Homework 4 : HTTP Lab

การบ้าน นี้นำมาจาก **HTTP Lab** ของ **Kurose**

- มีทั้งหมด ๔ ข้อใหญ่
  - **B** หน้า ๓-๑๒
  - **C** หน้า ๑๓-๑๗
  - **D** หน้า ๑๘-๒๓
  - **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 ...1.....รหัสนักศึกษา .6505036๘..... ชื่อ สกุล . ธนภัทร์ เกิดเปี่ยม

ทำเดี่ยว หรือ คู่ .....เดี่ยว.....

LAN หรือ WiFi .....LAN.....

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

กรณี WiFi ใช้ HOTSpot จากมือถือหรือไม่.....ไม่..... iOS หรือ Android .....-.....

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

หมายเลข IP ของเครื่องที่นักศึกษาใช้ (CIDR Format) 192.169.1.56 (บ้าน)
10.45.7.37 (Lab)

MAC Address ของเครื่องที่นักศึกษาใช้ .....C8-4B-D6-60-14-19 (Lab).....
C8-60-00-5E-C9-24 (บ้าน)

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
(ให้ใส่ √ สำหรับผู้ทำในข้อนั้นๆ)

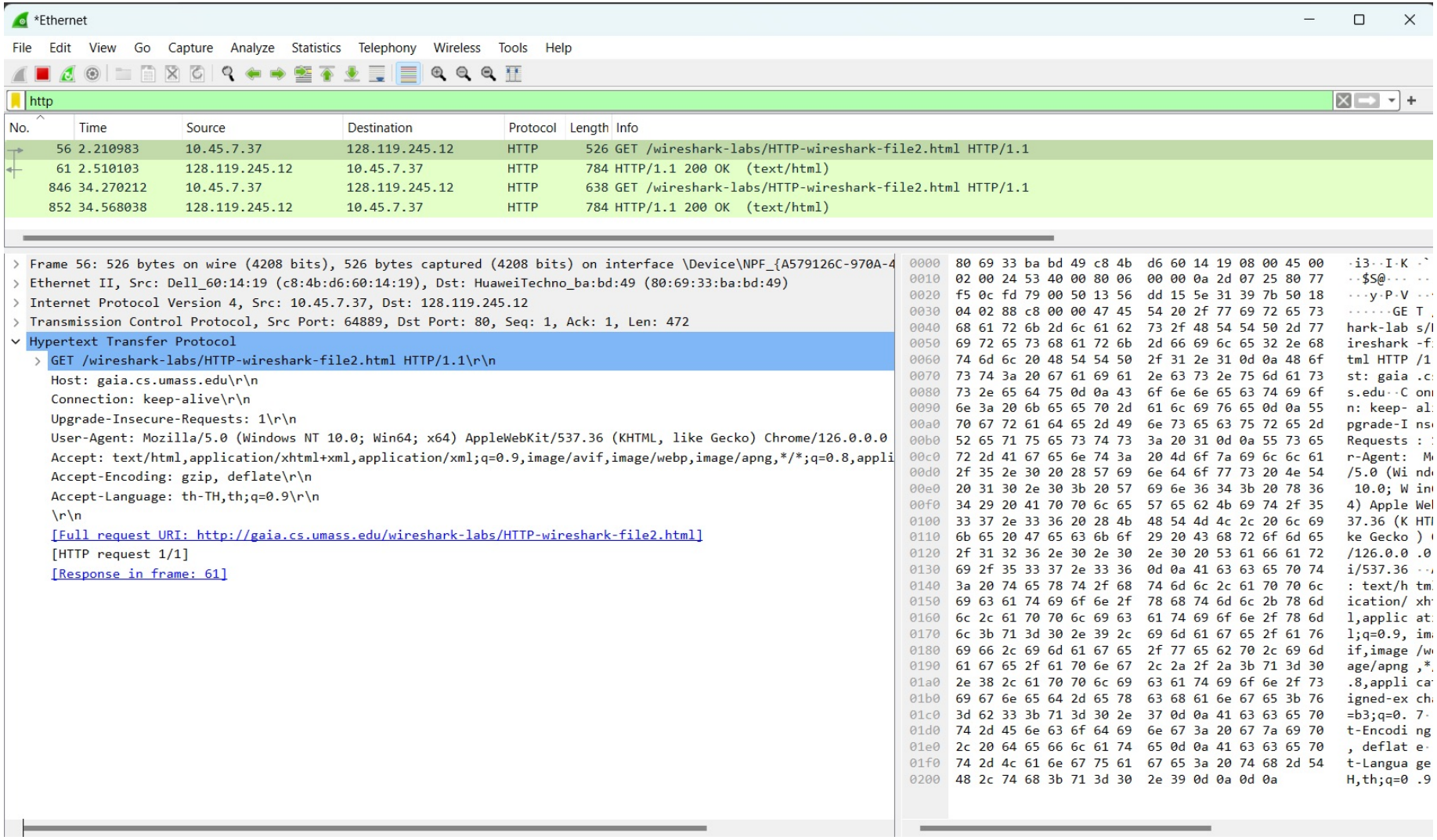
ข้อ	นักศึกษา	คู่ของนศ	ช่วยกันทำ	หมายเหตุ
B				
C				
D				
E				

B. The HTTP CONDITIONAL GET/response interaction

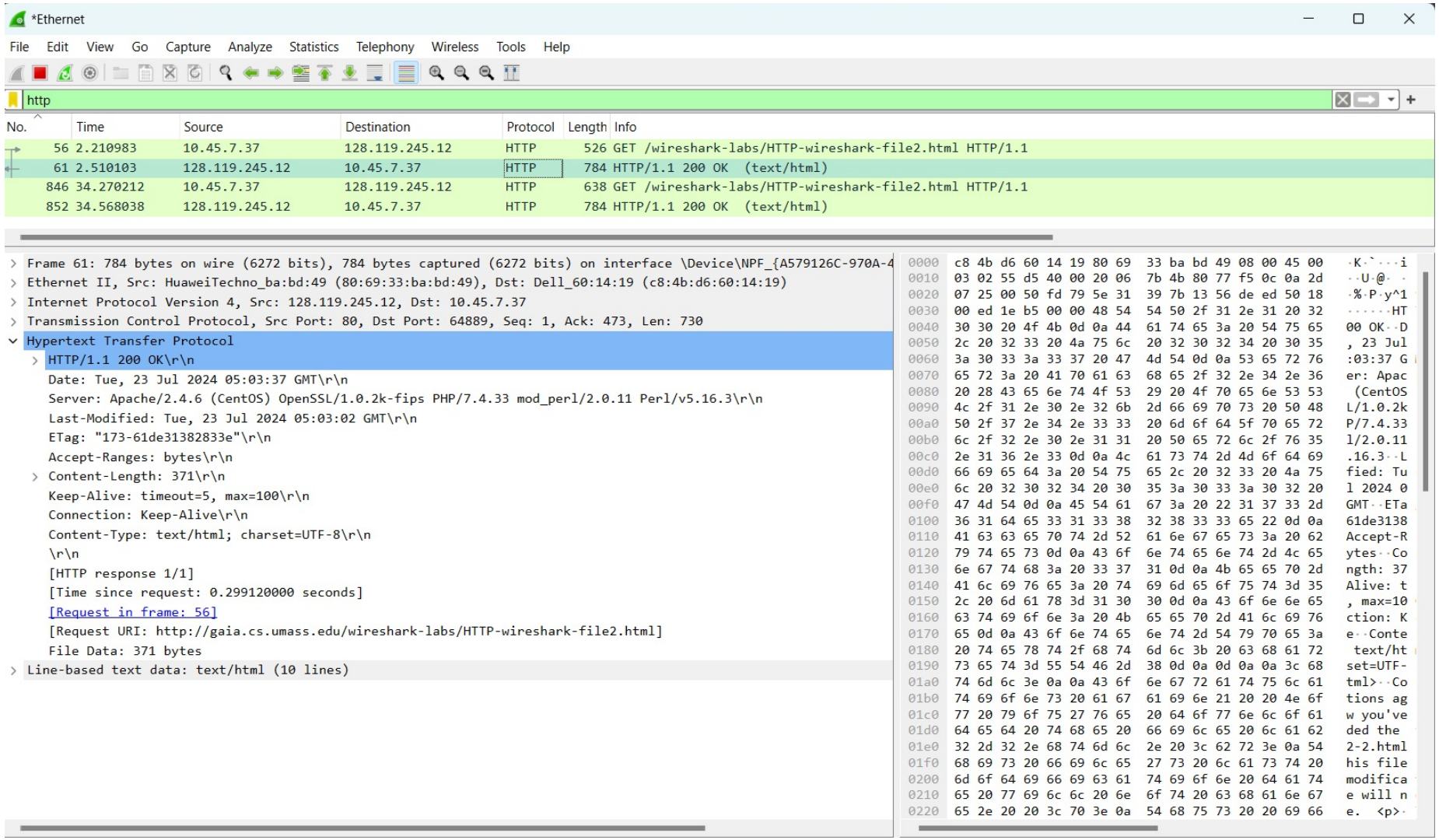
Instruction

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.

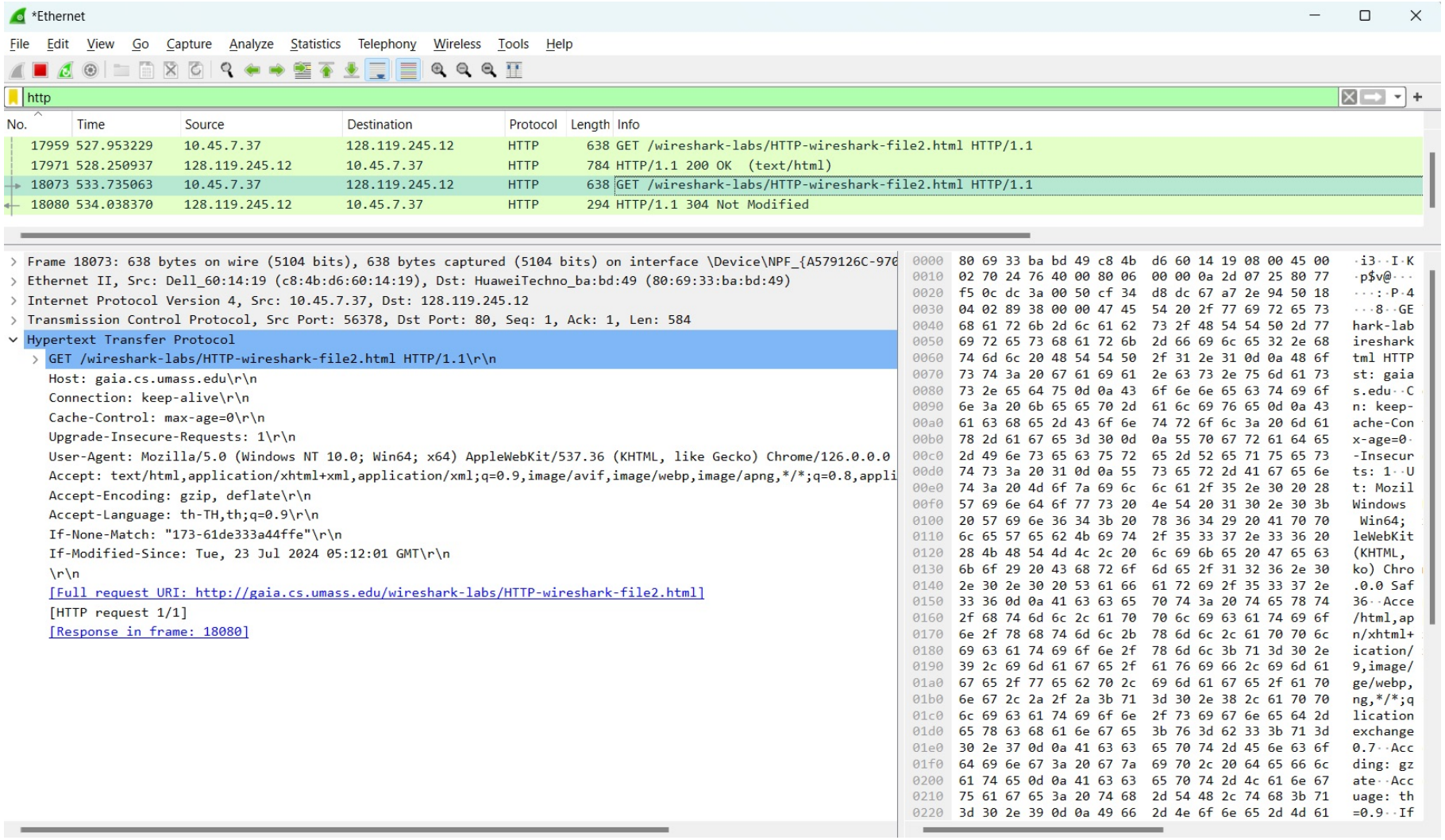
B1. Capture หน้าจอ Wireshark : HTTP Get Packet แรก



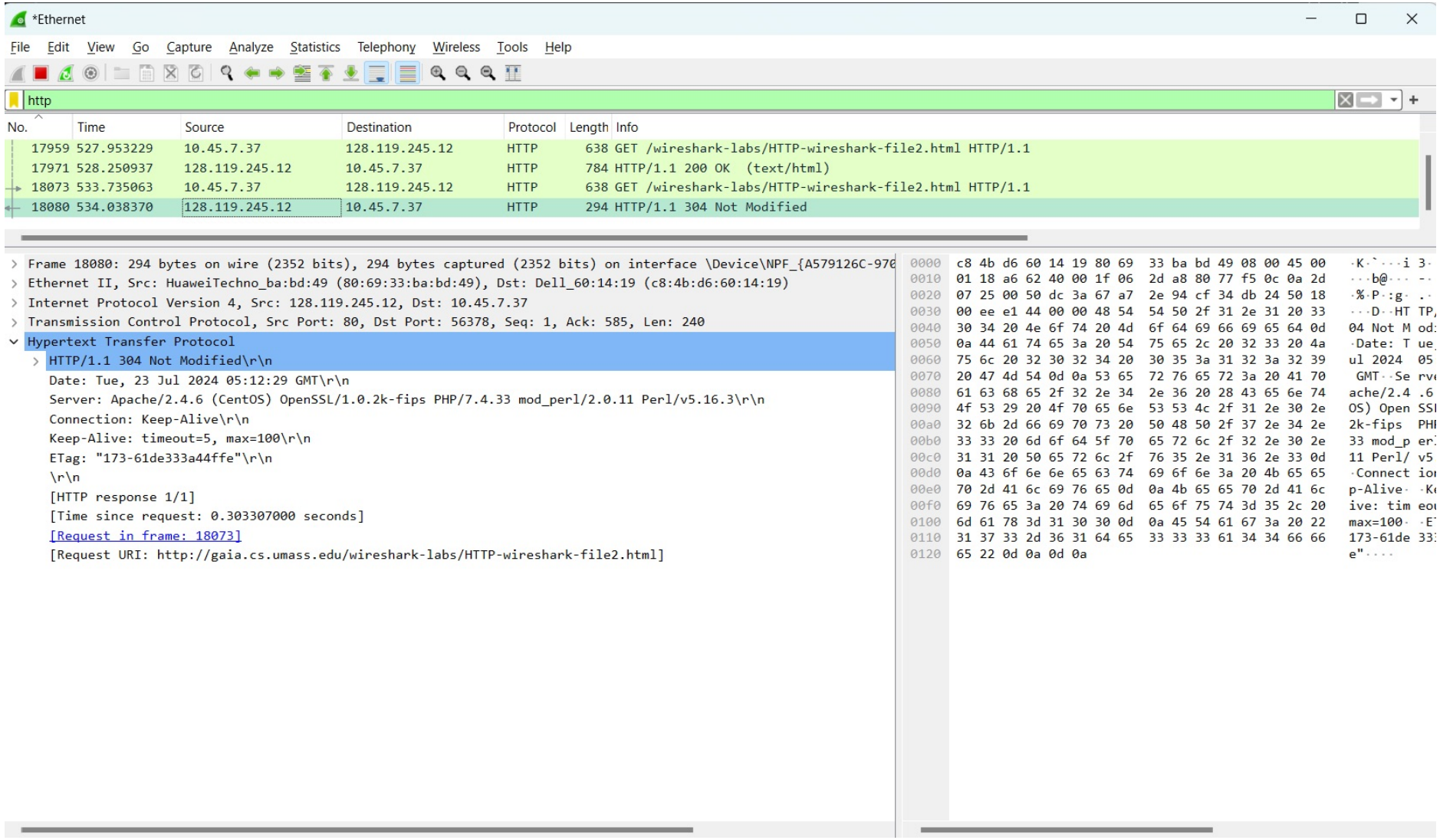
B2. Capture หน้าจอ Wireshark : HTTP Response packet แรก



B3. Capture หน้าจอ Wireshark : HTTP Get Packet ที่สอง

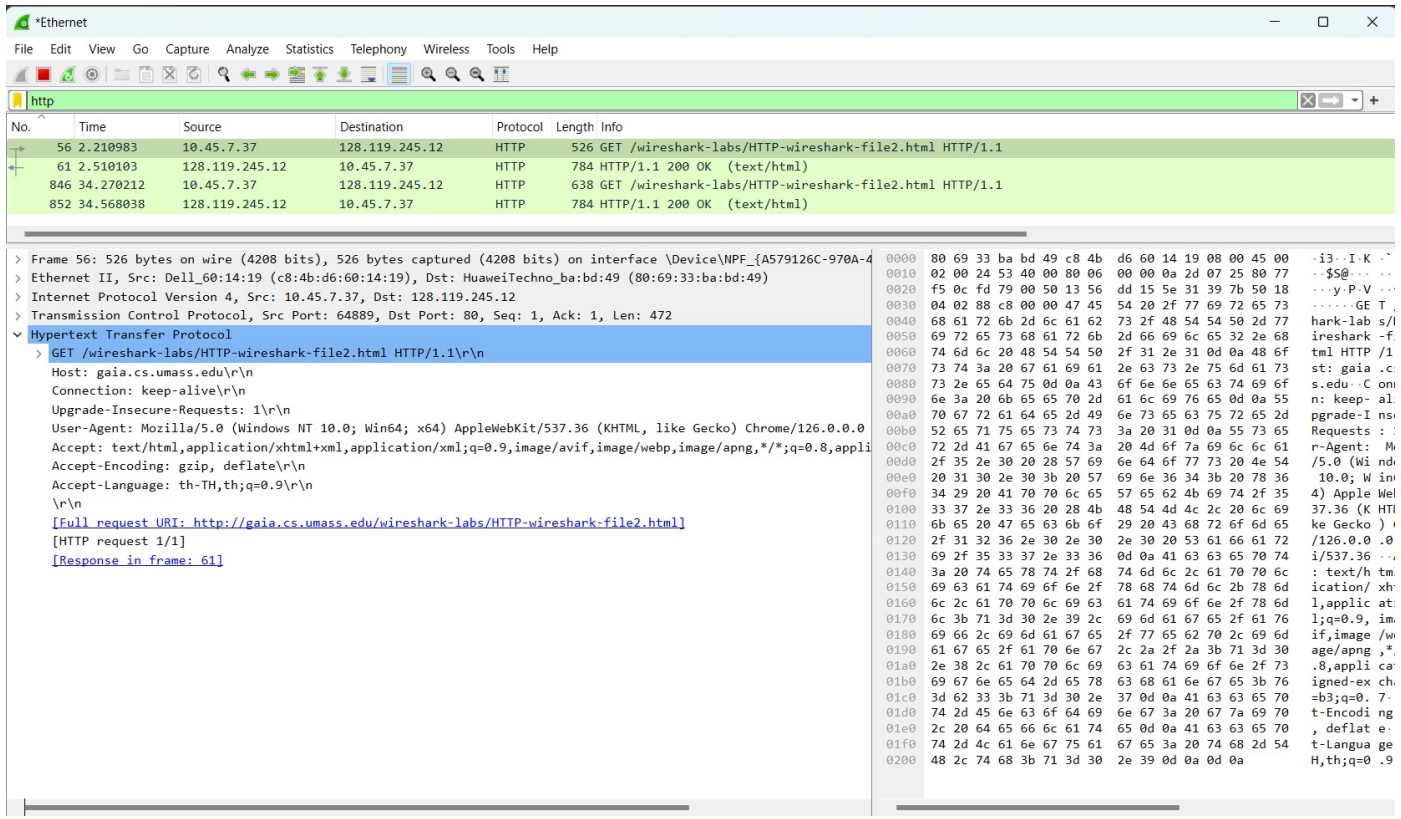


B4. Capture หน้าจอ Wireshark : HTTP Response packet ที่สอง (หลัง Reload)



B5.1 จงตอบคำถามต่อไปนี้

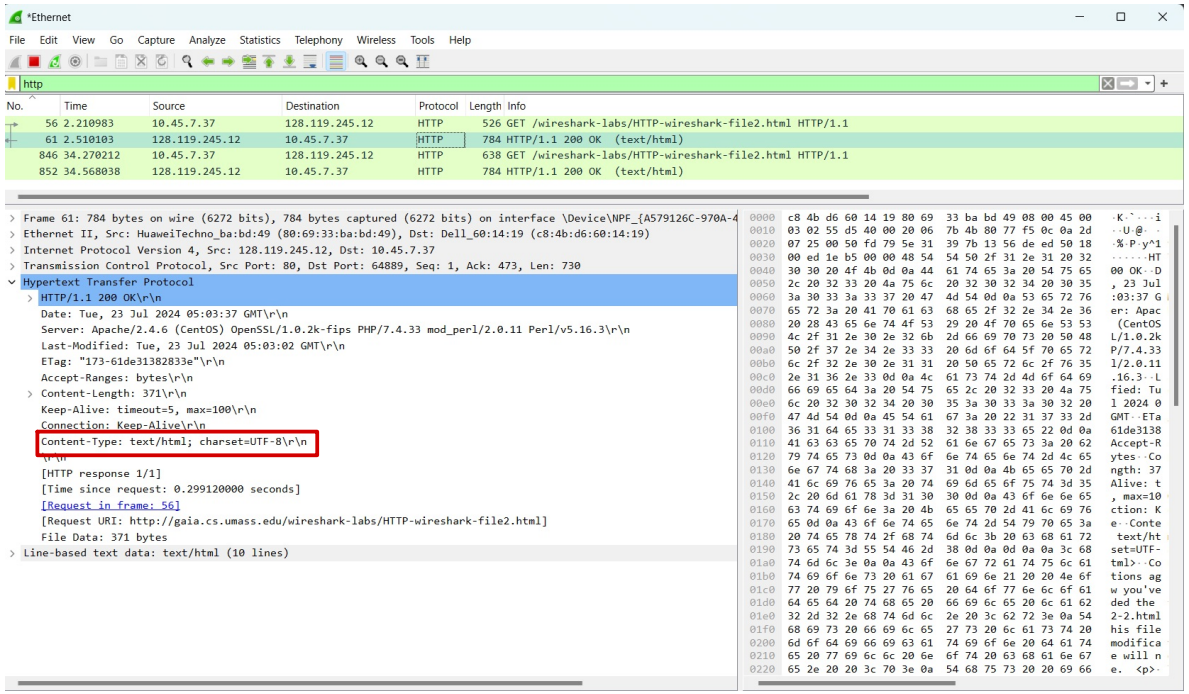
Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET? ตอบ เจอ ไม่เจอ ถ้าเจอ ให้วง



ไม่เจอ

B5.2 จงตอบคำถามต่อไปนี้

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

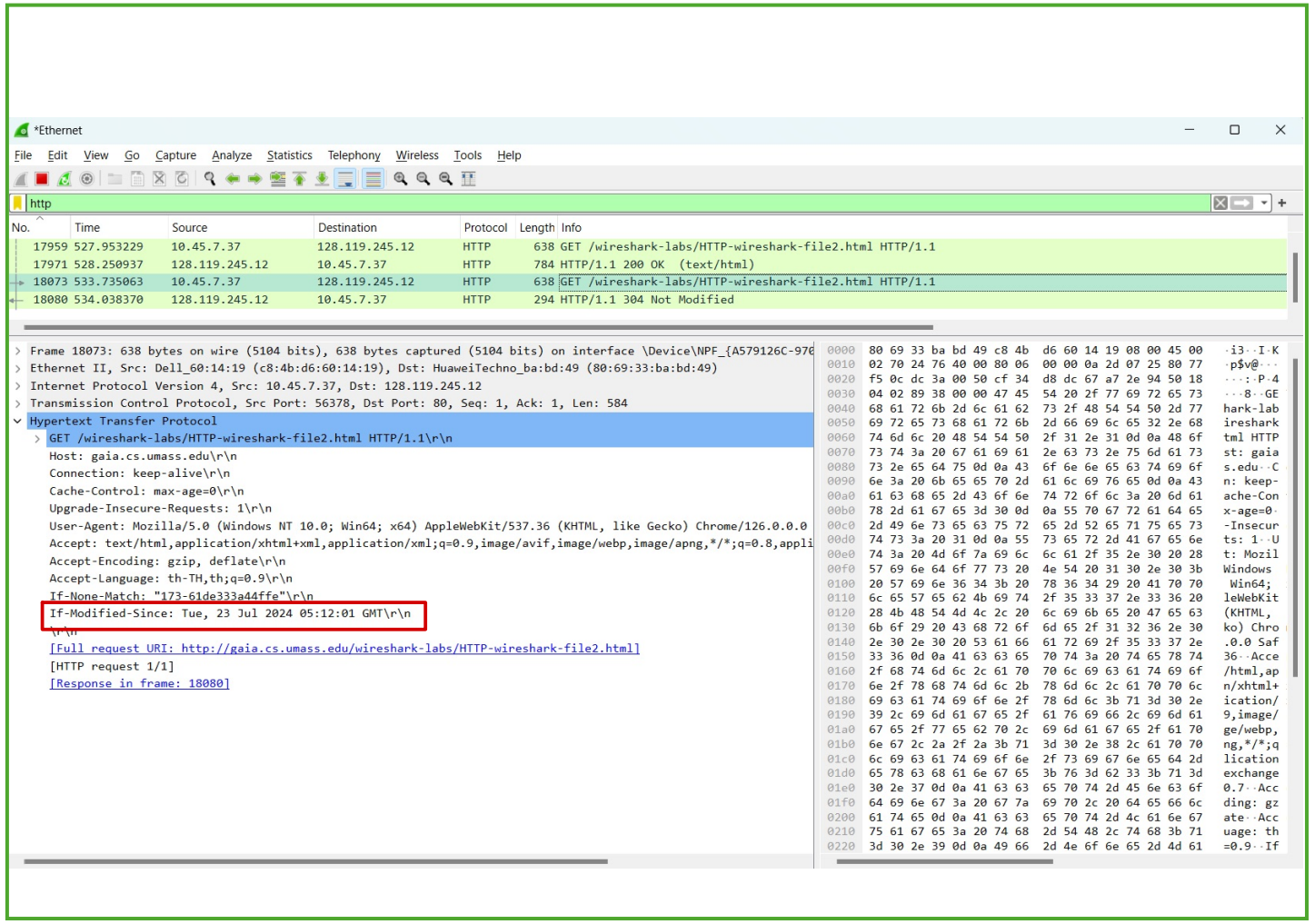


Answer here

content-type : text / html

B5.3 จงตอบคำถามต่อไปนี้

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?



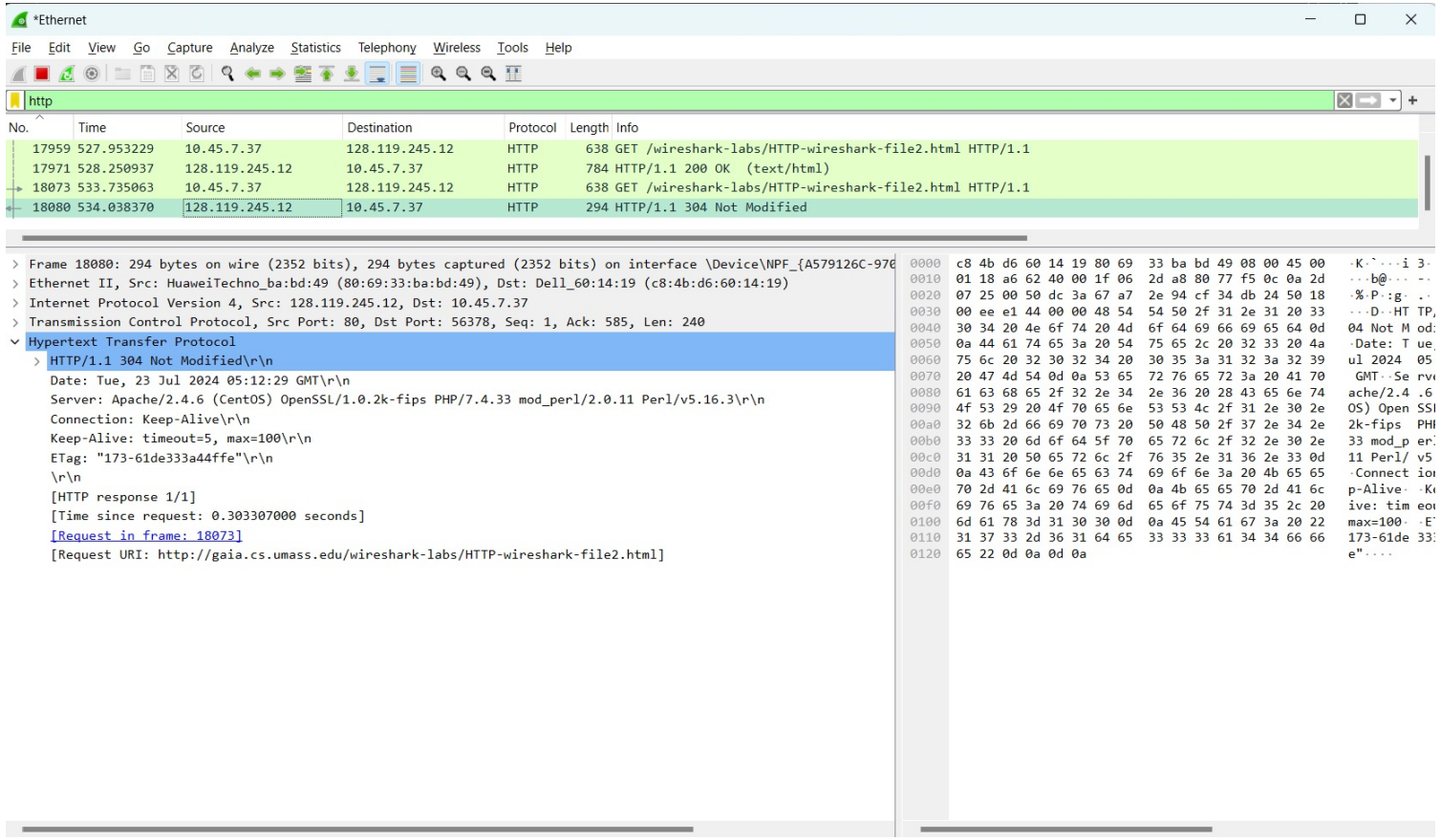
Answer here

Tue, 23 Jul 2024

05:12:01 GMT

B5.4 จงตอบคำถามต่อไปนี้

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.



Answer here

304 ไม่มีการ return เพราะเคยมีการขอ Data ไปแล้ว จึงนำข้อมูลเก่ามาให้ หรือ Catch

B5.5 จงตอบคำถามต่อไปนี้

- นักศึกษาคิดว่านักศึกษาได้เรียนรู้อะไรจาก Exercise B นี้ (สรุปมาอย่างน้อย 3 Bullet)
  1. ได้รู้ Status Code 304
  2. เรียนรู้การใช้ Wire shark
  3. การดู Content ที่ Response กลับมา
  4. การดูวัน Modified ที่เก็บ 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.

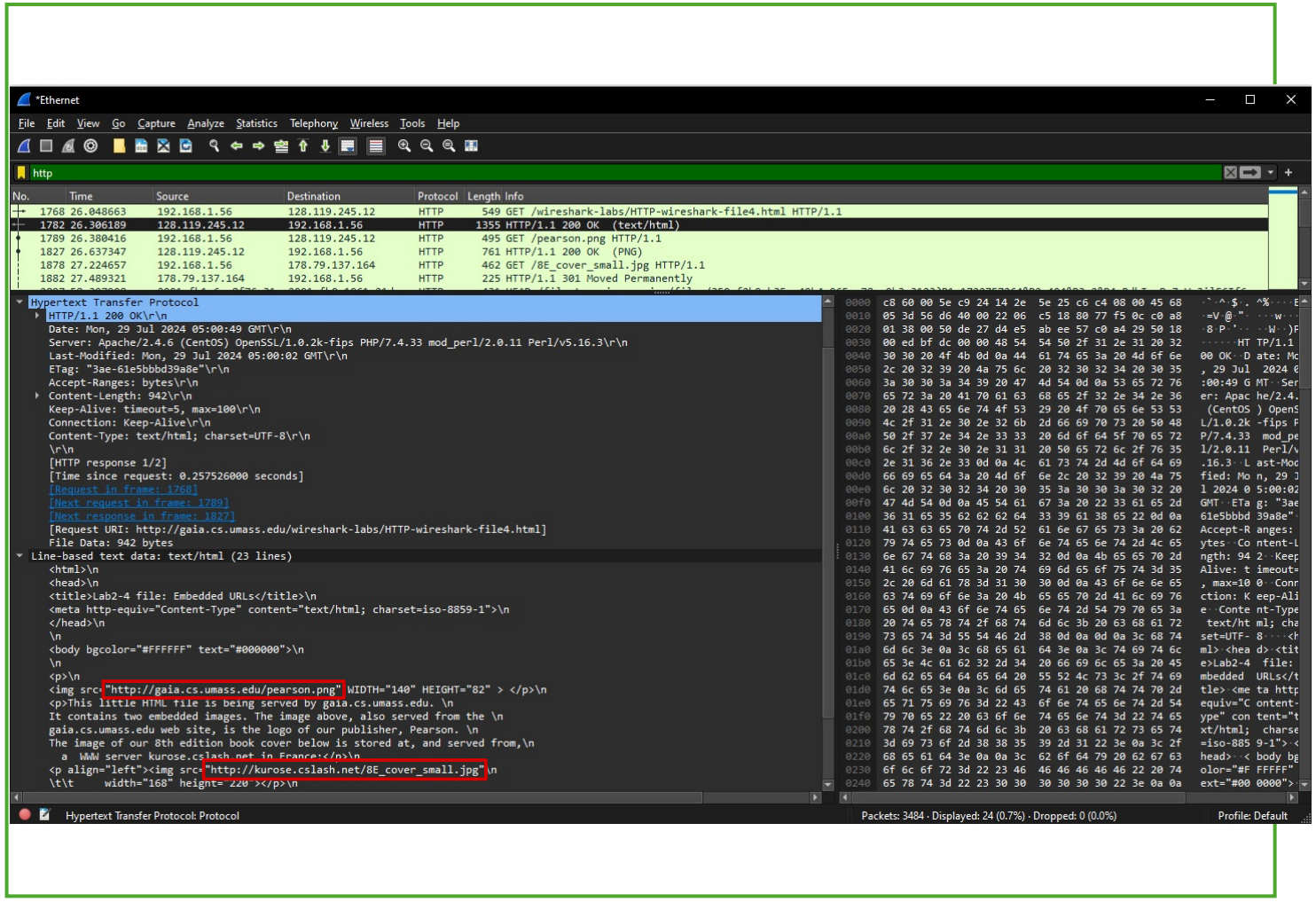
C1. อ่าน Paragraph ต่อไปนี้ ทำความเข้าใจ และเติมคำในช่องว่าง

- 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 web site.
- The image of the 8th edition cover of their book is retrieved from

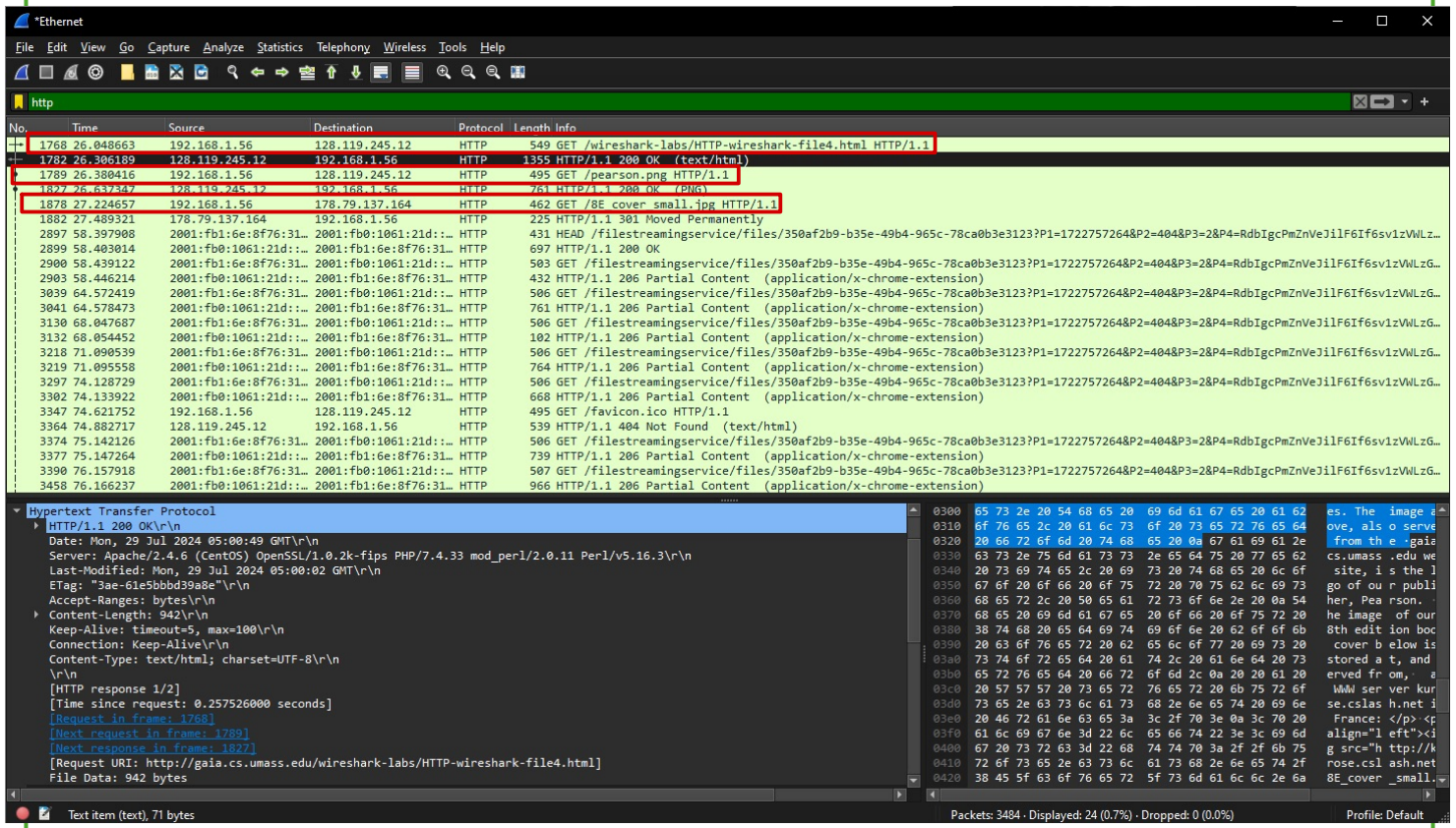
http://kurose.cslash.net/8E_cover_small.jpg

- Using Iplocation to find the location of the website of this images

London



C3. ตอบคำถามต่อไปนี้



C3.1 How many HTTP GET request messages did your browser send? (ตอบจำนวนของ packet และ หมายเลข packet)

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

.....

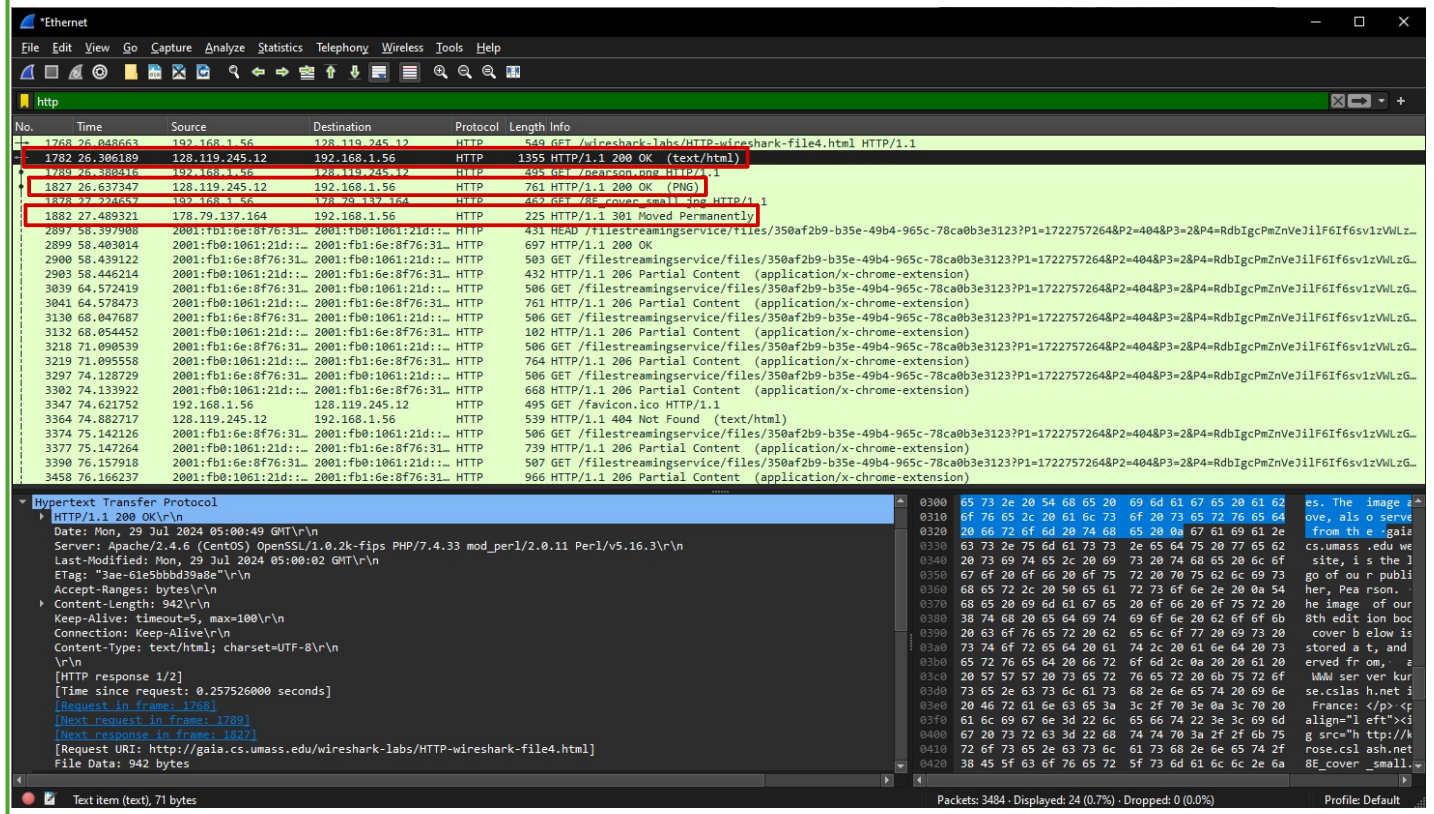
C3.2 To which Internet addresses were these GET requests sent?

(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?

โหลดแบบ Serially ทีละรูป

C4.3 Explain

Download โดยรอแต่ละอันเสร็จก่อน เพราะถ้าโหลดพร้อมกันต้องส่ง Request ไปพร้อมกัน แต่อันนี้รอ Response จากรูปแรกก่อนถึงส่ง Request รูปถัดไป

C5. จงตอบคำถามต่อไปนี้

- นักศึกษาคิดว่านักศึกษาได้เรียนรู้อะไรจาก Exercise C นี้ (สรุปมาอย่างน้อย 2 Bullet)
  1. ได้เรียนรู้การทำงานของการโหลดรูปภาพที่ละรูปเวลาเข้าเว็บ
  2. เรียนรู้ 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

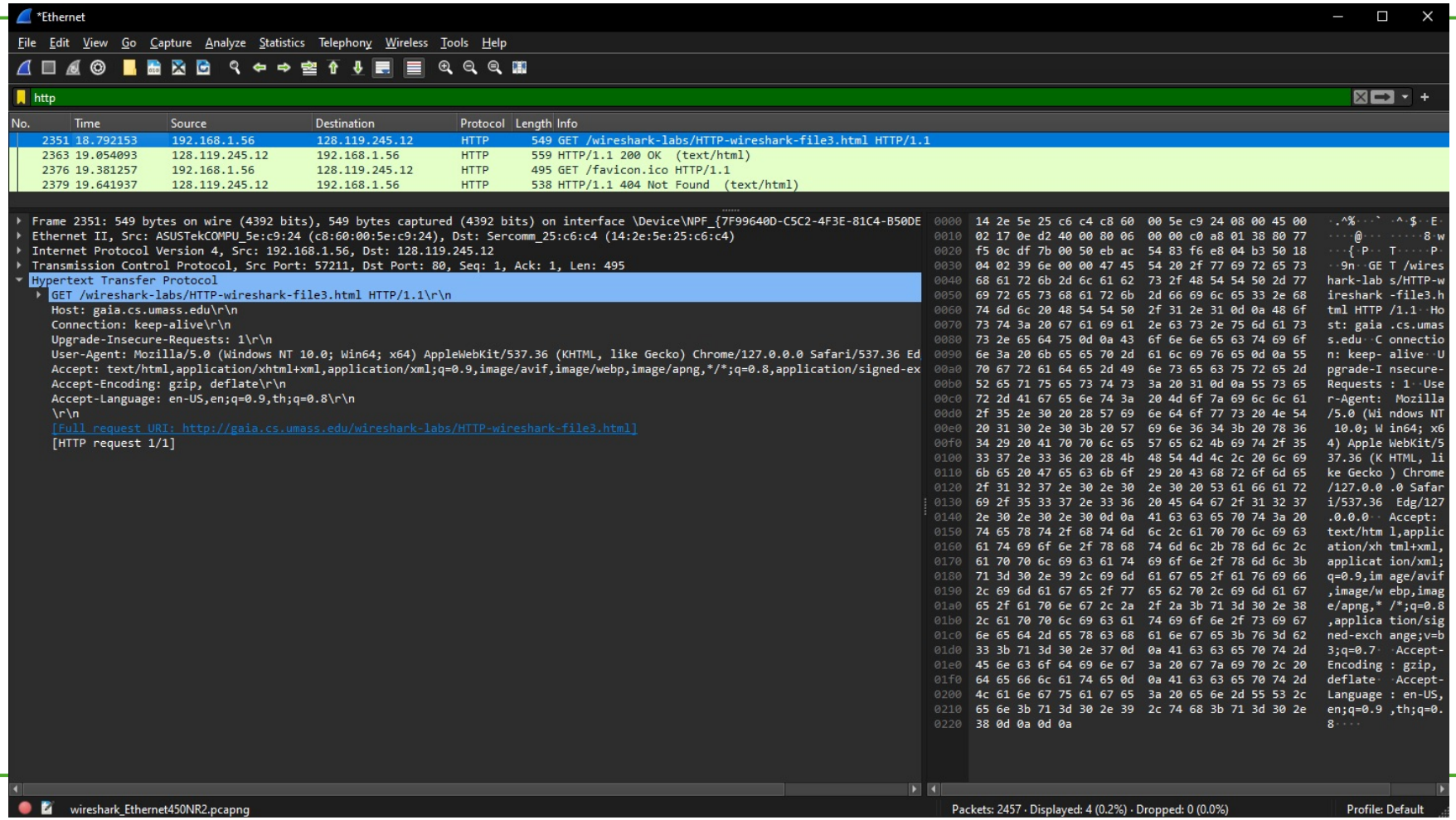
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

   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.

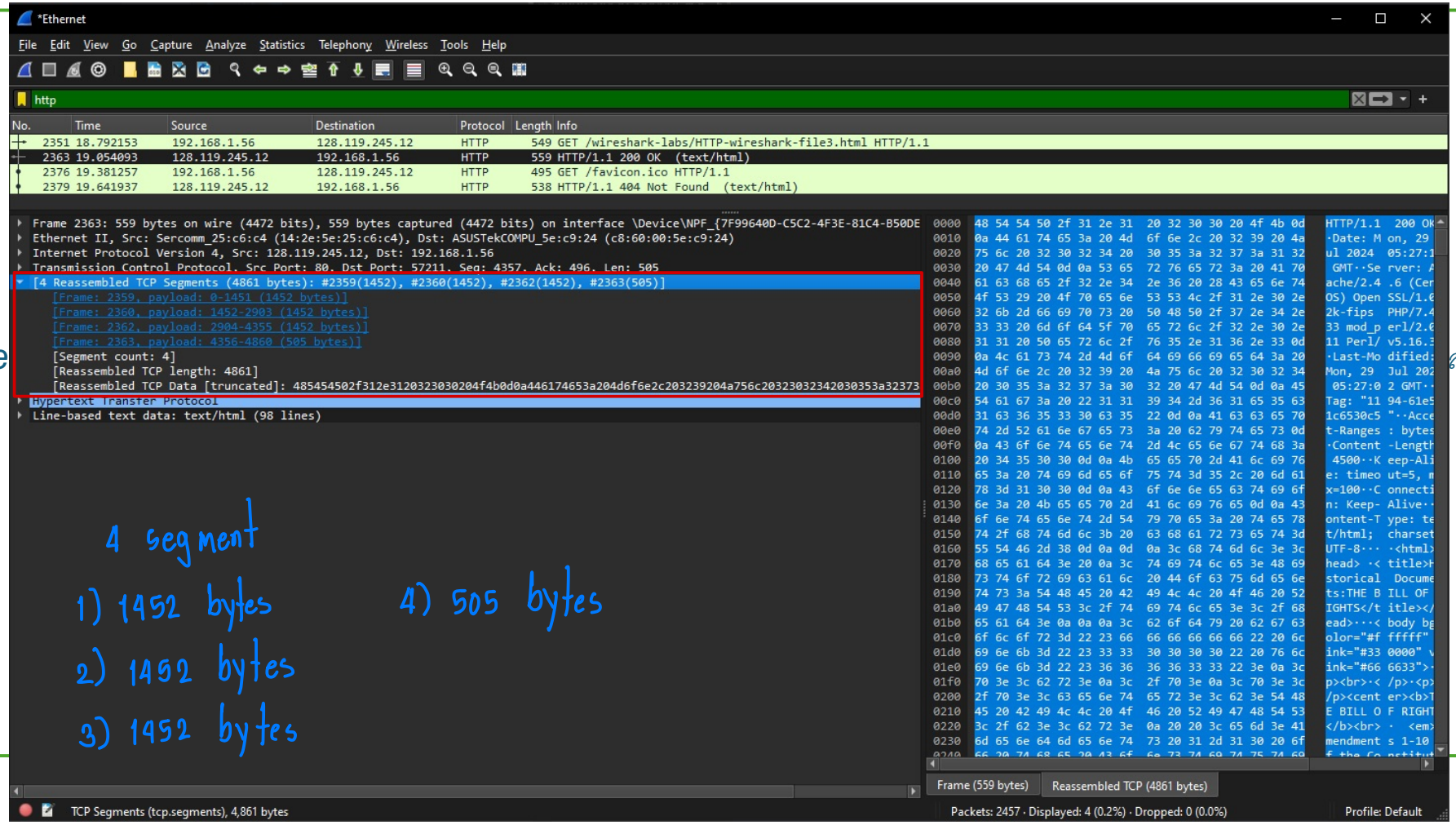
D1. อ่าน Paragraph ต่อไปนี้และทำความเข้าใจ

- 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 หน้าจอ Wireshark : HTTP Request ของ 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



แปะรูป Re ละ แต่ละ

D4. จงตอบคำถามต่อไปนี้

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

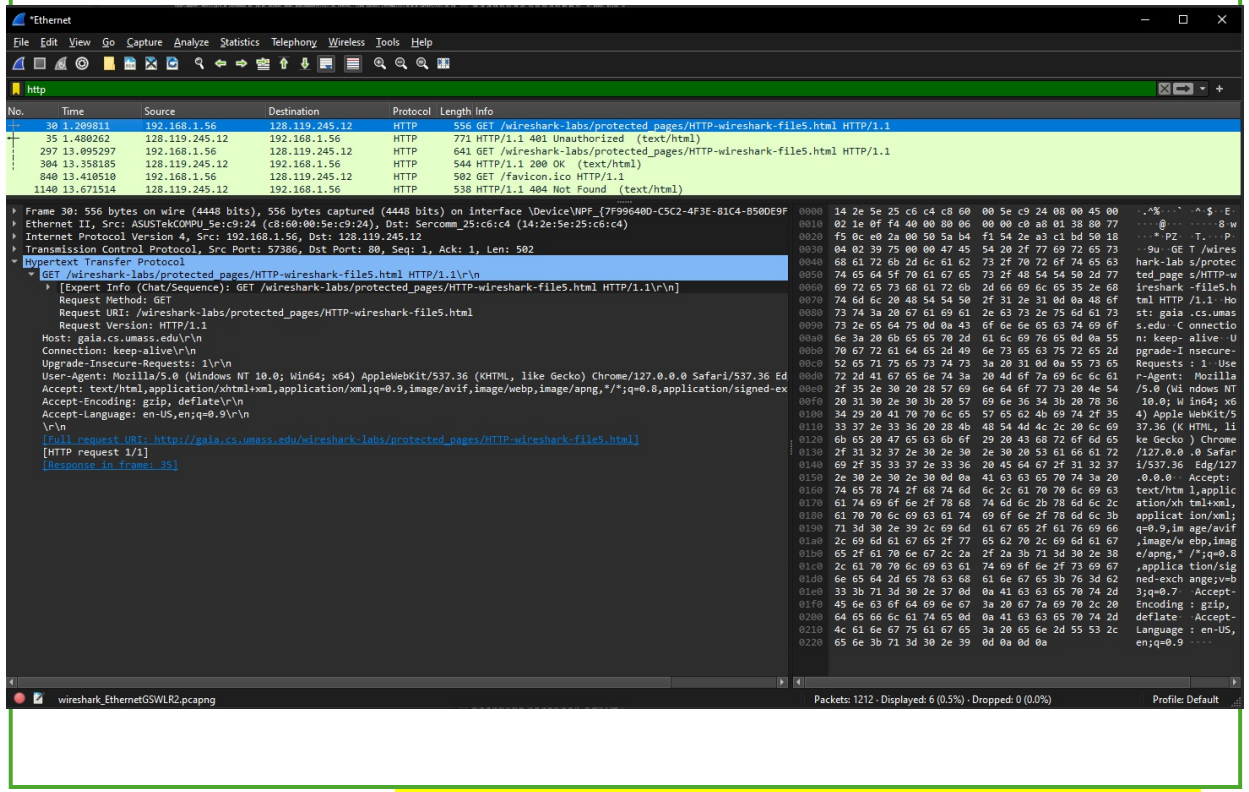
- นักศึกษาคิดว่านักศึกษาได้เรียนรู้อะไรจาก Exercise D นี้ (สรุปมาอย่างน้อย 2 Bullet)
  1. เรียนรู้เกี่ยวกับ TCP segment
  2. เรียนรู้การหา TCP segment ใน Wireshark
  3.
  4.

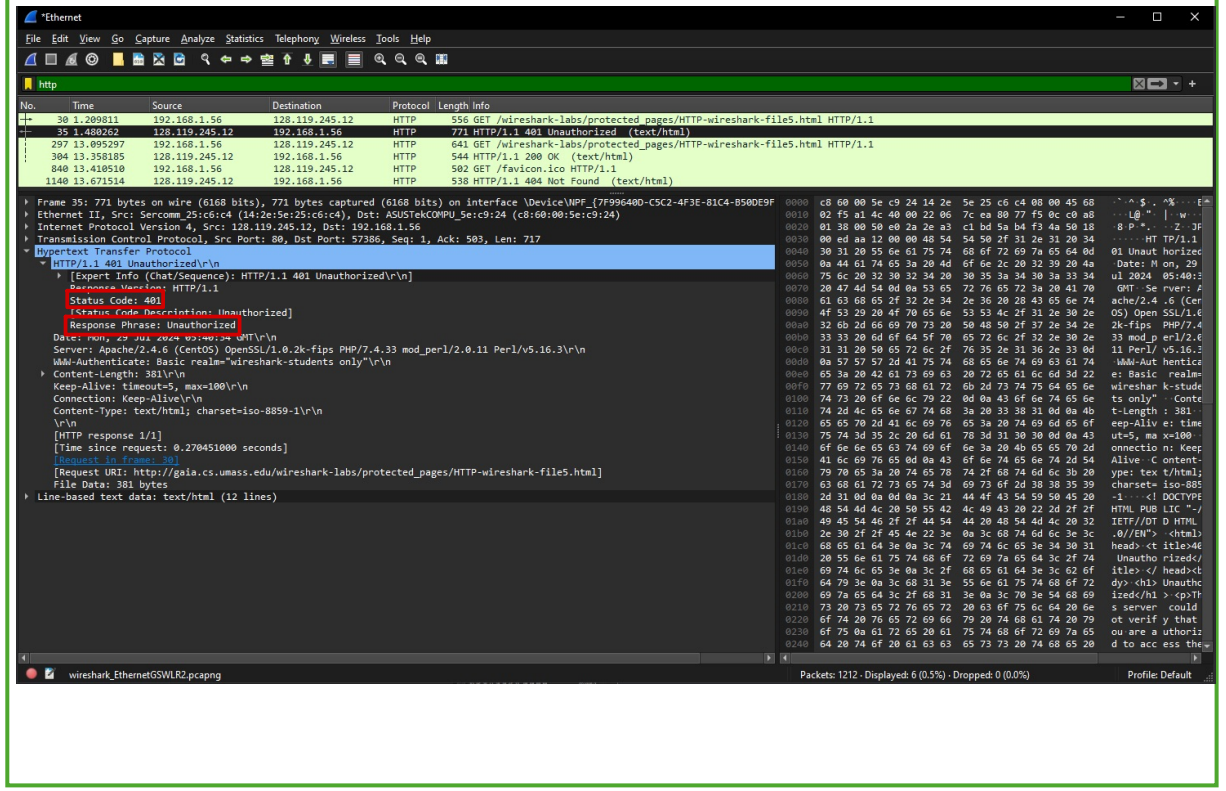
E1. HTTP Authentication

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
   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.

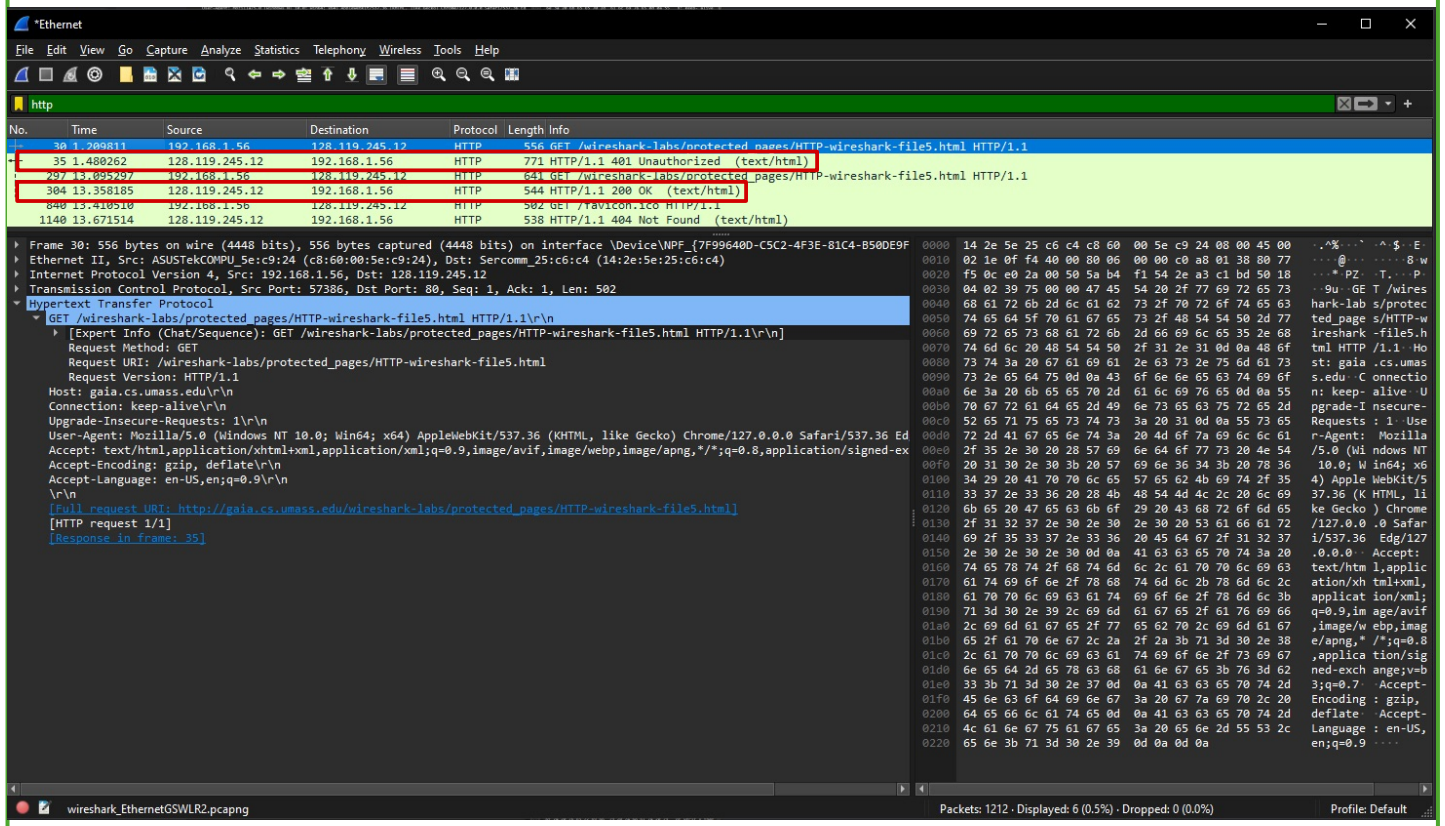
E2. Capture หน้าจอ Wireshark : HTTP Get Packet แรก และ Response ของ Get Packet นี้ และตอบคำถามข้อ E2.1





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



C4.1 *Response packet no. ของ Get แรก คือ* 35

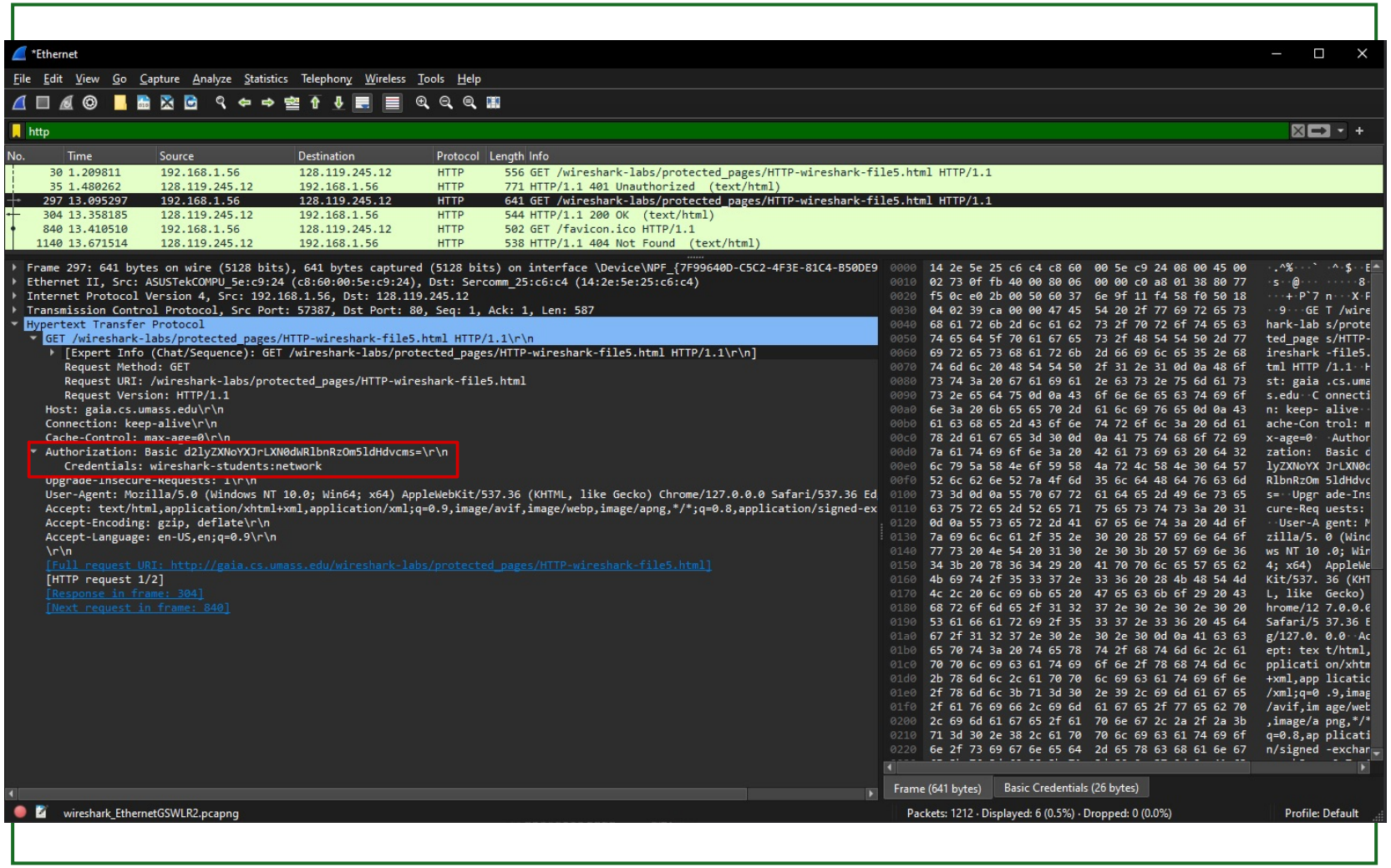
Response packet no. ของ Get ที่สองคือ 304

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 นักศึกษาคิดว่าจาก Capture Password ที่ได้ จาก http get message Hacker จะสามารถหา password นี้ได้หรือไม่

ได้

E4. Extracting the plaintext password

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

สามารถดูได้จาก Credentials ที่อยู่ใน Authorization field โดย format จะเป็น Username ตามด้วย : ตามด้วย Password (Username : Password)

E5. จงตอบคำถามต่อไปนี้

- นักศึกษาคิดว่านักศึกษาได้เรียนรู้อะไรจาก Exercise Eนี้ (สรุปมาอย่างน้อย 3 Bullet)
  1. เรียนรู้ว่า Hacker สามารถถอดรหัสเราได้
  2. เรียนรู้ Status Code 401
  3. เรียนรู้การทำ Plaintext Password
  4.