

Задание №1

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

И браузер, и сервер работают на HTTP версии 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?**

Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7

В порядке предпочтений: русский, американский английский и английский

Также серверу предоставляется версия моего браузера и версия моего мака

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

IP моего компьютера: 192.168.0.100, адрес сервера gaia.cs.umass.edu: 128.119.245.12

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

200 OK

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

Last-Modified: Thu, 23 Feb 2023 06:59:01 GMT (почти три часа назад относительно того момента, как я пишу этот текст)

6. **Сколько байтов контента возвращается вашему браузеру?**

Content-Length: 128

The image shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows Frame 201, which is a Hypertext Transfer Protocol (HTTP) packet. The packet details pane on the right shows the structure of the HTTP request, including the GET method, the URI /wireshark-labs/HTTP-wireshark-file1.html, and the HTTP version 1.1. The packet bytes pane at the bottom shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol header.

Frame 201: 565 bytes on wire (4520 bits), 565 bytes captured (4520 bits) on interface en0, id 0

Ethernet II, Src: Apple_b4:b4:b4:b4:b4:b4 (24:00:11:11:11:11), Dst: TP-Link_b5:c9:cd (e8:48:b8:b5:c9:cd)

Internet Protocol Version 4, Src: 192.168.0.100, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 51914, Dst Port: 80, Seq: 1, Ack: 1, Len: 499

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1]

[GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1]

[Severity level: Chat]

[Group: Sequence]

Request Method: GET

Request URI: /wireshark-labs/HTTP-wireshark-file1.html

Request Version: HTTP/1.1

Host: gaia.cs.umass.edu

Connection: keep-alive

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate

0000 e8 48 b8 b5 c9 cd 24 d0 df b4 ba c6 08 00 45 00 ..H...\$.E..

0010 02 27 00 00 40 00 40 06 02 41 c0 a8 00 64 80 77 ...@.@..A...d.w

0020 f5 0c ca ca 00 50 05 ab f9 00 92 44 f6 43 80 18P...D.C..

0030 08 0a 3e e5 00 00 01 01 08 0a 3a d3 c8 ac 79 fc ...>.....:..y.

0040 58 b2 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b X-GET /w ireshark

0050 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 72 65 73 ~labs/HT TP-wires

0060 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 6d 6c 20 hark-fil e1.html

0070 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ..Host:

0080 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 gaia.cs. umass.ed

0090 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b u-Conne ction: k

00a0 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 eep-aliv e-Upgra

00b0 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ

00c0 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 ests: 1- User-Ag

00d0 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Moz illa/5.0

00e0 20 2d 4d 61 63 69 6e 74 6f 73 68 3b 20 49 6e 74 (Macint osh; Int

00f0 65 6c 20 4d 61 63 20 4f 53 20 58 20 31 30 5f 31 eL Mac OS X 10_1

0100 35 5f 37 29 20 41 70 70 6c 65 57 65 62 4b 69 74 5.7) App leWebKit

0110 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 /537.36 (KHTML,

0120 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f like Gec ko) Chro

0130 6d 65 2f 31 30 39 2e 30 2e 30 2e 30 20 53 61 66 me/109.0 .0.0 Saf

0140 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 ari/537. 36 Acc

0150 70 74 3a 20 74 65 70 74 2f 68 74 6d 6c 2c 61 70 pt: text/html,ap

0160 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio n/xhtml1+

0170 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f xml,appl ication/

0180 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f xml;q=0. 9,image/

0190 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c avif,ima ge/webp,

01a0 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 image/ap ng,*/*;q

☒ Show packet bytes

Help Close

Задание №2

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

Такой строки нет

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

Явного содержимого файла не видно

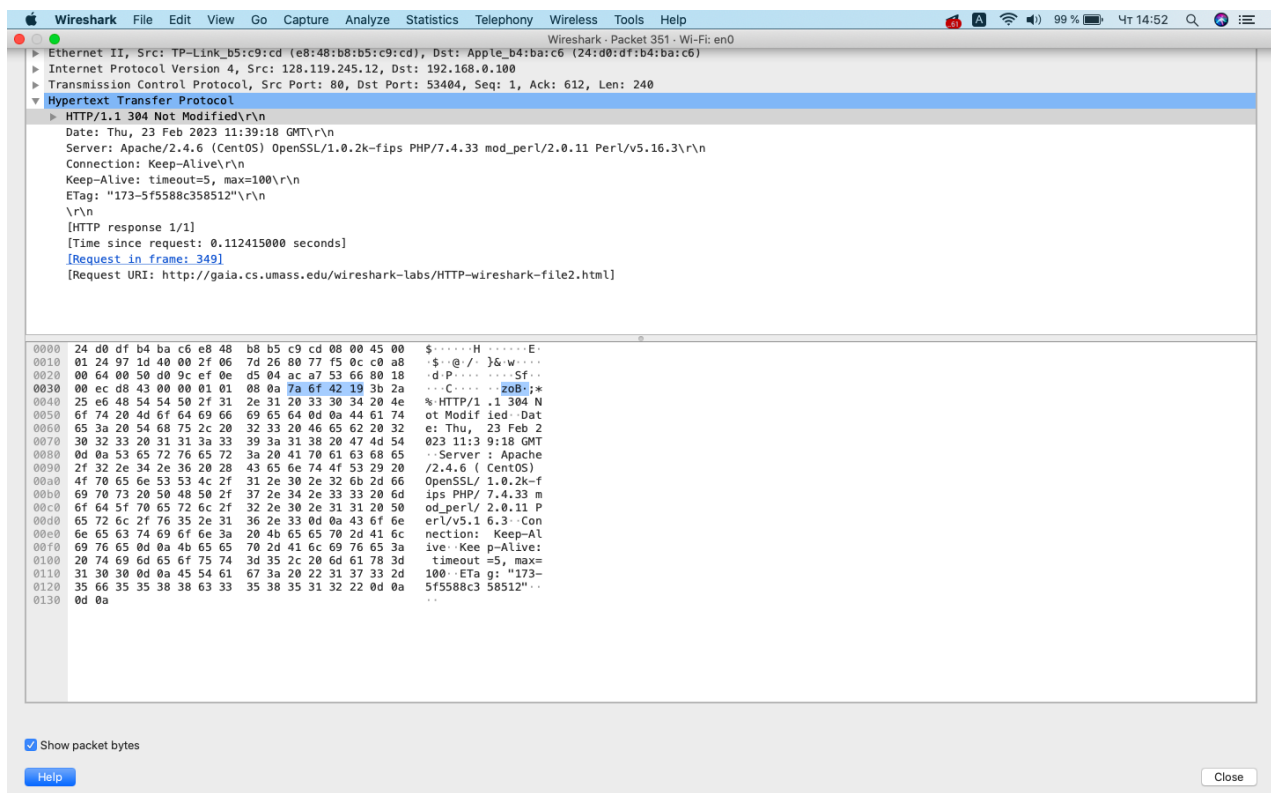
3. Теперь проверьте содержимое второго HTTP-запроса GET (из вашего браузера на сторону сервера). Видите ли вы строку «IF-MODIFIED-SINCE:» в HTTP GET? Если да, то какая информация следует за заголовком «IF-MODIFIED-SINCE:»?

If-Modified-Since: Thu, 23 Feb 2023 06:59:01 GMT ° (тут указано время последней модификации страницы)

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

код: *304 Not Modified*

явно содержимое файла не передаётся, только сообщение о том, что файл не модифицировался со времён первого запроса: *HTTP/1.1 304 Not Modified Date: Thu, 23 Feb 2023 11:39:18 GMT*



Задание №3

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

одно сообщение, номер пакета в трассировке: 277

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

пакет с номером 278

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

[4 Reassembled TCP Segments (4861 bytes): 279(1448), 280(1448), 281(1448), 282(517)] (4 сегмента)

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

я не нашёл в заголовках никакой информации, связанной с сегментацией TCP (наверное, оно и логично, так TCP находится ниже уровнем и HTTP ничего не знает про структуру его заголовков)

Frame 282: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface en0, id 0

Ethernet II, Src: TP-Link_b5:c9:cd (e8:48:b8:b5:c9:cd), Dst: Apple_b4:ba:c6 (24:d0:df:b4:ba:c6)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.100

Transmission Control Protocol, Src Port: 80, Dst Port: 53850, Seq: 4345, Ack: 500, Len: 517

[4 Reassembled TCP Segments (4861 bytes): #279(1448), #280(1448), #281(1448), #282(517)]

[Frame: 279, payload: 0-1447 (1448 bytes)]

[Frame: 280, payload: 1448-2895 (1448 bytes)]

[Frame: 281, payload: 2896-4343 (1448 bytes)]

[Frame: 282, payload: 4344-4860 (517 bytes)]

[Segment count: 4]

[Reassembled TCP length: 4861]

[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a46174653a205468752c203233204665622032_]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

[HTTP/1.1 200 OK\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.1

0000 24 d0 df b4 ba c6 e8 48 b8 b5 c9 cd 08 00 45 00 \$.....H.....E..

0010 02 39 e1 92 40 00 2f 06 31 9c 80 77 f5 0c c0 a8 .9..@./..1..w....

0020 00 64 00 50 d2 5a 1b e0 53 19 05 89 0e 1a 80 18 .d.P.Z..S.....

0030 00 eb d5 21 00 00 01 01 08 0a 7a 8c a3 af 3b 47 ...!.....z...;G

0040 72 ef 69 6d 70 6f 73 65 64 2c 20 6e 6f 72 20 63 r-impose d, nor c

0050 72 75 65 6c 20 61 6e 64 20 75 6e 75 73 75 61 6c ruel and unusual

0060 20 70 75 6e 69 73 68 6d 65 6e 74 73 20 69 6e 66 punishment s inf

0070 6c 69 63 74 65 64 2e 0a 0a 3c 2f 70 3e 3c 70 3e licted..</p><p>

0080 3c 61 20 6e 61 6d 65 3d 22 39 22 3e 3c 73 74 72 <str

0090 6f 6e 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 6e ong><h3> Amendmen

00a0 74 20 49 58 3c 2f 68 33 3e 3c 2f 73 74 72 6f 6e t IX</h3>></stron

00b0 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f 70 3e 3c g>..<p></p><

00c0 70 3e 54 68 65 20 65 6e 75 6d 65 72 61 74 69 6f p>The enumeration

00d0 6e 20 69 6e 20 74 68 65 20 43 6f 6e 73 74 69 74 n in the Constit

00e0 75 74 69 6f 6e 2c 20 6f 66 20 63 65 72 74 61 69 ution, o f certai

00f0 6e 20 72 69 67 68 74 73 2c 20 73 68 61 6c 6c 0a n rights , shall

0100 6e 6f 74 20 62 65 20 63 6f 6e 73 74 72 75 65 64 not be c onstrued

0110 20 74 6f 20 64 65 6e 79 20 6f 72 20 64 69 73 70 to deny or disp

0120 61 72 61 67 65 20 6f 74 68 65 72 73 20 72 65 74 arage ot hers ret

0130 61 69 6e 65 64 20 62 79 20 74 68 65 20 70 65 6f ained by the peo

0140 70 6c 65 2e 0a 0a 3c 2f 70 3e 3c 70 3e 3c 61 20 ple..</ p><p><a

0150 6e 61 6d 65 3d 22 31 30 22 3e 3c 73 74 72 6f 6e names="10 "><stron

0160 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 6e 74 20 g><h3>Am endment

0170 58 3c 2f 68 33 3e 3c 2f 73 74 72 6f 6e 67 3e 3c X</h3></ strong><

0180 2f 61 3e 0a 0a 3c 70 3e 3c 2f 70 3e 0a 3c 70 3e /a>..<p> </p> <p>

Frame (583 bytes) Reassembled TCP (4861 bytes)

No.: 282 - Time: 5.469313 - Source: 128.119.245.12 - Destination: 192.168.0.100 - Protocol: HTTP - Length: 583 - Info: HTTP/1.1 200 OK (text/html)

Show packet bytes

Help Close

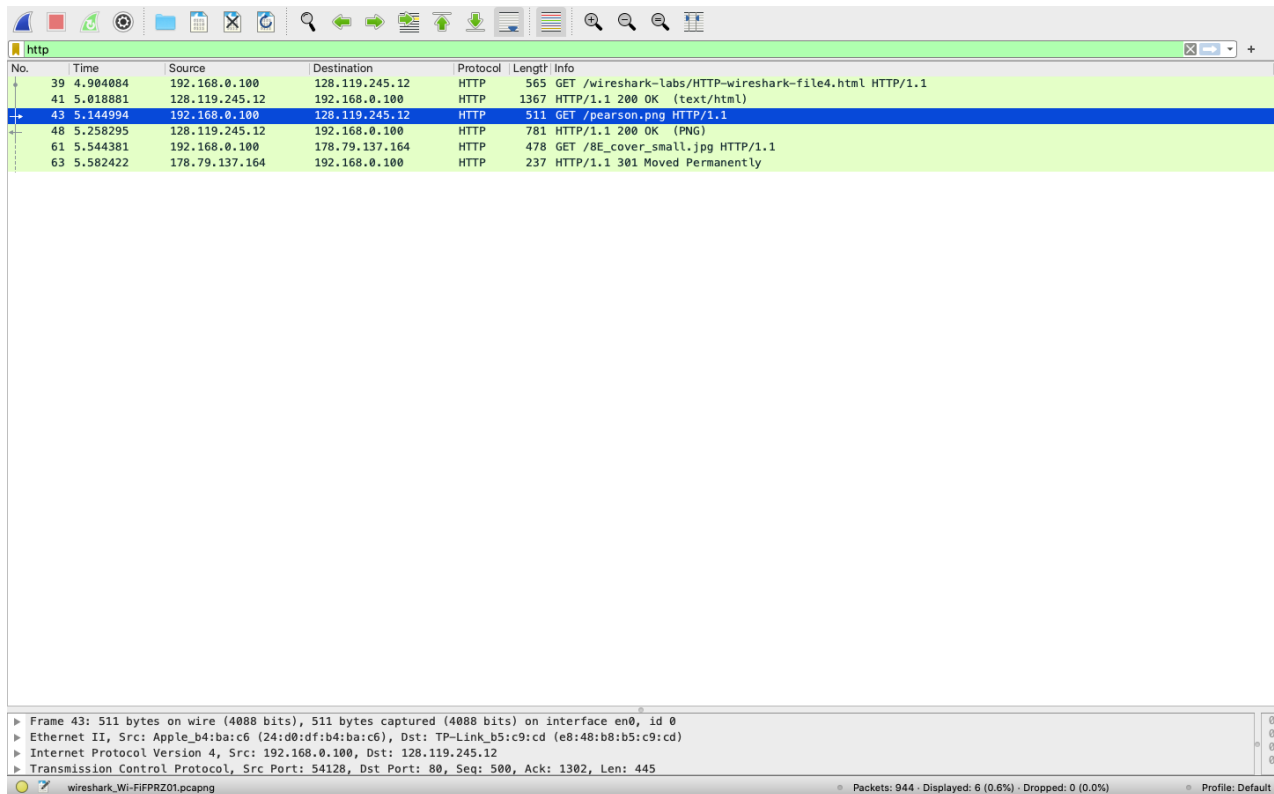
Задание №4

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

3 запроса, на сайт с html-документом, а также на два сайта с изображениями

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

Загрузка была последовательная, потому что прежде чем запросить второе изображение, пришёл ответный запрос с первым изображением (это хорошо видно на приложенном скрине с трассировкой HTTP запросов)



The screenshot shows a Wireshark packet capture of an HTTP session. The packet list pane displays six packets, with the first three highlighted in blue. The details pane for the selected packet (No. 43) shows the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers.

No.	Time	Source	Destination	Protocol	Length	Info
39	4.904084	192.168.0.100	128.119.245.12	HTTP	565	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
41	5.018881	128.119.245.12	192.168.0.100	HTTP	1367	HTTP/1.1 200 OK (text/html)
43	5.144994	192.168.0.100	128.119.245.12	HTTP	511	GET /pearson.png HTTP/1.1
48	5.258295	128.119.245.12	192.168.0.100	HTTP	781	HTTP/1.1 200 OK (PNG)
61	5.544381	192.168.0.100	178.79.137.164	HTTP	478	GET /8E_cover_small.jpg HTTP/1.1
63	5.582422	178.79.137.164	192.168.0.100	HTTP	237	HTTP/1.1 301 Moved Permanently

Frame 43: 511 bytes on wire (4088 bits), 511 bytes captured (4088 bits) on interface en0, id 0
Ethernet II, Src: Apple_b4:ba:c6 (24:d0:df:b4:ba:c6), Dst: TP-Link_b5:c9:cd (e8:48:b8:b5:c9:cd)
Internet Protocol Version 4, Src: 192.168.0.100, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54128, Dst Port: 80, Seq: 500, Ack: 1302, Len: 445

wireshark_Wi-FiFPRZ01.pcapng Packets: 944 - Displayed: 6 (0.6%) - Dropped: 0 (0.0%) Profile: Default

Задание №5

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

401 Unauthorized

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

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

Credentials: wireshark-students:network

(поле Authorization)

The image shows a Wireshark packet capture of an HTTP GET request and its response. The packet list on the left shows packet 191 selected, which is an HTTP response. The packet details pane on the right shows the structure of the response, including the status line (401 Unauthorized), headers (Host, Connection, Cache-Control, Authorization, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, Accept-Language), and the body (Full request URI, HTTP request 1/1, Response in frame: 191).

[Time since previous frame in this TCP stream: 0.000208000 seconds]

► [SEQ/ACK analysis]
TCP payload (660 bytes)

▼ Hypertext Transfer Protocol

► GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

▼ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n

Credentials: wireshark-students:network

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7\r\n

\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: 191]

0000 e8 48 b8 b5 c9 cd 24 d0 df b4 ba c6 08 00 45 02 .H...\$.E-
0010 02 8c 00 00 00 00 40 06 01 da c0 a8 00 64 80 77@.d.w
0020 f5 0c d3 a6 00 50 0d a4 ee 7b da c4 4f da 80 18P. {-Q..
0030 08 0a 49 94 00 00 01 01 08 0a 3b 69 43 ec 7a ae ..I.....;iC.z-
0040 8f 84 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b ..GET /w ireshark
0050 2d 6c 61 62 73 2f 70 72 6f 74 65 63 74 65 64 5f --labs/pr otedect_
0060 70 61 67 65 73 2f 48 54 54 50 2d 77 69 72 65 73 pages/HT TP-wires
0070 68 61 72 60 2d 66 69 6c 65 35 2e 68 74 6d 6c 20 hark-fil e5.html
0080 48 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 Host:
0090 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 gaia.cs. umass.ed
00a0 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b u- Conne ction: k
00b0 65 65 70 2d 61 6c 69 76 65 0d 0a 43 61 63 68 65 eep-aliv e- Cache
00c0 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 -Control : max-ag
00d0 65 3d 30 0d 0a 41 75 74 68 6f 72 69 7a 61 74 69 e-0 Aut horizati
00e0 6f 6e 3a 20 42 61 73 69 63 20 64 32 6c 79 5a 58 on: Basi c d2lyZX
00f0 4e 6f 59 58 4a 72 4c 58 4e 30 64 57 52 6c 62 6e NoYXJrLX N0dWRlbn
0100 52 7a 4f 6d 35 6c 64 48 64 76 63 6d 73 3d 0d 0a RzOm5ldH dvcms=
0110 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade= Insecu
0120 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 -Request si: 1-Us
0130 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent: Mozill
0140 61 2f 35 2e 30 20 28 4d 61 63 69 6e 74 6f 73 68 a/5.0 (M acintosh
0150 3b 20 49 6e 74 65 6c 20 4d 61 63 20 4f 53 20 58 ; Intel Mac OS X
0160 20 31 30 5f 31 35 5f 37 29 20 41 70 70 6c 65 57 10_15_7) AppleW
0170 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 ebKit/53 7.36 (KH
0180 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 TML, lik e Gecko)
0190 20 43 68 72 6f 6d 65 2f 31 30 39 2e 30 2e 30 2e Chrome/ 109.0.0.
01a0 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0 Safari /537.36

No.: 189 · Time: 25.107416 · Source: 192.168.0.100 · Destination: 128.119.245.12 · Protocol: HTTP · Length: 666 · Info: GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1

☒ Show packet bytes

Help Close