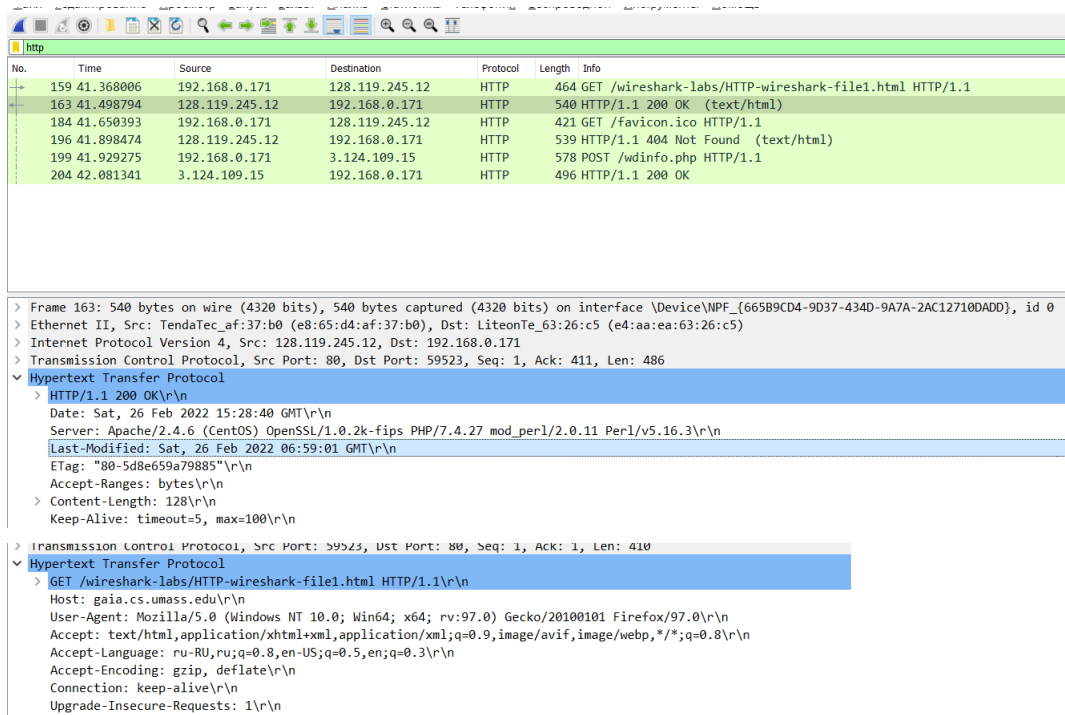


Домашнее задание 1

1. (a) И браузер, и сервер используют HTTP 1.1.
- (b) ru-RU, ru, en-US, en. Дополнительно сообщается версия браузера, операционная система пользователя, возможные файлы, которые может принять клиент.
- (c) Клиент - 192.168.0.171. Сервер - 128.119.245.12.
- (d) 200 OK.
- (e) Sat, 26 Feb 2022 06:59:01 GMT.
- (f) 128.



The image shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows several packets, with packet 163 selected. The packet details pane on the right shows the structure of the selected packet, which is an HTTP 200 OK response. The packet bytes pane at the bottom shows the raw data of the packet.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|--|
| 159 | 41.368006 | 192.168.0.171 | 128.119.245.12 | HTTP | 464 | GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1 |
| 163 | 41.498794 | 128.119.245.12 | 192.168.0.171 | HTTP | 540 | HTTP/1.1 200 OK (text/html) |
| 184 | 41.650393 | 192.168.0.171 | 128.119.245.12 | HTTP | 421 | GET /favicon.ico HTTP/1.1 |
| 196 | 41.898474 | 128.119.245.12 | 192.168.0.171 | HTTP | 539 | HTTP/1.1 404 Not Found (text/html) |
| 199 | 41.929275 | 192.168.0.171 | 3.124.109.15 | HTTP | 578 | POST /wdinfo.php HTTP/1.1 |
| 204 | 42.081341 | 3.124.109.15 | 192.168.0.171 | HTTP | 496 | HTTP/1.1 200 OK |

Frame 163: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{665B9CD4-9D37-4340-9A7A-2AC12710DADD}, id 0
> Ethernet II, Src: TendaTec_af:37:b0 (e8:65:d4:af:37:b0), Dst: LiteonTe_63:26:c5 (e4:aa:ea:63:26:c5)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.171
> Transmission Control Protocol, Src Port: 80, Dst Port: 59523, Seq: 1, Ack: 411, Len: 486
▼ Hypertext Transfer Protocol
 > HTTP/1.1 200 OK\r\n
 Date: Sat, 26 Feb 2022 15:28:40 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
> Transmission Control Protocol, Src Port: 59523, Dst Port: 80, Seq: 1, Ack: 410
▼ Hypertext Transfer Protocol
 > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 Host: gaia.cs.umass.edu\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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

2. (a) Нет.

| http | | | | | | |
|------|-----------|----------------|----------------|----------|--------|--|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 101 | 32.446031 | 192.168.0.171 | 128.119.245.12 | HTTP | 464 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 105 | 32.580998 | 128.119.245.12 | 192.168.0.171 | HTTP | 784 | HTTP/1.1 200 OK (text/html) |
| 146 | 32.698991 | 192.168.0.171 | 3.124.109.15 | HTTP | 578 | POST /wdinfo.php HTTP/1.1 |
| 149 | 32.728670 | 192.168.0.171 | 128.119.245.12 | HTTP | 421 | GET /favicon.ico HTTP/1.1 |
| 151 | 32.750645 | 3.124.109.15 | 192.168.0.171 | HTTP | 496 | HTTP/1.1 200 OK |
| 161 | 32.866961 | 128.119.245.12 | 192.168.0.171 | HTTP | 539 | HTTP/1.1 404 Not Found (text/html) |
| 230 | 50.226696 | 192.168.0.171 | 128.119.245.12 | HTTP | 576 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 232 | 50.360295 | 128.119.245.12 | 192.168.0.171 | HTTP | 294 | HTTP/1.1 304 Not Modified |

| | |
|---|---|
| > | Internet Protocol Version 4, Src: 192.168.0.171, Dst: 128.119.245.12 |
| > | Transmission Control Protocol, Src Port: 50392, Dst Port: 80, Seq: 1, Ack: 1, Len: 410 |
| ▼ | Hypertext Transfer Protocol |
| > | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n |
| | Host: gaia.cs.umass.edu\r\n |
| | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0\r\n |
| | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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-file2.html] |

(b) Да. Ответ отображается в поле Line-based text data.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|--|
| 101 | 32.446031 | 192.168.0.171 | 128.119.245.12 | HTTP | 464 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 105 | 32.580998 | 128.119.245.12 | 192.168.0.171 | HTTP | 784 | HTTP/1.1 200 OK (text/html) |
| 146 | 32.698991 | 192.168.0.171 | 3.124.109.15 | HTTP | 578 | POST /wdinfo.php HTTP/1.1 |
| 149 | 32.728670 | 192.168.0.171 | 128.119.245.12 | HTTP | 421 | GET /favicon.ico HTTP/1.1 |
| 151 | 32.750645 | 3.124.109.15 | 192.168.0.171 | HTTP | 496 | HTTP/1.1 200 OK |
| 161 | 32.866961 | 128.119.245.12 | 192.168.0.171 | HTTP | 539 | HTTP/1.1 404 Not Found (text/html) |
| 230 | 50.226696 | 192.168.0.171 | 128.119.245.12 | HTTP | 576 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 232 | 50.360295 | 128.119.245.12 | 192.168.0.171 | HTTP | 294 | HTTP/1.1 304 Not Modified |

| |
|--|
| [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 |
| \n |
| Congratulations again! Now you've downloaded the file lab2-2.html. \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 \n |
| will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE \n |
| field in your browser's HTTP GET request to the server.\n |
| \n |
| </html>\n |

(с) Да, за ним следует дата, когда файл последний раз обновлялся на сервере. Соответственно, если дата не изменилась, то возвращается закешированный браузером файл.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|--|
| 101 | 32.446031 | 192.168.0.171 | 128.119.245.12 | HTTP | 464 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 105 | 32.580998 | 128.119.245.12 | 192.168.0.171 | HTTP | 784 | HTTP/1.1 200 OK (text/html) |
| 146 | 32.698991 | 192.168.0.171 | 3.124.109.15 | HTTP | 578 | POST /wdinfo.php HTTP/1.1 |
| 149 | 32.728670 | 192.168.0.171 | 128.119.245.12 | HTTP | 421 | GET /favicon.ico HTTP/1.1 |
| 151 | 32.750645 | 3.124.109.15 | 192.168.0.171 | HTTP | 496 | HTTP/1.1 200 OK |
| 161 | 32.866961 | 128.119.245.12 | 192.168.0.171 | HTTP | 539 | HTTP/1.1 404 Not Found (text/html) |
| 230 | 50.226696 | 192.168.0.171 | 128.119.245.12 | HTTP | 576 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 232 | 50.360295 | 128.119.245.12 | 192.168.0.171 | HTTP | 294 | HTTP/1.1 304 Not Modified |

> Transmission Control Protocol, Src Port: 50398, Dst Port: 80, Seq: 1, Ack: 1, Len: 522
 > Hypertext Transfer Protocol
 > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
 Host: gaia.cs.umass.edu\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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
 If-Modified-Since: Sat, 26 Feb 2022 06:59:01 GMT\r\n
 If-None-Match: "173-5d8e659a790b5"\r\n
 Cache-Control: max-age=0\r\n

(d) 304 Not Modified. Явно файл не вернул.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|--|
| 101 | 32.446031 | 192.168.0.171 | 128.119.245.12 | HTTP | 464 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 105 | 32.580998 | 128.119.245.12 | 192.168.0.171 | HTTP | 784 | HTTP/1.1 200 OK (text/html) |
| 146 | 32.698991 | 192.168.0.171 | 3.124.109.15 | HTTP | 578 | POST /wdinfo.php HTTP/1.1 |
| 149 | 32.728670 | 192.168.0.171 | 128.119.245.12 | HTTP | 421 | GET /favicon.ico HTTP/1.1 |
| 151 | 32.750645 | 3.124.109.15 | 192.168.0.171 | HTTP | 496 | HTTP/1.1 200 OK |
| 161 | 32.866961 | 128.119.245.12 | 192.168.0.171 | HTTP | 539 | HTTP/1.1 404 Not Found (text/html) |
| 230 | 50.226696 | 192.168.0.171 | 128.119.245.12 | HTTP | 576 | GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 |
| 232 | 50.360295 | 128.119.245.12 | 192.168.0.171 | HTTP | 294 | HTTP/1.1 304 Not Modified |

> Frame 232: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{665B9CD4-9D37-434D-9A7A-2AC12710DADD}, id 0
 > Ethernet II, Src: TendaTec_af:37:b0 (e8:65:d4:af:37:b0), Dst: LiteonTe_63:26:c5 (e4:aa:ea:63:26:c5)
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.171
 > Transmission Control Protocol, Src Port: 80, Dst Port: 50398, Seq: 1, Ack: 523, Len: 240
 > Hypertext Transfer Protocol

3. (a) Два. Пакет №15.

(b) №22.

(c) Четыре.

(d) Нет.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--|
| 15 | 4.568523 | 192.168.0.171 | 128.119.245.12 | HTTP | 464 | GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 |
| 22 | 4.700554 | 128.119.245.12 | 192.168.0.171 | HTTP | 535 | HTTP/1.1 200 OK (text/html) |
| 29 | 4.792421 | 192.168.0.171 | 128.119.245.12 | HTTP | 421 | GET /favicon.ico HTTP/1.1 |
| 32 | 4.812964 | 192.168.0.171 | 3.124.109.15 | HTTP | 578 | POST /wdinfo.php HTTP/1.1 |
| 35 | 4.864716 | 3.124.109.15 | 192.168.0.171 | HTTP | 496 | HTTP/1.1 200 OK |
| 42 | 4.940655 | 128.119.245.12 | 192.168.0.171 | HTTP | 539 | HTTP/1.1 404 Not Found (text/html) |

> Frame 22: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{665B9CD4-9D37-434D-9A7A-2AC12710DADD}, id 0
 > Ethernet II, Src: TendaTec_af:37:b0 (e8:65:d4:af:37:b0), Dst: LiteonTe_63:26:c5 (e4:aa:ea:63:26:c5)
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.171
 > Transmission Control Protocol, Src Port: 80, Dst Port: 50509, Seq: 4381, Ack: 411, Len: 481
 > [4 Reassembled TCP Segments (4861 bytes): #19(1460), #20(1460), #21(1460), #22(481)]
 > Hypertext Transfer Protocol
 > Line-based text data: text/html (98 lines)

4. (a) Четыре GET запроса на адреса 128.119.245.12 и 178.79.137.164.
- (b) Картинки загружались параллельно, потому что запрос GET для второй картинки случился раньше, чем пришёл ответ на запрос GET для первой картинки.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--|
| 25 | 2.102398 | 192.168.0.171 | 128.119.245.12 | HTTP | 464 | GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 |
| 29 | 2.233086 | 128.119.245.12 | 192.168.0.171 | HTTP | 1355 | HTTP/1.1 200 OK (text/html) |
| 32 | 2.312461 | 192.168.0.171 | 128.119.245.12 | HTTP | 421 | GET /pearson.png HTTP/1.1 |
| 37 | 2.381230 | 192.168.0.171 | 178.79.137.164 | HTTP | 388 | GET /8E_cover_small.jpg HTTP/1.1 |
| 42 | 2.447761 | 128.119.245.12 | 192.168.0.171 | HTTP | 746 | HTTP/1.1 200 OK (PNG) |
| 45 | 2.449607 | 178.79.137.164 | 192.168.0.171 | HTTP | 225 | HTTP/1.1 301 Moved Permanently |
| 51 | 2.582595 | 192.168.0.171 | 128.119.245.12 | HTTP | 421 | GET /favicon.ico HTTP/1.1 |
| 59 | 2.716643 | 128.119.245.12 | 192.168.0.171 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |

> Frame 42: 746 bytes on wire (5968 bits), 746 bytes captured (5968 bits) on interface \Device\NPF_{665B9CD4-9D37-434D-9A7A-2AC12710DADD}, id 0
 > Ethernet II, Src: TendaTec_af:37:b0 (e8:65:d4:af:37:b0), Dst: LiteonTe_63:26:c5 (e4:aa:ea:63:26:c5)
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.171
 > Transmission Control Protocol, Src Port: 80, Dst Port: 65314, Seq: 2921, Ack: 368, Len: 692
 > [3 Reassembled TCP Segments (3612 bytes): #40(1460), #41(1460), #42(692)]
 > Hypertext Transfer Protocol
 > Portable Network Graphics

5. (a) 401 Unauthorized.
- (b) Появилось поле Credentials с логином и паролем.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|--|
| 81 | 21.002391 | 192.168.0.171 | 128.119.245.12 | HTTP | 480 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 85 | 21.138207 | 128.119.245.12 | 192.168.0.171 | HTTP | 771 | HTTP/1.1 401 Unauthorized (text/html) |
| 92 | 21.236813 | 192.168.0.171 | 3.124.109.15 | HTTP | 578 | POST /wdinfo.php HTTP/1.1 |
| 94 | 21.282825 | 3.124.109.15 | 192.168.0.171 | HTTP | 496 | HTTP/1.1 200 OK |
| 119 | 37.835808 | 192.168.0.171 | 128.119.245.12 | HTTP | 539 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 121 | 37.978447 | 128.119.245.12 | 192.168.0.171 | HTTP | 544 | HTTP/1.1 200 OK (text/html) |
| 125 | 38.074866 | 192.168.0.171 | 128.119.245.12 | HTTP | 437 | GET /favicon.ico HTTP/1.1 |
| 132 | 38.215478 | 128.119.245.12 | 192.168.0.171 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |

| | |
|---|---|
| > | Internet Protocol Version 4, Src: 192.168.0.171, Dst: 128.119.245.12 |
| > | Transmission Control Protocol, Src Port: 65366, Dst Port: 80, Seq: 1, Ack: 1, Len: 485 |
| ▼ | Hypertext Transfer Protocol |
| > | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n |
| | Host: gaia.cs.umass.edu\r\n |
| | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0\r\n |
| | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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 d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcmMs\r\n |
| | Credentials: wireshark-students:network |
| | \r\n |