

# Student: Павлова Александра, 19.Б05-мкн

## Task 1

Wireshark capture of an HTTP GET request. The packet list shows a GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details show the request headers, including Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Connection, Upgrade-Insecure-Requests, and the request URI. The packet bytes show the raw data of the request.

1. HTTP/1.1 и там, и там
2. *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*
3. Мой IP-адрес: 192.168.1.78, IP-адрес сервера: 128.119.245.12
4. первый: 200 OK, второй: 404 Not Found
5. *Last-Modified: Fri, 25 Feb 2022 06:59:01 GMT\r\n*
6. *File Data: 128 bytes*

## Task 2

Wireshark capture of an HTTP GET request. The packet list shows a GET request for /wireshark-labs/HTTP-wireshark-file2.html. The packet details show the request headers, including Accept-Ranges, Content-Length, Keep-Alive, Connection, Content-Type, and the request URI. The packet bytes show the raw data of the request.

1. no
2. yes; because we can see this: *File Data: 371 bytes + line-based text data*
3. yes; *If-Modified-Since: Fri, 25 Feb 2022 06:59:01 GMT\r\n*
4. *304 Not Modified\r\n*; no, there is no "File Data"

## Task 3

The screenshot shows a Wireshark capture of an HTTP transaction. The packet list pane shows two packets: packet 330 is a GET request for /wireshark-labs/HTTP-wireshark-file3.html, and packet 337 is the corresponding 200 OK response. The packet details pane for packet 337 is expanded, showing the Hypertext Transfer Protocol section with the response body. The packet bytes pane shows the raw data of the response body, which is HTML content.

No.	Time	Source	Destination	Protocol	Length	Info
330	21.647637	192.168.1.78	128.119.245.12	HTTP	464	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
337	21.770259	128.119.245.12	192.168.1.78	HTTP	535	HTTP/1.1 200 OK (text/html)

Frame 337: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF\_{C7039B83-B6F4-4CD3-998B-ED4D057519B5}, id 0  
> Ethernet II, Src: Keenetic\_Ad62:1c (50:ff:20:4d:62:1c), Dst: RealtekS\_68:34:0d (00:e0:4c:68:34:0d)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.78  
> Transmission Control Protocol, Src Port: 80, Dst Port: 61930, Seq: 4381, Ack: 411, Len: 481  
> [4 Reassembled TCP Segments (4861 bytes): #334(1460), #335(1460), #336(1460), #337(481)]  
Hypertext Transfer Protocol  
HTTP/1.1 200 OK\r\n  
Date: Sat, 26 Feb 2022 01:08:22 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: Fri, 25 Feb 2022 06:59:01 GMT\r\n  
ETag: "1194-5d8d23bd30166"\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  
...  
<a href="/wireshark-labs/HTTP-wireshark-file3.html">Wireshark File 3</a>  
...  
</p>  
</html>

- one (464 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1); number 330
- number 337 (535 HTTP/1.1 200 OK (text/html))
- 4
- [4 Reassembled TCP Segments (4861 bytes): #334(1460), #335(1460), #336(1460), #337(481)]
  - [Frame: 334, payload: 0-1459 (1460 bytes)]
  - [Frame: 335, payload: 1460-2919 (1460 bytes)]
  - [Frame: 336, payload: 2920-4379 (1460 bytes)]
  - [Frame: 337, payload: 4380-4860 (481 bytes)]
  - [Segment count: 4]
  - [Reassembled TCP length: 4861]
  - [Reassembled TCP Data: 485454502f312e3120323...

## Task 4

The screenshot shows a Wireshark capture of an HTTP transaction. The packet list pane shows two packets: packet 340 is a GET request for /wireshark-labs/HTTP-wireshark-file4.html, and packet 344 is the corresponding 200 OK response. The packet details pane for packet 344 is expanded, showing the Hypertext Transfer Protocol section with the response body. The packet bytes pane shows the raw data of the response body, which is HTML content.

No.	Time	Source	Destination	Protocol	Length	Info
340	9.913564	192.168.31.57	128.119.245.12	HTTP	464	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
344	10.031114	128.119.245.12	192.168.31.57	HTTP	1355	HTTP/1.1 200 OK (text/html)

Frame 340: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface \Device\NPF\_{2E2966C5-6F9C-4FB9-A922-FC8A0E734C76}, id 0  
> Ethernet II, Src: LiteonTe\_db5f:23 (80:30:49:db:5f:23), Dst: BeijingX\_b7:58:76 (28:d1:27:b7:58:76)  
> Internet Protocol Version 4, Src: 192.168.31.57, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 50444, Dst Port: 80, Seq: 1, Ack: 1, Len: 410  
> Hypertext Transfer Protocol

- 3

- a. GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
- b. GET /pearson.png HTTP/1.1
- c. GET /8E\_cover\_small.jpg HTTP/1.1

2. я не уверена, но, кажется, параллельно, судя по тому как расположены запросы GET -- RESPONSE

## Task 5

Wireshark capture of an HTTP 401 Unauthorized response. The packet list shows a GET request for a protected page followed by a 401 response. The packet details pane shows the Authorization header and the full request line. The packet bytes pane shows the raw data of the authorization header.

No.	Time	Source	Destination	Protocol	Length	Info
50	5.345158	192.168.31.57	128.119.245.12	HTTP	480	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
54	5.468329	128.119.245.12	192.168.31.57	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
240	27.319835	192.168.31.57	128.119.245.12	HTTP	539	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
252	27.437923	128.119.245.12	192.168.31.57	HTTP	544	HTTP/1.1 200 OK (text/html)

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 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 1/1]  
 [Response in frame: 252]

01d0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 41 7e -Request s: 1: Ju  
 01e0 74 68 6f 72 69 7a 61 74 69 6f 6e 3a 20 42 61 73 -thorizat ion: Bas  
 01f0 69 63 20 64 32 6c 79 5a 58 4e 6f 59 58 4a 72 4c -ic d2lyZ XNoYXJrL  
 0200 58 4e 30 64 57 52 6c 62 6e 52 7a 4f 6d 35 6c 64 -XN0dWRlbnRzOm5ld  
 0210 48 64 76 63 6d 73 3d 0d 0d 0a Hdvcms=.

HTTP Authorization header (http.authorization), 59 byte(s)

Пакеты: 381 · Показаны: 4 (1.0%) · Потеряно: 0 (0.0%) · Игнорировано: 2 (0.5%) | Профиль: Default

-1°C В ОСН. СОЛНЕЧНО 17:59 26.02.2022

1. HTTP/1.1 401 Unauthorized (text/html)
2. Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n  
Credentials: wireshark-students:network