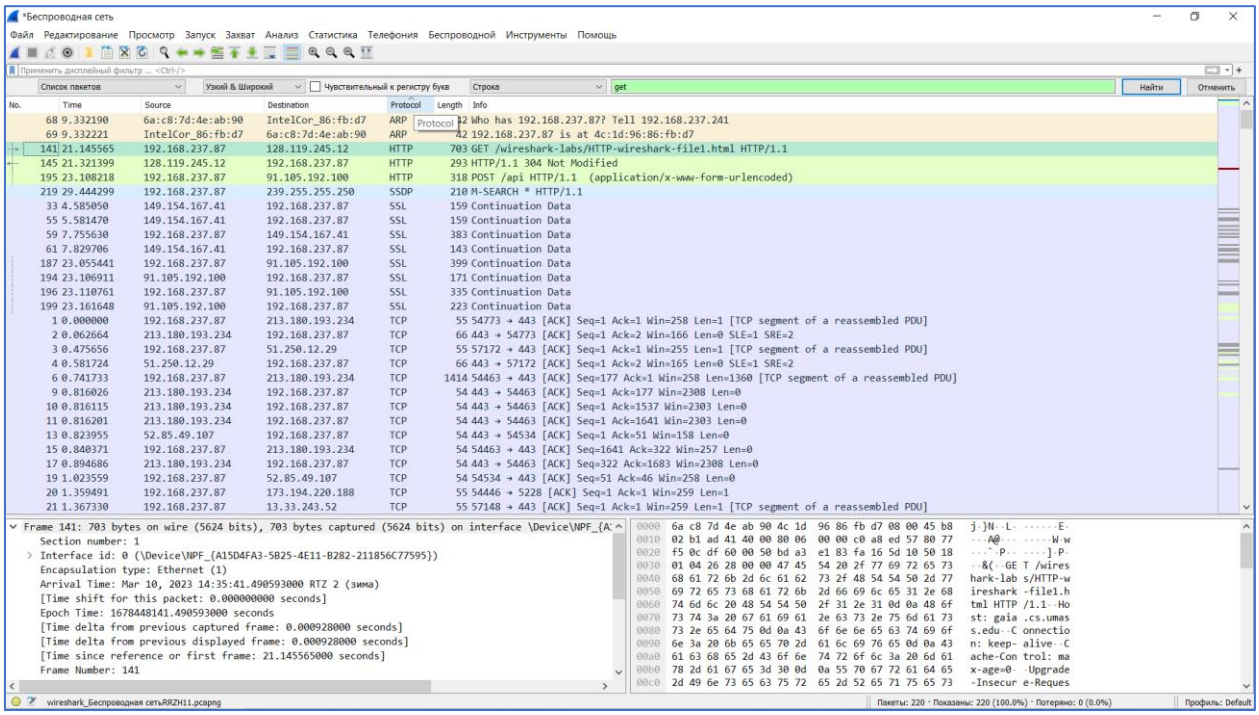
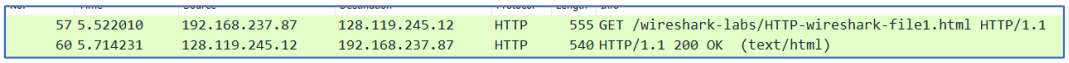
Лабораторная работа 2 “Wireshark: HTTP”

3. Взаимодействие посредством обычных GET-запросов

1. Перечислите любые 3 протокола, которые могут быть отображены в столбце Protocol (Протокол) при отключенном фильтре пакетов:

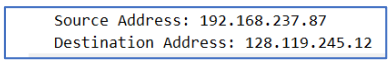


2. Сколько времени прошло от момента отправки сообщения GET протокола HTTP до получения ответного сообщения OK?

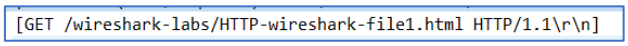


5,71 - 5,52 = 0,19

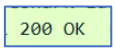
3. Какой IP-адрес у сервера gaia.cs.umass.edu (destination address) so(также известного как wwwnet.cs.umass.edu)? Каков адрес вашего компьютера(source address)?



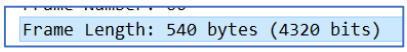
4. Какую версию HTTP использует ваш браузер?



5. Какой код состояния возвратил сервер браузеру?



6. Каков размер содержимого, которое возвратил сервер браузеру?



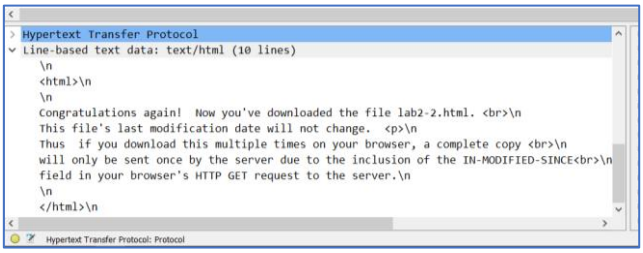
7. Экспортируйте указанные сообщения протокола HTTP (GET и OK), только выбранные пакеты.

4. Взаимодействие посредством условных GET-запросов

8. Изучите содержимое первого GET-запроса от вашего браузера серверу. Видите ли вы строку IF-MODIFIED-SINCE в запросе?

Нет

9. Проверьте ответ сервера. Возвращает ли он содержимое файла?

Да, 

10. Теперь изучите содержимое второго GET-запроса серверу. Видите ли вы теперь строку IF-MODIFIED-SINCE в запросе? Если да, то какая информация идет после заголовка IF-MODIFIED-SINCE?

содержит дату последнего изменения. If-Modified-Since: <day-name>, <day> <month> <year> <hour>:<minute>:<second> GMT

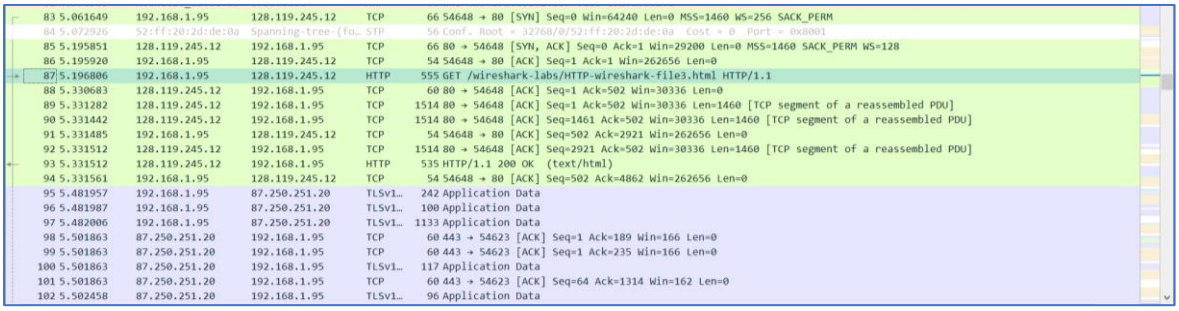
11. Что возвращает сервер в ответ на второй запрос (код состояния и фраза)? Возвращает ли он содержимое файла? Почему?

304 ошибка сервера означает, что запрашиваемый веб-сайт не обновлялся с момента последнего обращения к нему. Как правило, браузер сохраняет (или кеширует) веб-страницы, поэтому ему не нужно повторно загружать одну и ту же информацию.

5. Запрос больших документов

12. Сколько GET-запросов отправил ваш браузер?

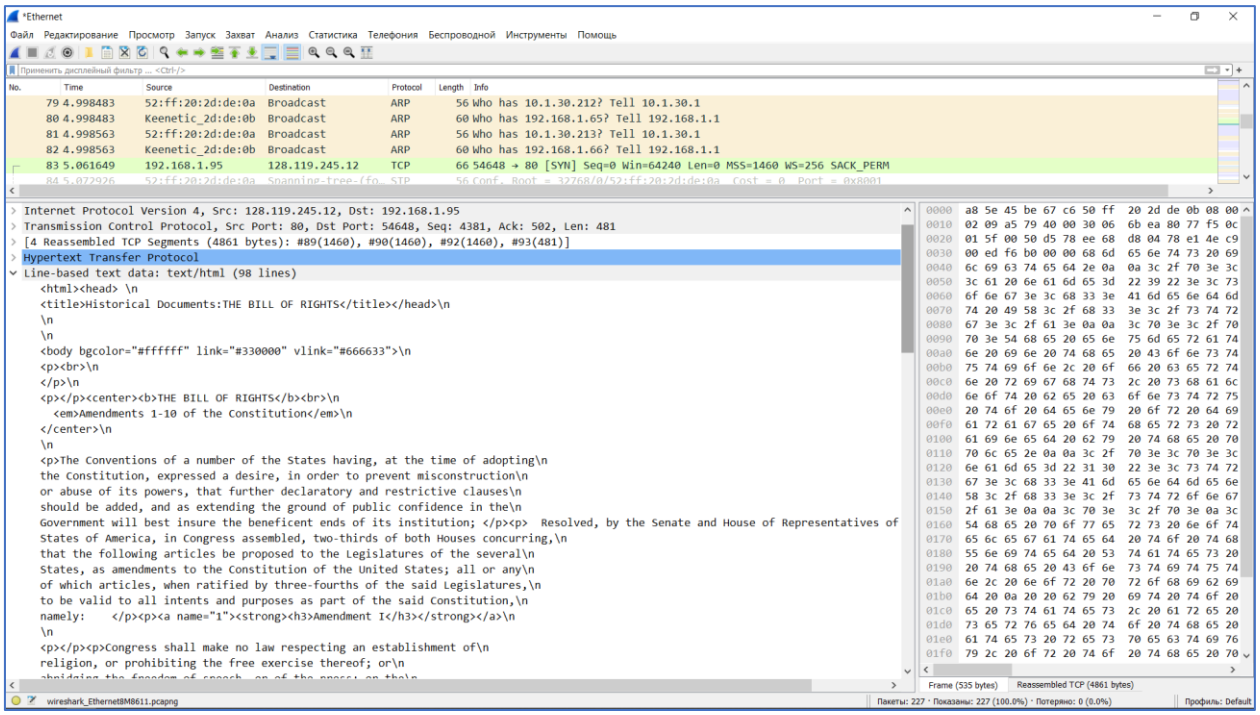
1 -



No.	Time	Source	Destination	Protocol	Length	Info
83	5.061649	192.168.1.95	128.119.245.12	TCP	66	54648 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
84	5.072926	52:ff:20:2d:de:0a	Spanning-tree-(fo…	STP	56	Conf. Root = 32768/0/52:ff:20:2d:de:0a Cost = 0 Port = 0x8001
85	5.195851	128.119.245.12	192.168.1.95	TCP	66	80 → 54648 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
86	5.195920	192.168.1.95	128.119.245.12	TCP	54	54648 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
87	5.196806	192.168.1.95	128.119.245.12	HTTP	555	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
88	5.330683	128.119.245.12	192.168.1.95	TCP	60	80 → 54648 [ACK] Seq=1 Ack=502 Win=30336 Len=0
89	5.331282	128.119.245.12	192.168.1.95	TCP	1514	80 → 54648 [ACK] Seq=1 Ack=502 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
90	5.331442	128.119.245.12	192.168.1.95	TCP	1514	80 → 54648 [ACK] Seq=1461 Ack=502 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
91	5.331485	192.168.1.95	128.119.245.12	TCP	54	54648 → 80 [ACK] Seq=502 Ack=2921 Win=262656 Len=0
92	5.331512	128.119.245.12	192.168.1.95	TCP	1514	80 → 54648 [ACK] Seq=2921 Ack=502 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
93	5.331512	128.119.245.12	192.168.1.95	HTTP	535	HTTP/1.1 200 OK (text/html)
94	5.331561	192.168.1.95	128.119.245.12	TCP	54	54648 → 80 [ACK] Seq=502 Ack=4862 Win=262656 Len=0
95	5.481957	192.168.1.95	87.250.251.20	TLSv1…	242	Application Data
96	5.481987	192.168.1.95	87.250.251.20	TLSv1…	100	Application Data
97	5.482006	192.168.1.95	87.250.251.20	TLSv1…	1133	Application Data
98	5.501863	87.250.251.20	192.168.1.95	TCP	60	443 → 54623 [ACK] Seq=1 Ack=189 Win=166 Len=0
99	5.501863	87.250.251.20	192.168.1.95	TCP	60	443 → 54623 [ACK] Seq=1 Ack=235 Win=166 Len=0
100	5.501863	87.250.251.20	192.168.1.95	TLSv1…	117	Application Data
101	5.501863	87.250.251.20	192.168.1.95	TCP	60	443 → 54623 [ACK] Seq=64 Ack=1314 Win=162 Len=0
102	5.502458	87.250.251.20	192.168.1.95	TLSv1…	96	Application Data

13. Какой код состояния и фраза в ответном сообщении?

No.	Time	Source	Destination	Protocol	Length	Info
93	5.331512	128.119.245.12	192.168.1.95	HTTP	535	HTTP/1.1 200 OK (text/html)



*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
79	4.998483	52:ff:20:2d:de:0a	Broadcast	ARP	56	Who has 10.1.30.212? Tell 10.1.30.1
80	4.998483	Keenetic_2d:de:0b	Broadcast	ARP	60	Who has 192.168.1.65? Tell 192.168.1.1
81	4.998563	52:ff:20:2d:de:0a	Broadcast	ARP	56	Who has 10.1.30.213? Tell 10.1.30.1
82	4.998563	Keenetic_2d:de:0b	Broadcast	ARP	60	Who has 192.168.1.66? Tell 192.168.1.1
83	5.061649	192.168.1.95	128.119.245.12	TCP	66	54648 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
84	5.072926	52:ff:20:2d:de:0a	Spanning-tree-(fo…	STP	56	Conf. Root = 32768/0/52:ff:20:2d:de:0a Cost = 0 Port = 0x8001

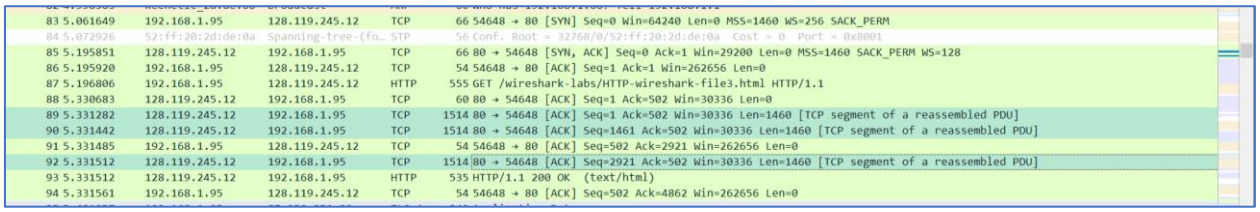
```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.95
> Transmission Control Protocol, Src Port: 80, Dst Port: 54648, Seq: 4381, Ack: 502, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #89(1460), #90(1460), #92(1460), #93(481)]
> Hypertext Transfer Protocol
v Line-based text data: text/html (98 lines)
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
    <p><br>\n
    </p>\n
    <p></p><center><b>THE BILL OF RIGHTS</b><br>\n
      <em>Amendments 1-10 of the Constitution</em>\n
    </center>\n
    \n
    <p>The Conventions of a number of the States having, at the time of adopting\n
    the Constitution, expressed a desire, in order to prevent misconstruction\n
    or abuse of its powers, that further declaratory and restrictive clauses\n
    should be added, and as extending the ground of public confidence in the\n
    Government will best insure the beneficent ends of its institution; </p><p>  Resolved, by the Senate and House of Representatives of
    States of America, in Congress assembled, two-thirds of both Houses concurring,\n
    that the following articles be proposed to the Legislatures of the several\n
    States, as amendments to the Constitution of the United States; all or any\n
    of which articles, when ratified by three-fourths of the said Legislatures,\n
    to be valid to all intents and purposes as part of the said Constitution,\n
    namely:    </p><p><a name="1"><strong><h3>Amendment I</h3></strong></a>\n
    \n
    <p></p><p>Congress shall make no law respecting an establishment of\n
    religion, or prohibiting the free exercise thereof; or\n
```

```
0000  a8 5e 45 be 67 c6 50 ff  20 2d de 0b 08 00
0010  02 09 a5 79 40 00 30 06  6b ea 80 77 f5 0c
0020  01 5f 00 50 d5 78 ee 68  d8 04 78 e1 4e c9
0030  00 ed f6 b0 00 00 68 6d  65 6e 74 73 20 69
0040  6c 69 63 74 65 64 2e 0a  0a 3c 2f 70 3e 3c
0050  3c 61 20 6e 61 6d 65 3d  22 39 22 3e 3c 73
0060  6f 6e 67 3e 3c 68 33 3e  41 6d 65 6e 64 6d
0070  74 20 49 58 3c 2f 68 33  3e 3c 2f 73 74 72
0080  67 3e 3c 2f 61 3e 0a 0a  3c 70 3e 3c 2f 70
0090  70 3e 54 68 65 20 65 6e  75 6d 65 72 61 74
00a0  6e 20 69 6e 20 74 68 65  20 43 6f 6e 73 74
00b0  75 74 69 6f 6e 2c 20 6f  66 20 63 65 72 74
00c0  6e 20 72 69 67 68 74 73  2c 20 73 68 61 6c
00d0  6e 6f 74 20 62 65 20 63  6f 6e 73 74 72 75
00e0  20 74 6f 20 64 65 6e 79  20 6f 72 20 64 69
00f0  61 72 61 67 65 20 6f 74  68 65 72 73 20 72
0100  61 69 6e 65 64 20 62 79  20 74 68 65 20 70
0110  70 6c 65 2e 0a 0a 3c 2f  70 3e 3c 70 3e 3c
0120  6e 61 6d 65 3d 22 31 30  22 3e 3c 73 74 72
0130  67 3e 3c 68 33 3e 41 6d  65 6e 64 6d 65 6e
0140  58 3c 2f 68 33 3e 3c 2f  73 74 72 6f 6e 67
0150  2f 61 3e 0a 0a 3c 70 3e  3c 2f 70 3e 0a 3c
0160  54 68 65 20 70 6f 77 65  72 73 20 6e 6f 74
0170  65 6c 65 67 61 74 65 64  20 74 6f 20 74 68
0180  55 6e 69 74 65 64 20 53  74 61 74 65 73 20
0190  20 74 68 65 20 43 6f 6e  73 74 69 74 75 74
01a0  6e 2c 20 6e 6f 72 20 70  72 6f 68 69 62 69
01b0  64 20 0a 20 20 62 79 20  69 74 20 74 6f 20
01c0  65 20 73 74 61 74 65 73  2c 20 61 72 65 20
01d0  73 65 72 76 65 64 20 74  6f 20 74 68 65 20
01e0  61 74 65 73 20 72 65 73  70 65 63 74 69 76
01f0  79 2c 20 6f 72 20 74 6f  20 74 68 65 20 70
```

Frame (535 bytes) Reassembled TCP (4861 bytes)

wireshark_Ethernet8M8611.pcapng Пакеты: 227 · Показаны: 227 (100.0%) · Потеряно: 0 (0.0%) Профиль: Default

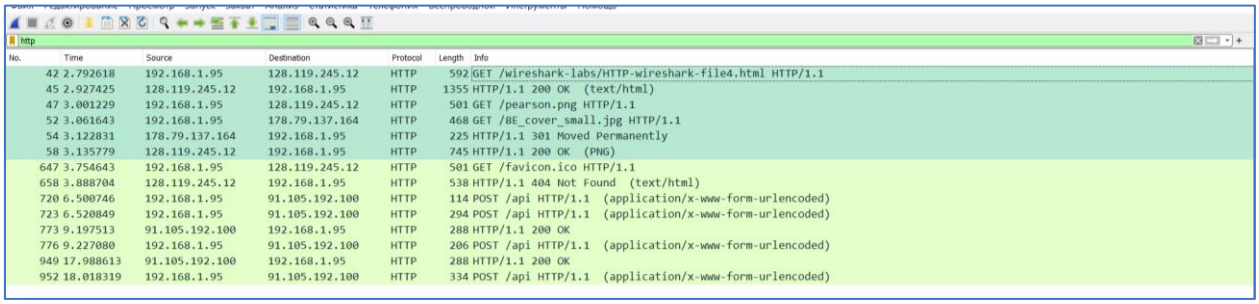
14. Сколько необходимо сегментов TCP для передачи HTTP-ответа и текста документа «THE BILL OF RIGHTS»?



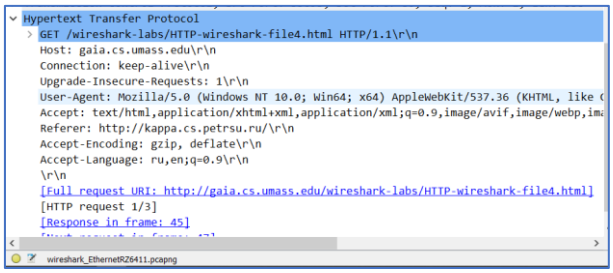
No.	Time	Source	Destination	Protocol	Length	Info
83	5.061649	192.168.1.95	128.119.245.12	TCP	66	54648 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
84	5.072926	52:ff:20:2d:de:0a	Spanning-tree-(fo…	STP	56	Conf. Root = 32768/0/52:ff:20:2d:de:0a Cost = 0 Port = 0x8001
85	5.195851	128.119.245.12	192.168.1.95	TCP	66	80 → 54648 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
86	5.195920	192.168.1.95	128.119.245.12	TCP	54	54648 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
87	5.196806	192.168.1.95	128.119.245.12	HTTP	555	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
88	5.330683	128.119.245.12	192.168.1.95	TCP	60	80 → 54648 [ACK] Seq=1 Ack=502 Win=30336 Len=0
89	5.331282	128.119.245.12	192.168.1.95	TCP	1514	80 → 54648 [ACK] Seq=1 Ack=502 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
90	5.331442	128.119.245.12	192.168.1.95	TCP	1514	80 → 54648 [ACK] Seq=1461 Ack=502 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
91	5.331485	192.168.1.95	128.119.245.12	TCP	54	54648 → 80 [ACK] Seq=502 Ack=2921 Win=262656 Len=0
92	5.331512	128.119.245.12	192.168.1.95	TCP	1514	80 → 54648 [ACK] Seq=2921 Ack=502 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
93	5.331512	128.119.245.12	192.168.1.95	HTTP	535	HTTP/1.1 200 OK (text/html)
94	5.331561	192.168.1.95	128.119.245.12	TCP	54	54648 → 80 [ACK] Seq=502 Ack=4862 Win=262656 Len=0

6. HTML-документы, включающие встроенные объекты

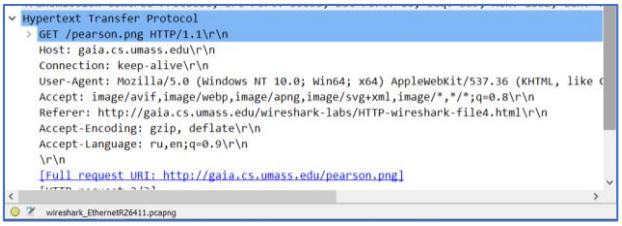
15. Сколько GET-запросов отправил ваш браузер? На какие IP-адреса в Интернете были отправлены эти запросы?



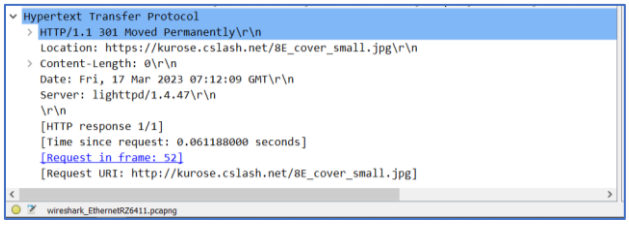
No.	Time	Source	Destination	Protocol	Length	Info
42	2.792618	192.168.1.95	128.119.245.12	HTTP	592	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
45	2.927425	128.119.245.12	192.168.1.95	HTTP	1355	HTTP/1.1 200 OK (text/html)
47	3.001229	192.168.1.95	128.119.245.12	HTTP	501	GET /pearson.png HTTP/1.1
52	3.061643	192.168.1.95	178.79.137.164	HTTP	468	GET /8E_cover_small.jpg HTTP/1.1
54	3.122831	178.79.137.164	192.168.1.95	HTTP	225	HTTP/1.1 301 Moved Permanently
58	3.135779	128.119.245.12	192.168.1.95	HTTP	745	HTTP/1.1 200 OK (PNG)
647	3.754643	192.168.1.95	128.119.245.12	HTTP	501	GET /favicon.ico HTTP/1.1
658	3.888704	128.119.245.12	192.168.1.95	HTTP	538	HTTP/1.1 404 Not Found (text/html)
720	6.500746	192.168.1.95	91.105.192.100	HTTP	114	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
723	6.520849	192.168.1.95	91.105.192.100	HTTP	294	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
773	9.197513	91.105.192.100	192.168.1.95	HTTP	288	HTTP/1.1 200 OK
776	9.227080	192.168.1.95	91.105.192.100	HTTP	206	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
949	17.988613	91.105.192.100	192.168.1.95	HTTP	288	HTTP/1.1 200 OK
952	18.018319	192.168.1.95	91.105.192.100	HTTP	334	POST /api HTTP/1.1 (application/x-www-form-urlencoded)



```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
  Referer: http://kappa.cs.petrsu.ru/\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: ru,en;q=0.9\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
  [HTTP request 1/3]
  [Response in frame: 45]
```

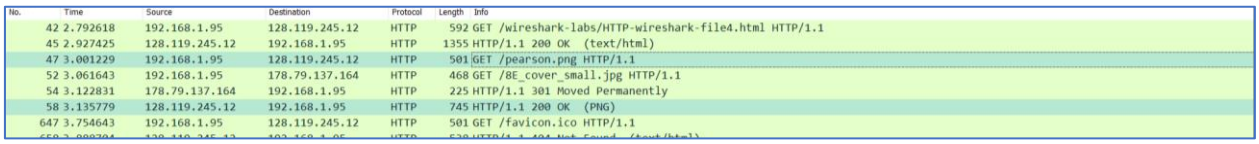


```
Hypertext Transfer Protocol
  GET /pearson.png HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
  Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: ru,en;q=0.9\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/pearson.png]
```



```
Hypertext Transfer Protocol
  HTTP/1.1 301 Moved Permanently\r\n
  Location: https://kurose.cslash.net/8E_cover_small.jpg\r\n
  Content-Length: 0\r\n
  Date: Fri, 17 Mar 2023 07:12:09 GMT\r\n
  Server: lighttpd/1.4.47\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.061188000 seconds]
  [Request in frame: 52]
  [Request URI: http://kurose.cslash.net/8E_cover_small.jpg]
```

16. Каким способом ваш браузер загрузил изображения с двух веб-сайтов – параллельно или один за другим? Объясните.



No.	Time	Source	Destination	Protocol	Length	Info
42	2.792618	192.168.1.95	128.119.245.12	HTTP	592	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
45	2.927425	128.119.245.12	192.168.1.95	HTTP	1355	HTTP/1.1 200 OK (text/html)
47	3.001229	192.168.1.95	128.119.245.12	HTTP	501	GET /pearson.png HTTP/1.1
52	3.061643	192.168.1.95	178.79.137.164	HTTP	468	GET /8E_cover_small.jpg HTTP/1.1
54	3.122831	178.79.137.164	192.168.1.95	HTTP	225	HTTP/1.1 301 Moved Permanently
58	3.135779	128.119.245.12	192.168.1.95	HTTP	745	HTTP/1.1 200 OK (PNG)
647	3.754643	192.168.1.95	128.119.245.12	HTTP	501	GET /favicon.ico HTTP/1.1

Иллюстрация 1, Лучшая приоритизация HTTP/2 для ускорения веба // Хабр URL: https://habr.com/ru/post/452020/ (дата обращения: 17.03.2023).

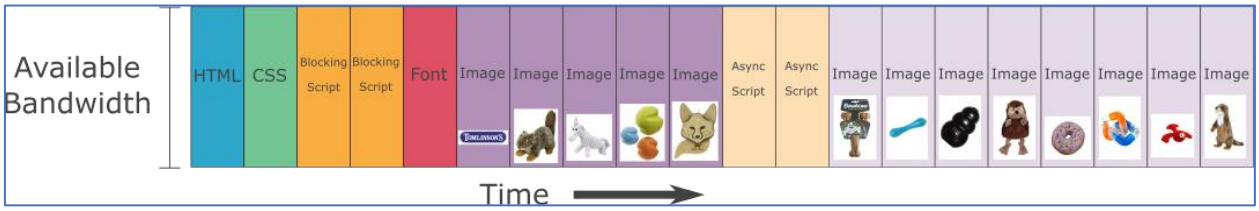
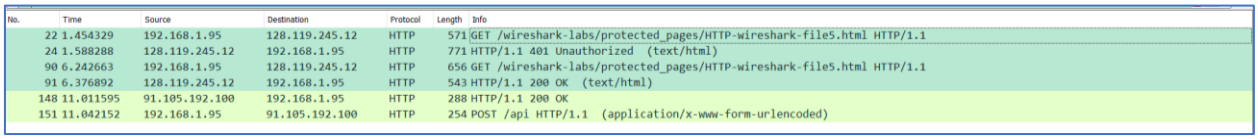


Иллюстрация 2, Лучшая приоритизация HTTP/2 для ускорения веба // Хабр URL: https://habr.com/ru/post/452020/ (дата обращения: 17.03.2023).

7. HTTP-Аутентификация

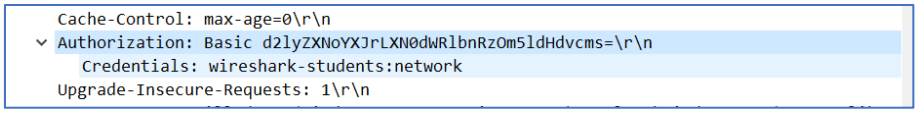
17. Каков первоначальный ответ сервера (код состояния и фраза) на первый GET-запрос вашего браузера?



No.	Time	Source	Destination	Protocol	Length	Info
22	1.454329	192.168.1.95	128.119.245.12	HTTP	571	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
24	1.588288	128.119.245.12	192.168.1.95	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
90	6.242663	192.168.1.95	128.119.245.12	HTTP	656	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
91	6.376892	128.119.245.12	192.168.1.95	HTTP	543	HTTP/1.1 200 OK (text/html)
148	11.011595	91.105.192.100	192.168.1.95	HTTP	288	HTTP/1.1 200 OK
151	11.042152	192.168.1.95	91.105.192.100	HTTP	254	POST /api HTTP/1.1 (application/x-www-form-urlencoded)

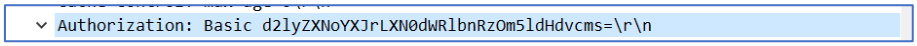
401 Unauthorized

18. Какие новые поля добавляются в GET-сообщение при втором запросе браузера?



```
Cache-Control: max-age=0\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
  Credentials: wireshark-students:network
Upgrade-Insecure-Requests: 1\r\n
```

19. В какой форме кодируются логин и пароль при передаче во втором запросе?



```
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
```

Строка **Basic** создается браузером следующим образом:
`base64_encode(username + ":" + password)`

Некоторые распространенные схемы аутентификации включают:

- **Basic** (смотреть RFC 7617, зашифрованные с помощью base64 учётные данные.),
- **Bearer** (смотреть RFC 6750, bearer токены для доступа OAuth 2.0-защищённых ресурсов),
- **Digest** (смотреть RFC 7616, Firefox 93 и более поздние версии поддерживают шифрование SHA-256. Предыдущие версии поддерживают только хэширование MD5 (не рекомендуется).),
- **HOBA** (смотреть RFC 7486, Секция 3, **H**TTP **O**rigin-**B**ound **A**uthentication, digital-signature-based),
- **Mutual** (смотреть draft-ietf-httpauth-mutual),
- **AWS4-HMAC-SHA256** (смотреть AWS документацию)

Материалы:

- Username and password in https url // stackoverflow URL: https://stackoverflow.com/questions/4980912/username-and-password-in-https-url (дата обращения: 17.03.2023).
- HTTP аутентификация // mdn web docs URL: https://developer.mozilla.org/ru/docs/Web/HTTP/Authentication (дата обращения: 17.03.2023).