

# Homework 4 : HTTP Lab

## การบ้าน นี้นำมานาจาก **HTTP Lab** ของ Kurose

- มีทั้งหมด ๕ ข้อใหญ่
  - **B** หน้า ๓-๑๒
  - **C** หน้า ๓๓-๑๗
  - **D** หน้า ๑๘-๙๓
  - **E** หน้า ๒๔-๒๙
- นักศึกษาสามารถทำการบ้านนี้เป็นคู่ได้ (**Sec** เดียวกันเท่านั้น) แต่ต้องส่งการบ้านทั้งคู่
  - โดยข้อ **B** ให้ต่างคนต่างทำ (เนื่องจากต่อเนื่องมาจากแบบฝึกหัดในห้อง)
  - แต่ ข้อ **C, D** และ **E** สามารถช่วยกันทำได้
- วันส่งการบ้าน **11.59 pm** ก่อนวันเรียน สัปดาห์ที่ ๕ (อาทิตย์หน้า)

Section ..... รหัสนักศึกษา **65050368** ชื่อ สกุล . **ธนาสกุล เกิดปั้น**

ทำเดียว หรือ คู่ ..... **เดียว**

LAN หรือ WiFi ..... **LAN**

สถานที่ที่ทำการบ้าน **Lab/หอ/บ้าน/ อื่นๆ ระบุ** ..... **Lab 224 ชั้น B / C-E ชั้น**

กรณี WiFi ใช้ HOTSpot จากมือถือหรือไม่ **บลู** ..... iOS หรือ Android .....

ISP (ใช้ IP location check) ที่ใช้ **True Internet Co. Ltd. (น้ำ)**

**192.169.1.56 (น้ำ)**

หมายเลข IP ของเครื่องที่นักศึกษาใช้ (CIDR Format) **10.45.7.37 (Lab)**

MAC Address ของเครื่องที่นักศึกษาใช้ **C8-4B-D6-60-14-19 (Lab)**

**C8-60-00-5E-C9-24 (น้ำ)**

# Homework 4 : กรณีทำคู่

ข้อมูลคู่ของนักศึกษา	
รหัสนักศึกษา .....	ชื่อ สกุล . .....
LAN หรือ WiFi .....	
สถานที่ที่ทำการบ้าน Lab/หอ/บ้าน/ อื่นๆ ระบุ .....	.....
กรณี WiFi ใช้ HOTSpot จากมือถือหรือไม่.....	iOS หรือ Android .....
ISP (ใช้ IP location check) ที่ใช้ .....	
หมายเลข IP ของเครื่องที่นักศึกษาใช้ (CIDR Format)	.....
MAC Address ของเครื่องนักศึกษาที่ใช้ .....	....

## การแบ่งงาน

(ให้เลือก ว สำหรับผู้ทำในข้อนั้นๆ )

ข้อ	นักศึกษา	คู่ของนศ	ช่วยกันทำ	หมายเหตุ
B				
C				
D				
E				

## B. The HTTP CONDITIONAL GET/response interaction

### Instruction

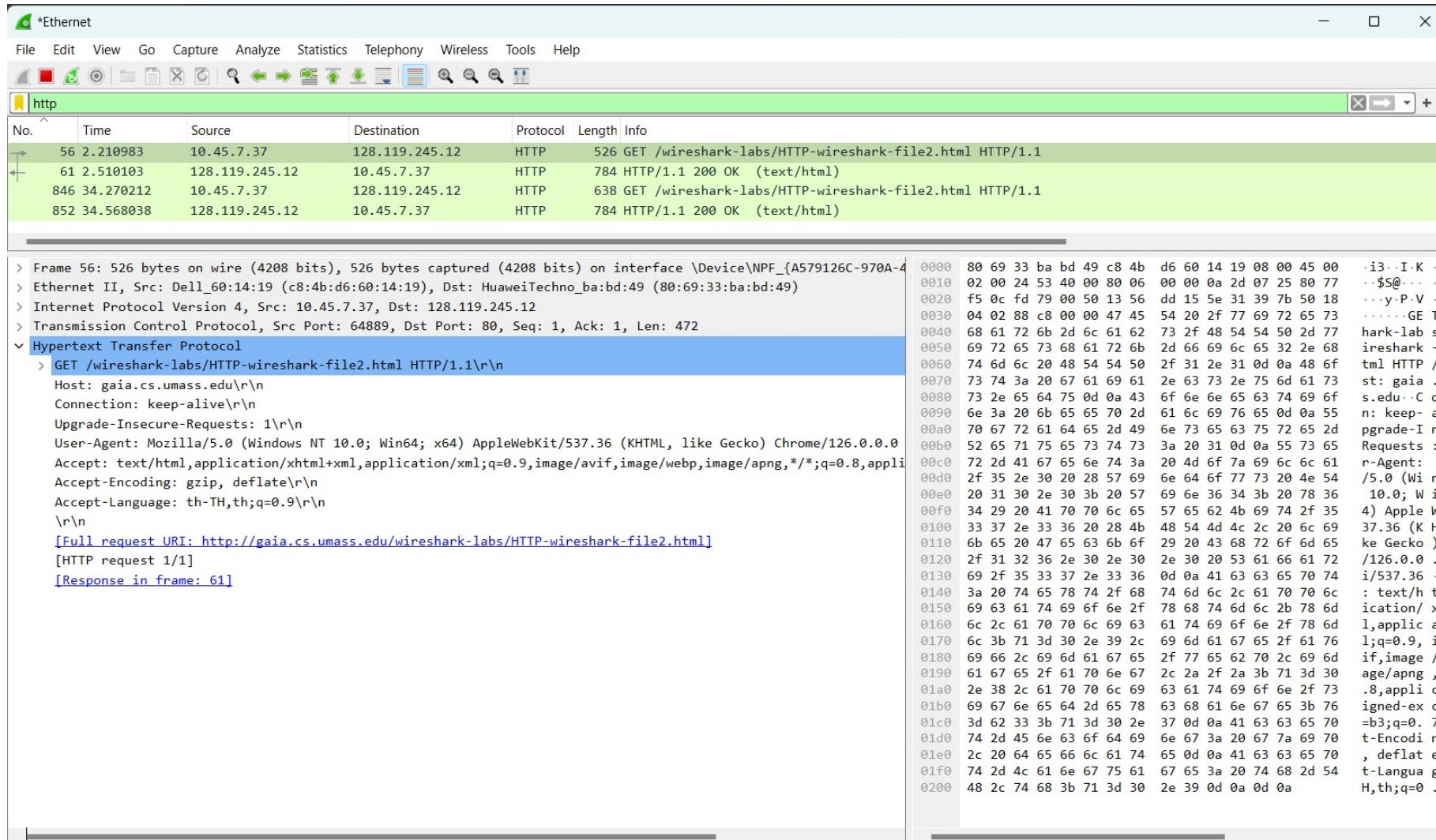
1. Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
2. Start up the Wireshark packet sniffer
3. Enter the following URL into your browser

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

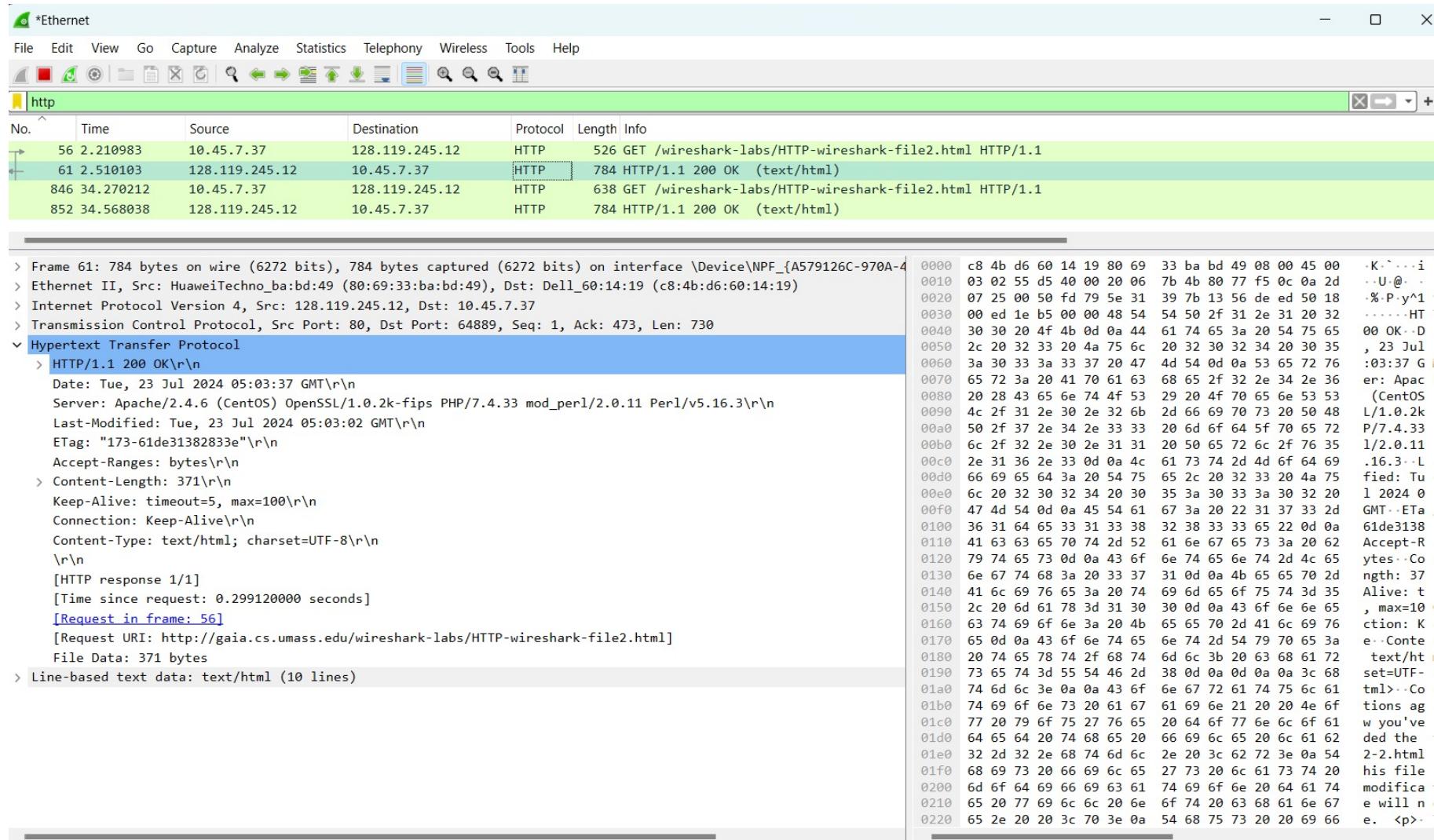
Your browser should **display** a very simple **five-line HTML file**.

4. Quickly enter the same URL into your browser again (or simply select the refresh button on your browser)
5. Stop Wireshark packet capture, and enter “http” (again, in lower case without the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

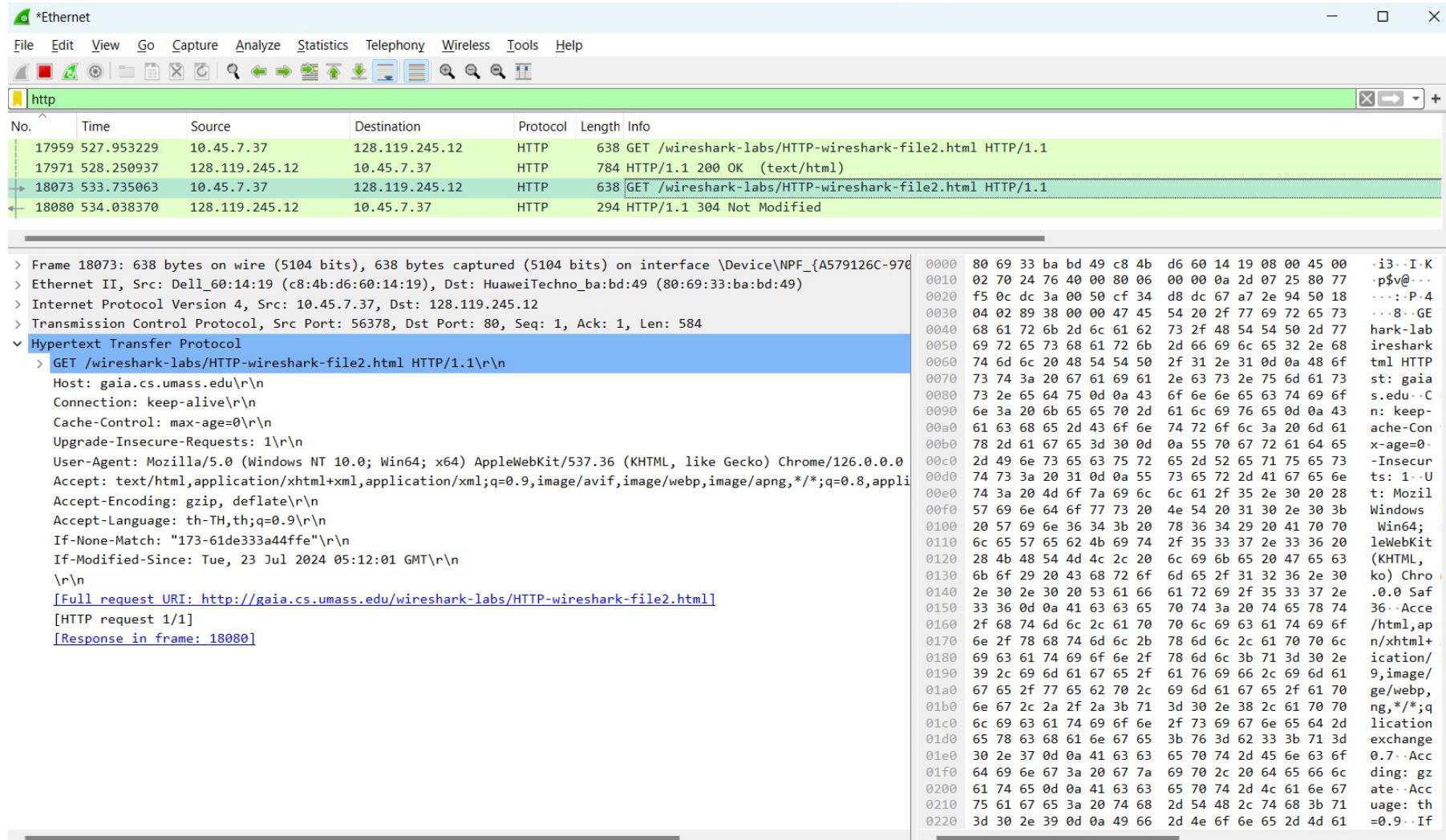
# B1. Capture នៃការ Wireshark : HTTP Get Packet នៅក្នុង



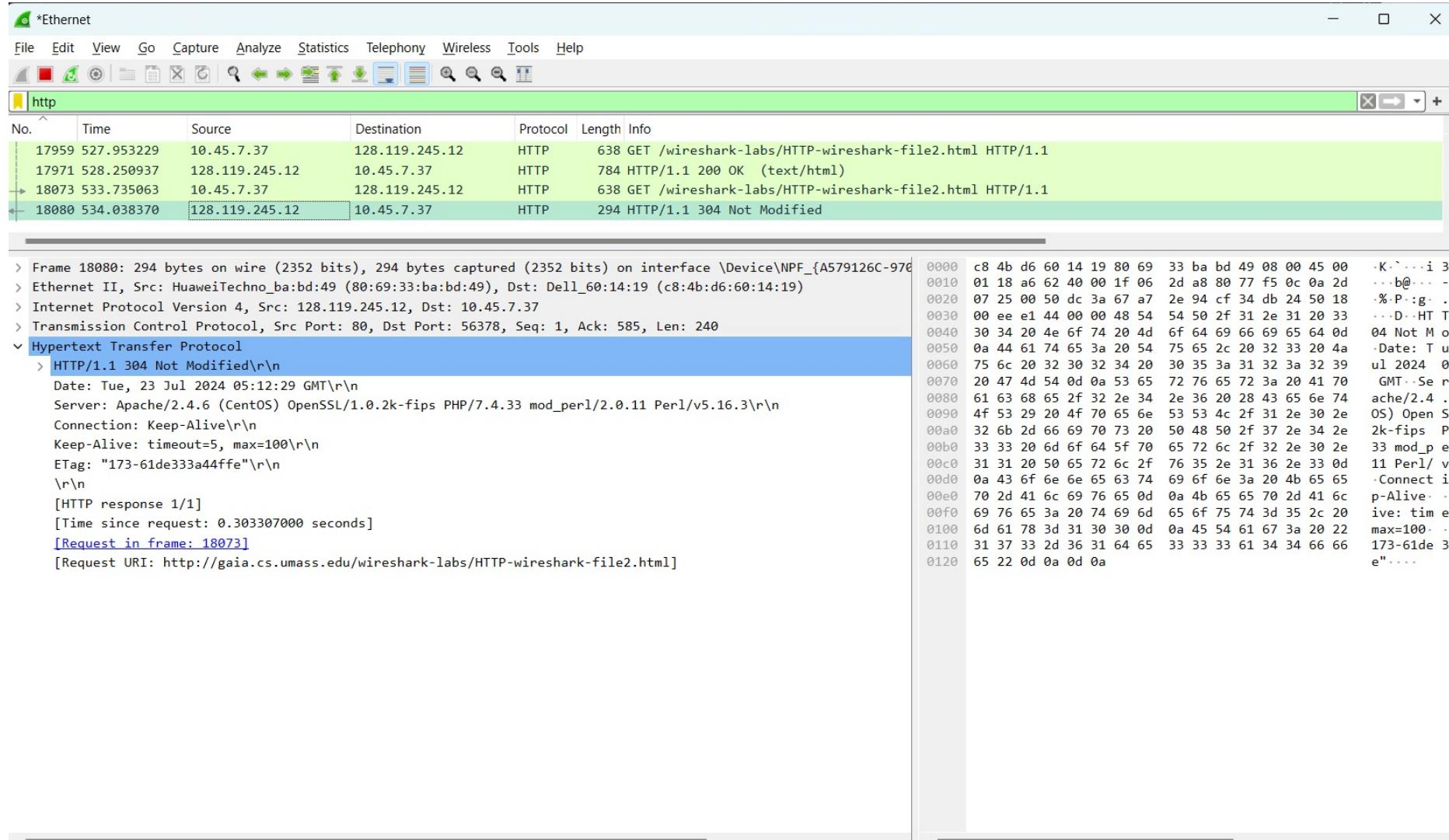
# B2. Capture នៃការ Wireshark : HTTP Response packet នៅក្នុង



# B3. Capture หน้าจอ Wireshark : HTTP Get Packet ที่สอง

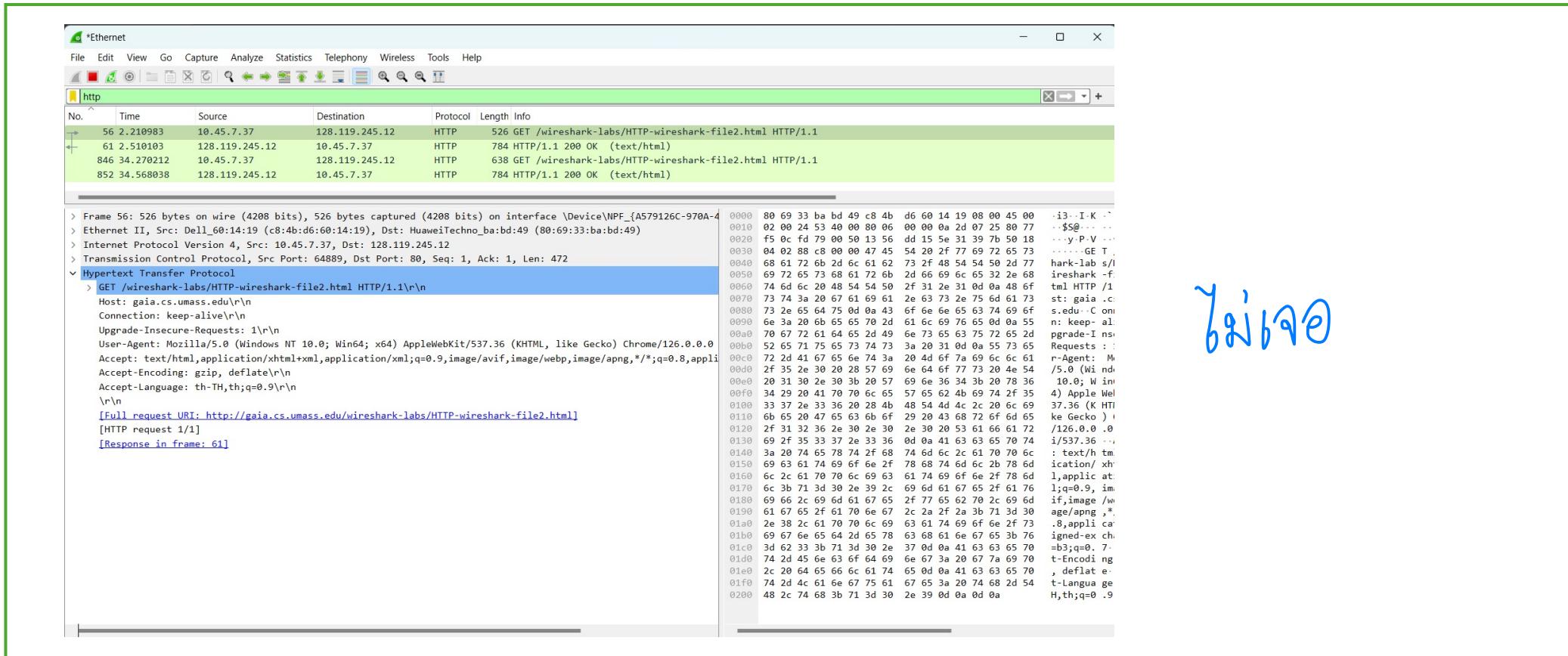


# B4. Capture หน้าจอ Wireshark : HTTP Response packet ที่สอง (หลัง Reload)



# B5.1 ຈົງຕອບກຳດາມຕ່ອງໄປນີ້

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? ຕອບ ເຈືນ ໄນເຈືນ ໄວ່າ



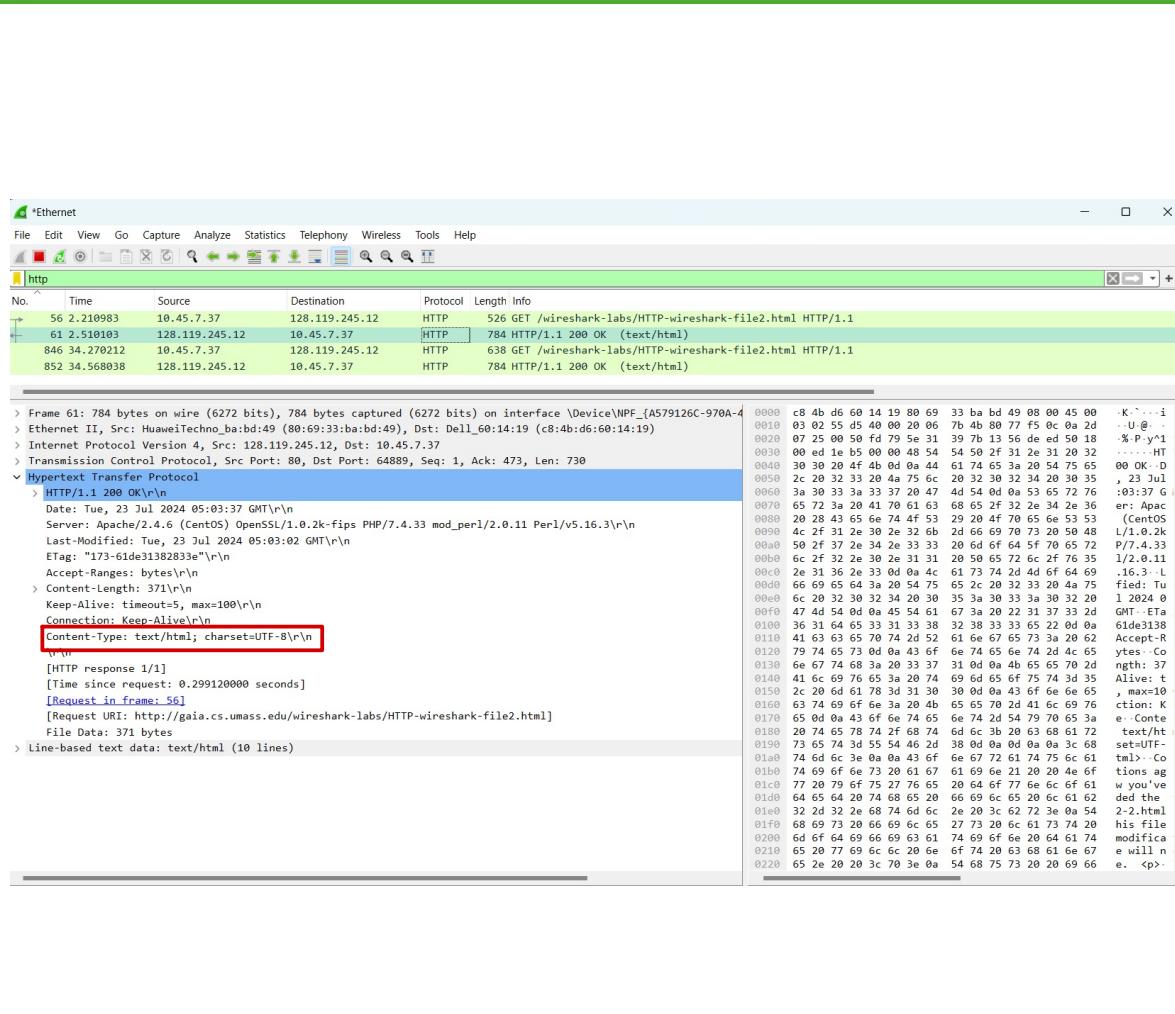
```
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
56 2.210983 10.45.7.37 128.119.245.12 HTTP 526 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
61 2.510103 128.119.245.12 10.45.7.37 HTTP 784 HTTP/1.1 200 OK (text/html)
846 34.270212 10.45.7.37 128.119.245.12 HTTP 638 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
852 34.568038 128.119.245.12 10.45.7.37 HTTP 784 HTTP/1.1 200 OK (text/html)

Frame 56: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{A579126C-970A-4
> Ethernet II, Src: Dell_60:14:19 (c8:4b:d6:60:14:19), Dst: HuaweiTechno_ba:bd:49 (80:69:33:ba:bd:49)
> Internet Protocol Version 4, Src: 10.45.7.37, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64889, 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/126.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
Accept-Encoding: gzip, deflate\r\n
Accept-Language: th-TH,th;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 61]
```

ຍິນຍັດ

## B5.2 ຈົງຕອບກຳຄານຕ່ອໄປນີ້

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



The screenshot shows a Wireshark capture on the 'Ethernet' interface. The packet list pane displays several HTTP transactions. A red box highlights the 'Content-Type: text/html; charset=UTF-8\r\n\r\n' line in the response body of frame 56, which corresponds to the request in frame 55. The details pane shows the full response content.

```
> Frame 56: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{A579126C-970A-4
> Ethernet II, Src: HuaweiTechno_ba:bd:49 (80:69:33:ba:bd:49), Dst: Dell_60:14:19 (c8:4b:d6:60:14:19)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.45.7.37
> Transmission Control Protocol, Src Port: 80, Dst Port: 64889, Seq: 1, Ack: 473, Len: 730
< Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Jul 2024 05:03:37 GMT\r\n
    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\n
    Last-Modified: Tue, 23 Jul 2024 05:03:37 GMT\r\n
    ETag: "173-61de3138283e"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\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
  [HTTP response 1/1]
  [Time since request: 0.299120000 seconds]
  [Request in frame: 55]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  File Data: 371 bytes
  Line-based text data: text/html (10 lines)
```

Answer here

content-type : text / html

# B5.3 ຈົງຕອບກຳດາມຕ່ອໄປນີ້

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 GET? If so, what information follows the “**IF-MODIFIED-SINCE:**” header?

The screenshot shows a Wireshark capture on the 'Ethernet' interface. The second row of the packet list displays an HTTP GET request from source IP 10.45.7.37 to destination IP 128.119.245.12. The details pane shows the raw request message, which includes the 'If-Modified-Since' header with the value 'Tue, 23 Jul 2024 05:12:01 GMT'.

Answer here

Tue, 23 Jul 2024

05:12:01 GMT

## B5.4 ຈົງຕອບຄໍາຄານຕ່ອງໄປນີ້

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 screenshot shows a Wireshark interface with the following details:

- Panels:** Top: Ethernet, http. Bottom: Details, Bytes.
- Packet List:** Shows four captured frames. Frame 18080 is highlighted.
- Details Panel:** Displays the captured data for Frame 18080:
  - Frame 18080: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF\_{A579126C-976...
  - Ethernet II, Src: HuaweiTechno\_ba:bd:49 (80:69:33:ba:bd:49), Dst: Dell\_60:14:19 (c8:4b:d6:60:14:19)
  - Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.45.7.37
  - Transmission Control Protocol, Src Port: 80, Dst Port: 56378, Seq: 1, Ack: 585, Len: 240
  - Hypertext Transfer Protocol**
    - HTTP/1.1 304 Not Modified
    - Date: Tue, 23 Jul 2024 05:12:29 GMT
    - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3
    - Connection: Keep-Alive
    - Keep-Alive: timeout=5, max=100
    - ETag: "173-61de333a44ffe"
    - [HTTP response 1/1]
    - [Time since request: 0.303307000 seconds]
    - [Request in frame: 18073]
    - [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
- Bytes Panel:** Shows the raw hex and ASCII data for the selected frame.

Answer here

304 ໄພນໍາການ return ພຽມະເຕຍຂົ້ນ  
ການຫອ Data ໄປແລ້ວ ຈົງໜ້າຂອ້ມຮູດ  
ເກຳມານິ້ນ ແຮຣອ Catch

## B5.5 ຈົງຕອບຄຳຄານຕ່ອໄປນີ້

- ນັກສຶກຂາຄືດວ່ານັກສຶກຂາໄດ້ເຮັດວຽກຈາກ Exercise B ນີ້ (ສຽງມາອ່າງນຳຍຸ 3 Bullet)

1. ໄດ້ຮູ້ Status Code 304

2. ເຮົາຍພຽບກາງທີ່ Wire shark

3. ກາງດູ Content ທີ່ Response ກລັນມາ

4. ກາງດູວັນ Modified ທີ່ເກີນ Cache

# C. HTML Documents with Embedded Objects

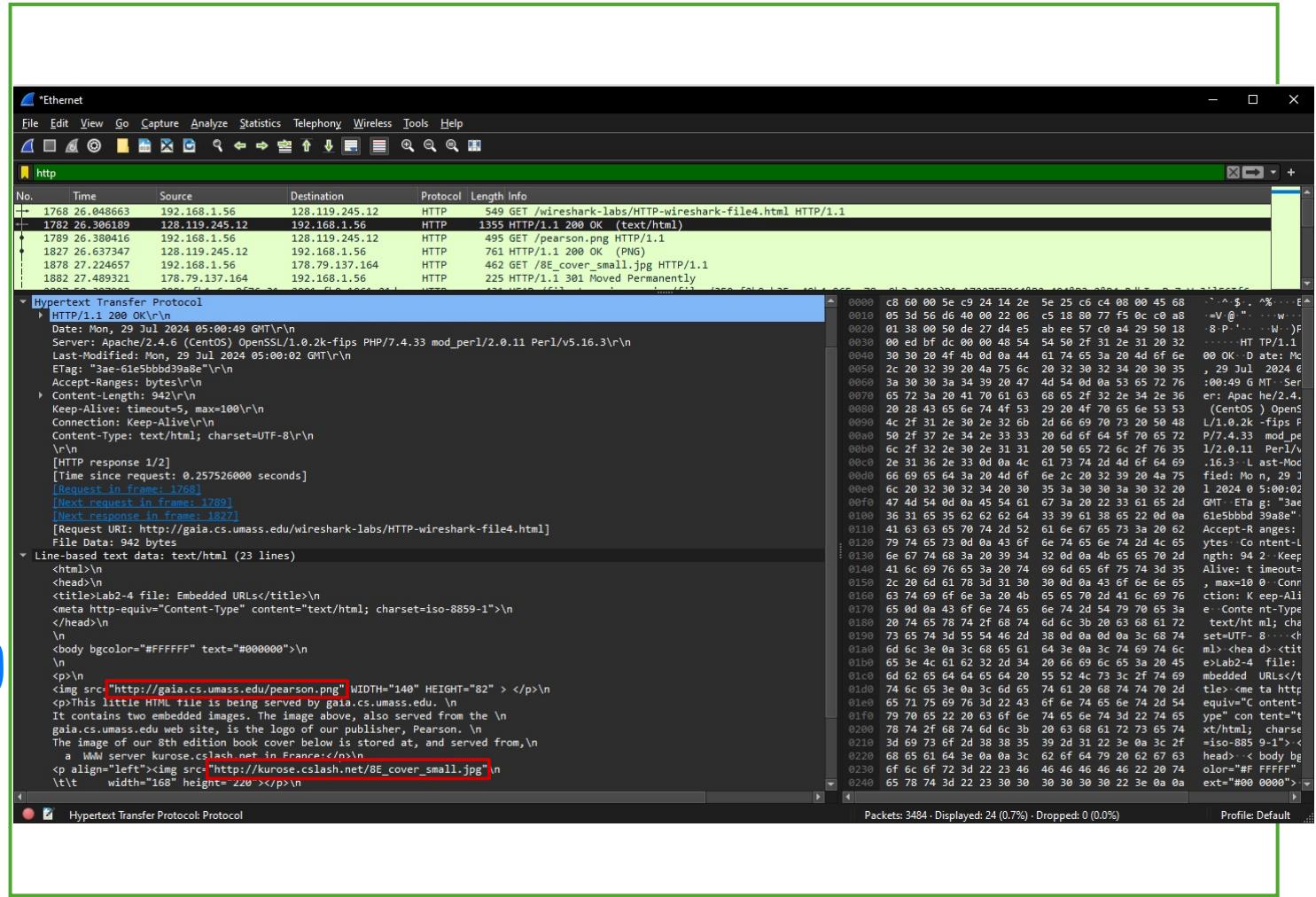
## Instruction

1. Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
2. Start up the Wireshark packet sniffer
3. Enter the following URL into your browser  
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>
4. Stop Wireshark packet capture,
  - and enter “http” in the display-filter-specification window, so that only captured HTTP messages will be displayed.

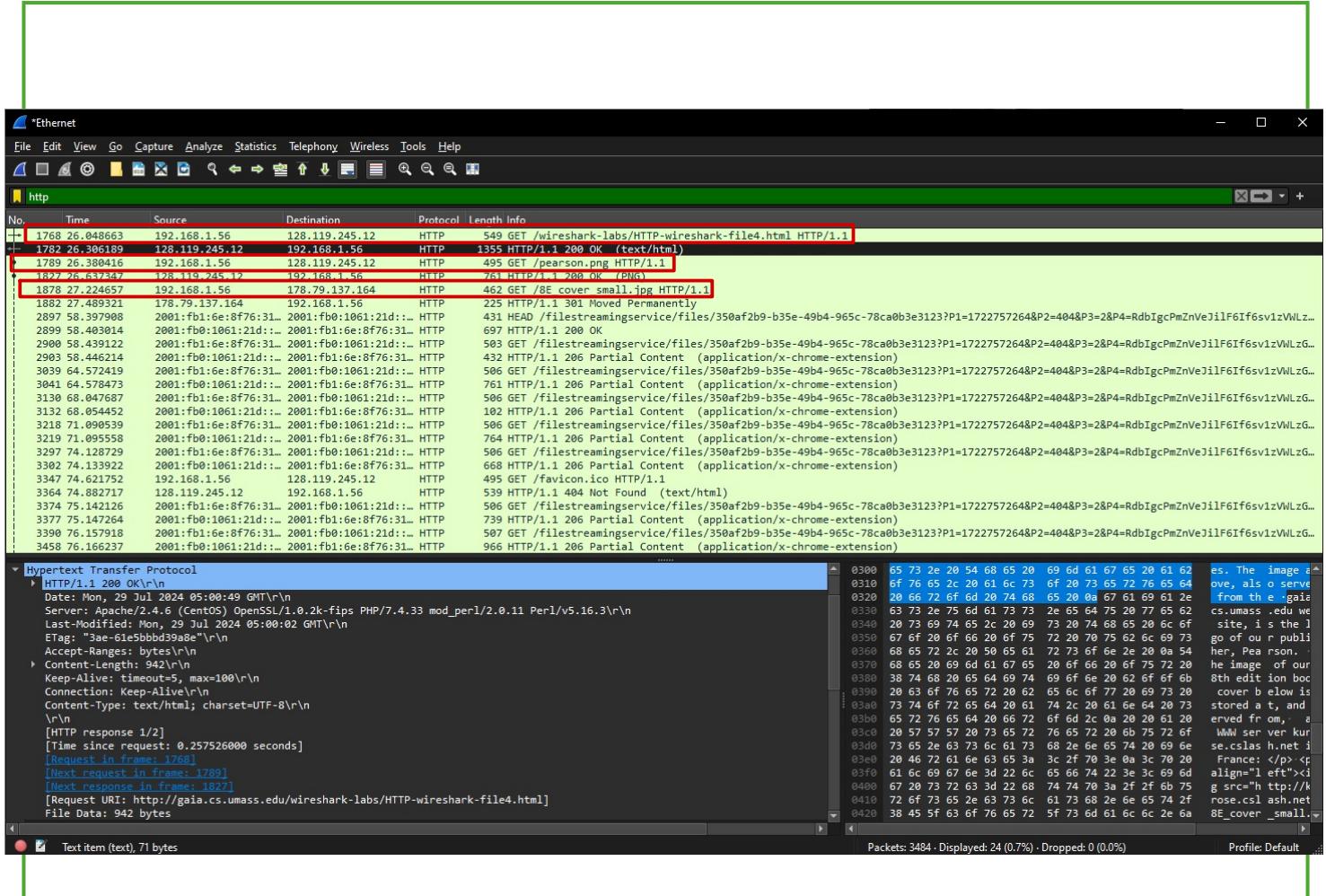
# C1. อ่าน Paragraph ต่อไปนี้ ทำความเข้าใจ และเติมคำในช่องว่าง

- Your browser should display a short HTML file with two images.
  - These two images are referenced in the base HTML file.
  - the images themselves are not contained in the HTML; instead their URLs are contained in the downloaded HTML file.
- The publisher's logo is retrieved from the [gaia.cs.umass.edu](http://gaia.cs.umass.edu) web site.
- The image of the 8th edition cover of their book is retrieved from  
<http://kurose.csplash.net/8E-cover-small.jpg>
- Using Iplocation to find the location of the website of this images

London



# C3. ຕອບຄຳຄານຕ່ອງໄປນີ້



C3.1 How many HTTP GET request messages did your browser send? (ຕອບຈຳນວນຂອງ packet ແລະ ມາຍເລີຂ packet)

3 packet ... 1768 / 1789 / 1878 ...  
.....

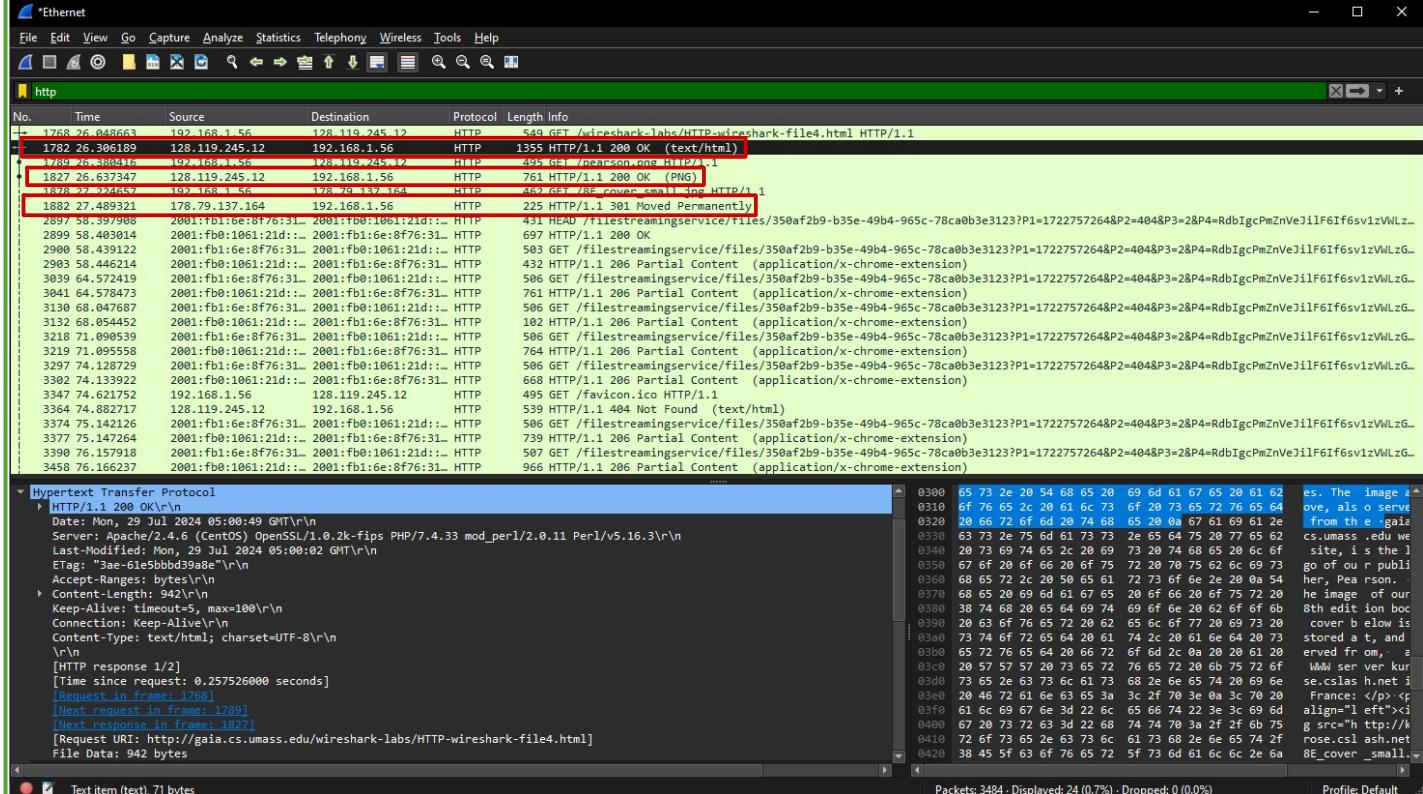
C3.2 To which Internet addresses were these GET requests sent?

(1) 128.119.245.12  
.....

(2) 178.79.137.164  
.....

(3) 128.119.245.12  
.....

# C4. ตอบคำถามต่อไปนี้



- C4.1 Response packet no. ของ Get แรก คือ..... 1782  
 Response packet no. ของ Get ที่สองคือ..... 1827  
 Response packet no. ของ Get ที่สามคือ..... 1882

C4.2 Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel?

ใช้ลากวางๆ . Serially . ที่ลากไว้

## C4.3 Explain

Download . ได้ยังไงก็จะรับได้ก่อน

따라서ค่าไฟล์ภาพร่วมกันต้องสั่ง Request

ไปพร้อมกัน แต่คันนี้รอ Response จึงปั๊วะ

ก่อนก็สั่ง Request ลุยกันไป

## C5. จงตอบคำถามต่อไปนี้

- นักศึกษาคิดว่า นักศึกษาได้เรียนรู้อะไรจาก Exercise C นี้ (สรุปมาอย่างน้อย 2 Bullet)
  1. โปรดอธิบายว่า การทำงานของาระบบดูไปทางใดทางหนึ่ง
  2. ระบุ Status Code 301
  - 3.
  - 4.

# D. Retrieving Long Documents

## Instruction

1. Start up your web browser, and make sure your browser's cache is cleared,
2. Start up the Wireshark packet sniffer

3. Enter the following URL into your browser

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

Your browser should **display** the rather **lengthy US Bill of Rights**.

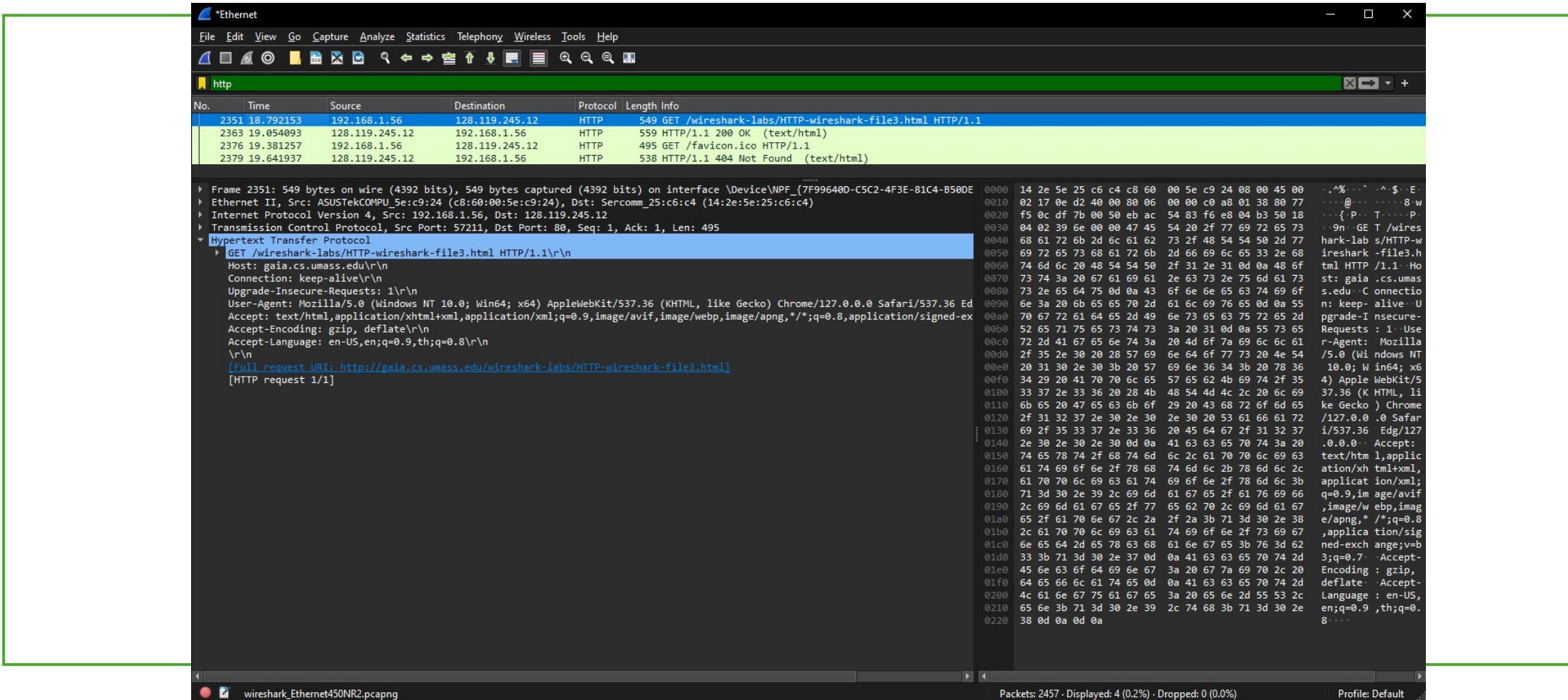
4. Stop Wireshark packet capture,
  - and **enter “http”** in the display-filter-specification window, so that only captured HTTP messages will be displayed.

# D1. อ่าน Paragraph ต่อไปนี้และทำความเข้าใจ

---

- Recall that
  - the HTTP response message consists of a status line, header lines, a blank line, and the entity body.
- In the case of this HTTP GET,
  - the entity body in the response is the *entire* requested HTML file.
  - this HTML file is **rather long**, and at **4500 bytes** is **too large to fit in one TCP packet**.
  - ดังนั้น
    - The **single** HTTP response message is thus **broken** into several pieces by TCP,
    - each piece = a separate TCP segment
    - In recent versions of Wireshark,
      - Wireshark indicates each TCP segment as a separate packet,
      - the **single** HTTP response was **fragmented** to multiple TCP packets
        - indicated by the “TCP segment of a reassembled PDU” in the Info column of the Wireshark display.

## D2. Capture នៅលើ Wireshark : HTTP Request ទៅ <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>



# D3. Capture หน้าจอ Wireshark : HTTP Response ของ <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

ແປ່ງຢັງ Reassembled TCP Segments (4861 bytes): #2359(1452), #2360(1452), #2362(1452), #2363(505)

4 Segment

- 1) 1452 bytes
- 2) 1452 bytes
- 3) 1452 bytes
- 4) 505 bytes

Frame (559 bytes) Reassembled TCP (4861 bytes)

Packets: 2457 - Displayed: 4 (0.2%) - Dropped: 0 (0.0%)

Profile: Default

## D4. ຈົດອັບຄຳຄາມຕ່ອໄປນີ້

1. 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?

Packet Number : 2351 / 1 packet

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

Packet Number : 2363

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

Status Code : 200 Response : OK

4. How many TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

4 TCP segment

## D5. จงตอบคำถามต่อไปนี้

- นักศึกษาคิดว่า นักศึกษาได้เรียนรู้อะไรจาก Exercise D นี้ (สรุปมาอย่างน้อย 2 Bullet)
  - เขียนหัว เกี่ยวกับ TCP segment
  - ตรวจสอบ TCP segment ใน Wireshark
  - .
  - .

# E1. HTTP Authentication

## Instruction

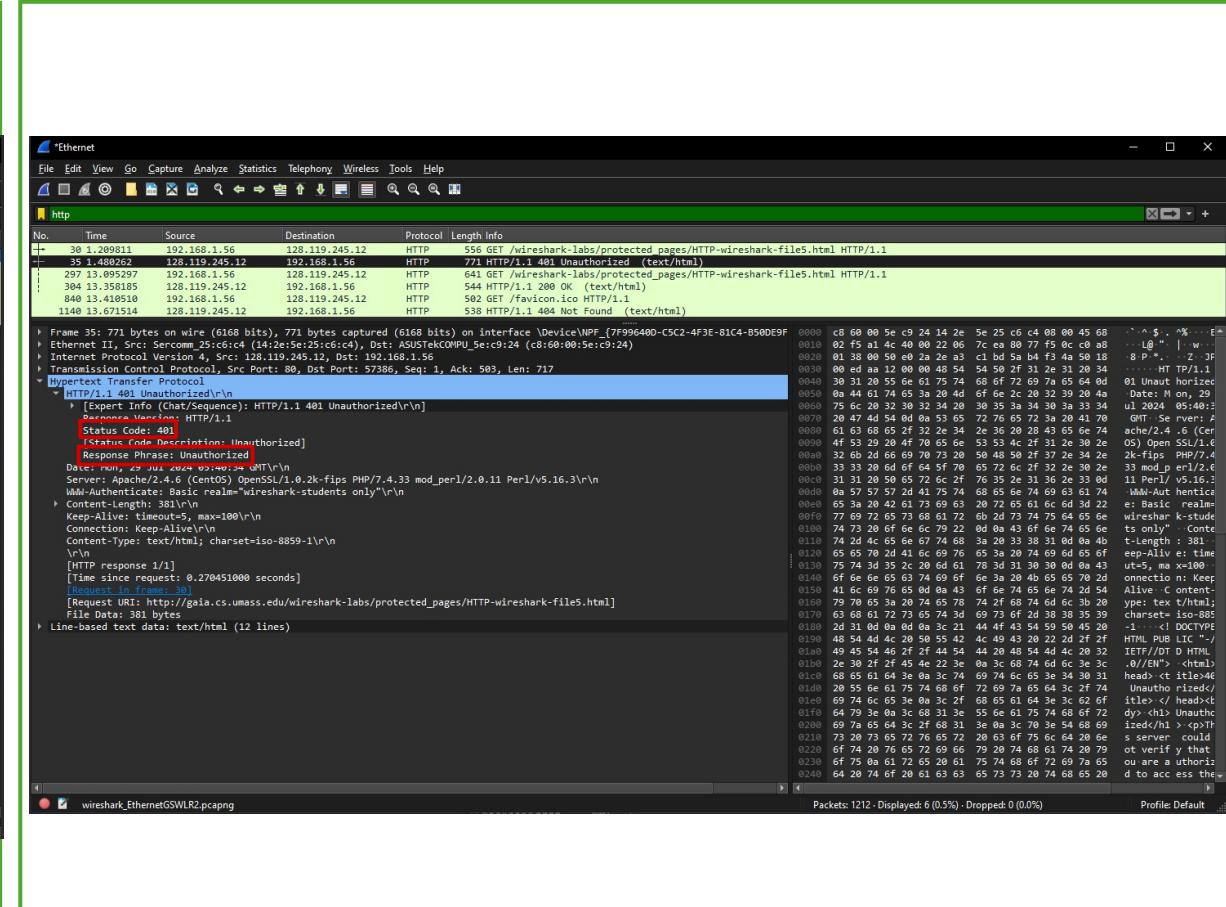
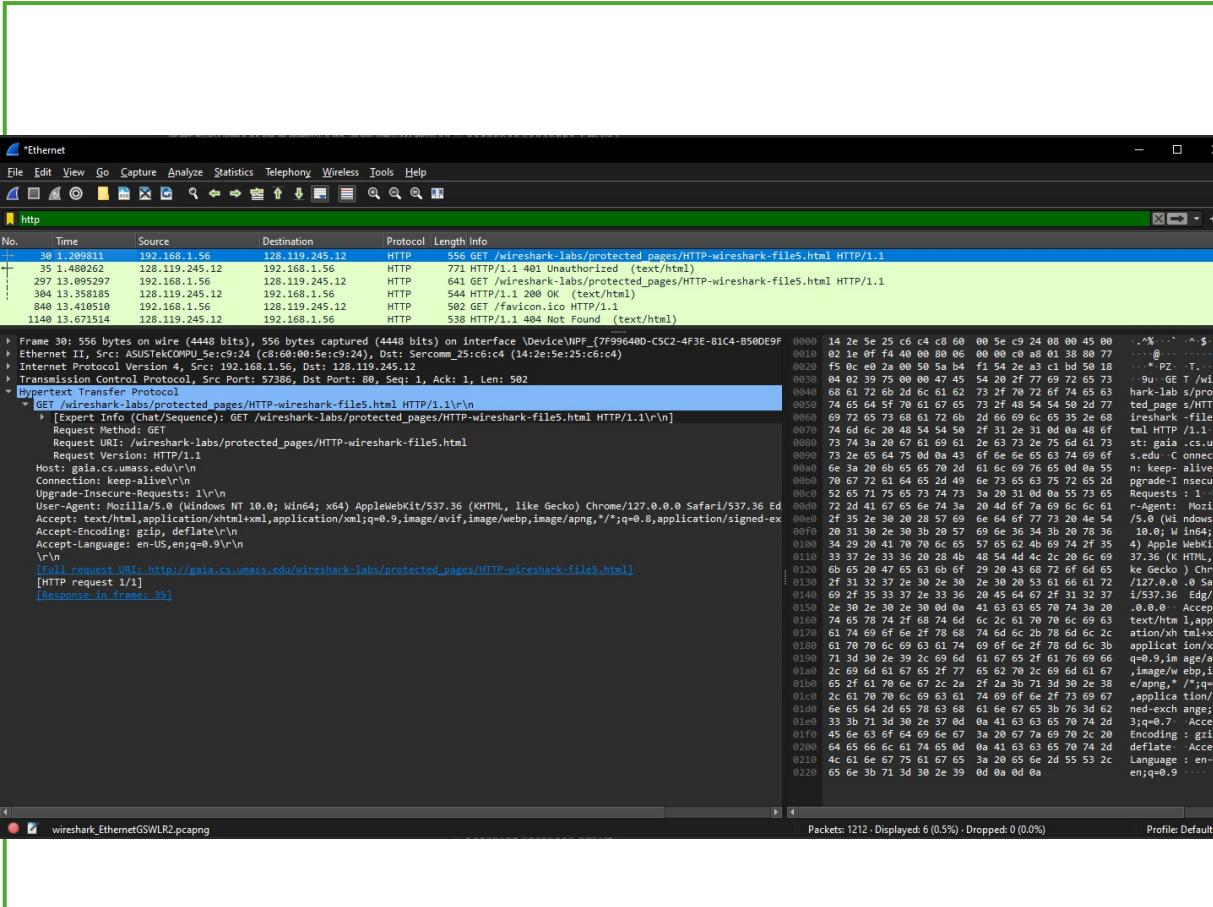
1. Make sure your browser's **cache is cleared**, and
2. **Close down** your browser.
3. **Start up** your browser
4. **Start up** the Wireshark packet sniffer
5. **Enter** the following URL into your browser

[http://gaia.cs.umass.edu/wireshark-labs/protected\\_pages/HTTP-wireshark-file5.html](http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html)

Type the requested user name : *wireshark-students* and password : *network* into the pop up box.

6. **Stop** Wireshark packet capture,
  - and enter “**http**” in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

# E2. Capture หน้าจอ Wireshark : HTTP Get Packet และ Response ของ Get Packet นี้ และตอบคำถามข้อ E2.1



E2.1 What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? **Status Code 401 Unauthorized**

# E2. ตอบคำถามต่อไปนี้

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No. Time Source Destination Protocol Length Info

38 1.200811 192.168.1.56 128.119.245.12 HTTP 556 GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html HTTP/1.1

35 1.488262 128.119.245.12 192.168.1.56 HTTP 771 HTTP/1.1 401 Unauthorized (text/html)

297 13.095297 192.168.1.56 128.119.245.12 HTTP 641 GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html HTTP/1.1

384 13.358185 128.119.245.12 192.168.1.56 HTTP 544 HTTP/1.1 200 OK (text/html)

840 13.410818 192.168.1.56 128.119.245.12 HTTP 502 GET /avicon.ico HTTP/1.1

1140 13.671514 128.119.245.12 192.168.1.56 HTTP 538 HTTP/1.1 404 Not Found (text/html)

Frame 30: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface \Device\NPF\_{7F99640D-C5C2-4F3E-81C4-B50DE9F

Ethernet II, Src: ASUSTekCOMPU\_5ec:9:24 (c8:00:0e:c8:02:24), Dst: Sercomm\_25:c6:4 (14:2e:5e:25:c6:4)

Internet Protocol Version 4, Src: 192.168.1.56, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 80, Seq: 1, Ack: 1, Len: 502

Hypertext Transfer Protocol

[GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]

[Expert Info (Chat/Sequence): GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /wireshark-labs/protected\_pages/HTTP-wireshark-file5.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/127.0.0.0 Safari/537.36 Ed

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

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9\r\n

[Request URL: http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html]

[HTTP request 1/1]

[Response in frame: 35]

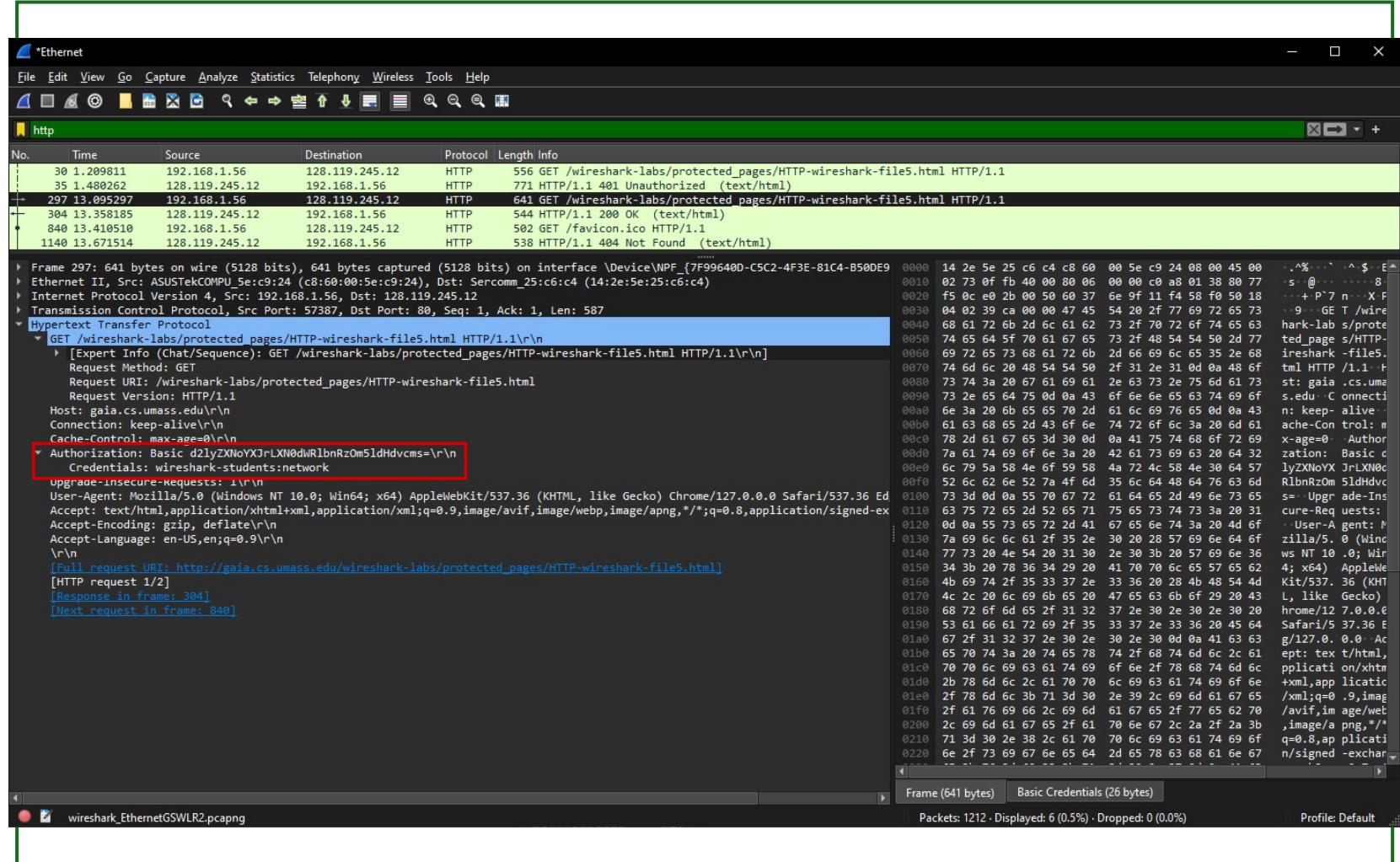
Packets: 1212 · Displayed: 6 (0.5%) · Dropped: 0 (0.0%) · Profile: Default

- C4.1 Response packet no. ของ Get แรก คือ..... 35
- Response packet no. ของ Get ที่สองคือ..... 304
- Response packet no. ของ Get ที่สามคือ..... -

..... Status Code 401 Unauthorized .....

..... Status Code 200 OK .....

# E3 Capture หน้าจอ Wireshark : HTTP Get Packet ที่สอง และตอบคำถาม E3.1 และ E3.2



E3.1. When your browser's sends the HTTP GET message for the second time, what **new field** is included in the HTTP GET message?

Authorization field

E3.2 ผู้ศึกษาคิดว่าจาก Capture Password ที่ได้ จาก http get message Hacker จะสามารถ password นี้ได้หรือไม่

ไม่

## E4. Extracting the plaintext password

- ถ้านักศึกษาตอบได้ในข้อ E3.2 ให้แสดงวิธีหา Plaintext Password ของ User name นี้

slugkanakut@kaig Credentials ที่อยู่ใน Authorization field แบบ format จะเป็น Username คันตัวย : ตามตัวย Password (Username:Password)

## E5. จงตอบคำถามต่อไปนี้

- นักศึกษาคิดว่า นักศึกษาได้เรียนรู้อะไรจาก Exercise E นี้ (สรุปมาอย่างน้อย 3 Bullet)
  - ระบุหัวข้อ Hacker สามารถตั้งรหัสอะไร
  - ระบุบัญชี Status Code 401
  - ระบุนรุ้ภารนา Plaintext Password
  -