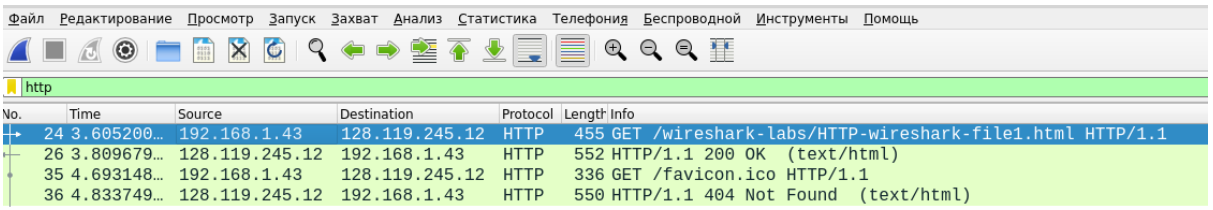
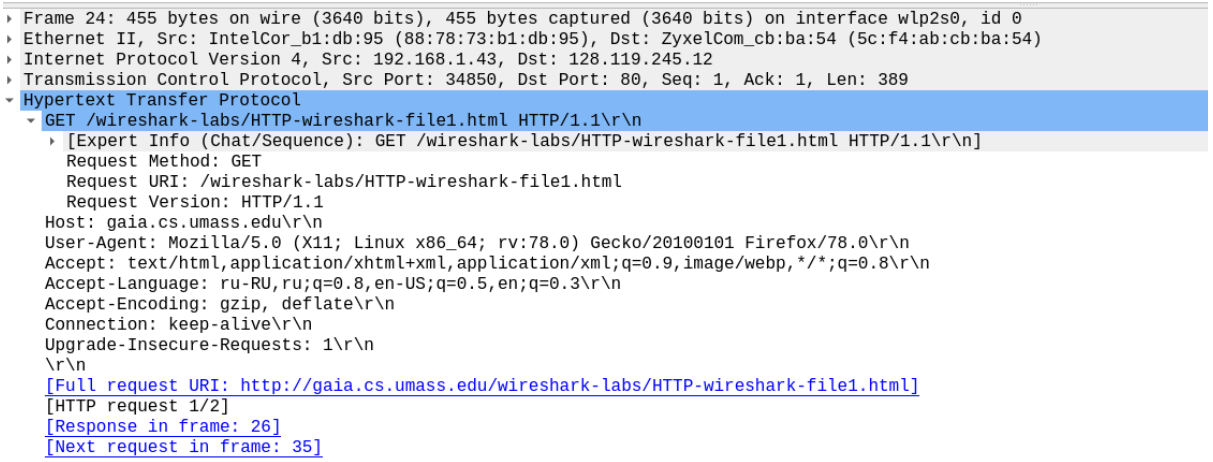
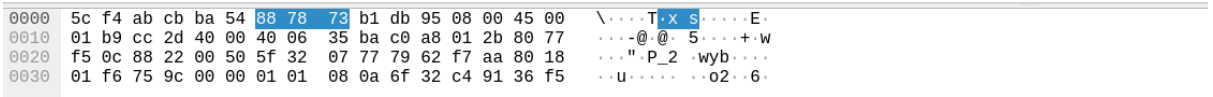
Практика 1. Wireshark

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

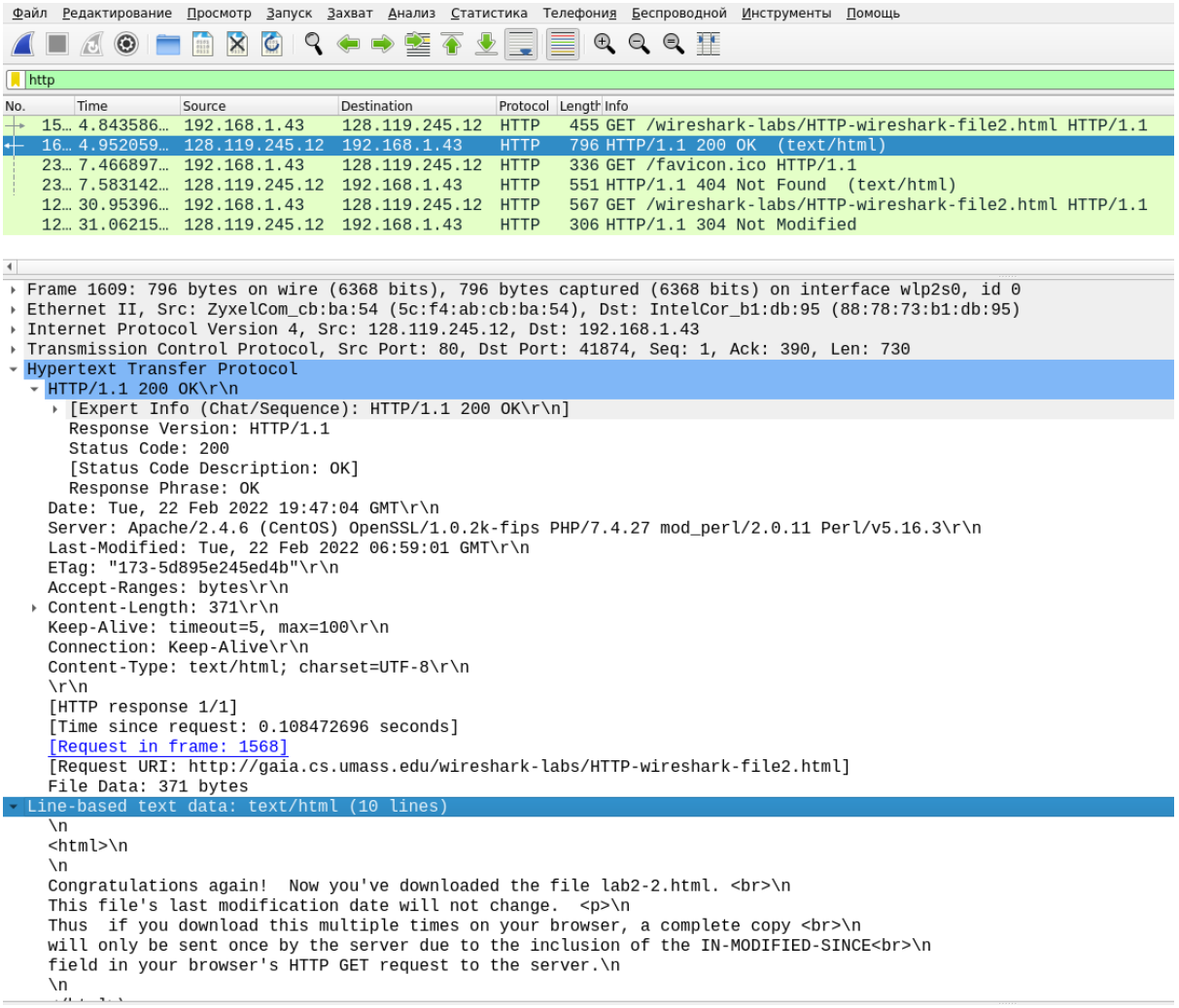






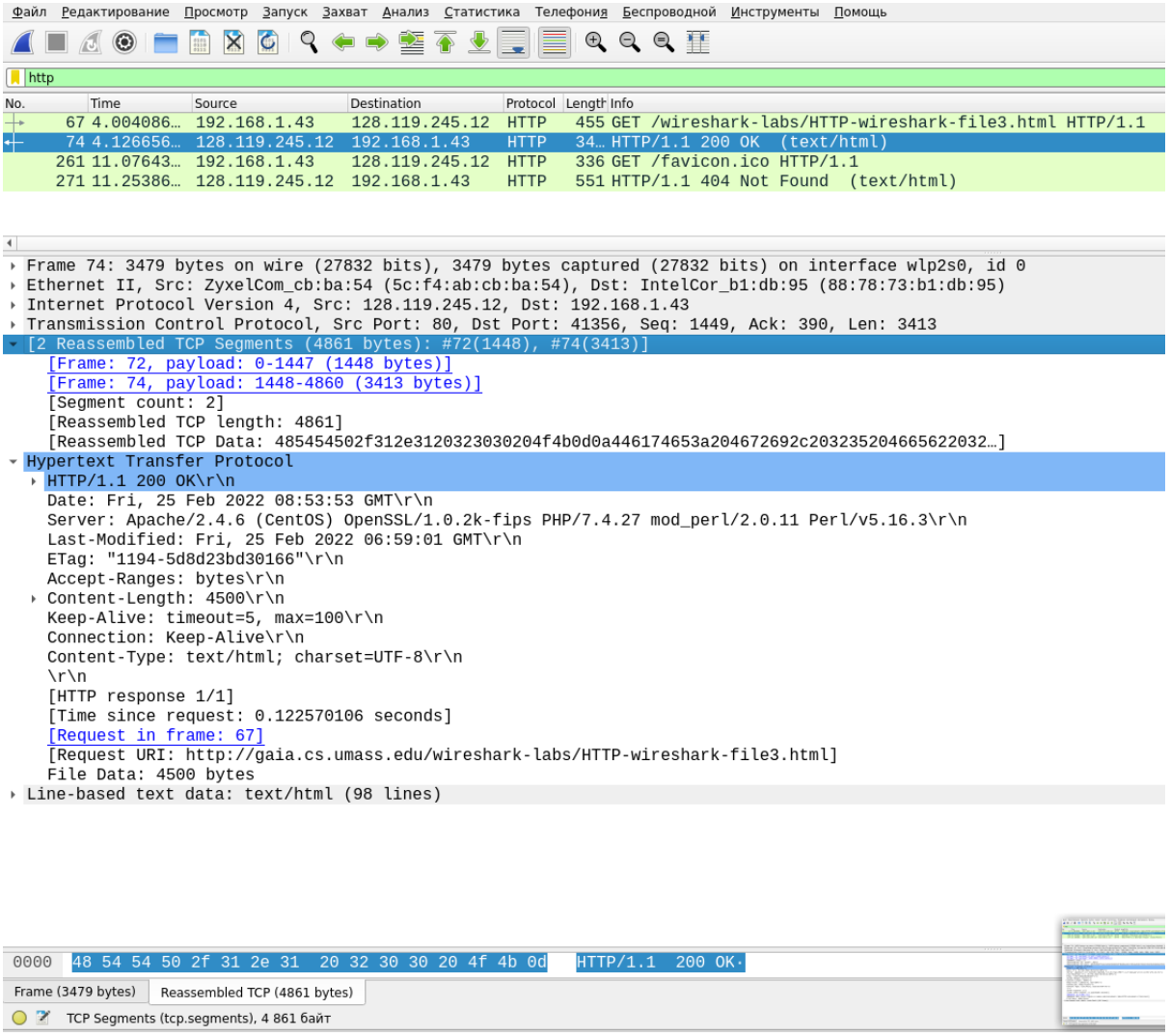
Задание 2.

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.



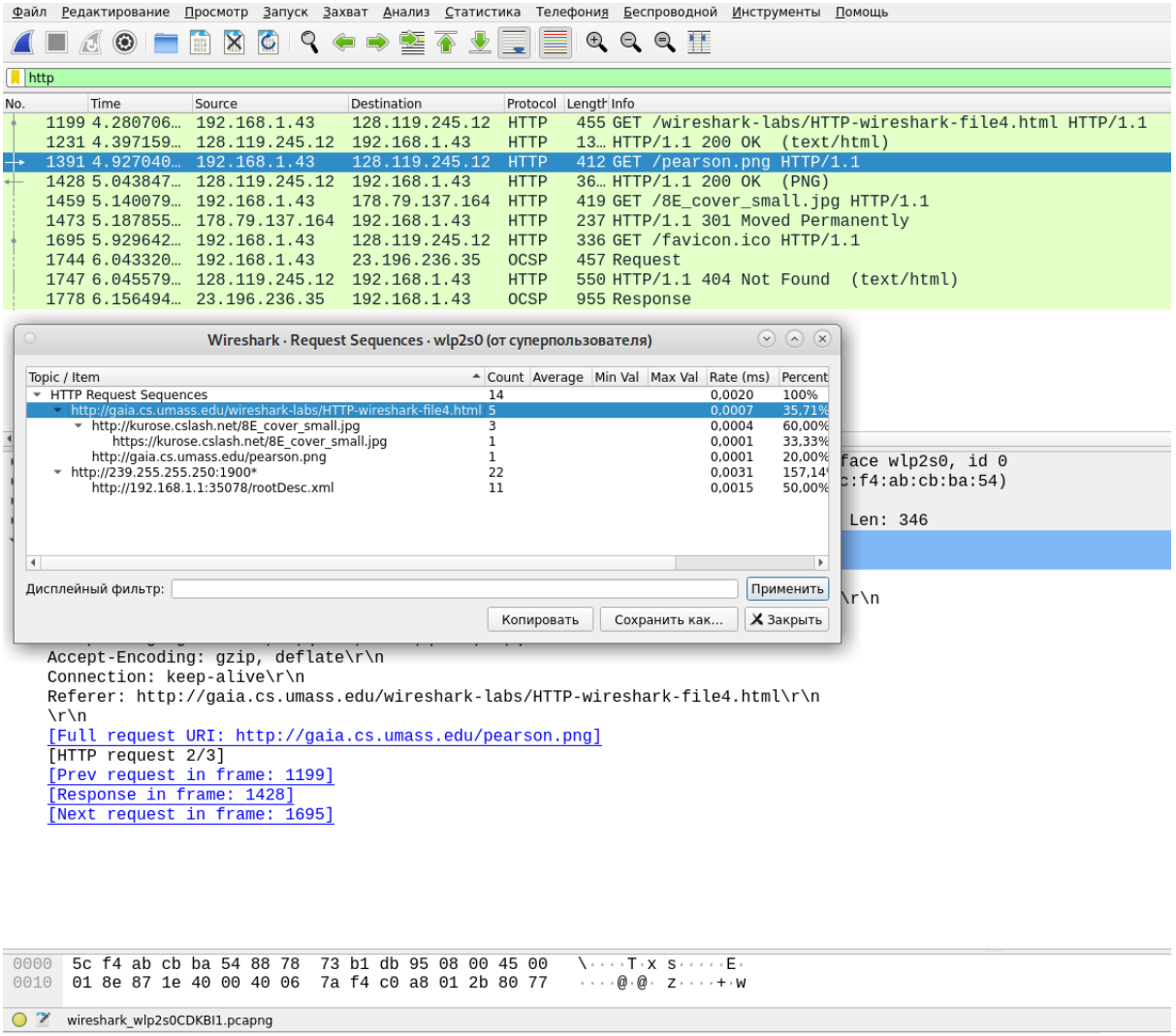
Задание 3.

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.



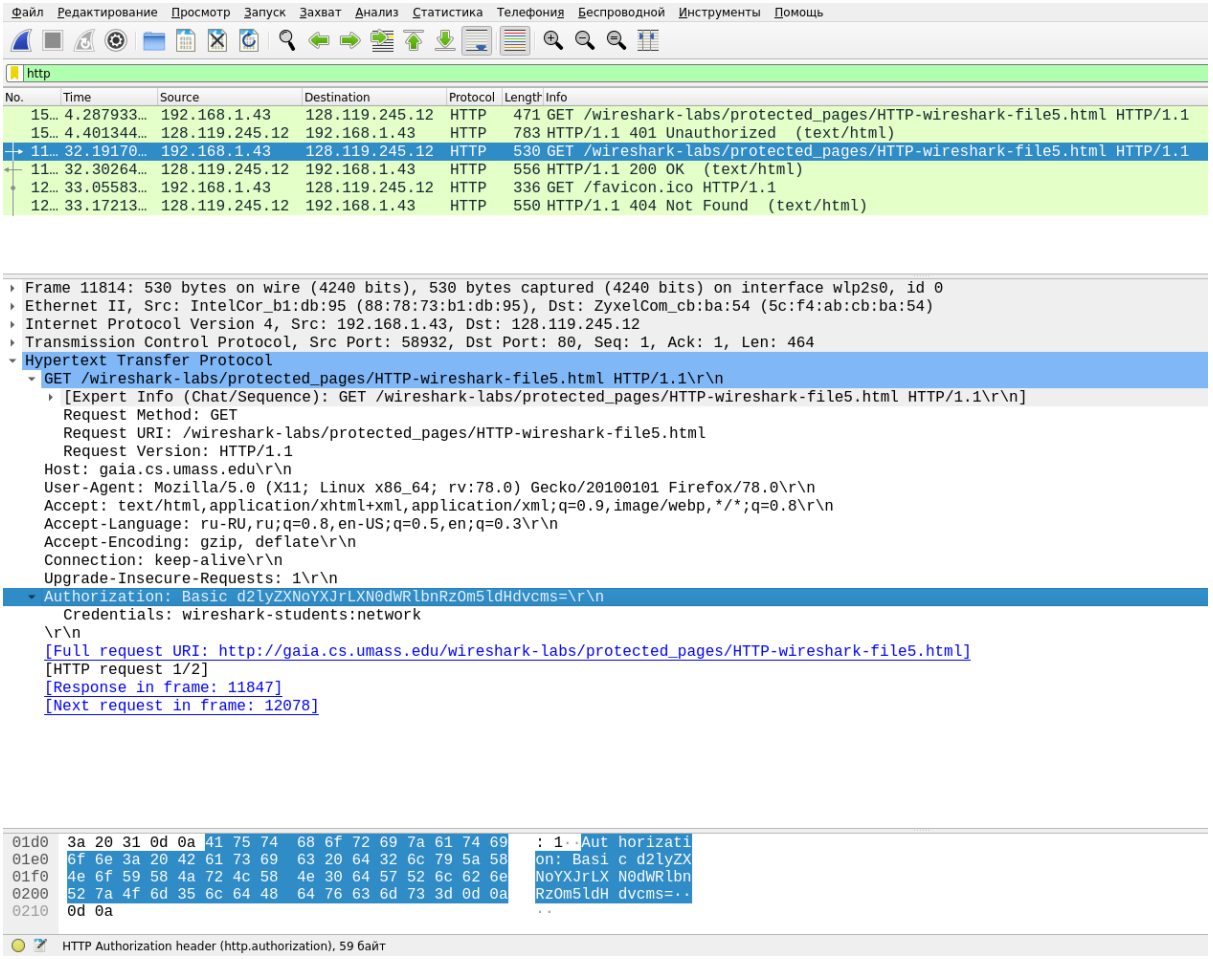
Задание 4.

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.



Задание 5.

1. Status Code: 401
   Status Code Description: Unauthorized
2. 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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\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 horizati
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