

# Практика 1. Wireshark

## Задание 1.

1. Request Version: HTTP/1.1  
Response Version: HTTP/1.1
2. Русский, английский языки  
Информация про браузер, его версию и архитектуру устройства:  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
3. Source Address: 192.168.1.43 (адрес моего компьютера)  
Destination Address: 128.119.245.12 (адрес gaia.cs.umass.edu)
4. Status Code: 200  
[Status Code Description: OK]
5. Last-Modified: Tue, 22 Feb 2022 06:59:01 GMT
6. Content length: 128

| Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь |             |                |                |          |        |  |
|--|-------------|----------------|----------------|----------|--------|--|
| http   |             |                |                |          |        |  |
| No.  | Time        | Source         | Destination    | Protocol | Length | Info   |
| 24   | 3.605200... | 192.168.1.43   | 128.119.245.12 | HTTP     | 455    | GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1 |
| 26   | 3.809679... | 128.119.245.12 | 192.168.1.43   | HTTP     | 552    | HTTP/1.1 200 OK (text/html)                            |
| 35   | 4.693148... | 192.168.1.43   | 128.119.245.12 | HTTP     | 336    | GET /favicon.ico HTTP/1.1                              |
| 36   | 4.833749... | 128.119.245.12 | 192.168.1.43   | HTTP     | 550    | HTTP/1.1 404 Not Found (text/html)                     |

```
Frame 24: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface wlp2s0, id 0
Ethernet II, Src: IntelCor_b1:db:95 (88:78:73:b1:db:95), Dst: ZyxelCom_cb:ba:54 (5c:f4:ab:cb:ba:54)
Internet Protocol Version 4, Src: 192.168.1.43, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 34850, Dst Port: 80, Seq: 1, Ack: 1, Len: 389
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file1.html
    Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 26]
    [Next request in frame: 35]
```

```
0000 5c f4 ab cb ba 54 88 78 73 b1 db 95 08 00 45 00  \....T.x.s....E.
0010 01 b9 cc 2d 40 00 40 06 35 ba c0 a8 01 2b 80 77  -.-@. 5....+w
0020 f5 0c 88 22 00 50 5f 32 07 77 79 62 f7 aa 80 18  ...".P_2 .wyb...
0030 01 f6 75 9c 00 00 01 01 08 0a 6f 32 c4 91 36 f5  .u.....o2..6.
```

## Задание 2.

1. Нет, if-modified-since не видно
2. Да, сервер вернул содержимое html-файла явно. Его можно увидеть в разделе Line-based text data: text/html (10 lines)
3. Имеется строчка If-Modified-Since: Tue, 22 Feb 2022 06:59:01 GMT
4. Status Code: 304  
Status Code Description: Not Modified  
Содержимое файла сервер не прислал.

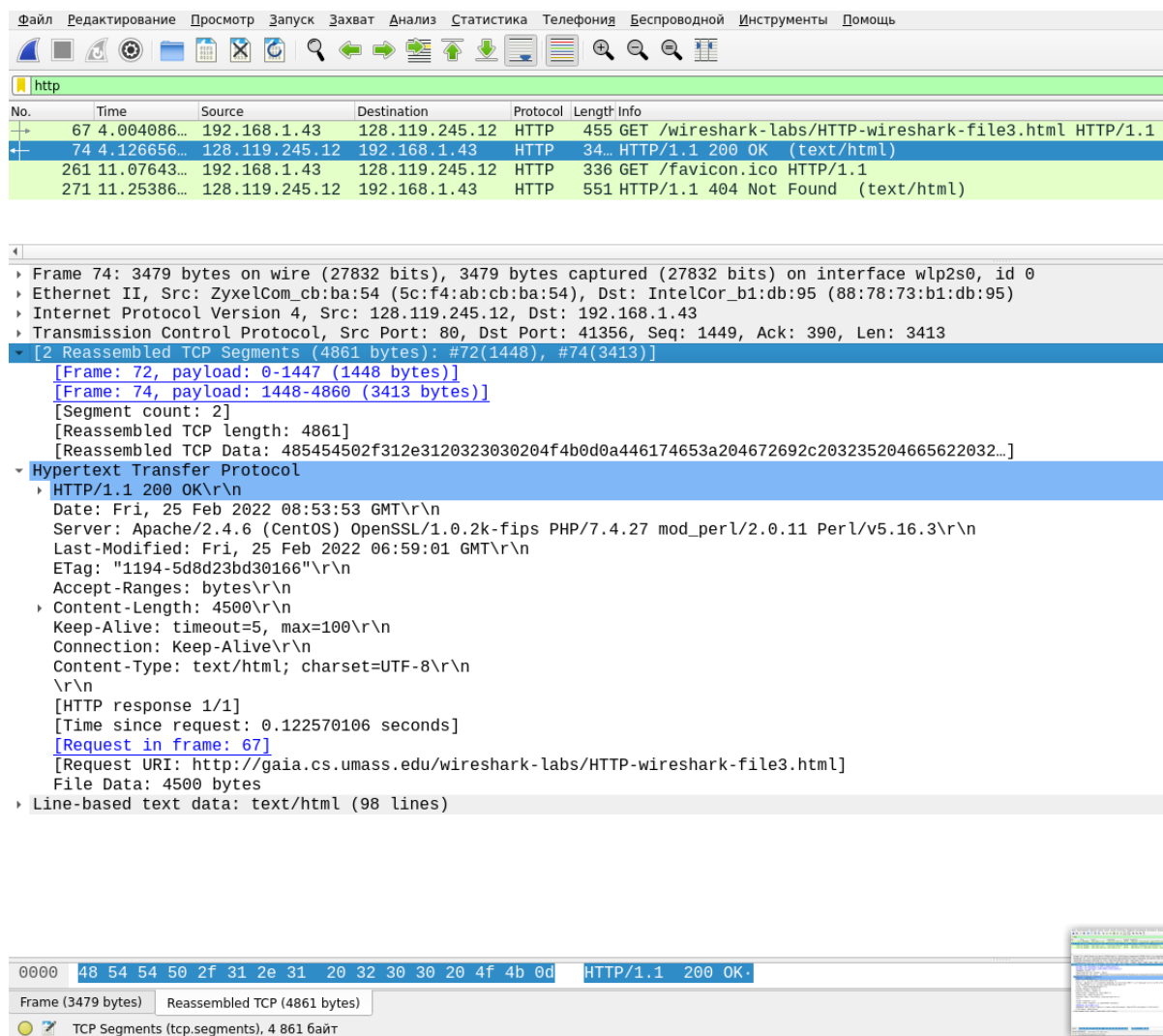
The image shows a Wireshark network traffic capture. The top pane displays a list of packets. Packet 16 is selected, showing an HTTP 200 OK response from 128.119.245.12 to 192.168.1.43. The middle pane shows the details of this packet, including the Hypertext Transfer Protocol section with fields like Response Version, Status Code (200), and Response Phrase (OK). The bottom pane shows the 'Line-based text data: text/html (10 lines)' section, which contains the HTML content of the response, including a congratulatory message and instructions about file modification dates.

| No.   | Time        | Source         | Destination    | Protocol | Length | Info   |
|-------|-------------|----------------|----------------|----------|--------|--|
| 15... | 4.843586... | 192.168.1.43   | 128.119.245.12 | HTTP     | 455    | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 16... | 4.952059... | 128.119.245.12 | 192.168.1.43   | HTTP     | 796    | HTTP/1.1 200 OK (text/html)                            |
| 23... | 7.466897... | 192.168.1.43   | 128.119.245.12 | HTTP     | 336    | GET /favicon.ico HTTP/1.1                              |
| 23... | 7.583142... | 128.119.245.12 | 192.168.1.43   | HTTP     | 551    | HTTP/1.1 404 Not Found (text/html)                     |
| 12... | 30.95396... | 192.168.1.43   | 128.119.245.12 | HTTP     | 567    | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 12... | 31.06215... | 128.119.245.12 | 192.168.1.43   | HTTP     | 306    | HTTP/1.1 304 Not Modified                              |

Frame 1609: 796 bytes on wire (6368 bits), 796 bytes captured (6368 bits) on interface wlp2s0, id 0  
Ethernet II, Src: ZyxelCom\_cb:ba:54 (5c:f4:ab:cb:ba:54), Dst: IntelCor\_b1:db:95 (88:78:73:b1:db:95)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.43  
Transmission Control Protocol, Src Port: 80, Dst Port: 41874, Seq: 1, Ack: 390, Len: 730  
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: Tue, 22 Feb 2022 19:47:04 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod\_perl/2.0.11 Perl/v5.16.3\r\nLast-Modified: Tue, 22 Feb 2022 06:59:01 GMT\r\nETag: "173-5d895e245ed4b"\r\nAccept-Ranges: bytes\r\nContent-Length: 371\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/1]  
[Time since request: 0.108472696 seconds]  
[\[Request in frame: 1568\]](#)  
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]  
File Data: 371 bytes  
Line-based text data: text/html (10 lines)  
\n<html>\n\nCongratulations again! Now you've downloaded the file lab2-2.html. <br>\nThis file's last modification date will not change. <p>\nThus if you download this multiple times on your browser, a complete copy <br>\nwill only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\nfield in your browser's HTTP GET request to the server.\n\n

## Задание 3.

1. 1 запрос GET (не считая GET /favicon.ico HTTP/1.1). Его номер 67.
2. 74
3. 2 Reassembled TCP Segments (4861 bytes): #72(1448), #74(3413)
4. В самом заголовке HTTP никакой информации про TCP сегменты не видно.



## Задание 4.

1. Были отправлены следующие запросы GET:
  - a. GET /wireshark-labs/HTTP-wireshark-file4.html
  - b. GET /pearson.png
  - c. GET /8E\_cover\_small.jpg
  - d. GET /favicon.ico (этот запрос, вероятно, нужен чтобы загрузить значок веб-сайта)
2. Не вижу ни доказательств, ни опровержений параллельной загрузке изображений. С одной стороны, ответ на запрос первой картинки был принят раньше, чем отправлен запрос второй картинки. Это может указывать на последовательную загрузку изображений, а может так совпало, что на GET по первой картинке быстро пришел ответ. С другой стороны, если запросить дерево запросов, будет видно, что GET картинок не зависят друг от друга, так что их можно выполнять параллельно.

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

http

| No.  | Time        | Source         | Destination    | Protocol | Length | Info   |
|------|-------------|----------------|----------------|----------|--------|--|
| 1199 | 4.280706... | 192.168.1.43   | 128.119.245.12 | HTTP     | 455    | GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 |
| 1231 | 4.397159... | 128.119.245.12 | 192.168.1.43   | HTTP     | 13..   | HTTP/1.1 200 OK (text/html)                            |
| 1391 | 4.927040... | 192.168.1.43   | 128.119.245.12 | HTTP     | 412    | GET /pearson.png HTTP/1.1                              |
| 1428 | 5.043847... | 128.119.245.12 | 192.168.1.43   | HTTP     | 36..   | HTTP/1.1 200 OK (PNG)                                  |
| 1459 | 5.140079... | 192.168.1.43   | 178.79.137.164 | HTTP     | 419    | GET /8E_cover_small.jpg HTTP/1.1                       |
| 1473 | 5.187855... | 178.79.137.164 | 192.168.1.43   | HTTP     | 237    | HTTP/1.1 301 Moved Permanently                         |
| 1695 | 5.929642... | 192.168.1.43   | 128.119.245.12 | HTTP     | 336    | GET /favicon.ico HTTP/1.1                              |
| 1744 | 6.043320... | 192.168.1.43   | 23.196.236.35  | OCSP     | 457    | Request  |
| 1747 | 6.045579... | 128.119.245.12 | 192.168.1.43   | HTTP     | 550    | HTTP/1.1 404 Not Found (text/html)                     |
| 1778 | 6.156494... | 23.196.236.35  | 192.168.1.43   | OCSP     | 955    | Response   |

Wireshark - Request Sequences - wlp2s0 (от суперпользователя)

| Topic / Item  | Count | Average | Min Val | Max Val | Rate (ms) | Percent |
|---|-------|---------|---------|---------|-----------|---------|
| HTTP Request Sequences  | 14    |         |         |         | 0,0020    | 100%    |
| http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html | 5     |         |         |         | 0,0007    | 35,71%  |
| http://kurose.cslash.net/8E_cover_small.jpg                       | 3     |         |         |         | 0,0004    | 60,00%  |
| https://kurose.cslash.net/8E_cover_small.jpg                      | 1     |         |         |         | 0,0001    | 33,33%  |
| http://gaia.cs.umass.edu/pearson.png                              | 1     |         |         |         | 0,0001    | 20,00%  |
| http://239.255.255.250:1900*                                      | 22    |         |         |         | 0,0031    | 157,14% |
| http://192.168.1.1:35078/rootDesc.xml                             | 11    |         |         |         | 0,0015    | 50,00%  |

Дисплейный фильтр:  Применить

Копировать Сохранить как... Закрыть

Accept-Encoding: gzip, deflate\r\n  
 Connection: keep-alive\r\n  
 Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n  
 \r\n  
[\[Full request URI: http://gaia.cs.umass.edu/pearson.png\]](http://gaia.cs.umass.edu/pearson.png)  
[\[HTTP request 2/3\]](#)  
[\[Prev request in frame: 1199\]](#)  
[\[Response in frame: 1428\]](#)  
[\[Next request in frame: 1695\]](#)

```

0000  5c f4 ab cb ba 54 88 78 73 b1 db 95 08 00 45 00  \....T.x s....E.
0010  01 8e 87 1e 40 00 40 06 7a f4 c0 a8 01 2b 80 77  ....@.@. z....+..W

```

wireshark\_wlp2s0CDKB1.pcapng

## Задание 5.

- Status Code: 401  
Status Code Description: Unauthorized
- Появилось поле Authorization. В нем содержатся введенные логин и пароль:  
Credentials: wireshark-students:network

| Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь |             |                |                |          |        |  |
|--|-------------|----------------|----------------|----------|--------|--|
| http   |             |                |                |          |        |  |
| No.  | Time        | Source         | Destination    | Protocol | Length | Info   |
| 15...  | 4.287933... | 192.168.1.43   | 128.119.245.12 | HTTP     | 471    | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 15...  | 4.401344... | 128.119.245.12 | 192.168.1.43   | HTTP     | 783    | HTTP/1.1 401 Unauthorized (text/html)                                  |
| 11...  | 32.19170... | 192.168.1.43   | 128.119.245.12 | HTTP     | 530    | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 11...  | 32.30264... | 128.119.245.12 | 192.168.1.43   | HTTP     | 556    | HTTP/1.1 200 OK (text/html)  |
| 12...  | 33.05583... | 192.168.1.43   | 128.119.245.12 | HTTP     | 336    | GET /favicon.ico HTTP/1.1  |
| 12...  | 33.17213... | 128.119.245.12 | 192.168.1.43   | HTTP     | 550    | HTTP/1.1 404 Not Found (text/html)                                     |

```

Frame 11814: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface wlp2s0, id 0
Ethernet II, Src: IntelCor_b1:db:95 (88:78:73:b1:db:95), Dst: ZyxelCom_cb:ba:54 (5c:f4:ab:cb:ba:54)
Internet Protocol Version 4, Src: 192.168.1.43, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58932, Dst Port: 80, Seq: 1, Ack: 1, Len: 464
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
    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
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
  Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=\r\n
    Credentials: wireshark-students:network
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
[HTTP request 1/2]
[Response in frame: 11847]
[Next request in frame: 12078]

```

```

01d0 3a 20 31 0d 0a 41 75 74 68 6f 72 69 7a 61 74 69 : 1...Aut horizat1
01e0 6f 6e 3a 20 42 61 73 69 63 20 64 32 6c 79 5a 58 on: Basi c d2lyZX
01f0 4e 6f 59 58 4a 72 4c 58 4e 30 64 57 52 6c 62 6e NoYXJrLX N0dWRlbn
0200 52 7a 4f 6d 35 6c 64 48 64 76 63 6d 73 3d 0d 0a RzOm5ldH dvcms=..
0210 0d 0a ..

```

HTTP Authorization header (http.authorization), 59 байт