

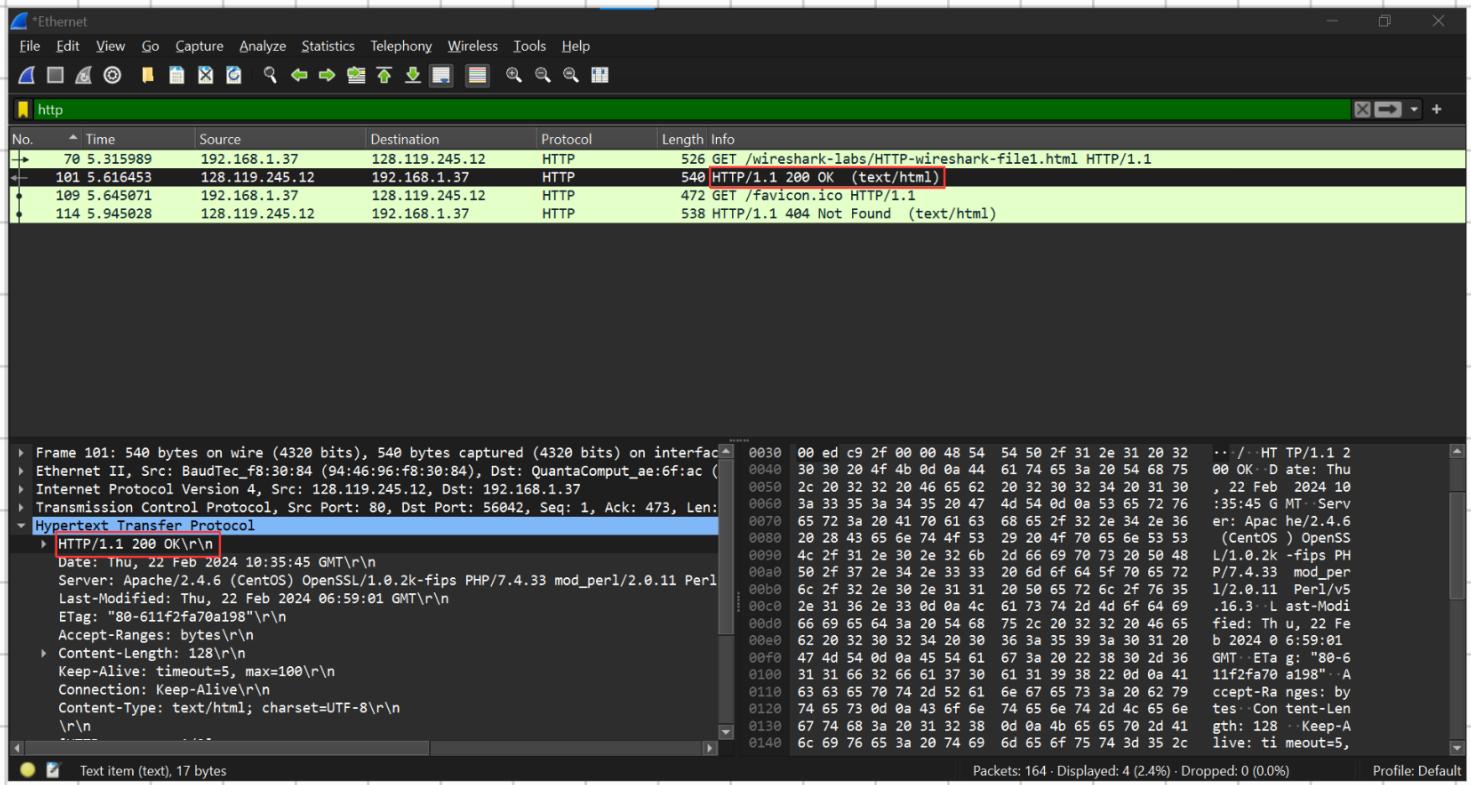
Wireshark Lab 01: HTTP

Section 650001

Group ID : G02

สมาชิกกลุ่ม
นายธีรภัทร เกิดไพบูลย์ 6509650468

1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?



The screenshot shows a Wireshark capture of network traffic on the "Ethernet" interface. The "http" display filter is applied. Several HTTP requests are listed in the packet list, with their details and bytes panes visible. The selected packet is the response to a GET request for "/favicon.ico", which includes the following response body:

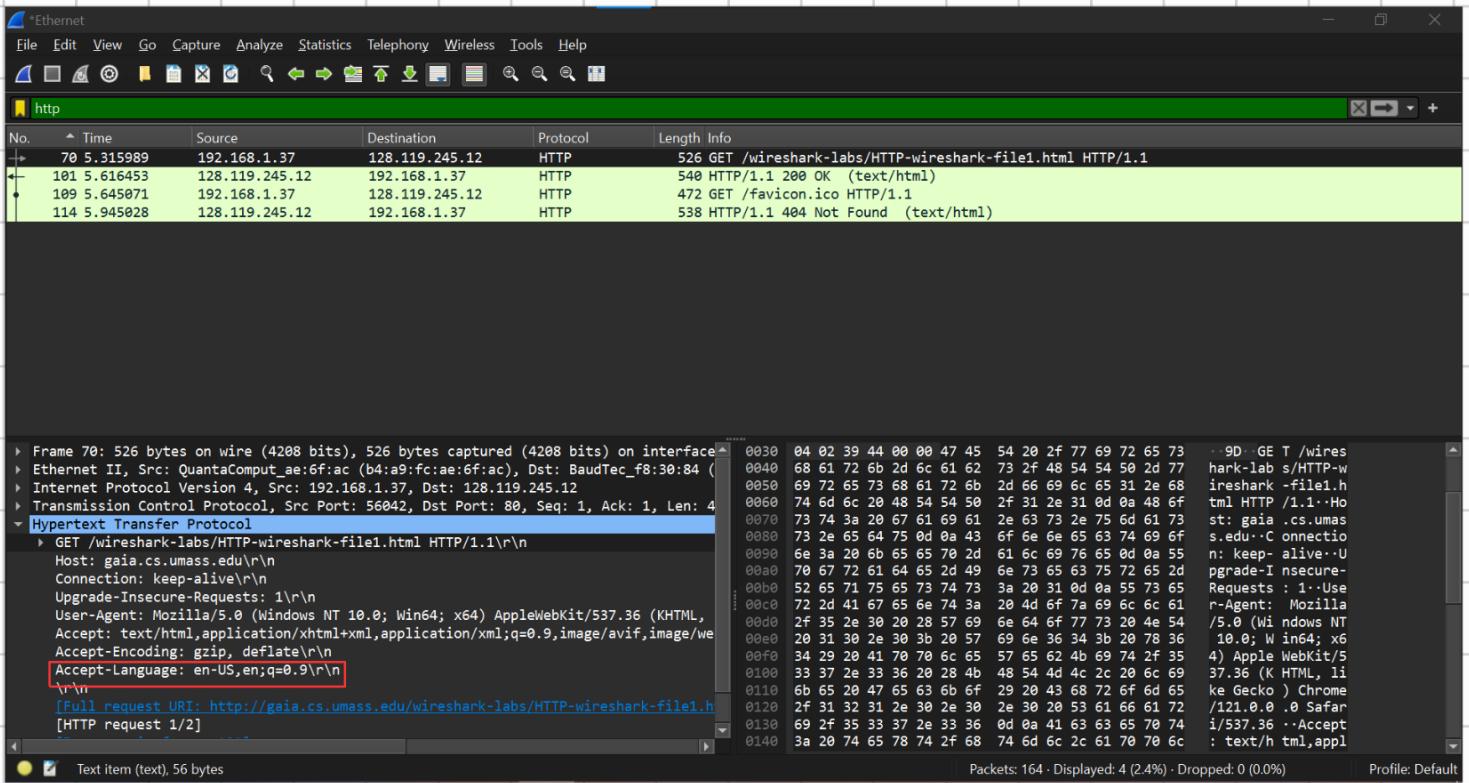
```
> Frame 101: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface ...
> Ethernet II, Src: BaudTec_f8:30:84 (94:46:96:f8:30:84), Dst: QuantaComput_ae:6f:ac (...
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.37
> Transmission Control Protocol, Src Port: 80, Dst Port: 56042, Seq: 1, Ack: 473, Len: ...
> Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Date: Thu, 22 Feb 2024 10:35:45 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl...
Last-Modified: Thu, 22 Feb 2024 06:59:01 GMT\r\n
ETag: "80-61f2fa70a198"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
```

The bytes pane shows the raw hex and ASCII representation of the selected packet.

ເວຼັກສິນຂອງ HTTP ທີ່ຮັບນະເບາເຊື່ອຂອງນັກສຶກຂາ ຄື້ອ 1.1

ເວຼັກສິນຂອງ HTTP ທີ່ຮັບນະເບີຣີຟເວຼົກ ຄື້ອ 1.1

2. What languages (if any) does your browser indicate that it can accept to the server?



The screenshot shows a Wireshark capture window titled "Ethernet". The "http" tab is selected. The packet list pane shows several HTTP requests. The selected packet is frame 70, which is a GET request for "/wireshark-labs/HTTP-wireshark-file1.html". The packet details pane displays the raw HTTP headers, including "Accept-Language: en-US,en;q=0.9\r\n". The bytes pane shows the binary representation of the packet.

```
Frame 70: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface
Ethernet II, Src: QuantaComput_ae:6f:ac (b4:a9:fc:ae:6f:ac), Dst: BaudTec_f8:30:84 (08:00:27:00:00:04)
Internet Protocol Version 4, Src: 192.168.1.37, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56042, Dst Port: 80, Seq: 1, Ack: 1, Len: 4
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.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 Gecko) Chrome/121.0.0.0 Safari/1537.36\r\n
        Accept-Encoding: gzip, deflate\r\n
        Accept-Language: en-US,en;q=0.9\r\n
    \r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.h
[HTTP request 1/2]
```

Packets: 164 · Displayed: 4 (2.4%) · Dropped: 0 (0.0%) · Profile: Default

ເບີຣາວ໌ເຊອຣ໌ຂອງນັກສຶກພາທີ່ໃຊ້ຮະນຸວ່າຈະຍອມຮັບພາຫາອັງກຸນ-ສຫະລູອເມືອງ (English-US)ແລະພາຫາອັງກຸນ (English)ຈາກເຊື້ອົງກຸນ

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

The screenshot shows the Wireshark interface with the following details:

- Selected Packet:** Frame 70, Source: 192.168.1.37, Destination: 128.119.245.12, Protocol: HTTP.
- HTTP Request Headers:**

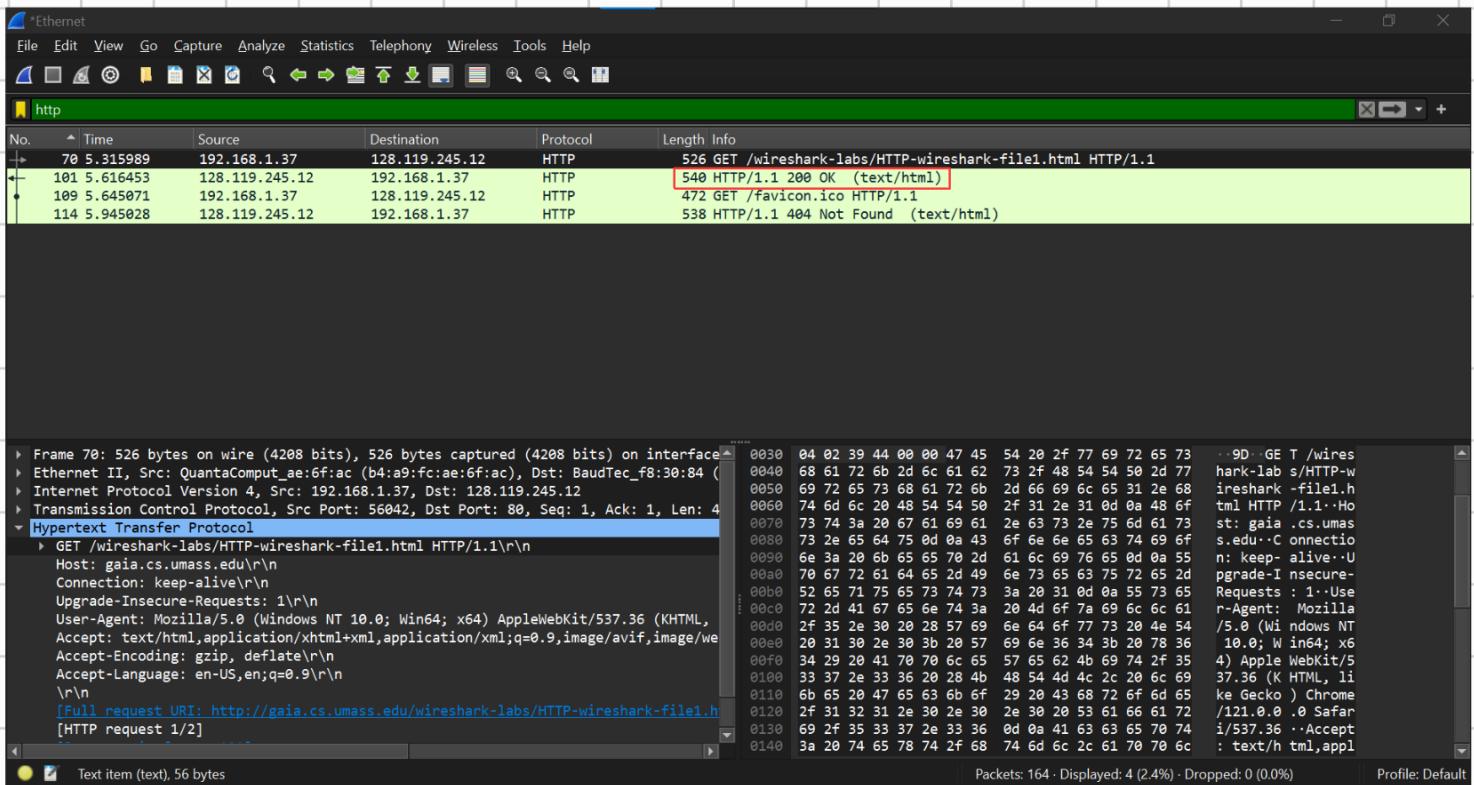
```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n
```
- HTTP Response Headers:**

```
HTTP/1.1 200 OK\r\nContent-Type: text/html\r\nContent-Length: 526\r\nLast-Modified: Mon, 01 Jan 2024 00:00:00 GMT\r\nCache-Control: max-age=0\r\nExpires: -1\r\nServer: Apache/2.4.41 (Ubuntu)\r\nContent-Security-Policy: frame-ancestors 'self'\r\nX-Content-Type-Options: nosniff\r\nX-XSS-Protection: 1; mode=block\r\nDate: Mon, 01 Jan 2024 00:00:00 GMT\r\nContent-Encoding: gzip
```
- Packets:** 164 · Displayed: 4 (2.4%) · Dropped: 0 (0.0%)

IP address คอมพิวเตอร์ของนักศึกษา คือ 192.168.1.37

IP address ของเซิร์ฟเวอร์ คือ 128.119.245.12

4. What is the status code returned from the server to your browser?

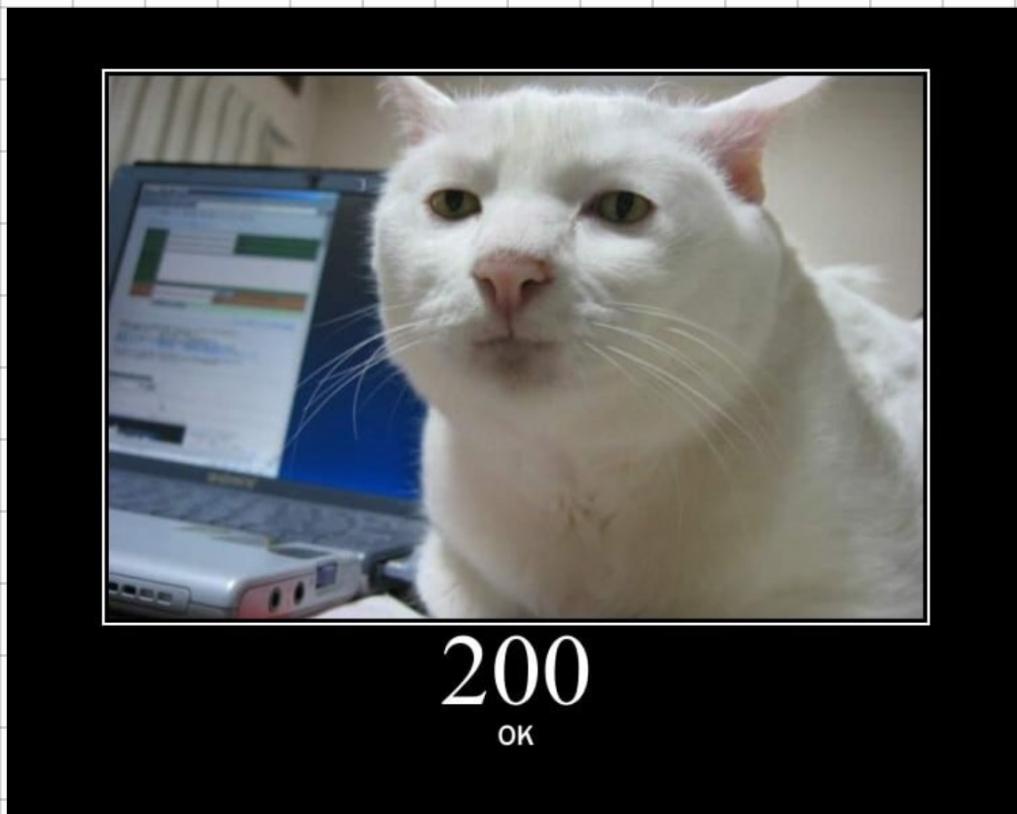


The Wireshark interface shows several network packets. The packet at index 70 is highlighted with a red box, indicating it is the one we are interested in. This packet is a GET request to the URL `/wireshark-labs/HTTP-wireshark-file1.html`. The response to this request, which is the one highlighted, has a status code of 200 OK. Other visible packets include a 540 HTTP/1.1 response and a 404 Not Found response.

Frame 70: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface
Ethernet II, Src: QuantaComput_ae:6f:ac (b4:a9:fc:ae:6f:ac), Dst: BaudTec_f8:30:84 (08:00:27:00:00:00)
Internet Protocol Version 4, Src: 192.168.1.37, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56042, Dst Port: 80, Seq: 1, Ack: 1, Len: 400
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.64 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-File1.h
[HTTP request 1/2]

0030 04 02 39 44 00 00 47 45 54 20 2f 77 69 72 65 73 9D GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 ireshark -file1.h
0060 74 6d 6c 20 48 54 54 58 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1-Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umass
0080 73 2e 65 64 75 0d 0a 43 6f 6e 65 63 74 69 6f s.edu .C onnectio
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep- alive-U
00a0 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-
00b0 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 Requests : 1 -Use
00c0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
00d0 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 /5.0 (Wi ndows NT
00e0 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 10.0; W in64; x6
00f0 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 4) Apple WebKit/5
0100 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 37.36 (K HTML, li
0110 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 ke Gecko) Chrome
0120 2f 31 32 31 2e 30 2e 30 2e 30 20 53 61 66 61 72 /121.0.0.0 Safar
0130 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 i/537.36 ·Accept
0140 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c : text/h tml,appl

HTTP Status Code ที่ส่งคืนมาคือ 200 OK



5. When was the HTML file that you are retrieving last modified at the server?

The screenshot shows the Wireshark interface with the following details:

- Frame 101:** 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface Ethernet II.
- Ethernet II:** Src: BaudTec_f8:30:84 (94:46:96:f8:30:84), Dst: QuantaComput_ae:6f:ac (08:00:27:a8:6f:ac).
- Internet Protocol Version 4:** Src: 128.119.245.12, Dst: 192.168.1.37.
- Transmission Control Protocol:** Src Port: 80, Dst Port: 56042, Seq: 1, Ack: 473, Len: 526.
- Hypertext Transfer Protocol:**
 - HTTP/1.1 200 OK\r\n
 - Date: Thu, 22 Feb 2024 10:35:45 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/5.34 Last-Modified: Thu, 22 Feb 2024 06:59:01 GMT\r\n
 - ETag: "80-611f2fa70a198"\r\n
 - Accept-Ranges: bytes\r\n
 - Content-Length: 128\r\n
 - Keep-Alive: timeout=5, max=100\r\n
 - Connection: Keep-Alive\r\n
 - Content-Type: text/html; charset=UTF-8\r\n

The "Last-Modified" header is highlighted with a red box. The packet details pane shows the raw hex and ASCII data for the response, including the modified timestamp.

วันพุธที่ 22 กุมภาพันธ์ ค.ศ. 2024 เวลา 06:59:01
(Thu, 22 Feb 2024 06:59:01 GMT)

6. How many bytes of content are being returned to your browser?

The screenshot shows a Wireshark capture window titled "Ethernet". The "http" tab is selected. The packet list pane shows four HTTP requests:

No.	Time	Source	Destination	Protocol	Length	Info
70	5.315989	192.168.1.37	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
101	5.616453	128.119.245.12	192.168.1.37	HTTP	540	HTTP/1.1 200 OK (text/html)
109	5.645071	192.168.1.37	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
114	5.945028	128.119.245.12	192.168.1.37	HTTP	538	HTTP/1.1 404 Not Found (text/html)

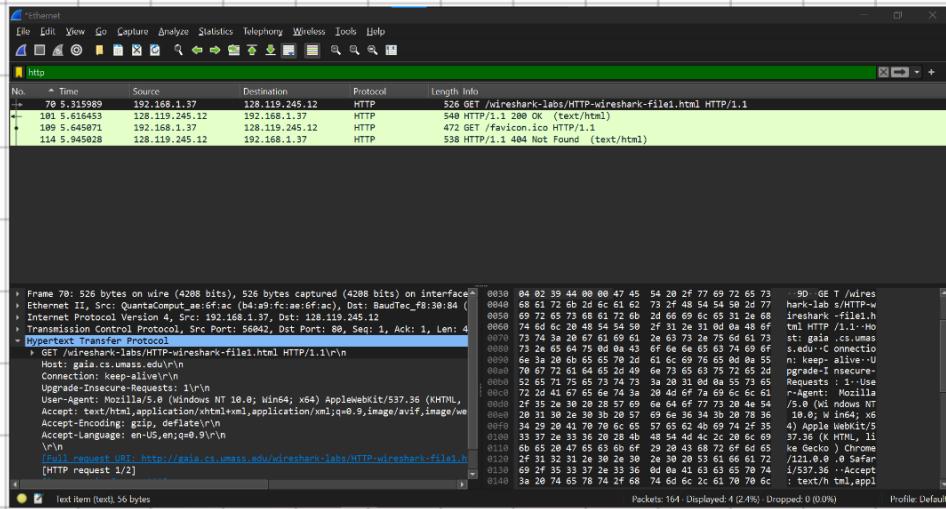
The details pane shows the selected packet (HTTP 200 OK) with its raw content:

```
HTTP/1.1 200 OK\r\nDate: Thu, 22 Feb 2024 10:35:45 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/5.30 Last-Modified: Thu, 22 Feb 2024 06:59:01 GMT\r\nETag: "80-61f2fa70a198"\r\nAccept-Ranges: bytes\r\nContent-Length: 128\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n
```

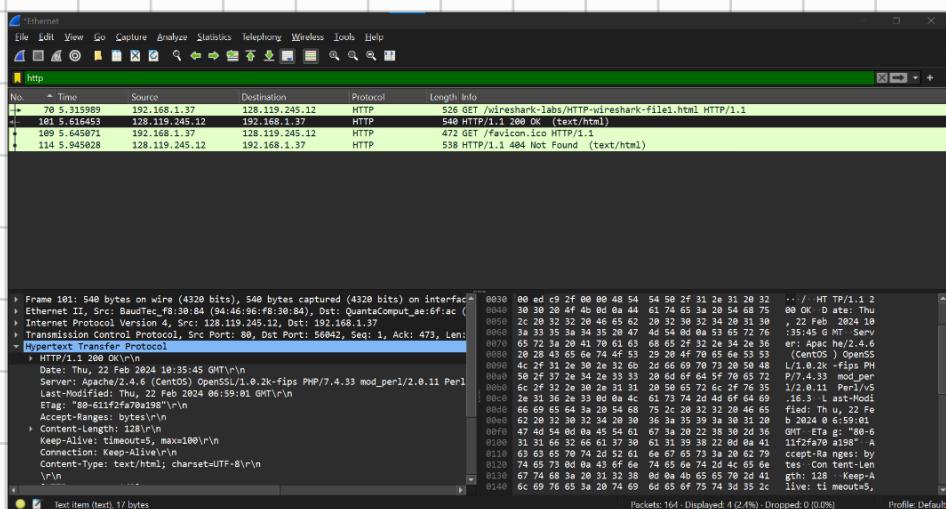
The bytes pane shows the binary representation of the content length field.

128 bytes

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.



HTTP Request
message



HTTP Response
message

จากการเปรียบเทียบ packet content กับ packet list ของทั้งสอง packet (HTTP Request message และ HTTP Response message) ปรากฏว่าไม่พบความแตกต่างใด ๆ

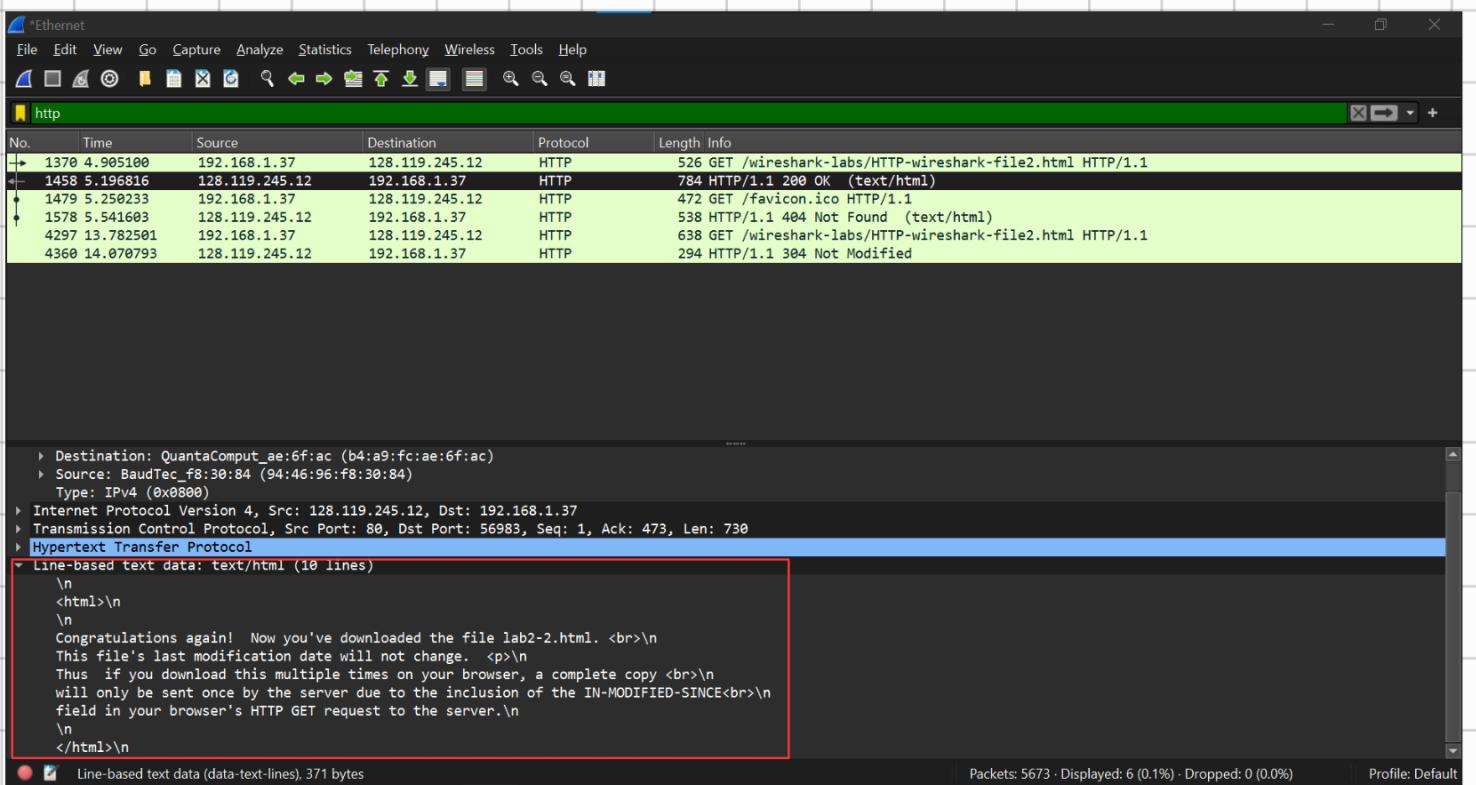
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

The Wireshark interface is shown with the following details:

- Network Interface:** *Ethernet
- File Menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help
- Toolbar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help
- Selected Column:** http
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info
- Table Data:** Several rows of network traffic are listed, with the first row highlighted in yellow. The first row shows a GET request from 192.168.1.37 to 128.119.245.12. The "Info" column for this row shows "526 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1".
- Packet Details:** The selected packet (row 1370) is expanded. It shows the following details:
 - Ethernet II, Src: QuantaComput_ae:6f:ac (b4:a9:fc:ae:6f:ac), Dst: BaudTec_f8:30:84 (94:46:96:f8:30:84)
 - Internet Protocol Version 4, Src: 192.168.1.37, Dst: 128.119.245.12
 - Transmission Control Protocol, Src Port: 56983, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
 - Hypertext Transfer Protocol
 - GET /wireshark-labs/HTTP-wireshark-file2.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 Gecko) Chrome/121.0.0.0 Safari/537.36\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: en-US,en;q=0.9\r\n
 - [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
 - [HTTP request 1/2]
 - [Response in frame: 1458]
 - [Next request in frame: 1479]
- Bottom Status Bar:** Packets: 5673 - Displayed: 6 (0.1%) - Dropped: 0 (0.0%) - Profile: Default

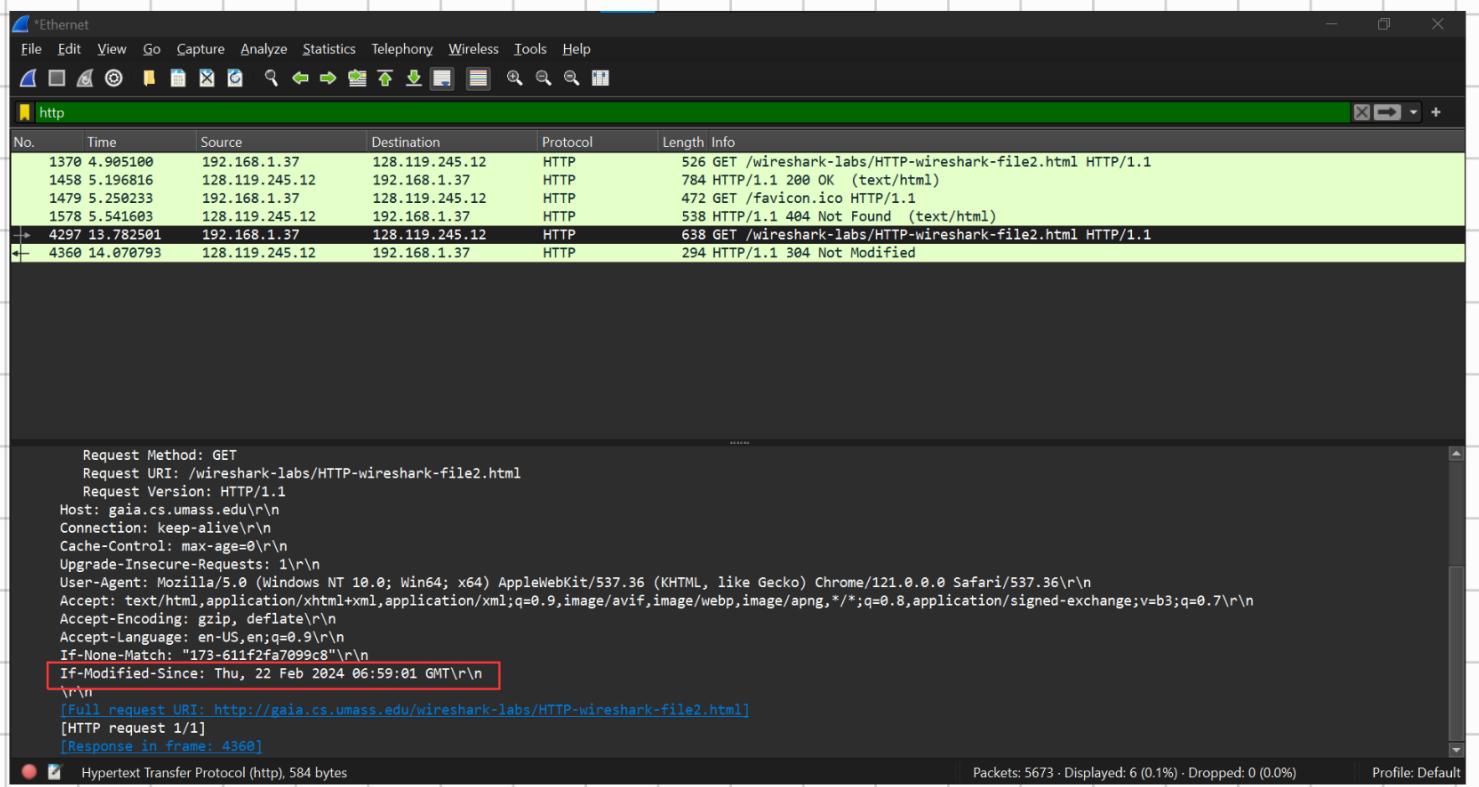
ไม่มีบรรทัด IF-MODIFIED-SINCE ใน HTTP GET ครั้งที่หนึ่ง

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?



เชิร์ฟเวอร์ส่งคืนเนื้อหาของไฟล์อย่างชัดเจน ใน Wireshark มีส่วนที่เรียกว่า “Line-Based Text Data” ซึ่งจะแสดงสิ่งที่เชิร์ฟเวอร์ส่งกลับไปยังเบราว์เซอร์ของนักศึกษา ซึ่งเป็นสิ่งที่เก็บไว้แสดงให้นักศึกษาเห็นเมื่อเปิดดูในเบราว์เซอร์ของนักศึกษา

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET6 ? If so, what information follows the "IF-MODIFIED-SINCE:" header?



ใน HTTP GET Request ครั้งที่สองจะมีบรรทัด IF-MODIFIED-SINCE รวมอยู่ด้วย ข้อมูลที่แสดงคือวันที่และเวลาที่นักศึกษาเข้าดูหน้าเว็บครั้งล่าสุด

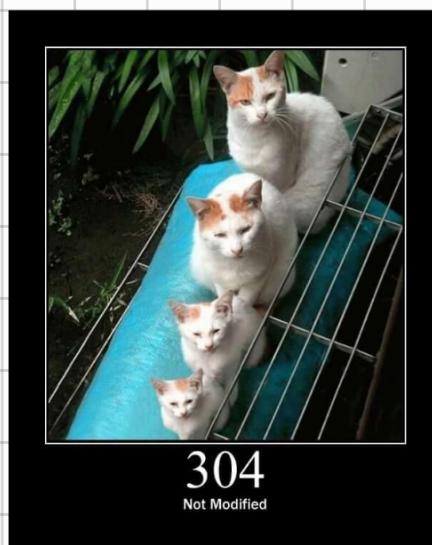
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

The Wireshark interface is shown with the "http" protocol selected in the top navigation bar. The main pane displays several HTTP requests and responses. A specific response is expanded, showing the following details:

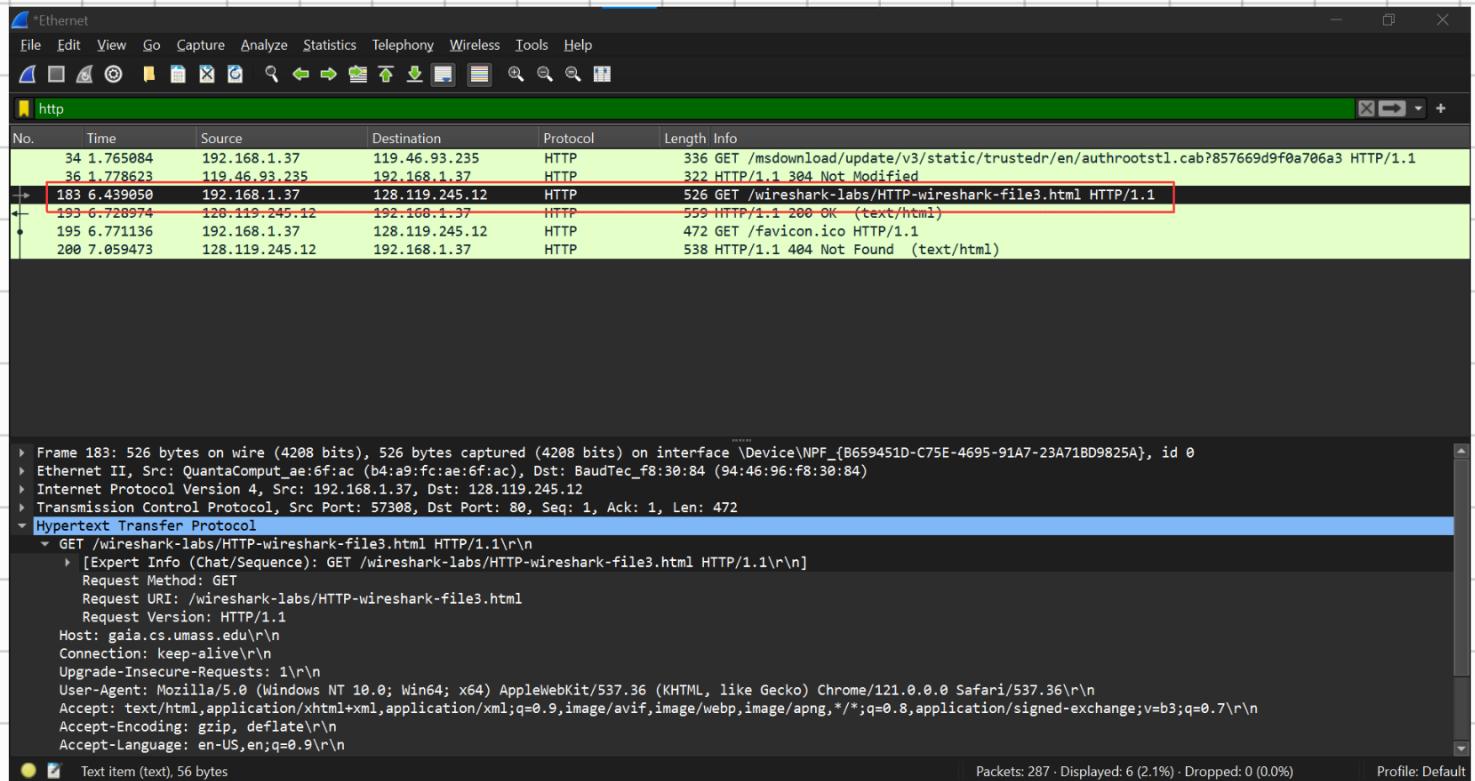
- Status Code:** 304
- [Status Code Description: Not Modified]**
- Response Phrase:** Not Modified

The expanded view also shows the full HTTP response message, including headers like Date, Server, and Content-Type, and the body which is empty for a 304 response.

HTTP Status Code และ phrase คือ “304 Not Modified”
เซิร์ฟเวอร์ไม่ได้ส่งคืนเนื้อหาของไฟล์ เบราร์เซอร์เพียงแค่ดึง
เนื้อหาจากแคช และสั่งเกต ได้ว่า ใน Wireshark ไม่ปรากฏ
บรรทัด "Line-based text data" ของ HTTP Status Code 304

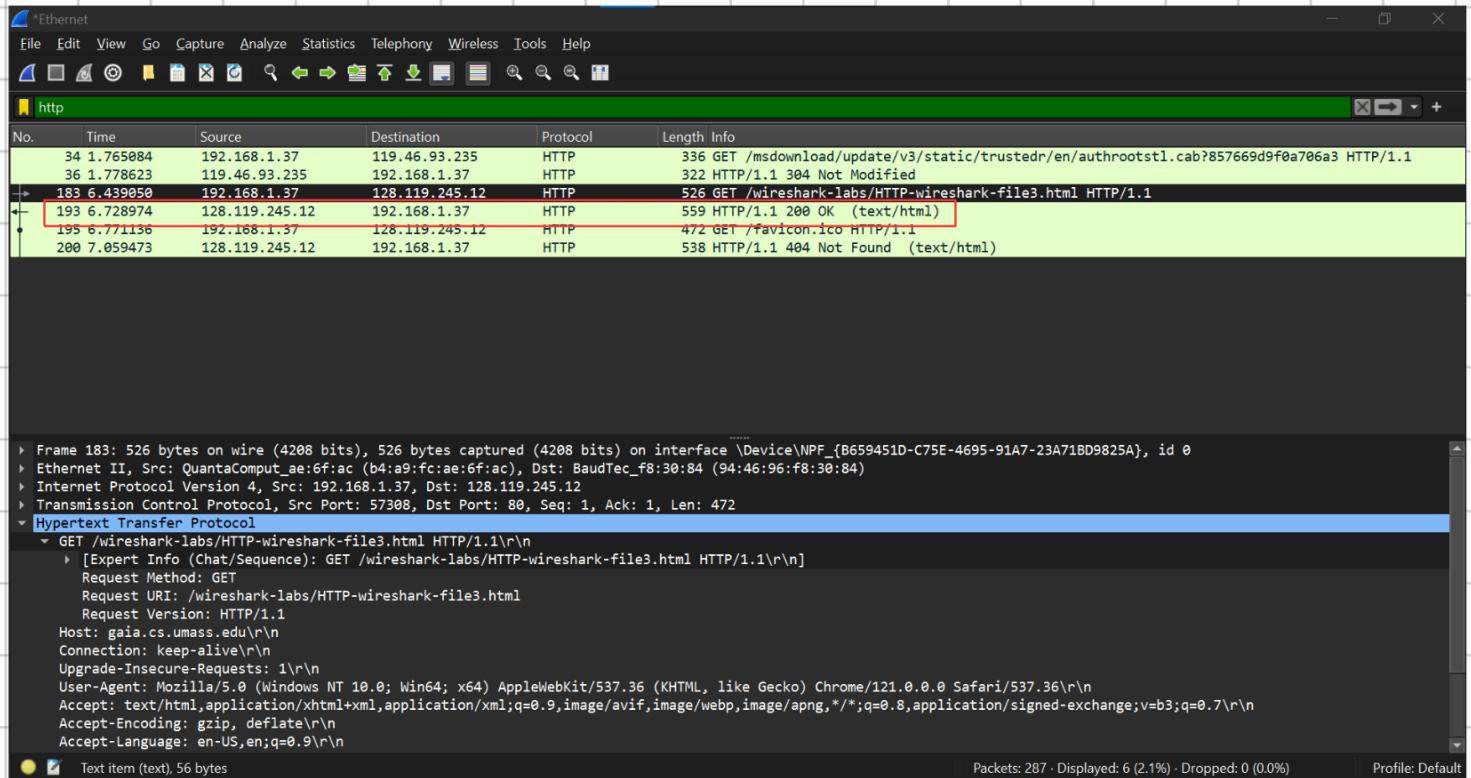


12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?



ເບຣວ່ເຊວ້ງຂອງນັກສຶກຫາສ່າງ HTTP GET Request ເພີ້ມ 1
ຮາຍການໄປຢັ້ງເຊື່ອງ
ແພັກເກີດທີ່ມີຂໍ້ຄວາມ GET ຄື່ອ ແພັກເກີດໝາຍເລີ່ມ 183

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?



ແພັກເກີດໜາຍເລີ່ມ 193

14. What is the status code and phrase in the response?

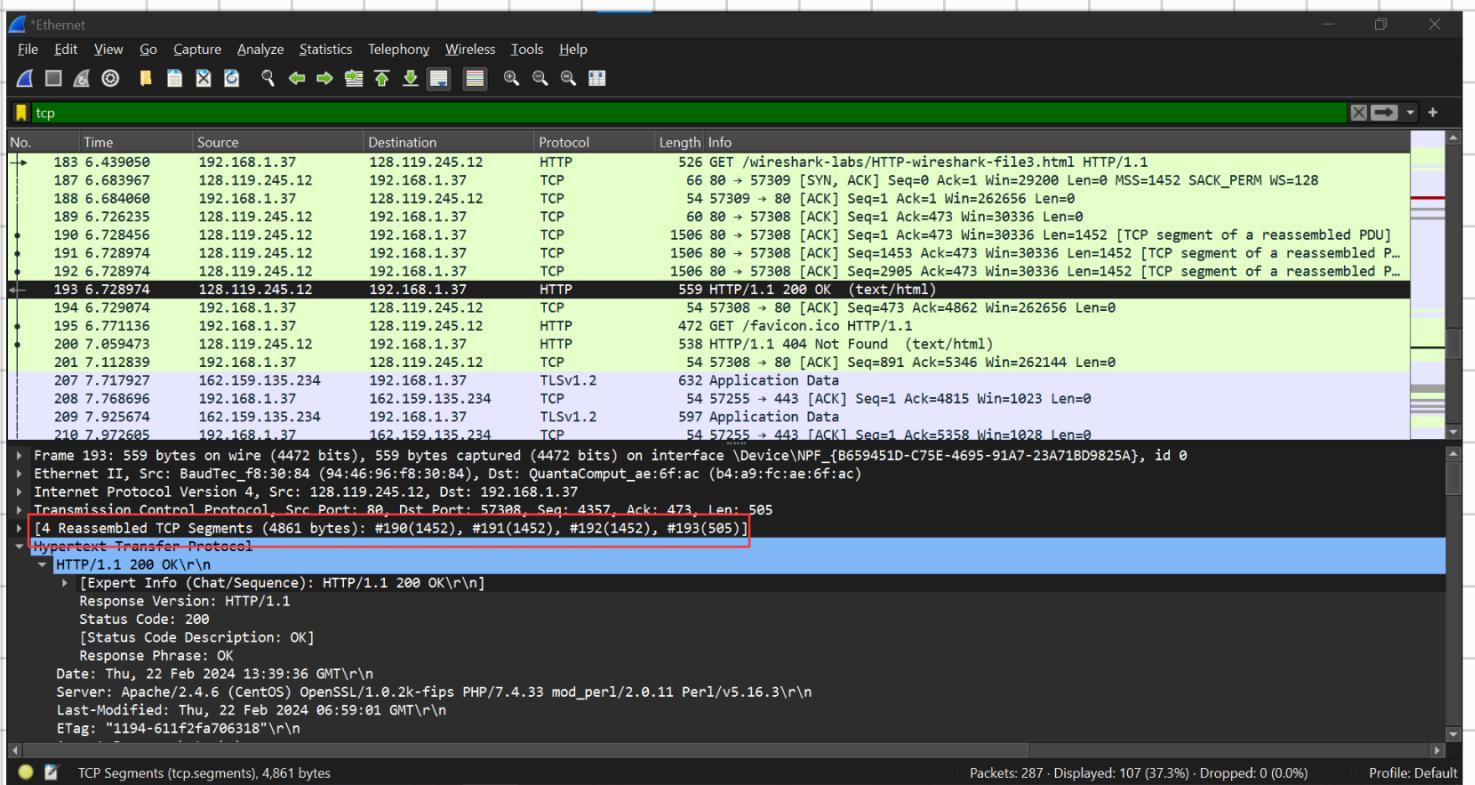
The Wireshark interface is shown with the following details:

- Network Interface:** Ethernet
- Selected Protocol:** http
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info
- Table Data:** Several rows of network traffic are listed, with row 193 highlighted in yellow. The Info column for row 193 shows: Frame 193: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{B659451D-C75E-4695-91A7-23A71BD9825A}, id 0 Ethernet II, Src: BaudTec_f8:30:84 (94:46:96:f8:30:84), Dst: QuantaComput_ae:6f:ac (b4:a9:fc:ae:6f:ac) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.37 Transmission Control Protocol, Src Port: 80, Dst Port: 57308, Seq: 4357, Ack: 473, Len: 505 [4 Reassembled TCP Segments (4861 bytes): #190(1452), #191(1452), #192(1452), #193(505)] Hypertext Transfer Protocol HTTP/1.1 200 OK\r\n[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\nn Response Version: HTTP/1.1 Status Code: 200 [Status Code Description: OK] Response Phrase: OK Date: Thu, 22 Feb 2024 13:39:36 GMT\r\nn Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\nn Last-Modified: Thu, 22 Feb 2024 06:59:01 GMT\r\nn ETag: "1194-611f2fa706318"\r\nn Accept-Ranges: bytes\r\nn]
- Bottom Status Bar:** Packets: 287 - Displayed: 6 (2.1%) - Dropped: 0 (0.0%) - Profile: Default

Status Code และ Phrase คือ 200 OK

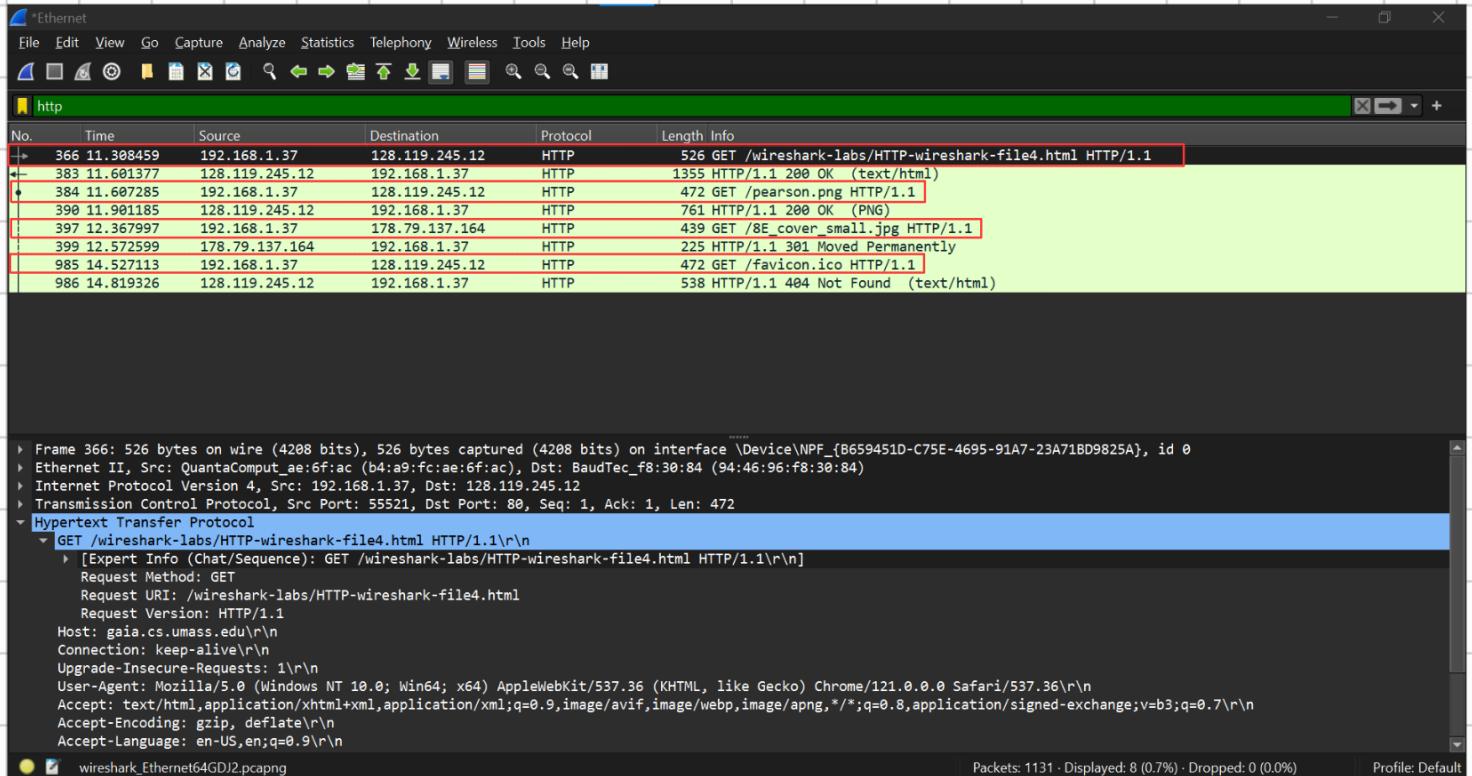


15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?



4 Data-containing TCP segments (ໄດ້ແກ່ແພັກເກີ້ຕໍ່ມາຍເລີ່ມ
190, 191, 192, 193)

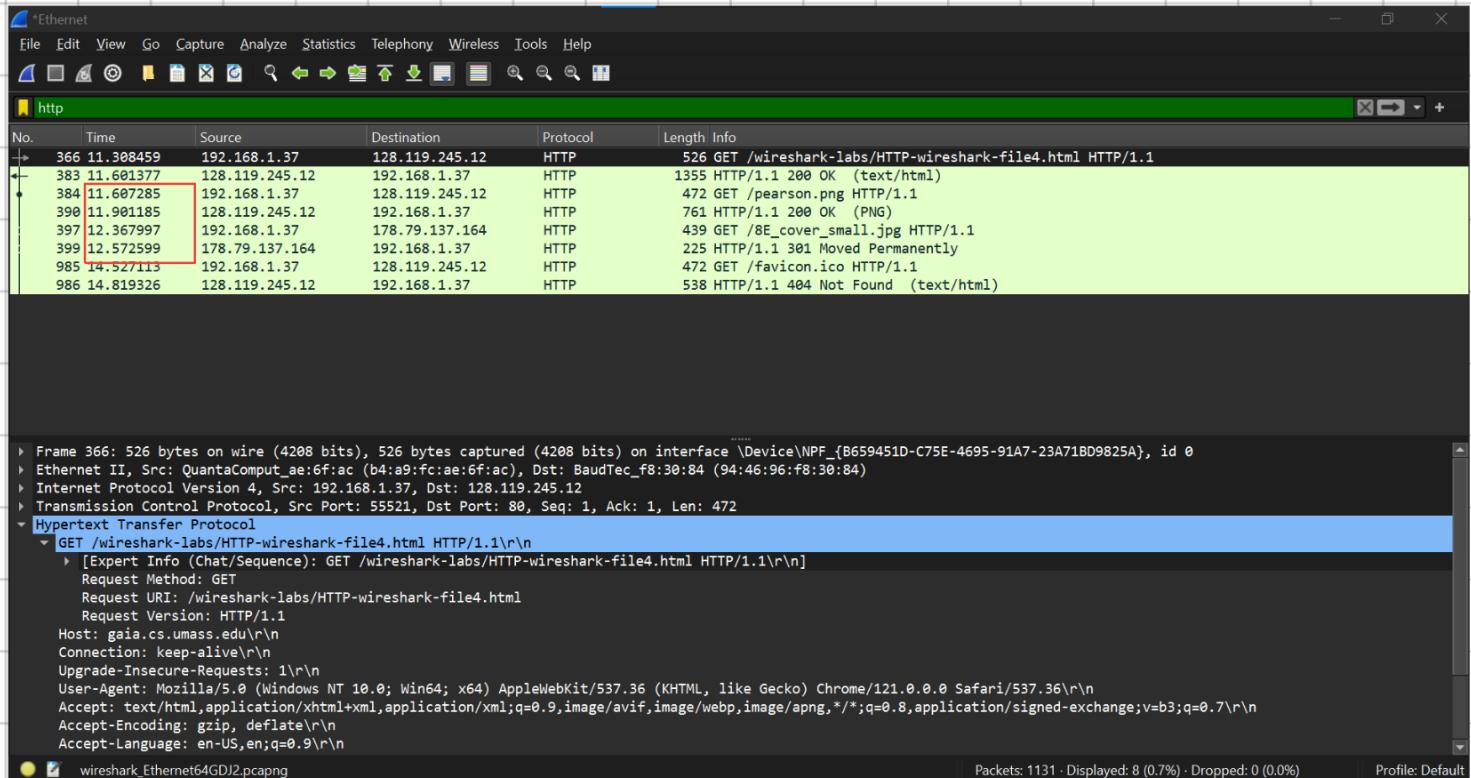
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?



4 แพ็คเก็ต โดยแต่ละแพ็คเก็ตส่ง GET Request ไปตาม Internet addresses ดังต่อไปนี้

- แพ็คเก็ตหมายเลข 366 ส่งไปที่ 128.119.245.12 (HTTP-wireshark-file4.html) (Base file)
- แพ็คเก็ตหมายเลข 384 ส่งไปที่ 128.119.245.12 (pearson.png) (Pearson Logo)
- แพ็คเก็ตหมายเลข 397 ส่งไปที่ 178.79.137.164 (8E_cover_small.jpg) (the 8th edition book cover)
- แพ็คเก็ตหมายเลข 985 ส่งไปที่ 128.119.245.12 (favicon.ico)

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.



Frame 366: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{B659451D-C75E-4695-91A7-23A71BD9825A}, id 0
Ethernet II, Src: QuantaComput_ae:6f:ac (b4:a9:fc:ae:6f:ac), Dst: BaudTec_f8:30:84 (94:46:96:f8:30:84)
Internet Protocol Version 4, Src: 192.168.1.37, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55521, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
Hypertext Transfer Protocol
 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n Request Method: GET
 Request URI: /wireshark-labs/HTTP-wireshark-file4.html
 Request Version: HTTP/1.1
 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 Gecko) Chrome/121.0.0.0 Safari/537.36\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n Accept-Encoding: gzip, deflate\r\n Accept-Language: en-US,en;q=0.9\r\n

จากคอลัมน์เวลาแสดงให้เห็นว่ามีการดาวน์โหลดรูปภาพ pearson.png หลังจากส่ง GET Request ครั้งที่ 2 และรูปภาพ 8E_cover_small.jpg ถูกดาวน์โหลดหลังจากส่ง GET Request ครั้งที่ 3 ดังนั้นจึงสรุปได้ว่าตามเป็นการดาวน์โหลดตามลำดับ (serially)



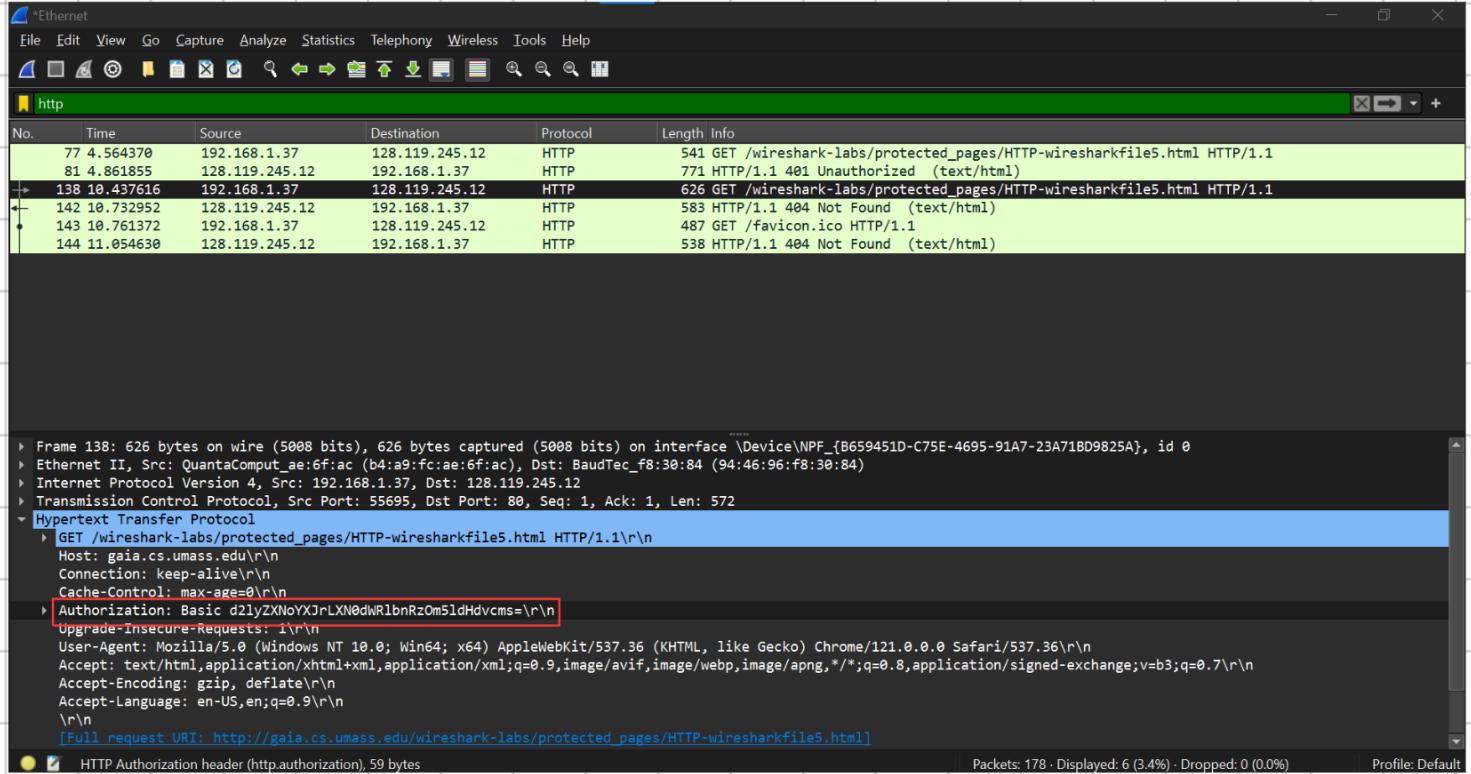
18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

The Wireshark interface is shown with the 'http' protocol selected in the top bar. The main pane displays a list of network packets, with the 401 Unauthorized response highlighted in blue. The details pane shows the captured bytes and ASCII representation of the packet. The selected packet is expanded to show its structure, with the status code '401' and its description 'Unauthorized' highlighted in red. The bottom status bar indicates 'Packets: 178 · Displayed: 6 (3.4%) · Dropped: 0 (0.0%)' and 'Profile: Default'.

Status Code และ Phrase คือ “401 Unauthorized”



19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?



The Wireshark interface is shown with the "http" protocol selected in the top bar. The main pane displays a list of network packets. The selected packet (highlighted in blue) is a GET request to "GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1". The packet details pane shows the following fields:

```
> Frame 138: 626 bytes on wire (5008 bits), 626 bytes captured (5008 bits) on interface \Device\NPF_{B659451D-C75E-4695-91A7-23A71BD9825A}, id 0
> Ethernet II, Src: QuantaComput_ae:6f:ac (b4:a9:fc:ae:6f:ac), Dst: BaudTec_f8:30:84 (94:46:96:f8:30:84)
> Internet Protocol Version 4, Src: 192.168.1.37, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55695, Dst Port: 80, Seq: 1, Ack: 1, Len: 572
> Hypertext Transfer Protocol
  | GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.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
  | Upgrade-Insecure-Requests: 1\r\n
  | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 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=0.7\r\n
  | Accept-Encoding: gzip, deflate\r\n
  | Accept-Language: en-US,en;q=0.9\r\n
  | \r\n
  | [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html]
```

The "Authorization" header is highlighted with a red box. The status bar at the bottom right indicates "Packets: 178 · Displayed: 6 (3.4%) · Dropped: 0 (0.0%) · Profile: Default".

HTTP GET ครั้งที่สองเพิ่มส่วน Authorization: Basic