2K-fip s PHP/7.0.2.4.30 mod_perl/2.4.3 0.11 Per l/v5.16.
>				00a0 50 2e 32 6b 20 66 69 70 73 28 50 48 50 2f 37 2e 0.2K-fip s PHP/7.0.2.4.30 mod_perl/2.4.3 0.11 Per l/v5.16.
>				00b0 34 2e 33 30 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 0.2K-fip s PHP/7.0.2.4.30 mod_perl/2.4.3 0.11 Per l/v5.16.
>				00c0 30 2e 31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 0.2K-fip s PHP/7.0.2.4.30 mod_perl/2.4.3 0.11 Per l/v5.16.

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

```
~ $ arp -a
? (192.168.0.1) at f0:b4:d2:c8:1f:fe on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

Stulpeliai:

- IP adresas
- MAC adresas
- NIC interface, kuriam priklauso šis įrašas
- Įrašo tipas: „permanent“ ar ne

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

18 2.504657	Apple_36:4b:9b	Broadcast	ARP	42 Who has 192.168.0.1? Tell 192.168.0.54
19 2.512930	D-LinkIn_c8:1f:fe	Apple_36:4b:9b	ARP	42 192.168.0.1 is at f0:b4:d2:c8:1f:fe

```
> Frame 18: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
> Ethernet II, Src: Apple_36:4b:9b [88:66:5a:36:4b:9b], Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Address Resolution Protocol (request)
  0000 ff ff ff ff ff ff 88 66 5a 36 4b 9
  0010 08 00 06 04 00 01 88 66 5a 36 4b 9
  0020 00 00 00 00 00 00 c0 a8 00 01
```

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

```
> Frame 1584: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{...}
  Ethernet II, Src: Technico_6a:6f:5b (d4:35:1d:6a:6f:5b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ..1. .... .... .... = IG bit: Group address (multicast/broadcast)
    Source: Technico_6a:6f:5b (d4:35:1d:6a:6f:5b)
      Address: Technico_6a:6f:5b (d4:35:1d:6a:6f:5b)
      .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
      .... ..0. .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806) ARP protokolas
```