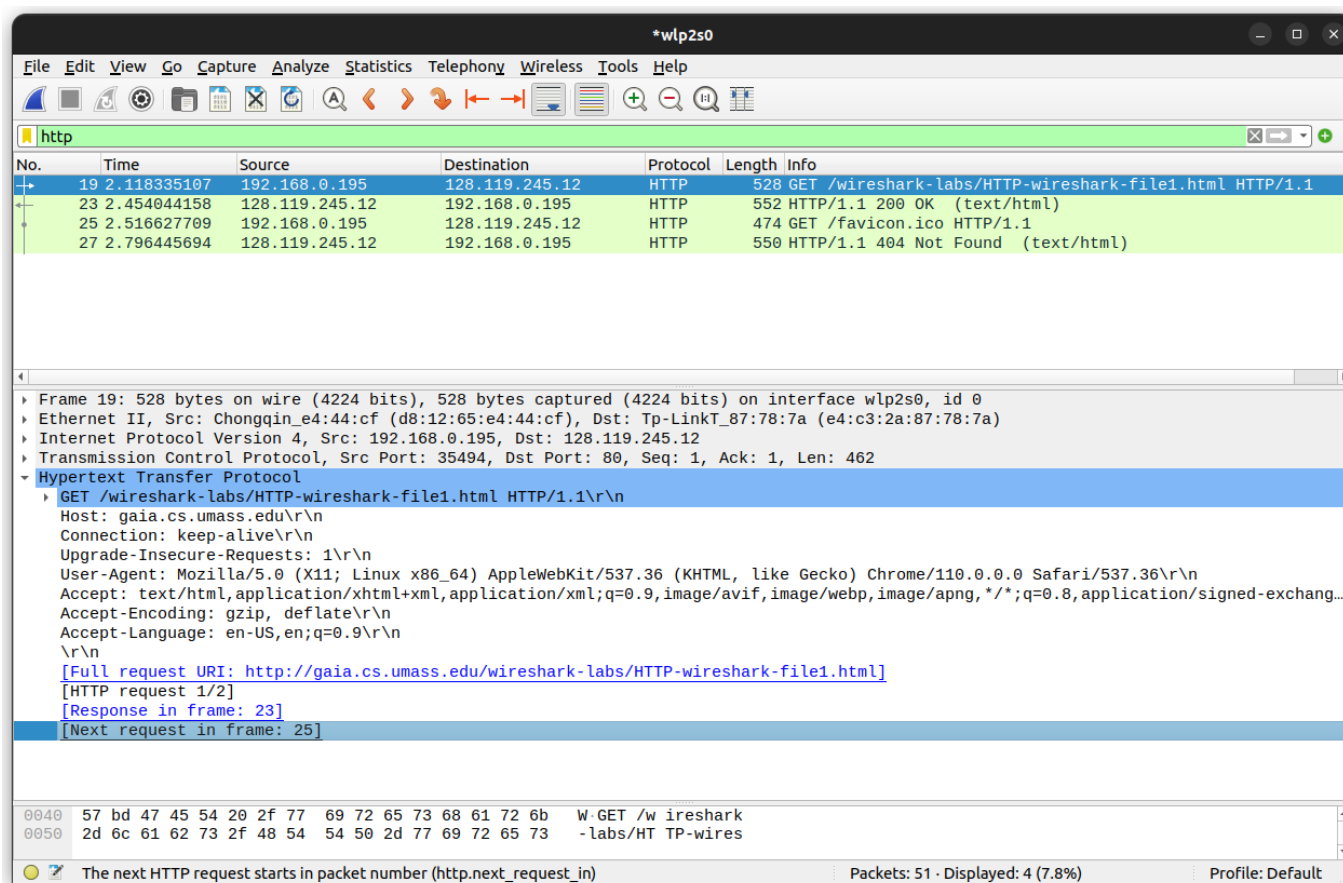


Практика 1. Wireshark: HTTP

Задание 1. Базовое взаимодействие HTTP GET/response



1. Использует ли ваш браузер HTTP версии 1.0 или 1.1? Какая версия HTTP работает на сервере?

Как видим из строки `GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n`, браузер использует **HTTP версии 1.1**.

Сервер присылает нам ответ `HTTP/1.1 200 OK\r\n`, из которого можно понять, что на сервере **та же версия 1.1**

2. Какие языки (если есть) ваш браузер может принимать? В захваченном сеансе какую еще информацию (если есть) браузер предоставляет серверу относительно пользователя/браузера?

Посмотрим на следующую строчку GET запроса: `Accept-Language: en-US,en;q=0.9\r\n`. Из неё понятно, что браузер может принимать только **en-US**.

Ещё в http запросе можно найти request header User-Agent: `User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36\r\n`. Как видим, в запросе есть информация о нашей ОС, браузере и других технических характеристиках.

3. Какой IP-адрес вашего компьютера? Какой адрес сервера gaia.cs.umass.edu?

Посмотрим на **IPv4** часть нашего запроса. В нём есть следующее поле: **Source Address: 192.168.0.195**. Этот адрес является локальным адресом моего роутера. Адрес сервера можно узнать из следующей строчки: **Destination Address: 128.119.245.12**

4. Какой код состояния возвращается с сервера на ваш браузер?

Узнаём это из **Status Code: Status Code: 200**

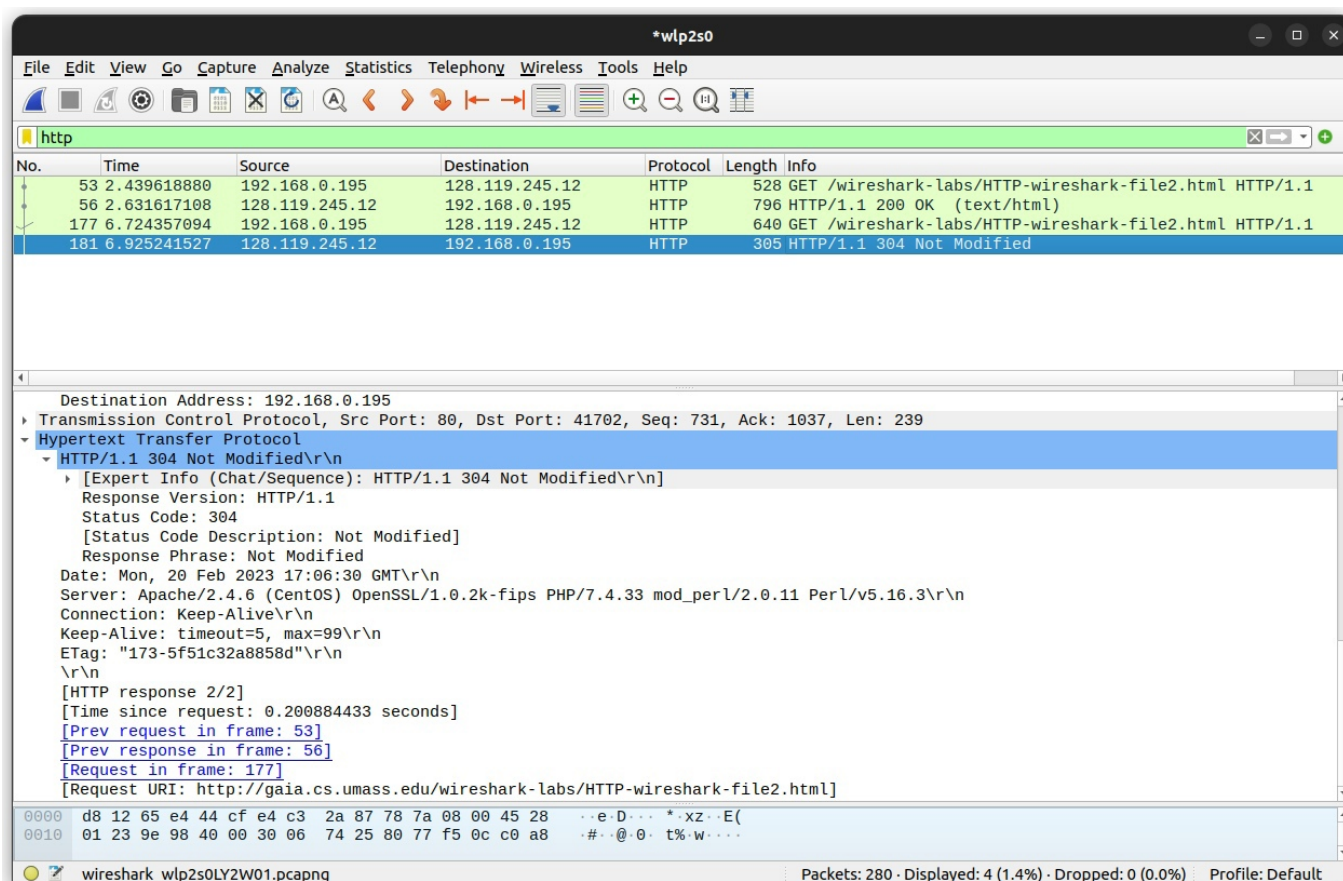
5. Когда HTML-файл, который вы извлекаете, последний раз модифицировался на сервере?

Посмотрим на заголовок **Last-Modified: Last-Modified: Mon, 20 Feb 2023 06:59:01 GMT\r\n**

6. Сколько байтов контента возвращается вашему браузеру?

Нам вернулось **128 байт** данных: **File Data: 128 bytes**

Задание 2. HTTP CONDITIONAL GET/response



1. Проверьте содержимое первого HTTP-запроса GET. Видите ли вы строку «IF-MODIFIED-SINCE» в HTTP GET?

В первом GET запросе строки "IF-MODIFIED-SINCE" **нет**

2. Проверьте содержимое ответа сервера. Вернул ли сервер содержимое файла явно? Как вы это можете увидеть?

В ответе сервера содержится **полный html-документ**, который отобразил мой браузер. Он отображается в поле **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
```

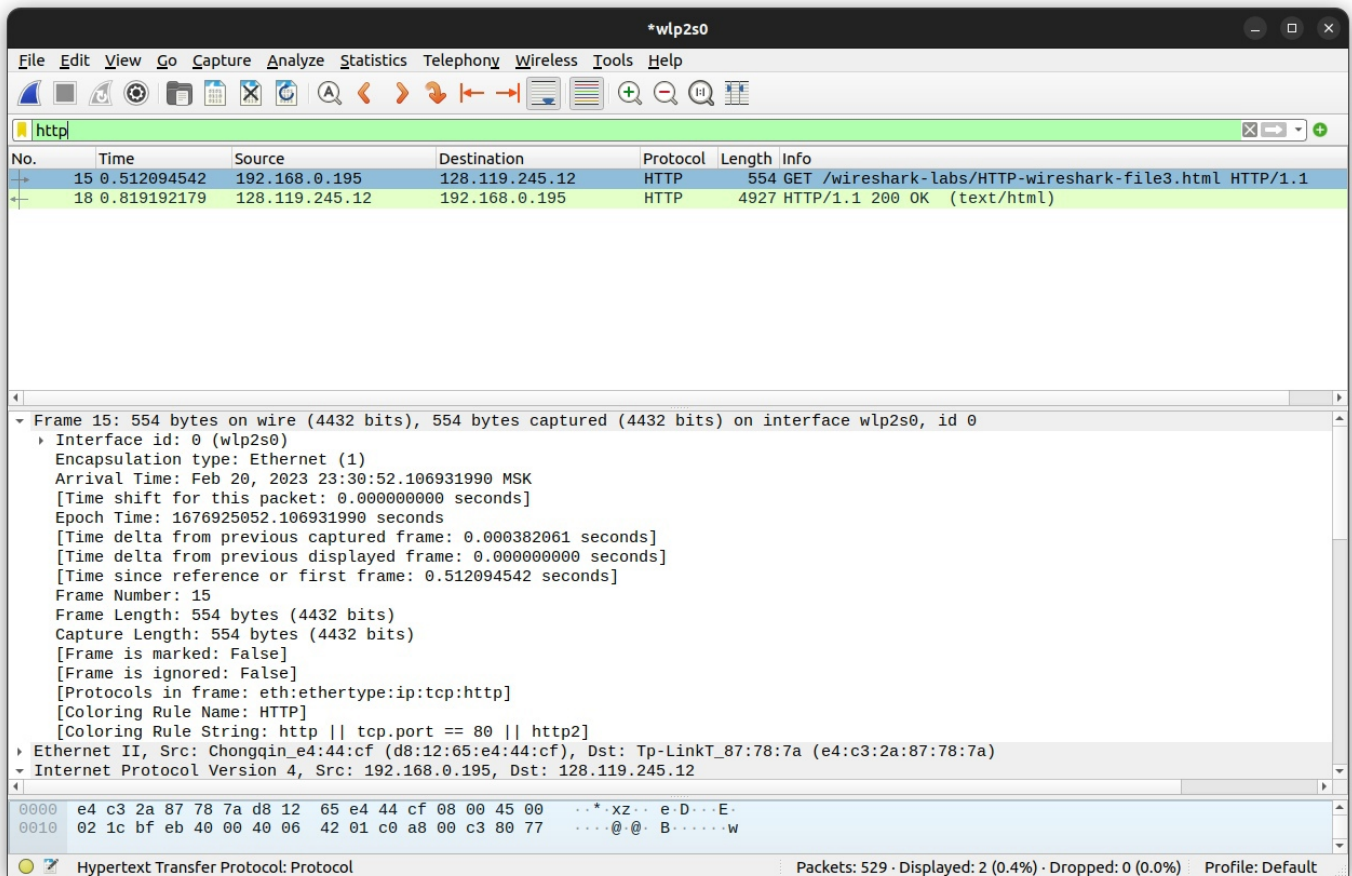
3. Теперь проверьте содержимое второго HTTP-запроса GET (из вашего браузера на сторону сервера). Видите ли вы строку IF-MODIFIED-SINCE:» в HTTP GET? Если да, то какая информация следует за заголовком «IF-MODIFIED-SINCE:»?

Да, такая строка присутствует: **If-Modified-Since: Mon, 20 Feb 2023 06:59:01 GMT\r\n**.
Время, указанное в ней, говорит серверу, что отправить обратно контент нужно только в то случае, если он модифицирован позже указанной даты.

4. Какой код состояния HTTP и фраза возвращаются сервером в ответ на этот второй запрос HTTP GET? Вернул ли сервер явно содержимое файла?

Нам возвращается запрос с **кодом 304 Not Modified**: **Status Code: 304**. При таком статусе возврата никакого содержимого страницы не передаётся.

Задание 3. Получение длинных документов



The screenshot shows the Wireshark interface with the filter `http` applied. The packet list displays two packets: packet 15, an HTTP GET request, and packet 18, the corresponding 200 OK response. The packet details pane for packet 15 is expanded, showing the Ethernet II header, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol section.

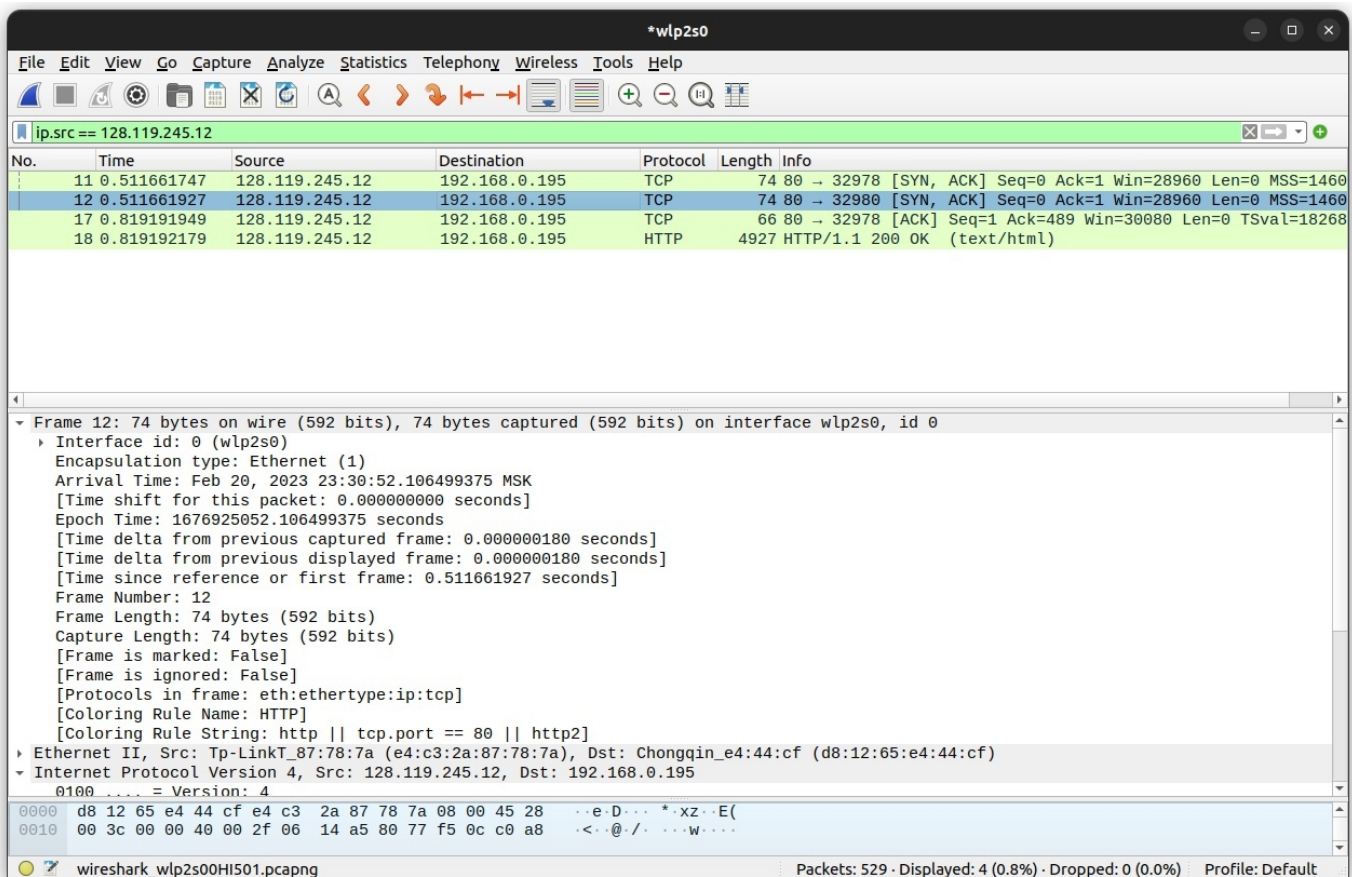
No.	Time	Source	Destination	Protocol	Length	Info
15	0.512094542	192.168.0.195	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
18	0.819192179	128.119.245.12	192.168.0.195	HTTP	4927	HTTP/1.1 200 OK (text/html)

Frame 15: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface wlp2s0, id 0

- Interface id: 0 (wlp2s0)
- Encapsulation type: Ethernet (1)
- Arrival Time: Feb 20, 2023 23:30:52.106931990 MSK
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1676925052.106931990 seconds
- [Time delta from previous captured frame: 0.000382061 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 0.512094542 seconds]
- Frame Number: 15
- Frame Length: 554 bytes (4432 bits)
- Capture Length: 554 bytes (4432 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: Chongqin_e4:44:cf (d8:12:65:e4:44:cf), Dst: Tp-LinkT_87:78:7a (e4:c3:2a:87:78:7a)
- Internet Protocol Version 4, Src: 192.168.0.195, Dst: 128.119.245.12

0000 e4 c3 2a 87 78 7a d8 12 65 e4 44 cf 08 00 45 00 ...*xz...e.D...E.
0010 02 1c bf eb 40 00 00 06 42 01 c0 a8 00 c3 80 77@.@.B.....w

Hypertext Transfer Protocol: Protocol Packets: 529 · Displayed: 2 (0.4%) · Dropped: 0 (0.0%) Profile: Default



The screenshot shows the Wireshark interface with the filter `ip.src == 128.119.245.12` applied. The packet list displays four packets: two TCP SYN/ACK exchanges (packets 11 and 12) and the HTTP GET request (packet 15). The packet details pane for packet 12 is expanded, showing the Ethernet II header, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol section.

No.	Time	Source	Destination	Protocol	Length	Info
11	0.511661747	128.119.245.12	192.168.0.195	TCP	74	80 → 32978 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
12	0.511661927	128.119.245.12	192.168.0.195	TCP	74	80 → 32980 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
17	0.819191949	128.119.245.12	192.168.0.195	TCP	66	80 → 32978 [ACK] Seq=1 Ack=489 Win=30080 Len=0 TSval=18268
18	0.819192179	128.119.245.12	192.168.0.195	HTTP	4927	HTTP/1.1 200 OK (text/html)

Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp2s0, id 0

- Interface id: 0 (wlp2s0)
- Encapsulation type: Ethernet (1)
- Arrival Time: Feb 20, 2023 23:30:52.106499375 MSK
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1676925052.106499375 seconds
- [Time delta from previous captured frame: 0.000000180 seconds]
- [Time delta from previous displayed frame: 0.000000180 seconds]
- [Time since reference or first frame: 0.511661927 seconds]
- Frame Number: 12
- Frame Length: 74 bytes (592 bits)
- Capture Length: 74 bytes (592 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp]
- [Coloring Rule Name: HTTP]
- [Coloring Rule String: http || tcp.port == 80 || http2]
- Ethernet II, Src: Tp-LinkT_87:78:7a (e4:c3:2a:87:78:7a), Dst: Chongqin_e4:44:cf (d8:12:65:e4:44:cf)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.195
- 0100 = Version: 4

0000 d8 12 65 e4 44 cf e4 c3 2a 87 78 7a 08 00 45 28 ...e.D...*xz...E(
0010 00 3c 00 00 40 00 2f 06 14 a5 80 77 f5 0c c0 a8 ...<.@./...w....

wireshark_wlp2s00HI501.pcapng Packets: 529 · Displayed: 4 (0.8%) · Dropped: 0 (0.0%) Profile: Default

1. Сколько сообщений HTTP GET отправил ваш браузер? Какой номер пакета в трассировке содержит сообщение GET?

Браузер отправил **1 GET запрос** (№15).

2. Какой номер пакета в трассировке содержит код состояния и фразу, связанные с ответом на HTTP-запрос GET?

Это пакет под номером **18**

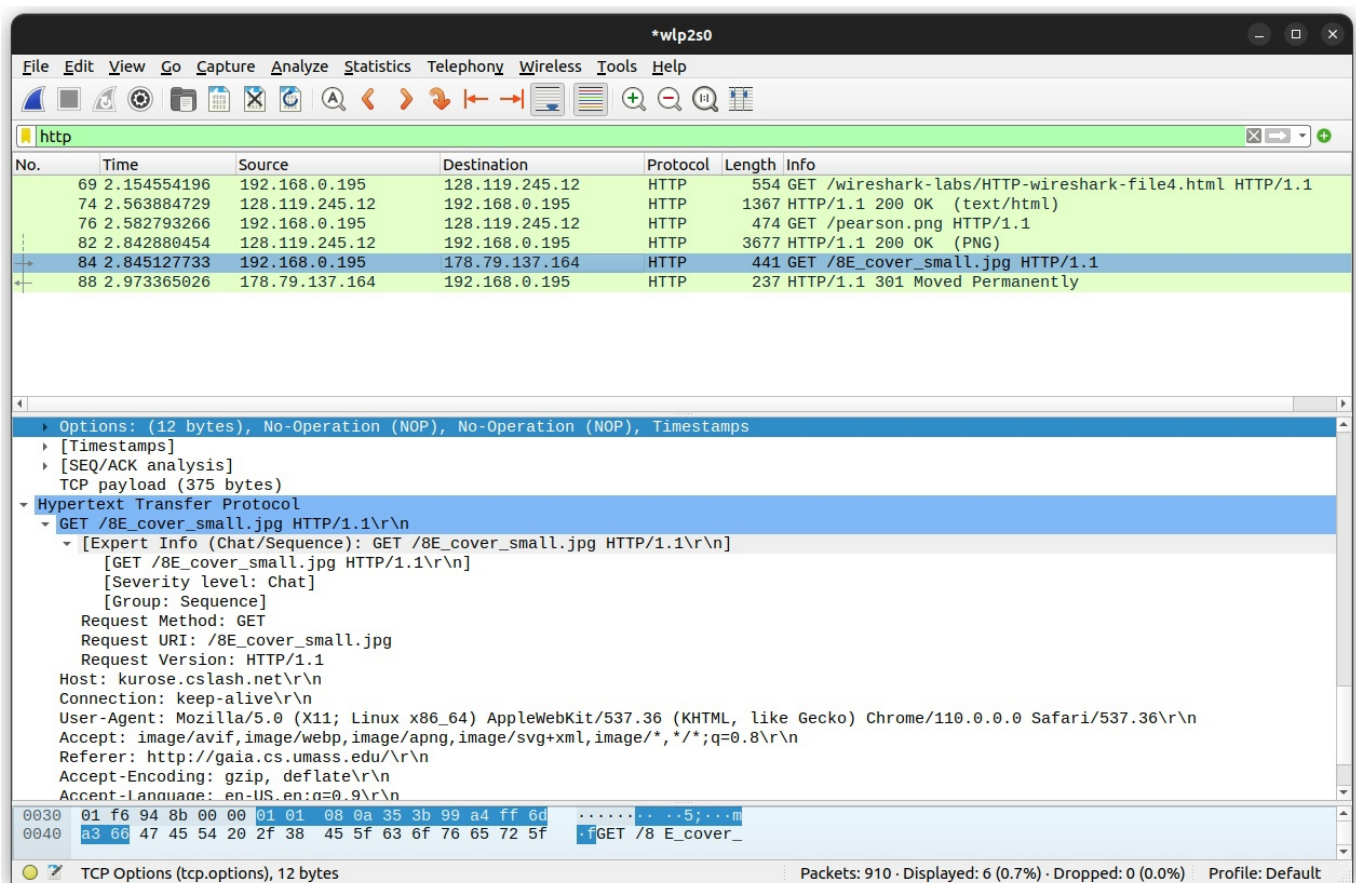
3. Сколько сегментов TCP, содержащих данные, потребовалось для передачи одного HTTP-ответа?

Всего было передано **3 пакета** (11, 12, 17)

4. Есть ли в передаваемых данных какая-либо информация заголовка HTTP, связанная с сегментацией TCP?

HTTP присутствует только в последнем переданном пакете и в его заголовках **нет информации** о сегментации TCP.

Задание 4. HTML-документы со встроенными объектами



1. Сколько HTTP GET запросов было отправлено вашим браузером? На какие Интернет-адреса были отправлены эти GET-запросы?

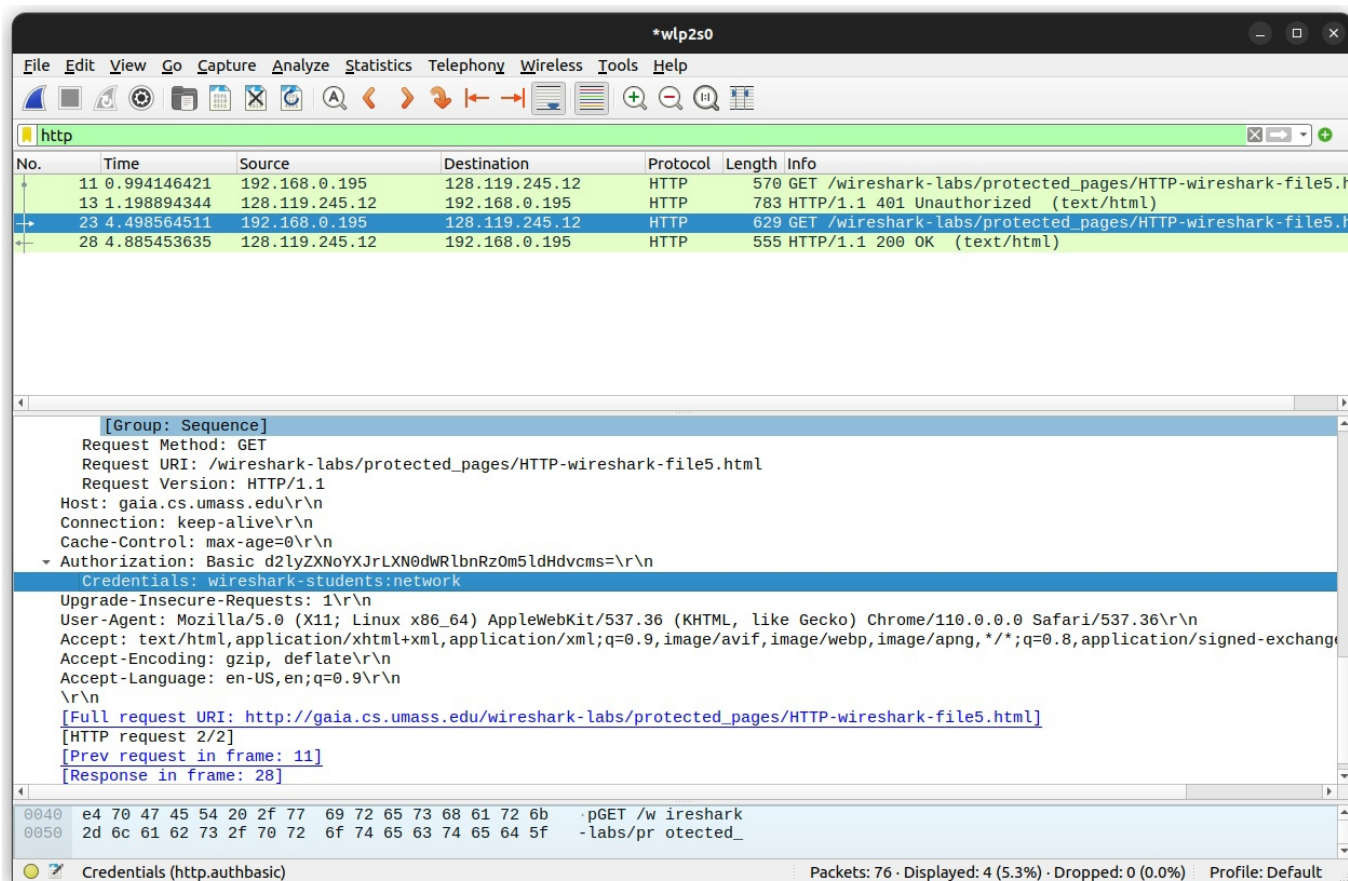
Всего было отправлено **3 запроса** на следующие адреса:

69) Destination Address: 128.119.245.12
 76) Destination Address: 128.119.245.12
 84) Destination Address: 178.79.137.164

2. Можете ли вы сказать, загрузил ли ваш браузер два изображения последовательно или они были загружены с веб-сайтов параллельно? Объясните

Если исходить из ситуации, которую мы видим на скриншоте, то загрузка происходила **последовательно** - второй GET запрос (84) был выслан только после того, как был получен ответ на первый (76)

Задание 5. HTTP-аутентификация



1. Каков ответ сервера (код состояния и фраза) в ответ на начальное HTTP-сообщение GET от вашего браузера?

Сервер присылает ответ с кодом 401: **Status Code: 401** и фразой **Response Phrase: Unauthorized**

2. Когда ваш браузер отправляет сообщение HTTP GET во второй раз, какое новое поле включается в сообщение HTTP GET?

В GET запрос на этот раз включены новые строки:

```

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=\r\n
Credentials: wireshark-students:network

```

Как мы видим, пароли по http лучше не передавать....

Для себя

favicon.ico - это небольшой файл, содержащий изображение (иконку), которое отображается браузером рядом с адресной строкой или в закладках. Браузер автоматически запрашивает этот файл у веб-сервера.