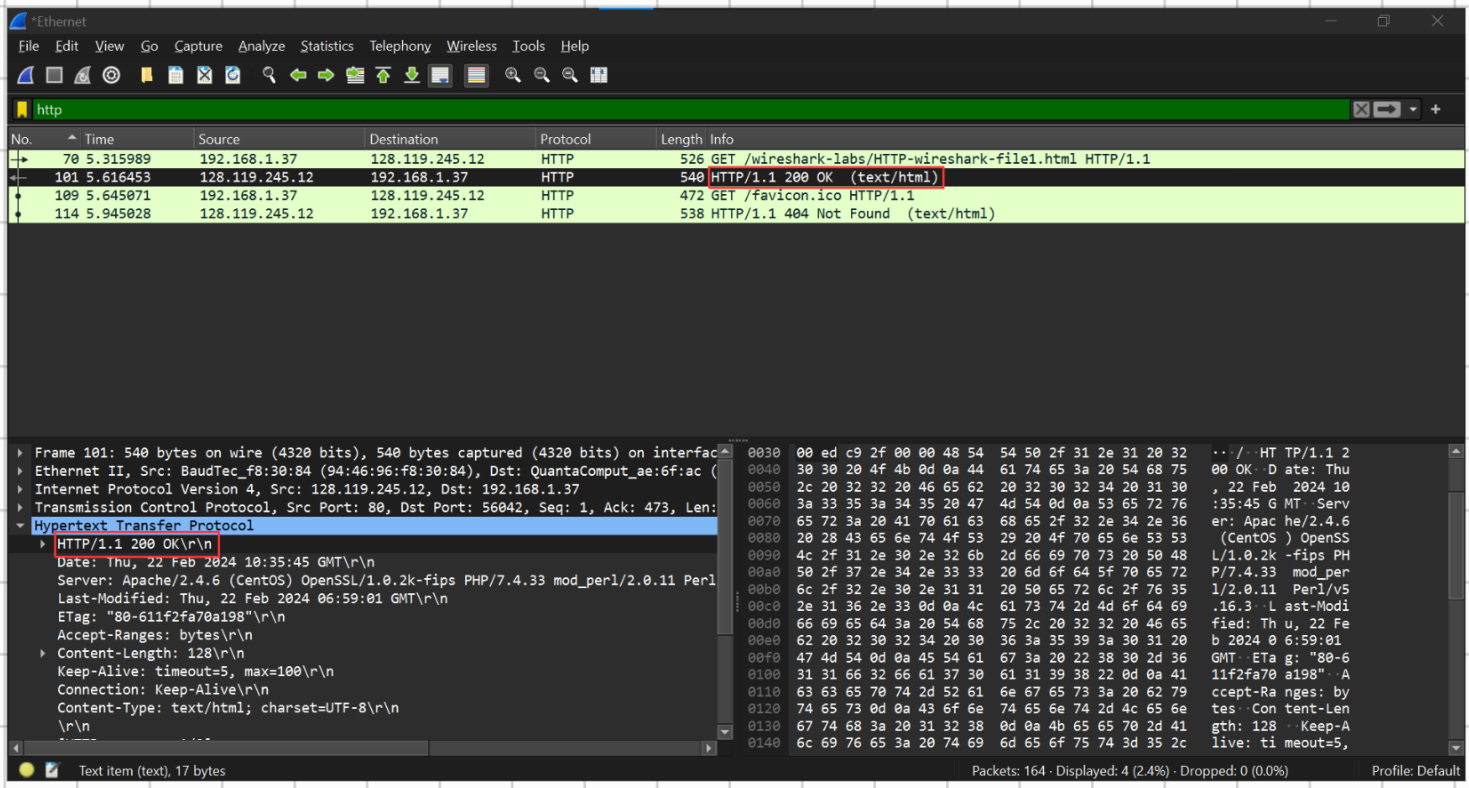
Wireshark Lab 01: HTTP

Section 650001

Group ID : G02

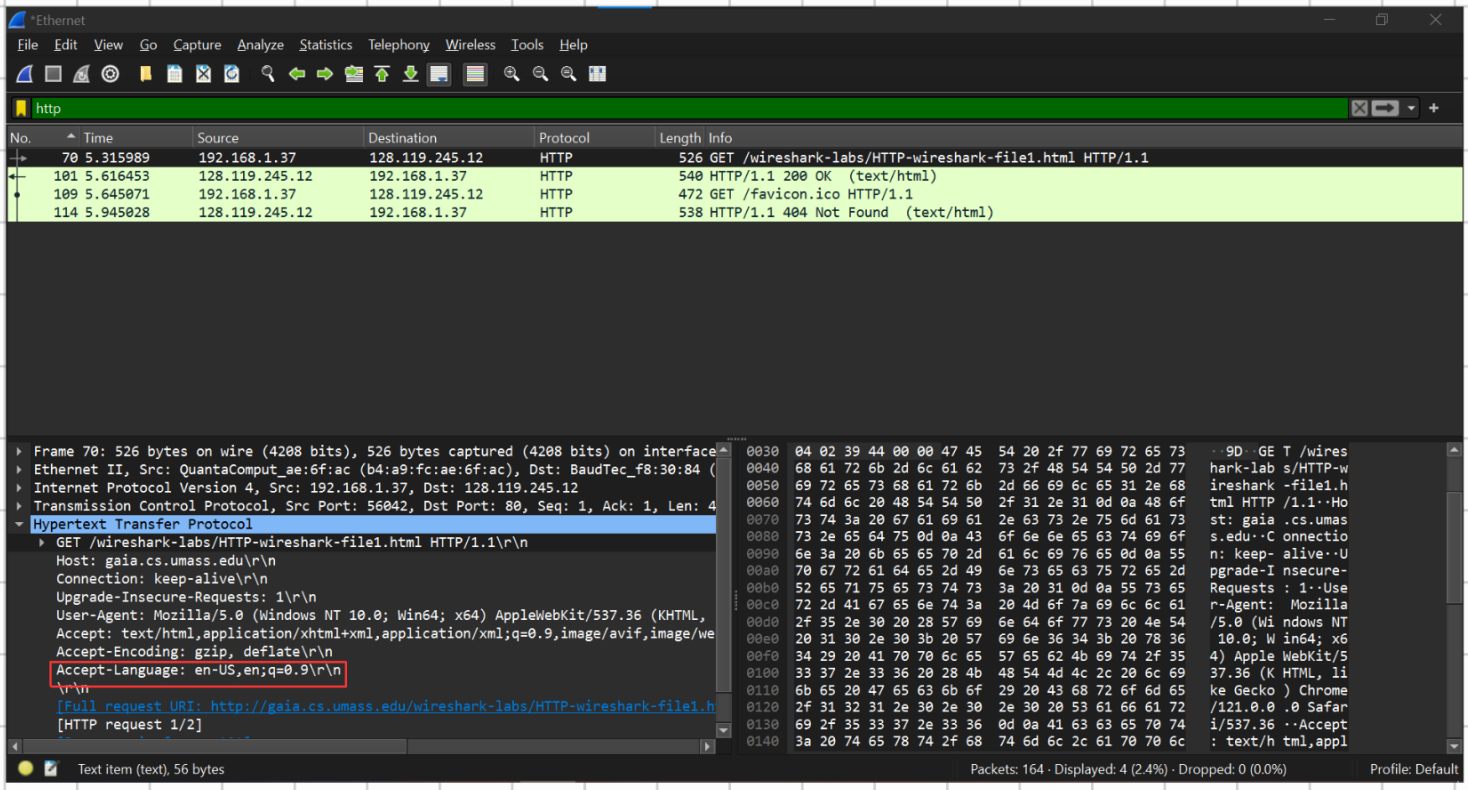
สมาชิกกลุ่ม
นายธีรภัทร เกิดไพบูลย์ 6509650468

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



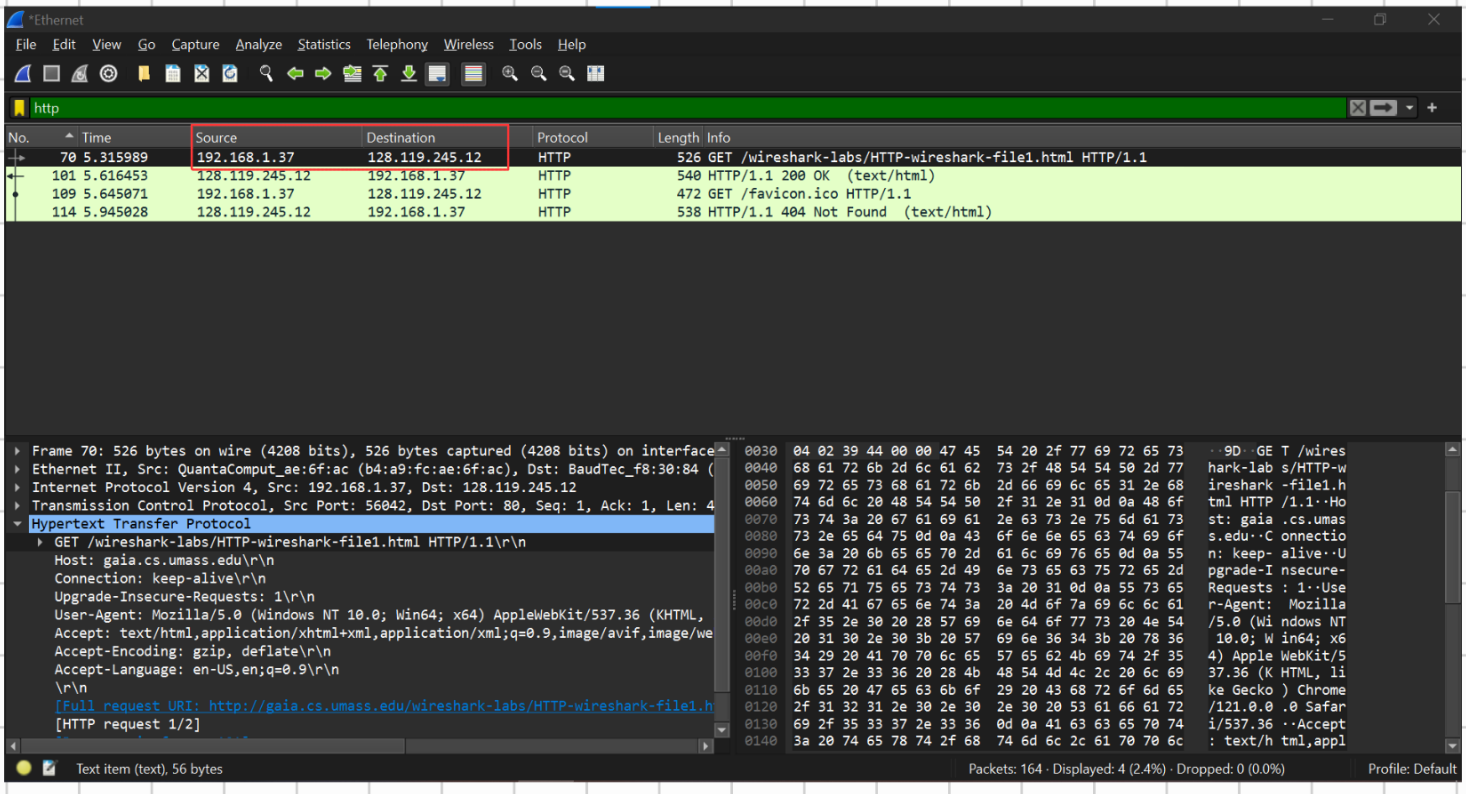
เวอร์ชันของ HTTP ที่รันบนเบราเซอร์ของนักศึกษา คือ 1.1
เวอร์ชันของ HTTP ที่รันบนเซิร์ฟเวอร์ คือ 1.1

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



เบราว์เซอร์ของนักศึกษาที่ใช้ระบุว่าจะยอมรับภาษาอังกฤษ-สหรัฐอเมริกา (English-US)และภาษาอังกฤษ (English)จากเซิร์ฟเวอร์

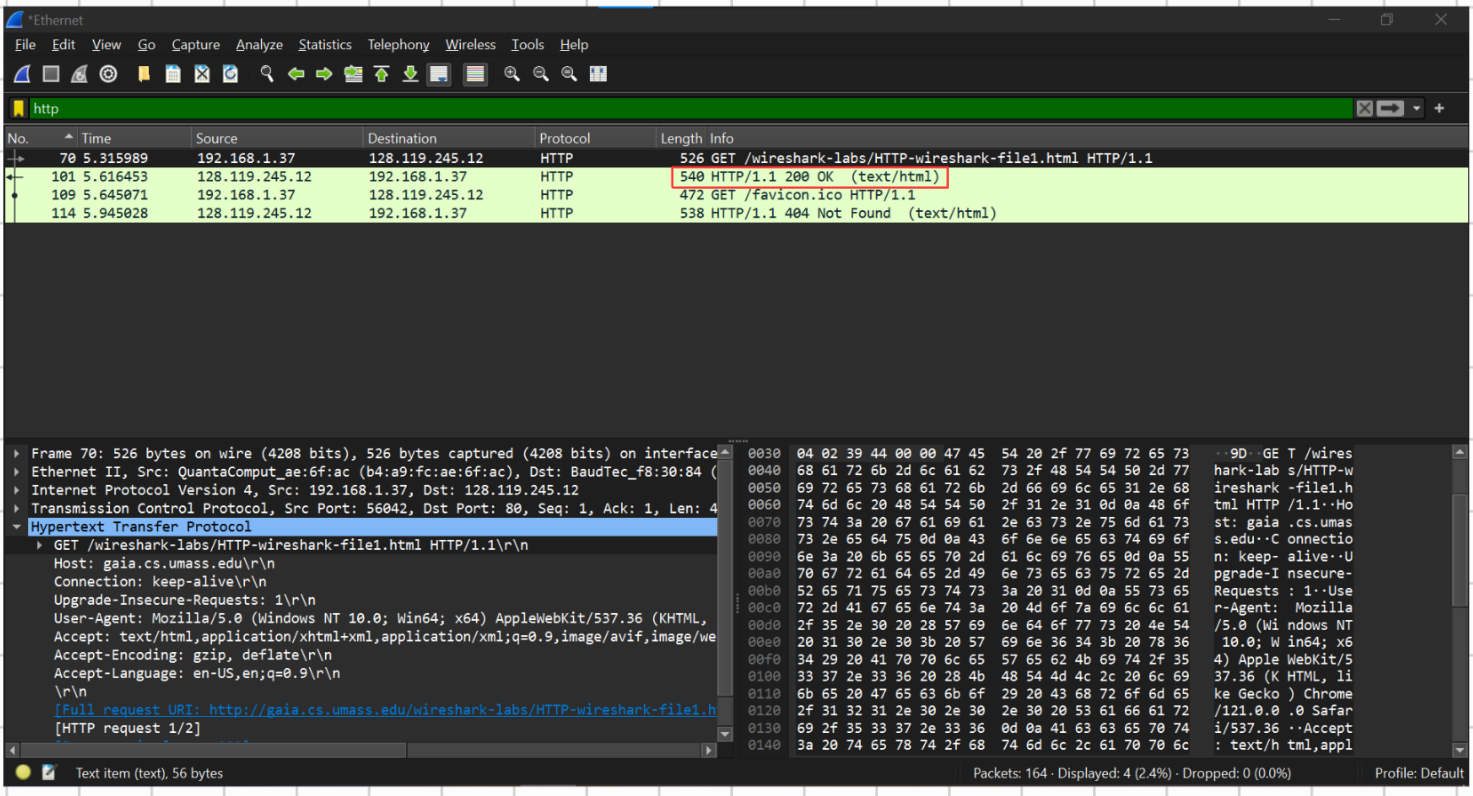
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?



IP address คอมพิวเตอร์ของนักศึกษา คือ 192.168.1.37

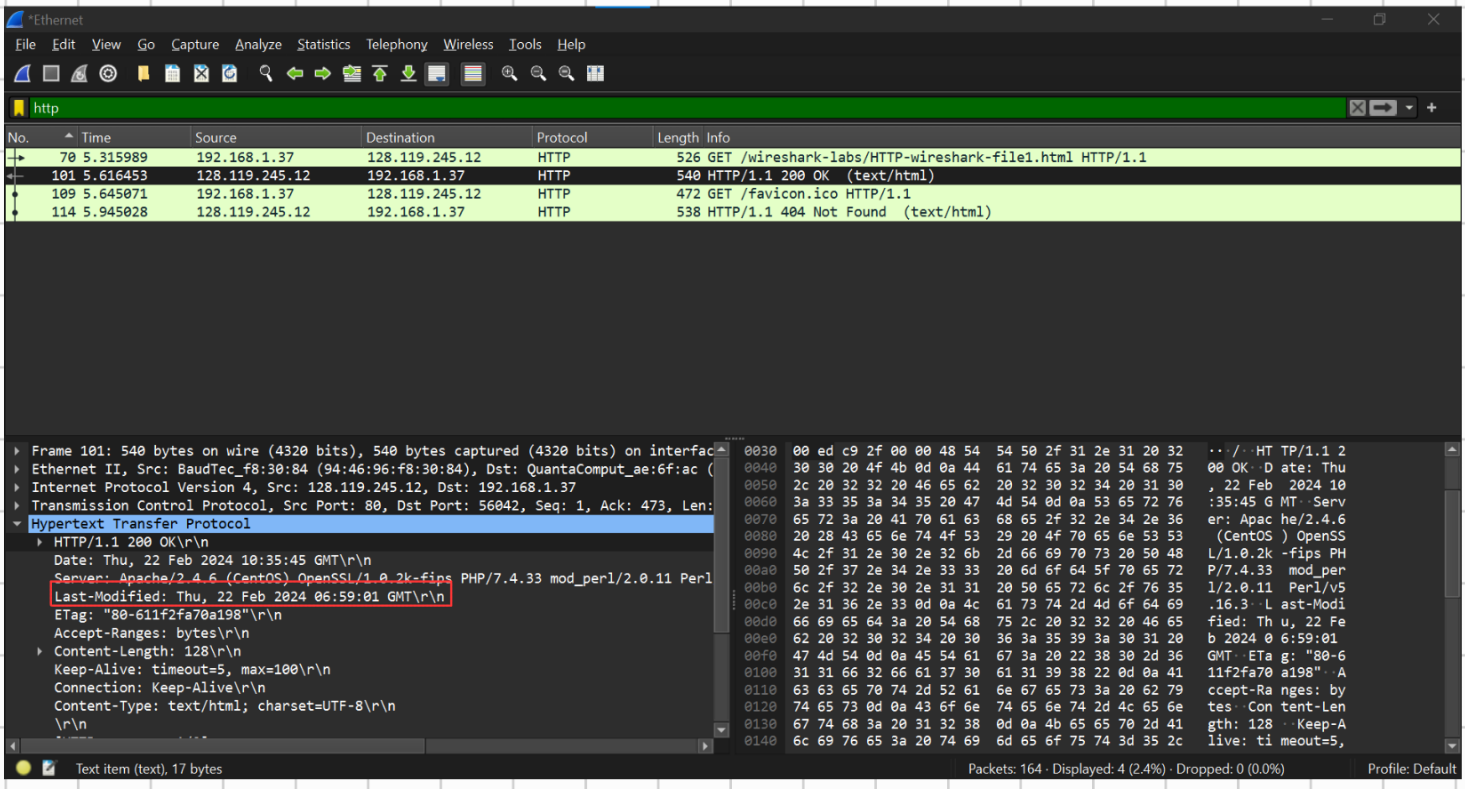
IP address ของเซิร์ฟเวอร์ คือ 128.119.245.12

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



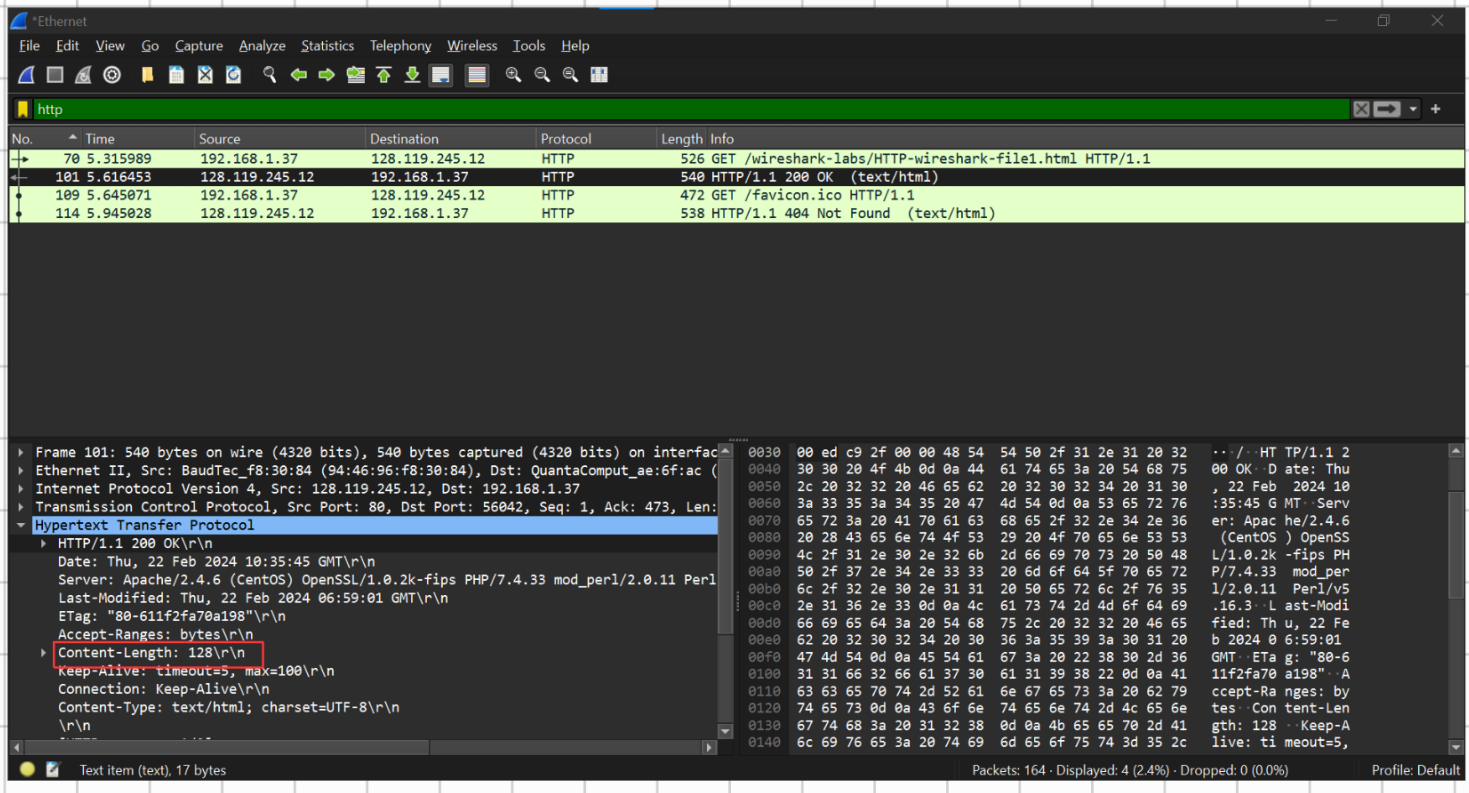
HTTP Status Code ที่ส่งคืนมาคือ 200 OK

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



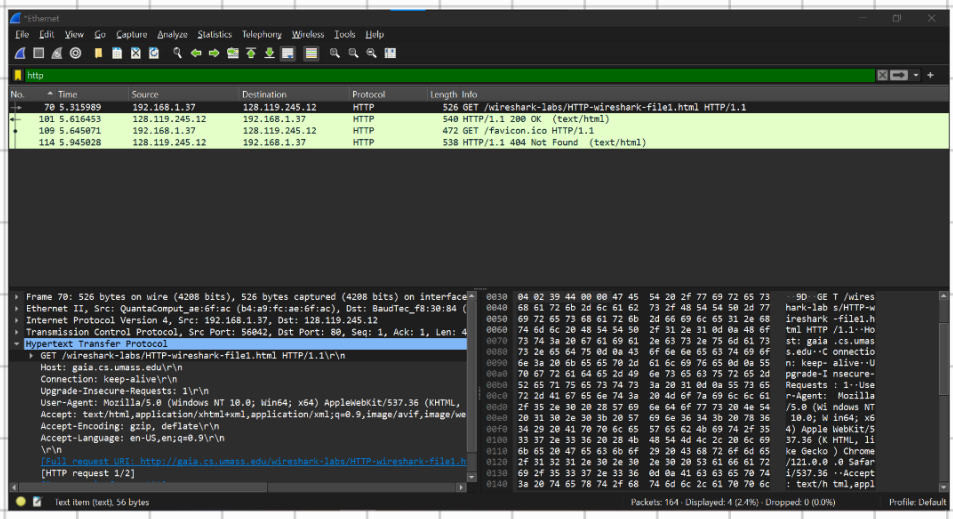
วันพฤหัสบดีที่ 22 กุมภาพันธ์ ค.ศ. 2024 เวลา 06:59:01 (Thu, 22 Feb 2024 06:59:01 GMT)

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

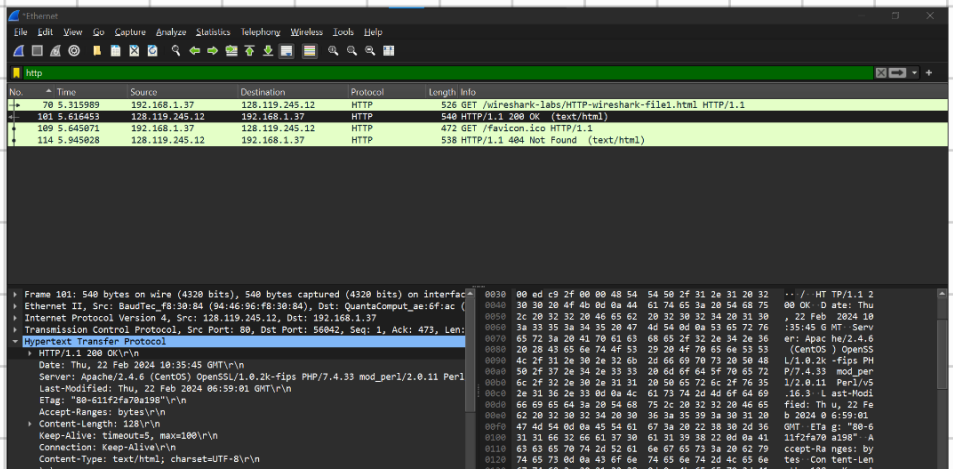


128 bytes

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.



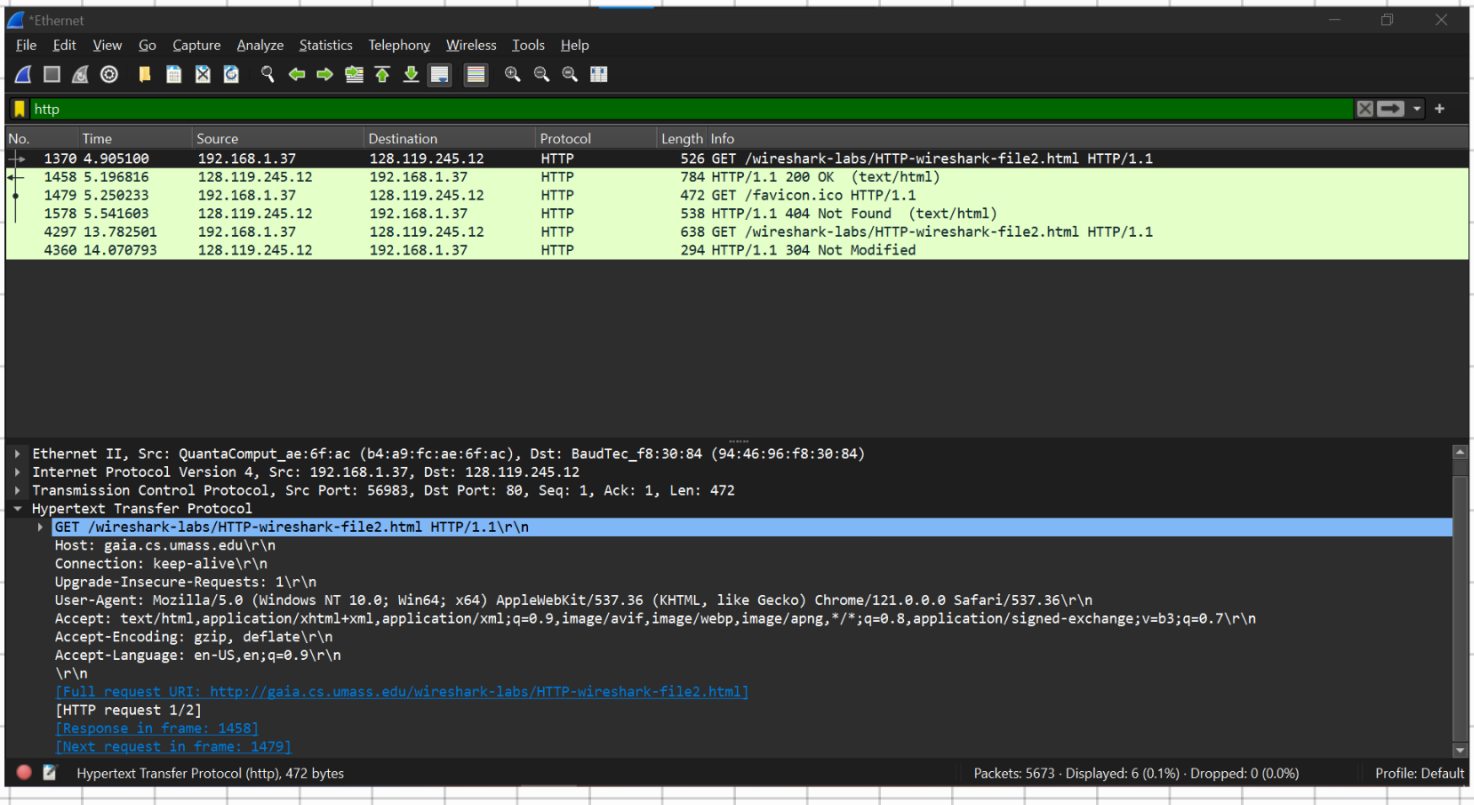
HTTP Request message



HTTP Response message

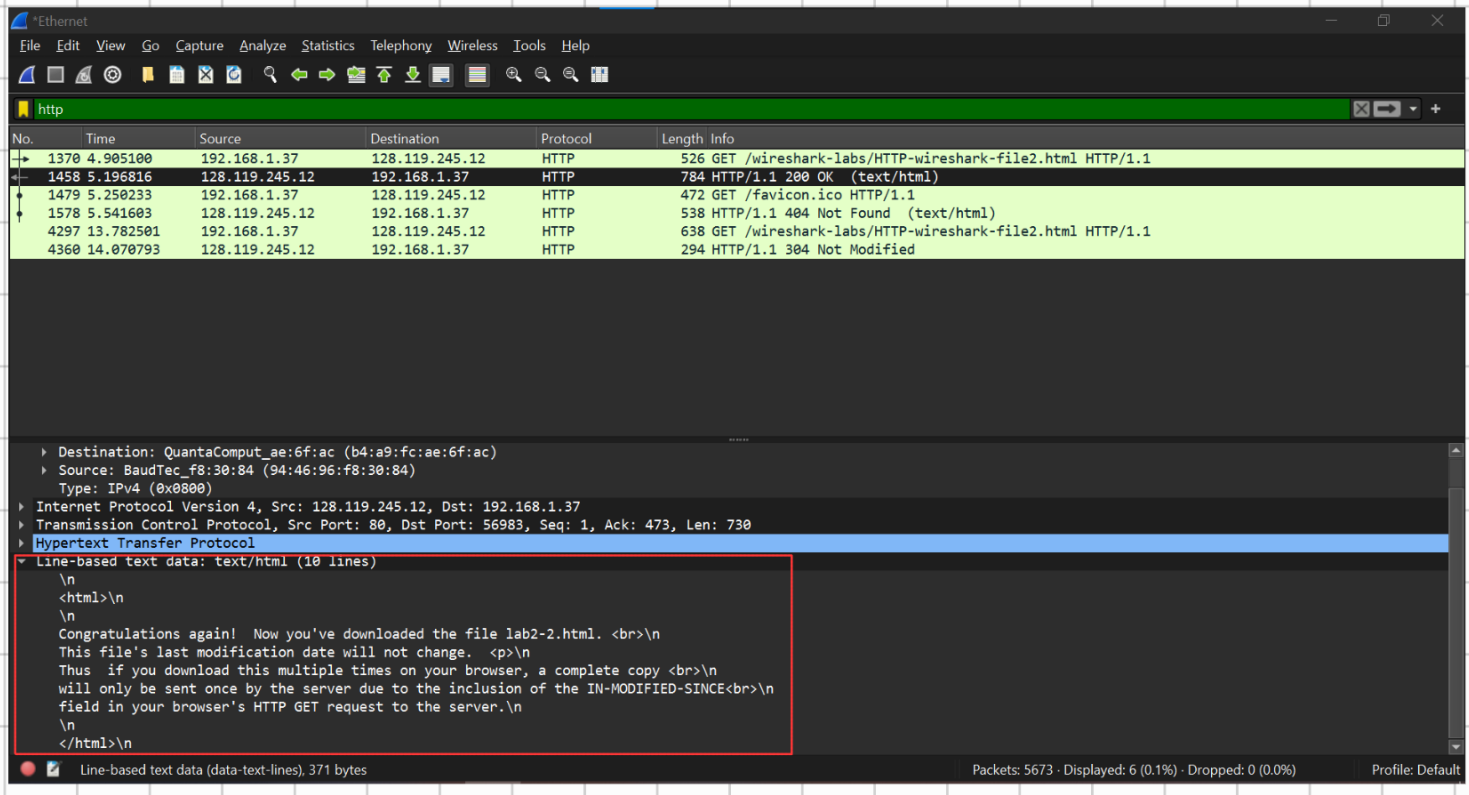
จากการเปรียบเทียบ packet content กับ packet list ของทั้งสอง packet (HTTP Request message และ HTTP Response message) ปรากฏว่าไม่พบความแตกต่างใด ๆ

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?



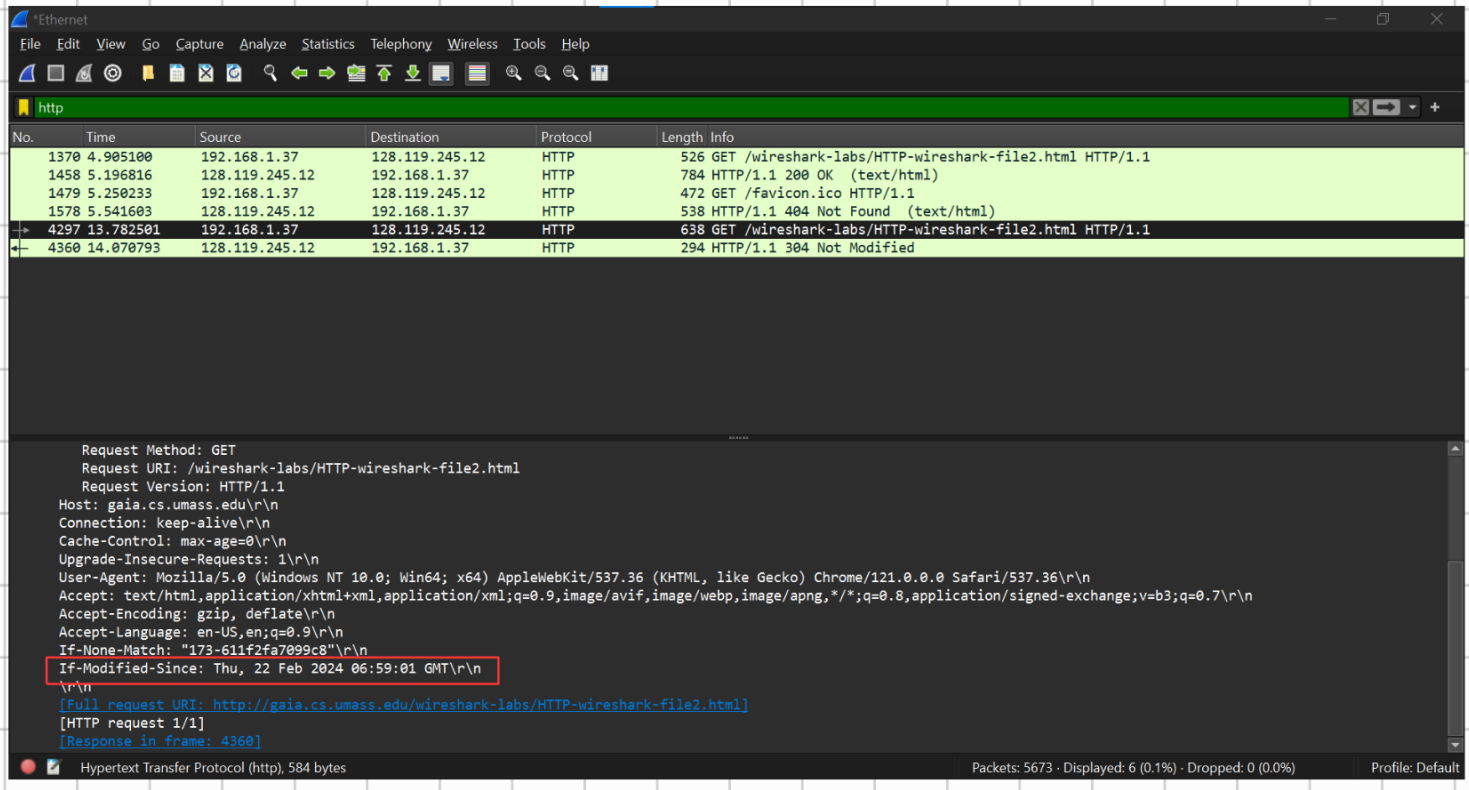
ไม่มีบรรทัด IF-MODIFIED-SINCE ใน HTTP GET ครั้งที่หนึ่ง

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



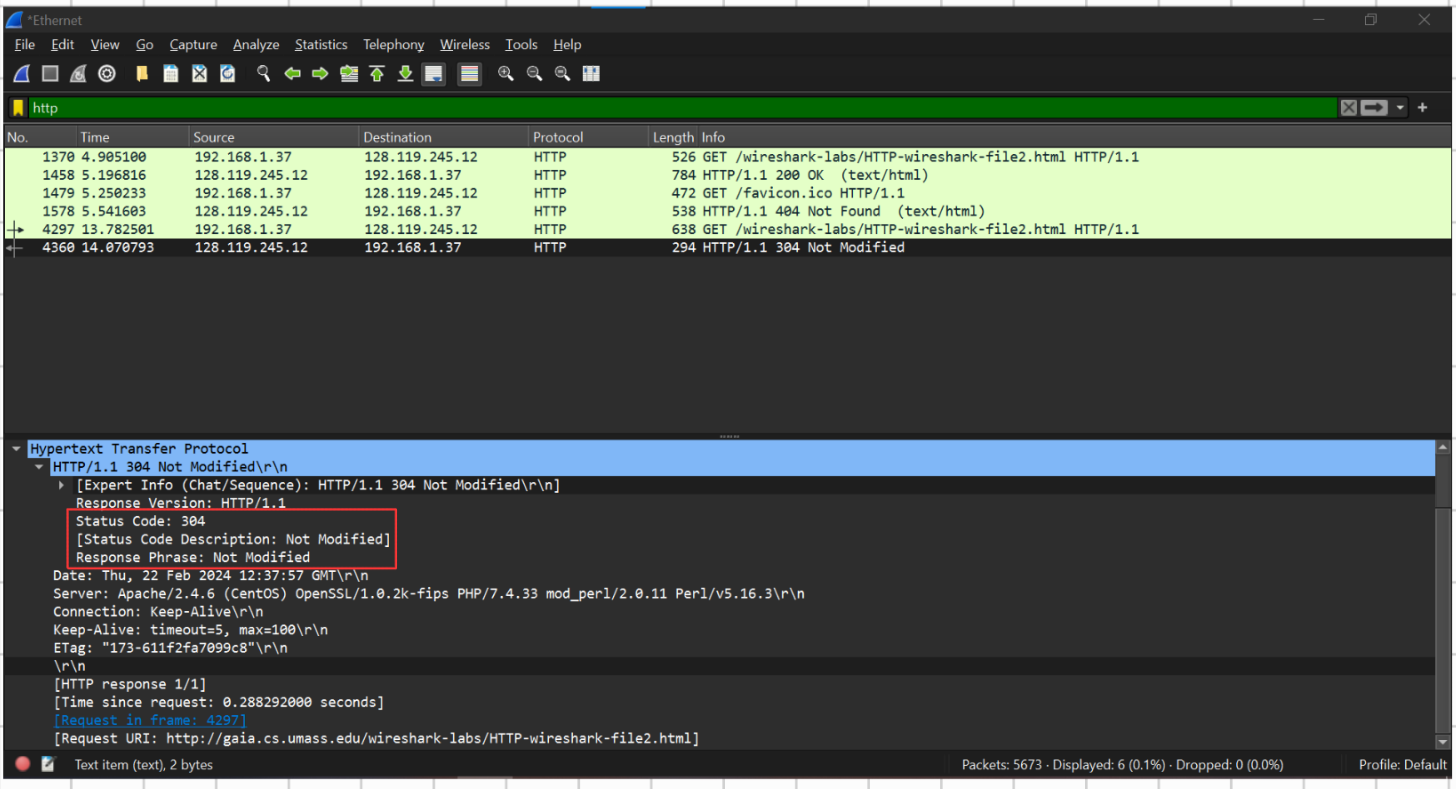
เซิร์ฟเวอร์ส่งคืนเนื้อหาของไฟล์อย่างชัดเจน ใน Wireshark มีส่วนที่เรียกว่า “Line-Based Text Data” ซึ่งจะแสดงสิ่งที่เซิร์ฟเวอร์ส่งกลับไปยังเบราว์เซอร์ของนักศึกษา ซึ่งเป็นสิ่งที่เว็บไซต์แสดงให้นักศึกษาเห็นเมื่อเปิดดูในเบราว์เซอร์ของนักศึกษา

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?

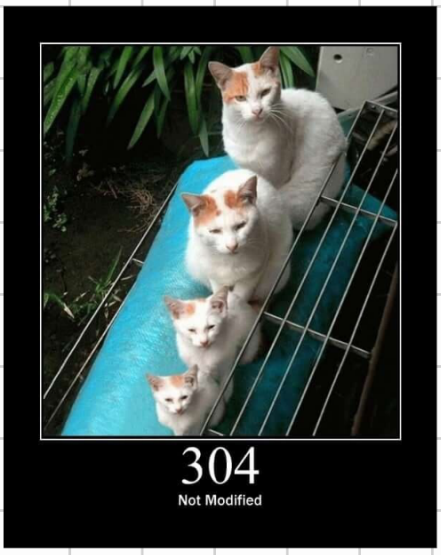


ใน HTTP GET Request ครั้งที่สองจะมีบรรทัด IF-MODIFIED-SINCE รวมอยู่ด้วย ข้อมูลที่แสดงคือวันที่และเวลาที่นักศึกษาเข้าดูหน้าเว็บครั้งล่าสุด

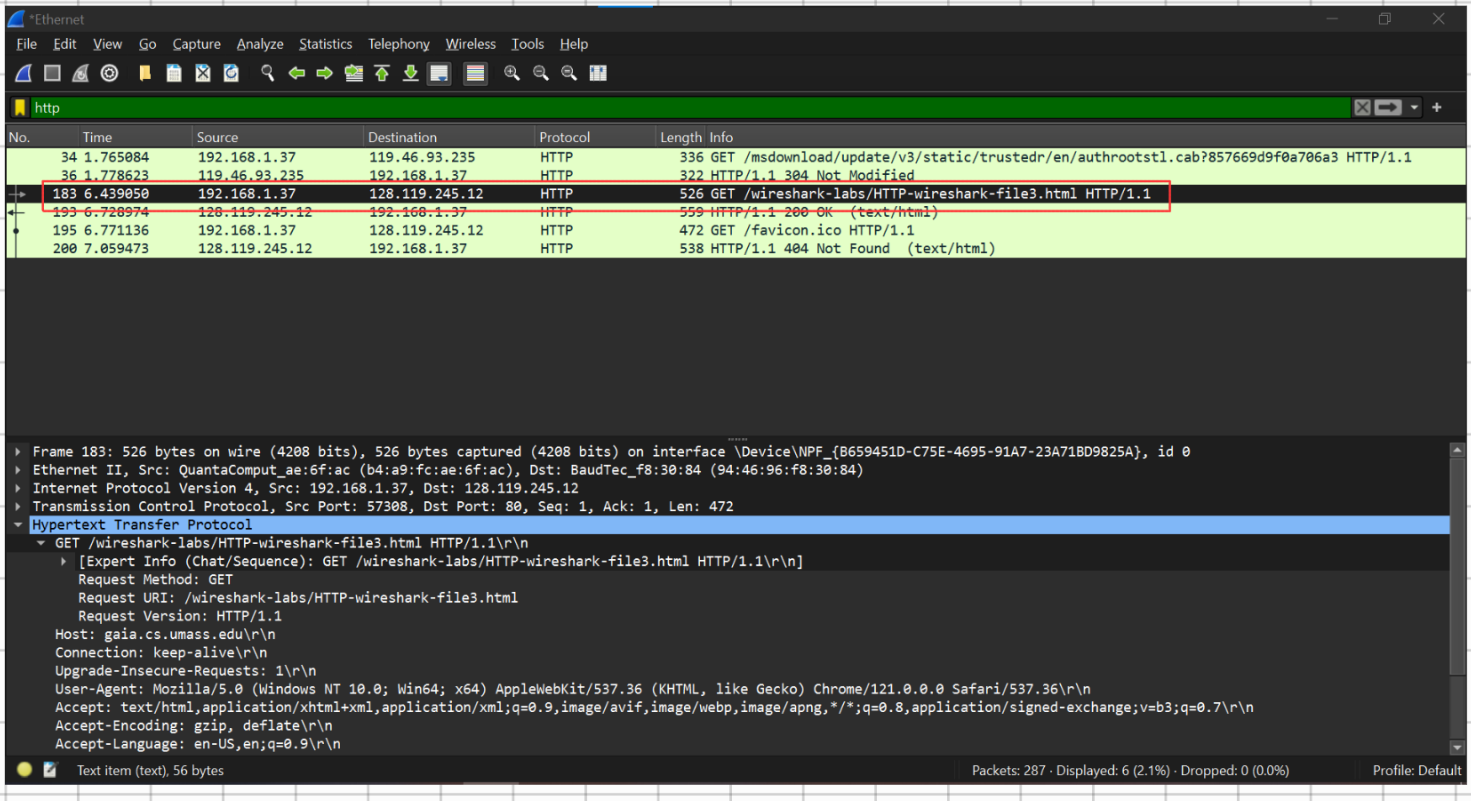
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.



HTTP Status Code และ phrase คือ “304 Not Modified” เซิร์ฟเวอร์ไม่ได้ส่งคืนเนื้อหาของไฟล์ เบราว์เซอร์เพียงแค่ดึงเนื้อหาจากแคช และสังเกตได้ว่าใน Wireshark ไม่ปรากฏบรรทัด "Line-based text data" ของ HTTP Status Code 304

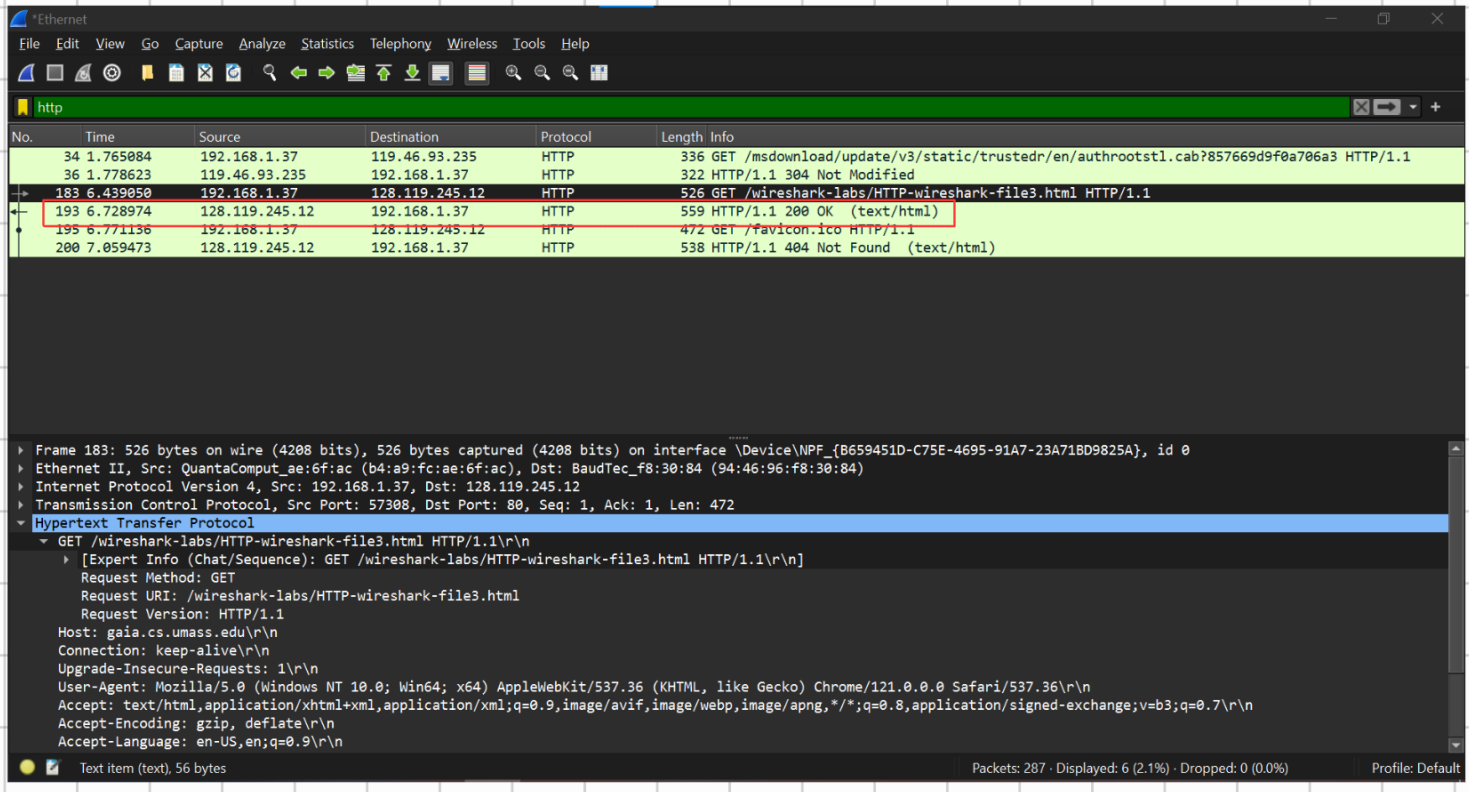


12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?



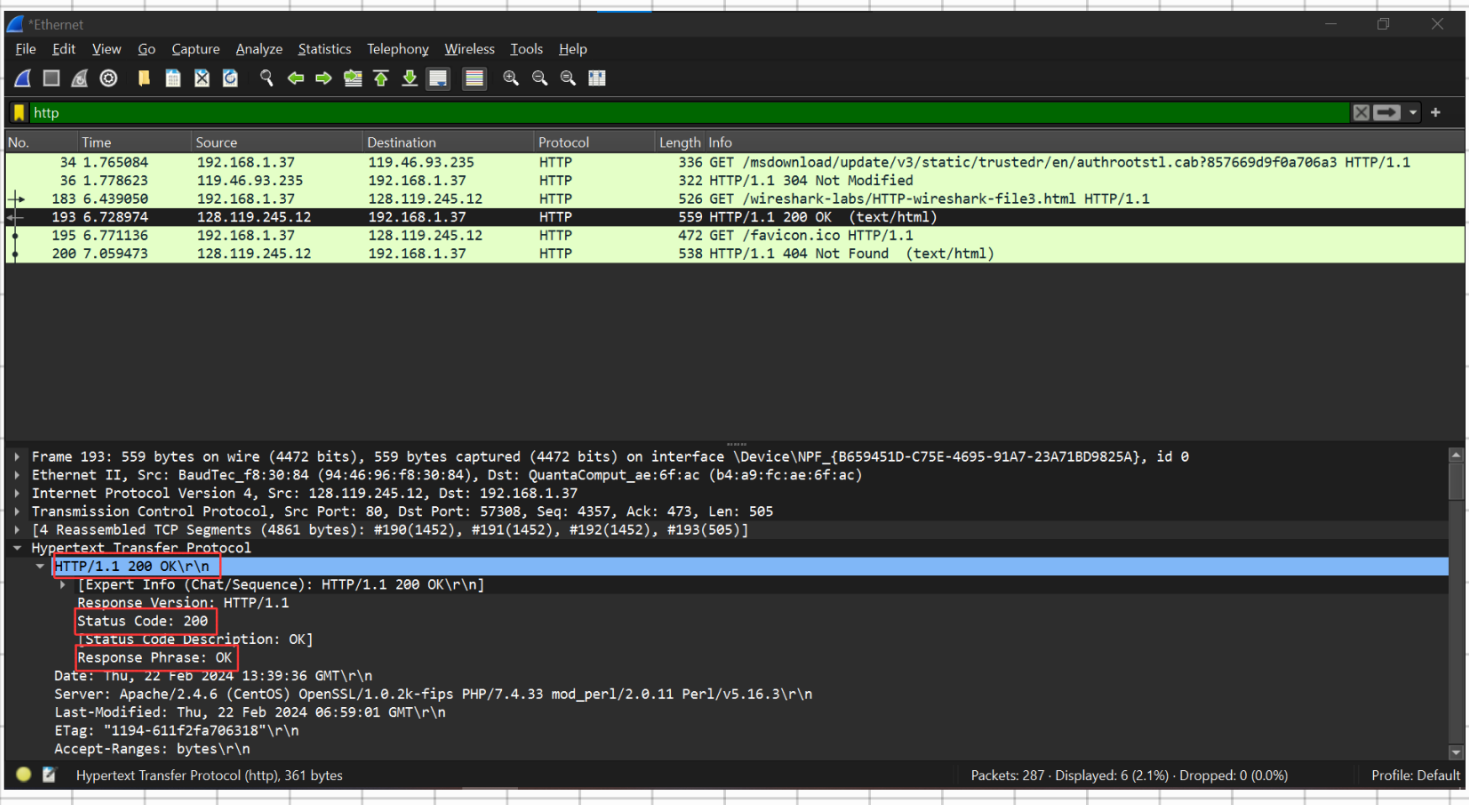
เบราว์เซอร์ของนักศึกษาส่ง HTTP GET Request เพียง 1 รายการไปยังเซิร์ฟเวอร์
แพ็กเก็ตที่มีข้อความ GET คือ แพ็กเก็ตหมายเลข 183

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



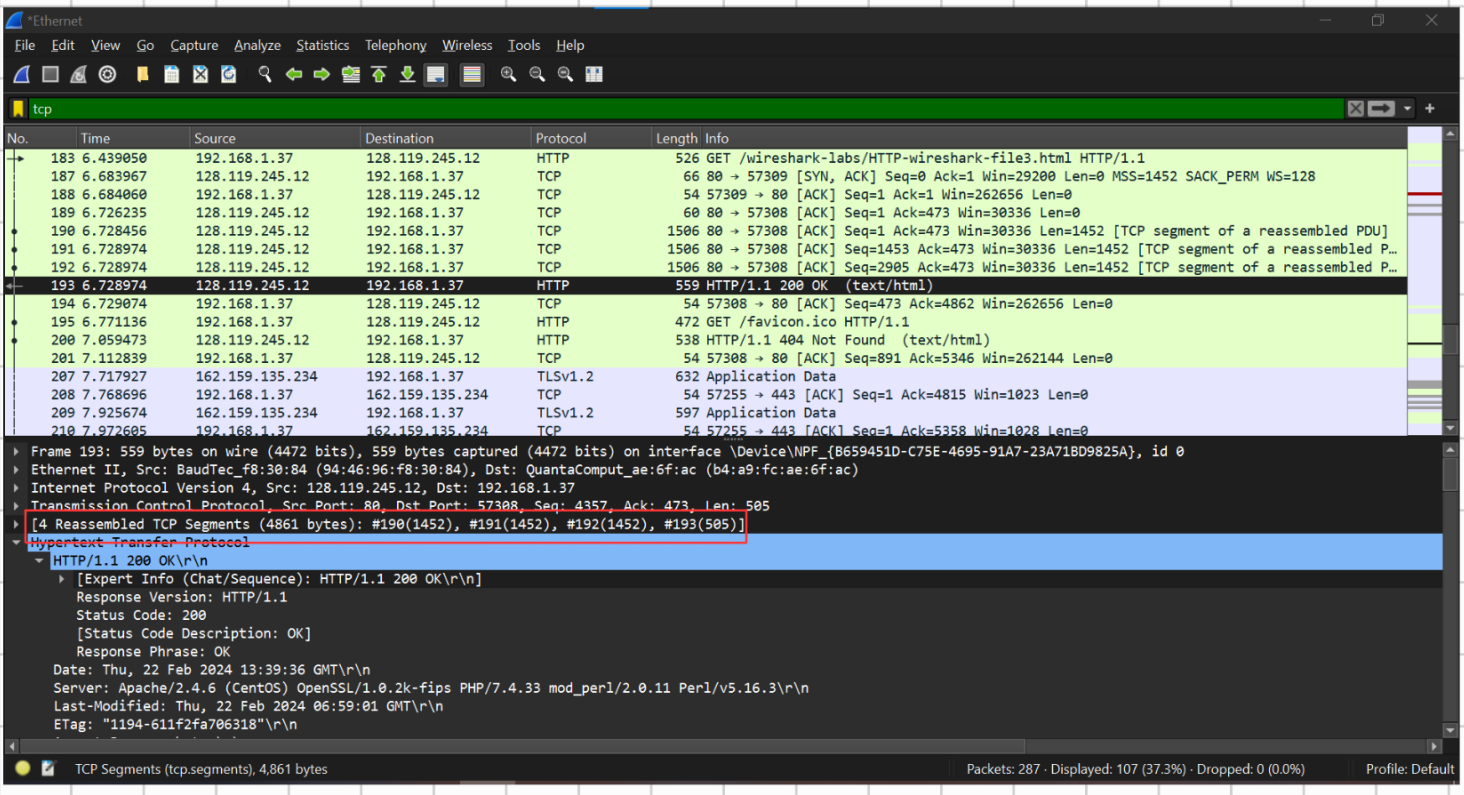
แพ็กเก็ตหมายเลข 193

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



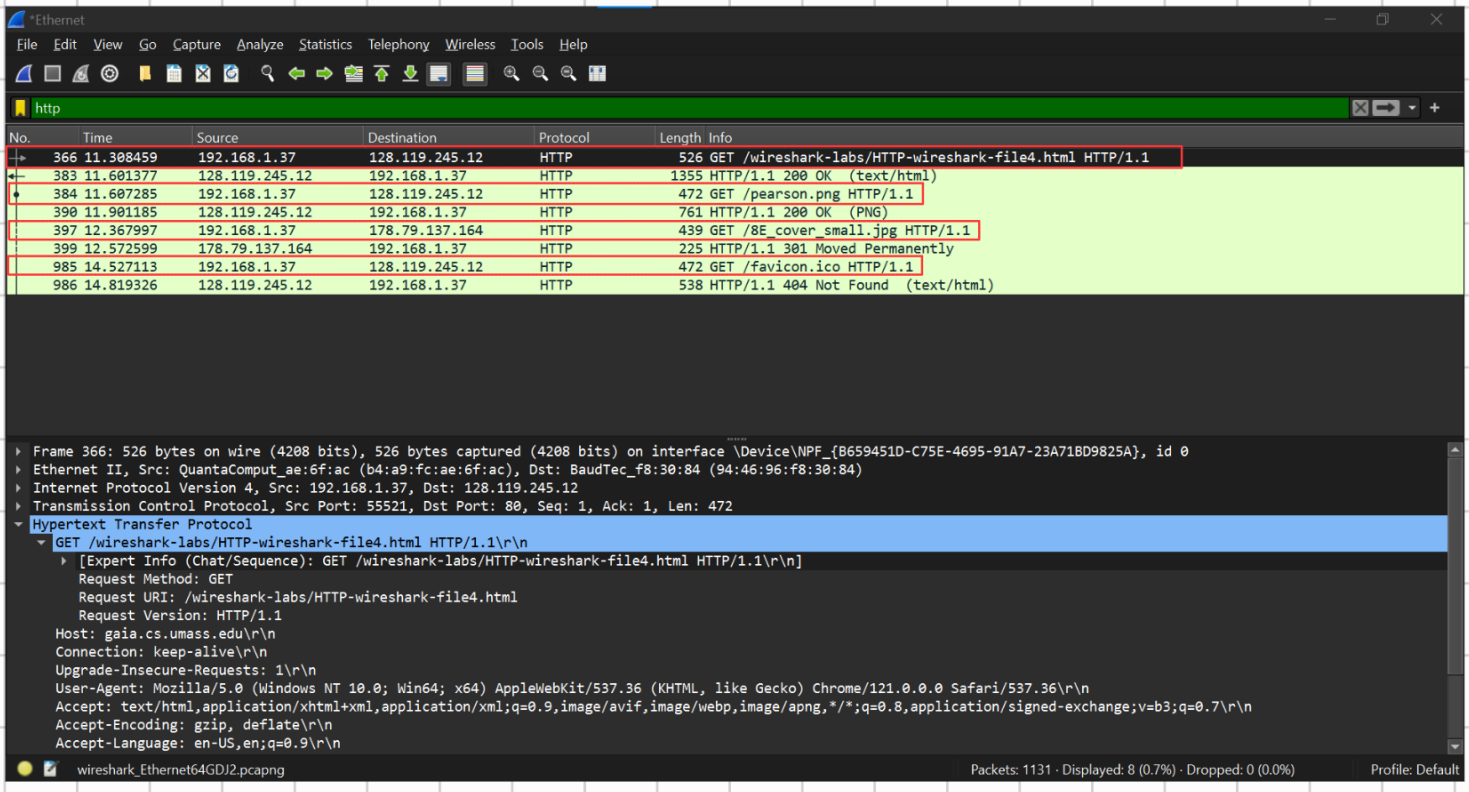
Status Code และ Phrase คือ 200 OK

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 (ได้แก่แพ็กเก็ตหมายเลข 190, 191, 192, 193)

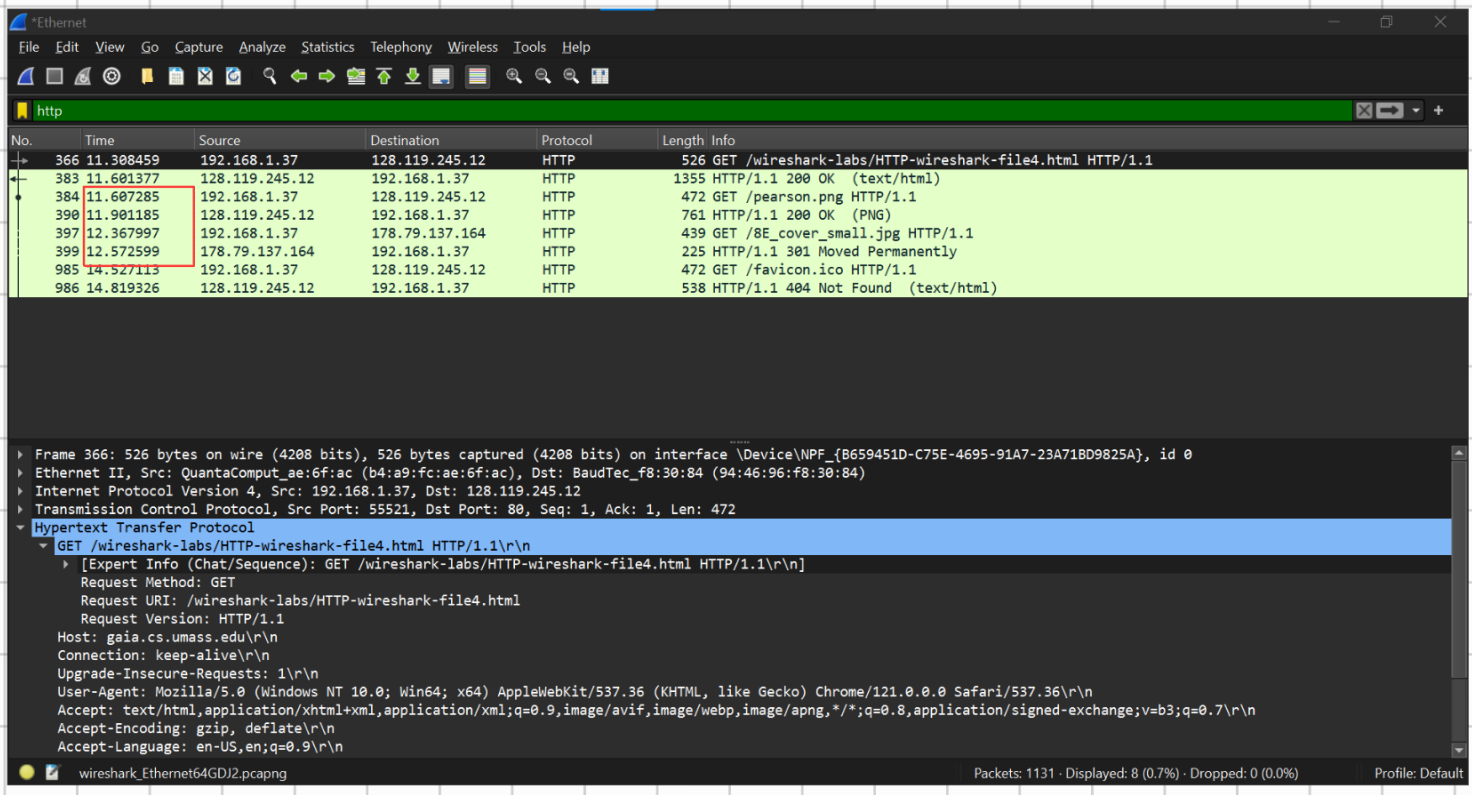
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?



4 แพ็กเก็ต โดยแต่ละแพ็กเก็ตส่ง GET Request ไปตาม Internet addresses ดังต่อไปนี้

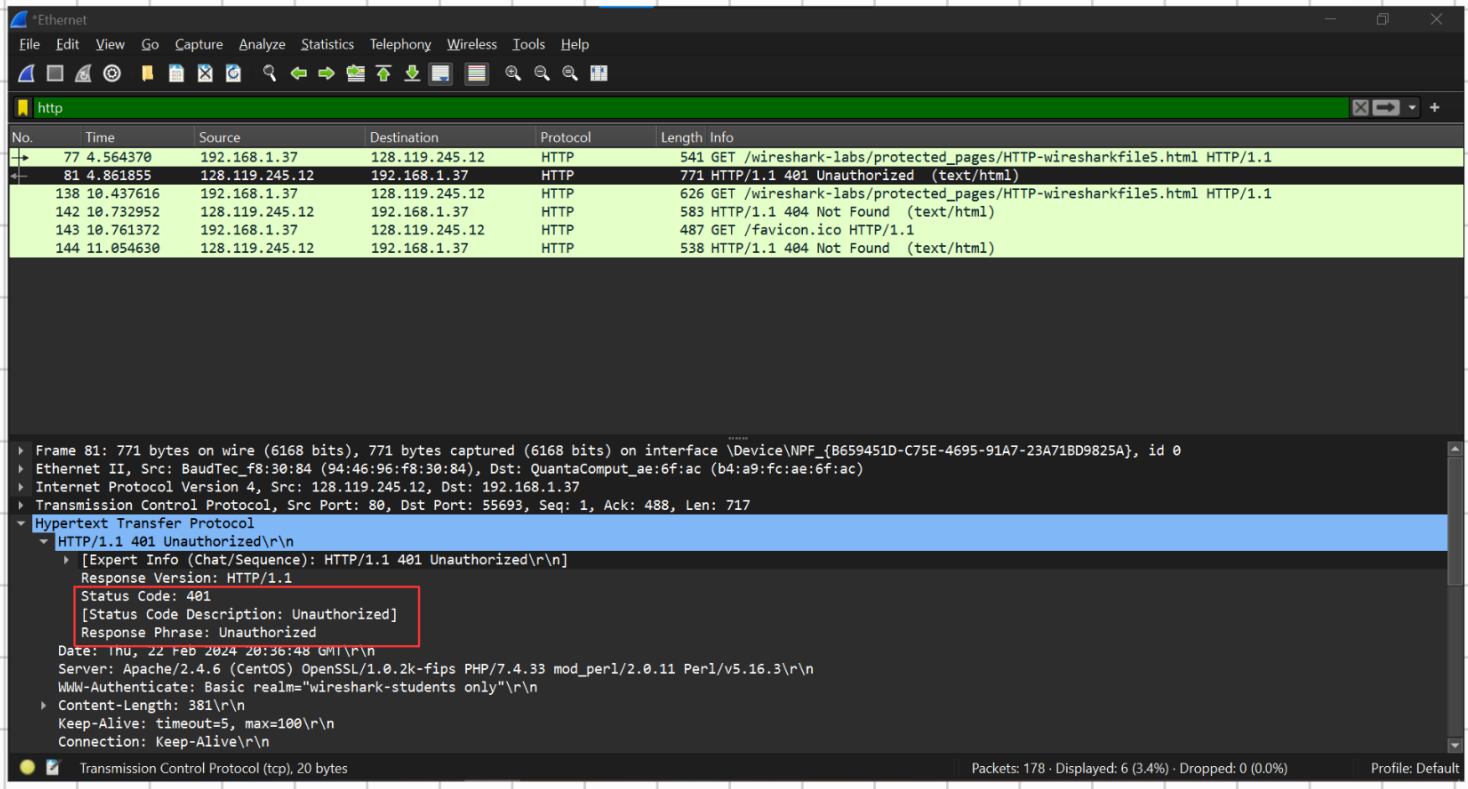
- แพ็กเก็ตหมายเลข 366 ส่งไปที่ 128.119.245.12 (HTTP-wireshark-file4.html) (Base file)
- แพ็กเก็ตหมายเลข 384 ส่งไปที่ 128.119.245.12 (pearson.png) (Pearson Logo)
- แพ็กเก็ตหมายเลข 397 ส่งไปที่ 178.79.137.164 (8E_cover_small.jpg) (the 8th edition book cover)
- แพ็กเก็ตหมายเลข 985 ส่งไปที่ 128.119.245.12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



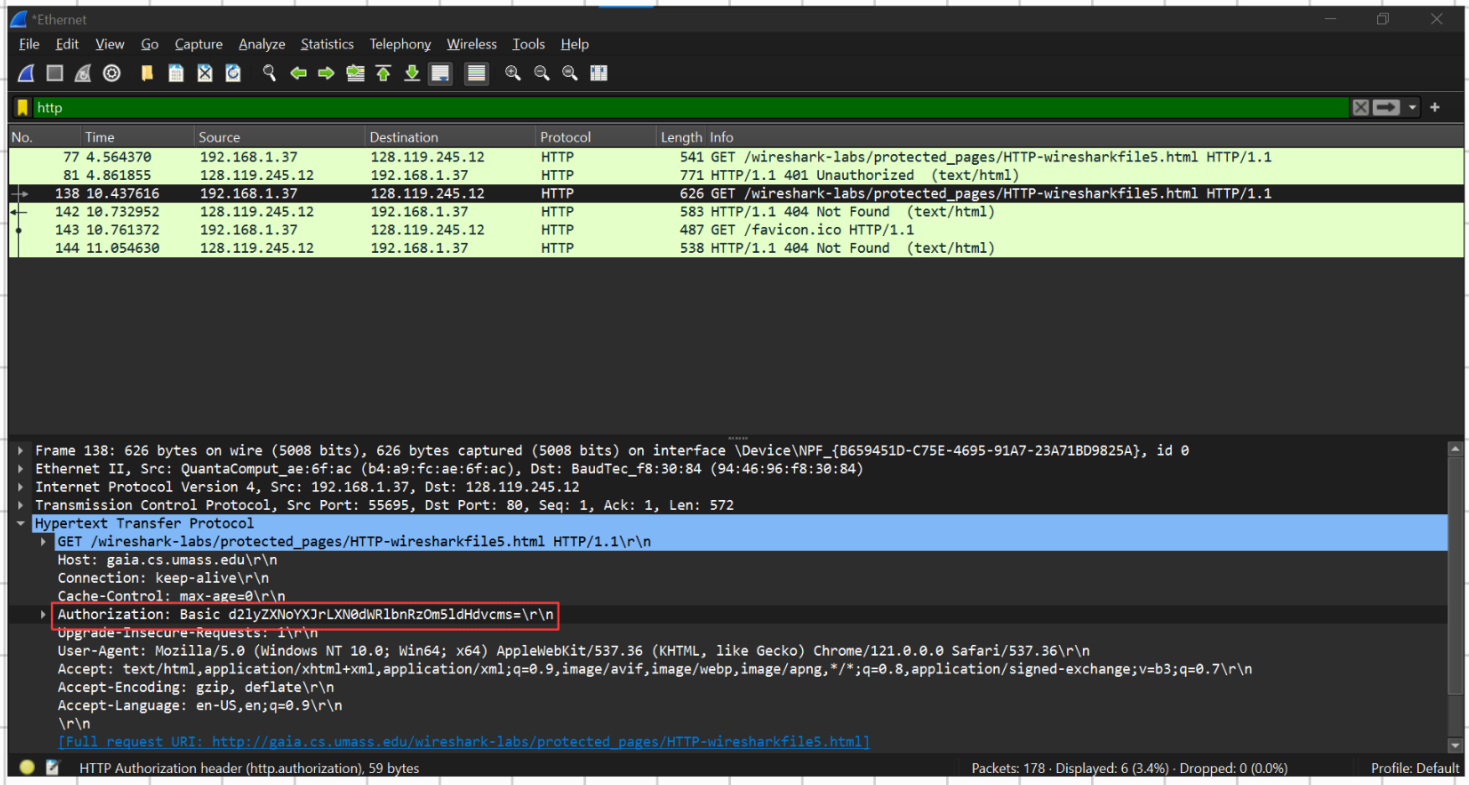
จากคอลัมน์เวลาแสดงให้เห็นว่ามีการดาวน์โหลดรูปภาพ pearson.png หลังจากส่ง GET Request ครั้งที่ 2 และรูปภาพ 8E_cover_small.jpg ถูกดาวน์โหลดหลังจากส่ง GET Request ครั้งที่ 3 ดังนั้นจึงสรุปได้ว่าตามเป็นการดาวน์โหลดตามลำดับ (serially)

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



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?



HTTP GET ครั้งที่สองเพิ่มส่วน Authorization: Basic