

Networks, 1

Айну́р Иба́тов

26 февраля 2022 г.

## Задание 1. Базовое взаимодействие HTTP GET/response

No.	Time	Source	Destination	Protocol	Length	Info
150	7.391356536	192.168.1.4	128.119.245.12	HTTP	652	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
156	7.582134013	128.119.245.12	192.168.1.4	HTTP	552	HTTP/1.1 200 OK (text/html)
158	7.671278089	192.168.1.4	128.119.245.12	HTTP	513	GET /favicon.ico HTTP/1.1
159	7.883031968	128.119.245.12	192.168.1.4	HTTP	550	HTTP/1.1 404 Not Found (text/html)

  

▶ Frame 150: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits) on interface wlo1, id 0  
 ▶ Ethernet II, Src: 64:6e:e0:a2:6f:89 (64:6e:e0:a2:6f:89), Dst: Netgear\_0a:c2:48 (c4:04:15:0a:c2:48)  
 ▶ Internet Protocol Version 4, Src: 192.168.1.4, Dst: 128.119.245.12  
 ▶ Transmission Control Protocol, Src Port: 35534, Dst Port: 80, Seq: 1, Ack: 1, Len: 586  
 ▶ Hypertext Transfer Protocol

```

GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
DNT: 1\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.174 YaBrowser/22.1.3.856 (beta) Yowser/2.5 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ru\r\n
If-None-Match: "80-5d86da696911b"\r\n
If-Modified-Since: Sun, 20 Feb 2022 06:59:01 GMT\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: 156]
[Next request in frame: 158]
  
```

1. В обоих случаях HTTP1.1

2.

Асепт-Language: ru

Серверу про пользователя передается еще

User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/96.0.4664.174 YaBrowser/22.1.3.856 (beta) Yowser/2.5 Safari/537.36\r\n

3. 192.168.1.4 – мой, 128.119.245.12 – сервера

4. 200 OK

No.	Time	Source	Destination	Protocol	Length	Info
150	7.391356536	192.168.1.4	128.119.245.12	HTTP	652	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
156	7.582134013	128.119.245.12	192.168.1.4	HTTP	552	HTTP/1.1 200 OK (text/html)
158	7.671278089	192.168.1.4	128.119.245.12	HTTP	513	GET /favicon.ico HTTP/1.1
159	7.883031968	128.119.245.12	192.168.1.4	HTTP	550	HTTP/1.1 404 Not Found (text/html)

  

▶ Frame 156: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface wlo1, id 0  
 ▶ Ethernet II, Src: Netgear\_0a:c2:48 (c4:04:15:0a:c2:48), Dst: 64:6e:e0:a2:6f:89 (64:6e:e0:a2:6f:89)  
 ▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.4  
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 35534, Seq: 1, Ack: 587, Len: 486  
 ▶ Hypertext Transfer Protocol

```

HTTP/1.1 200 OK\r\n
Date: Sat, 26 Feb 2022 13:28:35 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sat, 26 Feb 2022 06:59:01 GMT\r\n
ETag: "80-5d8e659a79885"\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 1/2]
[Time since request: 0.190777477 seconds]
[Request in frame: 150]
[Next request in frame: 158]
[Next response in frame: 159]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
Line-based text data: text/html (4 lines)
  
```

5. Last-Modified: Sat, 26 Feb 2022 06:59:01 GMT

6. 552 bytes (4416 bits)

## Задание 2. HTTP CONDITIONAL GET/response

No.	Time	Source	Destination	Protocol	Length	Info
501	11.414199064	192.168.1.4	128.119.245.12	HTTP	593	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
508	11.641327122	128.119.245.12	192.168.1.4	HTTP	796	HTTP/1.1 200 OK (text/html)
568	15.242993174	192.168.1.4	128.119.245.12	HTTP	679	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
571	15.375355879	128.119.245.12	192.168.1.4	HTTP	395	HTTP/1.1 304 Not Modified

```

Frame 501: 593 bytes on wire (4744 bits), 593 bytes captured (4744 bits) on interface wlo1, id 0
Ethernet II, Src: 64:6e:e0:a2:6f:89 (64:6e:e0:a2:6f:89), Dst: Netgear_0a:c2:48 (c4:04:15:0a:c2:48)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 35546, Dst Port: 80, Seq: 1, Ack: 1, Len: 527
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  DNT: 1\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.174 YaBrowser/22.1.3.856 (beta) Yowser/2.5 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: ru\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 1/2]
  [Response in frame: 508]
  [Next request in frame: 568]

```

## 1. Her

The image shows a Wireshark packet capture of an HTTP transaction. The packet list shows four packets: a GET request (501), a 200 OK response (508), a second GET request (568), and a 304 Not Modified response (571). The packet details pane for packet 508 shows the full HTTP response, including headers like Date, Server, Last-Modified, ETag, and Content-Length. The packet bytes pane shows the raw HTML content of the response, which is a 10-line text document.

## 2. Да, вижу вполне явно содержимое

Line-based text data: text/html (10 lines)

```

\n
<html>\n
\n

```

Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n

This file's last modification date will not change. <p>\n

Thus if you download this multiple times on your browser, a complete copy <br>\n

will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n

field in your browser's HTTP GET request to the server.\n  
 \n  
 </html>\n

The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows four packets: a GET request (501), a 200 OK response (508), another GET request (568), and another 200 OK response (571). The details pane for packet 568 is expanded, showing the Hypertext Transfer Protocol section. The request is for the file `/wireshark-labs/HTTP-wireshark-file2.html` with a status of 304 Not Modified. The 'If-Modified-Since' header is set to 'Sat, 26 Feb 2022 06:59:01 GMT'. The pane also includes links for the full request URI, the previous request in the frame, and the response in the frame.

3. Да, вот она:

If-Modified-Since: Sat, 26 Feb 2022 06:59:01 GMT\r\n

The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows four packets: a GET request (501), a 200 OK response (508), another GET request (568), and a 304 Not Modified response (571). The details pane for packet 571 is expanded, showing the Hypertext Transfer Protocol section. The response is a 304 Not Modified status. The 'If-Modified-Since' header is set to 'Sat, 26 Feb 2022 13:37:07 GMT'. The pane also includes links for the previous request in the frame, the previous response in the frame, the request in the frame, and the request URI.

4. 304 Not Modified; нет, явно файла не видно

*Задание 3. Получение длинных документов*



No.	Time	Source	Destination	Protocol	Length	Info
270	10.501040689	192.168.1.4	128.119.245.12	HTTP	567	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
276	10.651911359	128.119.245.12	192.168.1.4	HTTP	4927	HTTP/1.1 200 OK (text/html)

  

Frame 270: 567 bytes on wire (4536 bits), 567 bytes captured (4536 bits) on interface wlo1, id 0

- Interface id: 0 (wlo1)
  - Encapsulation type: Ethernet (1)
  - Arrival Time: Feb 26, 2022 16:38:55.496566951 MSK
  - [Time shift for this packet: 0.000000000 seconds]
  - Epoch Time: 1645882735.496566951 seconds
  - [Time delta from previous captured frame: 0.000535344 seconds]
  - [Time delta from previous displayed frame: 0.000000000 seconds]
  - [Time since reference or first frame: 10.501040689 seconds]
- Frame Number: 270
  - Frame Length: 567 bytes (4536 bits)
  - Capture Length: 567 bytes (4536 bits)
  - [Frame is marked: False]
  - [Frame is ignored: False]
  - [Protocols in frame: eth:ethertype:ip:tcp:http]
  - [Coloring Rule Name: HTTP]
  - [Coloring Rule String: http || tcp.port == 80 || http2]
- Ethernet II, Src: 64:6e:e0:a2:6f:89 (64:6e:e0:a2:6f:89), Dst: Netgear\_0a:c2:48 (c4:04:15:0a:c2:48)
- Internet Protocol Version 4, Src: 192.168.1.4, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 35552, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
- Hypertext Transfer Protocol
  - GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
  - Host: gaia.cs.umass.edu\r\n
  - Connection: keep-alive\r\n
  - DNT: 1\r\n
  - Upgrade-Insecure-Requests: 1\r\n
  - User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.174 YaBrowser/22.1.3.856 (beta) Yowser/2.5 Safari/537.36\r\n
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  - Accept-Encoding: gzip, deflate\r\n
  - Accept-Language: ru\r\n
  - \r\n

- Один, 270
- Всё тот же 276

No.	Time	Source	Destination	Protocol	Length	Info
270	10.501040689	192.168.1.4	128.119.245.12	HTTP	567	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
276	10.651911359	128.119.245.12	192.168.1.4	HTTP	4927	HTTP/1.1 200 OK (text/html)

  

Frame 276: 4927 bytes on wire (39416 bits), 4927 bytes captured (39416 bits) on interface wlo1, id 0

- Ethernet II, Src: Netgear\_0a:c2:48 (c4:04:15:0a:c2:48), Dst: 64:6e:e0:a2:6f:89 (64:6e:e0:a2:6f:89)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.4
- Transmission Control Protocol, Src Port: 80, Dst Port: 35552, Seq: 1, Ack: 502, Len: 4861
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
  - Date: Sat, 26 Feb 2022 13:38:54 GMT\r\n
  - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod\_perl/2.0.11 Perl/v5.16.3\r\n
  - Last-Modified: Sat, 26 Feb 2022 06:59:01 GMT\r\n
  - ETag: "1194-5d8e659a73ac5"\r\n
  - Accept-Ranges: bytes\r\n
  - Content-Length: 4500\r\n
  - Keep-Alive: timeout=5, max=100\r\n
  - Connection: Keep-Alive\r\n
  - Content-Type: text/html; charset=UTF-8\r\n
  - \r\n
  - [HTTP response 1/1]
  - [Time since request: 0.150870661 seconds]
  - [Request in frame: 270]
  - [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
  - File Data: 4500 bytes
- Line-based text data: text/html (98 lines)

- Ноль, вообще не сегментировалось на TCP
- Нет

#### Задание 4. HTML-документы со встроенными объектами

No.	Time	Source	Destination	Protocol	Length	Info
372	7.099308529	192.168.1.4	128.119.245.12	HTTP	567	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
396	7.238097815	128.119.245.12	192.168.1.4	HTTP	1367	HTTP/1.1 200 OK (text/html)
401	7.296519137	192.168.1.4	128.119.245.12	HTTP	513	GET /pearson.png HTTP/1.1
435	7.371923179	192.168.1.4	178.79.137.164	HTTP	480	GET /8E_cover_small.jpg HTTP/1.1
441	7.440690562	128.119.245.12	192.168.1.4	HTTP	2277	HTTP/1.1 200 OK (PNG)
444	7.448000558	178.79.137.164	192.168.1.4	HTTP	237	HTTP/1.1 301 Moved Permanently

- Три:

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>,  
<http://gaia.cs.umass.edu/pearson.png>,  
[http://kurose.cslash.net/8E\\_cover\\_small.jpg](http://kurose.cslash.net/8E_cover_small.jpg)

2. Не очень понял, но сработало примерно так: есть два гет запроса к изначальному хосту, там все норм, также каким-то образом появляется ТСП запрос (вот тут я не понял каким), который вызывает гет запрос на картинку по последнему урлу, который отвечает 301 и редиректит на https версию. Такое чувство, что параллельность скрывается как раз за магическим появлением ТСП. По экспериментальным запускам, думаю, что можно сказать, что все делается последовательно, но явной информации про это я не нашел.

### Задание 5. HTTP-аутентификация

No.	Time	Source	Destination	Protocol	Length	Info
72	2.272722679	192.168.1.4	128.119.245.12	HTTP	668	GET /wireshark-labs/protected_pages/HTTP-wireshark-fil...
82	2.415744178	128.119.245.12	192.168.1.4	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
112	4.547949836	192.168.1.4	128.119.245.12	HTTP	753	GET /wireshark-labs/protected_pages/HTTP-wireshark-fil...
113	4.769984978	128.119.245.12	192.168.1.4	HTTP	555	HTTP/1.1 200 OK (text/html)

  

» Frame 112: 753 bytes on wire (6024 bits), 753 bytes captured (6024 bits) on interface wlo1, id 0  
 » Ethernet II, Src: 64:6e:e0:a2:6f:89 (64:6e:e0:a2:6f:89), Dst: Netgear\_0a:c2:48 (c4:04:15:0a:c2:48)  
 » Internet Protocol Version 4, Src: 192.168.1.4, Dst: 128.119.245.12  
 » Transmission Control Protocol, Src Port: 35560, Dst Port: 80, Seq: 603, Ack: 718, Len: 687  
 - Hypertext Transfer Protocol  
   » GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n  
     Host: gaia.cs.umass.edu\r\n  
     Connection: keep-alive\r\n  
     Cache-Control: max-age=0\r\n  
     Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm9z\r\n  
     DNT: 1\r\n  
     Upgrade-Insecure-Requests: 1\r\n  
     User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.174 YaBrowser/22.1.3.856 (beta) Yowser/2.5 Safari/537.36\r\n  
     Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n  
     Accept-Encoding: gzip, deflate\r\n  
     Accept-Language: ru\r\n  
     If-None-Match: "84-5d86da696a0bb"\r\n  
     If-Modified-Since: Sun, 20 Feb 2022 06:59:01 GMT\r\n  
     \r\n  
     [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html]  
     [HTTP request 2/2]  
     [Prev request in frame: 72]  
     [Response in frame: 113]

1. 401 Unauthorized
2. Cache-Control и Authorization