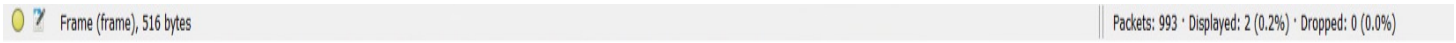
ปิยะ วิริยะกุล 63010871 SEC 03
(ห้อง LAB : จ. 13.00-16.00)

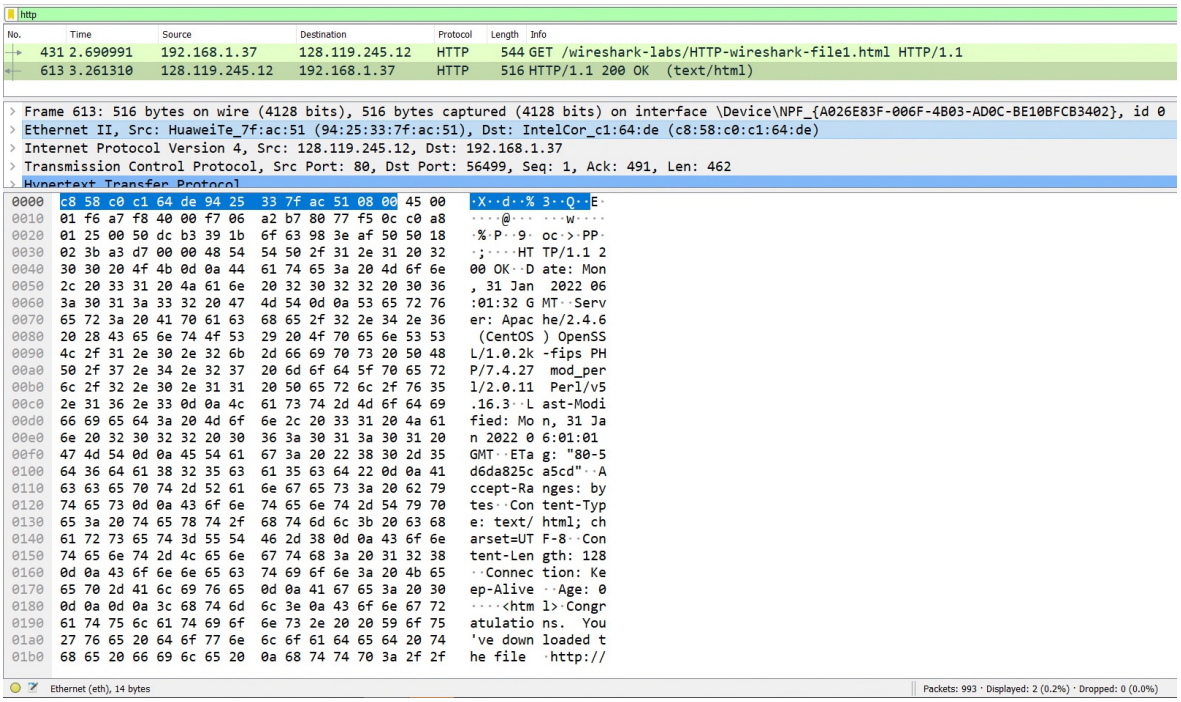
กิจกรรมที่ 4 : HTTP

ในกิจกรรมที่ผ่านมา จะเป็นการแนะนำการใช้งาน Wireshark เป็นส่วนใหญ่ในกิจกรรมครั้งนี้ จะเริ่มทำความรู้จักกับ Protocol ใน Application Layer โดย Protocol แรก คือ HTTP (Hypertext Transport Protocol)

1. ให้ใช้ Wireshark เริ่มทำการ Capture และป้อน url : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html เสร็จแล้วให้หยุด
2. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP (ถ้าทำถูกจะมีแค่ 2 บรรทัด แต่อาจมี favicon และ Not Found ติดมาไม่ต้องไปสนใจ)
   (กรณีบรรทัดที่ 2 (Response) เป็น 304 Not Modified ให้เคลียร์แคชของ Browser แล้วทำใหม่)
3. ใน Packet HTTP **Response** มีความยาวเฟรมทั้งหมดเท่าไร 516 Bytes ให้ Capture หน้าจอส่วนที่แสดงความยาวประกอบ

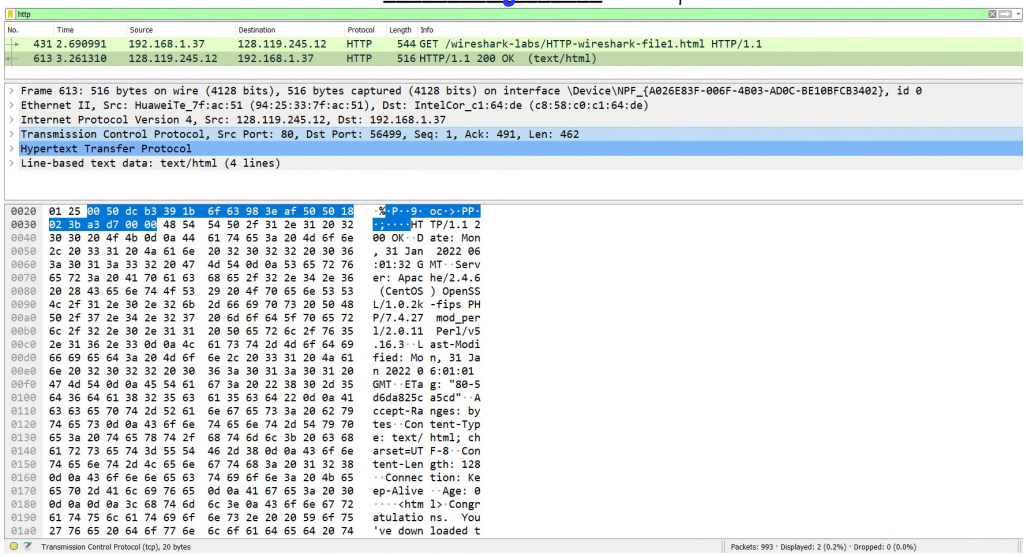


4. ใน Packet ข้อ 3 ความยาวของ Header Ethernet II เป็นเท่าไร 14 Bytes ให้ Capture หน้าจอส่วนที่แสดงความยาวประกอบ (Hint : ใช้ Packet Byte Pane)



ศิริชัย วิริยะกุล 63010871 SEC 03
(เรียน LAB : จ. 13.00-16.00)

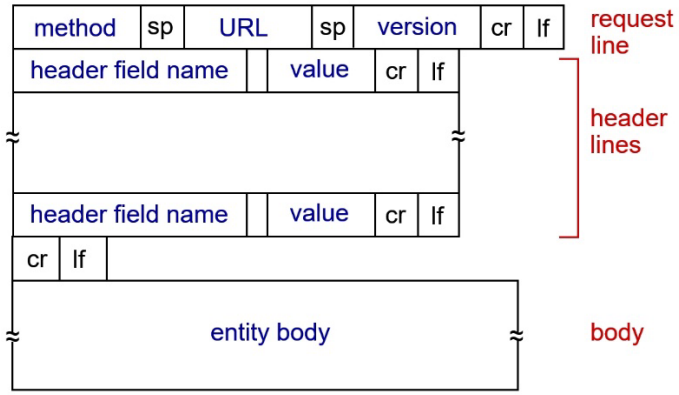
5. ใน Packet ข้อ 3 ความยาวของ TCP Header เป็นเท่าไร 20 Bytes ให้ Capture หน้าจอส่วนที่แสดงความยาวประกอบ



6. เหตุผลที่ Header ของข้อมูลต้องซ้อนเป็นชั้นๆ คือ

ที่ต้องมี encapsulation ทำให้ layer ของเครื่องปลายทางรู้ว่าจะส่งต่อไปยัง layer ถัดไปอย่างไร จาก L7→L1 ซึ่งจะทำให้ต้องมีการเพิ่มข้อมูล Header and Trailers ตามชั้น layer.

7. จากรูปแบบของ HTTP Message ตามรูป และ HTTP Request และ Response ที่ดักจับได้ ให้ตอบคำถามต่อไปนี้ (สามารถใช้วิธี Capture แล้ว Highlight ข้อมูลเพื่อตอบคำถามได้)



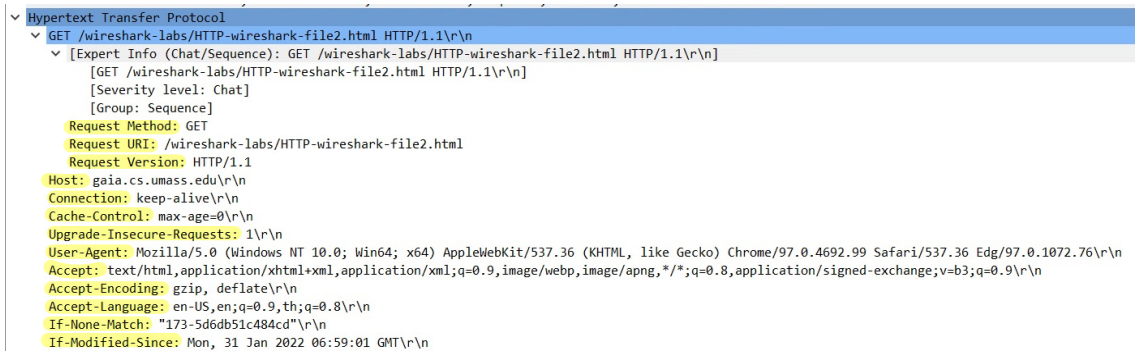
- Browser และ Server ใช้ HTTP version ใด HTTP version 1.1 , server : apache/2.4.6
- Browser เป็นโปรแกรมอะไร Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.99 Safari/537.36 Edg/97.0.1072.76\r\n
- Server เป็นโปรแกรมอะไร Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
- ภาษาที่ Browser ระบุว่าสามารถรับจาก Server ได้ en-US
- Status Code ที่ส่งกลับมาจาก Server มายัง Browser 200 (OK)
- ค่าของ Last-Modified ของไฟล์ที่ Server Mon, 31 Jan 2022 06:01:01 GMT
- มีข้อมูลกี่ไบต์ที่ส่งมายัง Browser 128 Bytes

```
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
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Mon, 31 Jan 2022 06:01:32 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Mon, 31 Jan 2022 06:01:01 GMT\r\n
  ETag: "80-5d6da825ca5cd"\r\n
  Accept-Ranges: bytes\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  Content-Length: 128\r\n
    [Content length: 128]
  Connection: Keep-Alive\r\n
  Age: 0\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.570319000 seconds]
  [Request in frame: 431]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
  File Data: 128 bytes
```

ศิริระ วิริยะกุล 63010871 SEC 03
(ที่ห้อง LAB : จ. 13.00-16.00)

- ให้สรุปว่า header field name ตาม HTTP message format ของข้อมูลที่ส่งกลับมีอะไรบ้าง

```
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
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Mon, 31 Jan 2022 06:59:39 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Mon, 31 Jan 2022 06:59:01 GMT\r\n
  ETag: "173-5d6db51c484cd"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 371\r\n
    [Content length: 371]
  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 1/2]
  [Time since request: 0.613823000 seconds]
  [Request in frame: 77]
  [Next request in frame: 115]
  [Next response in frame: 117]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  File Data: 371 bytes
```



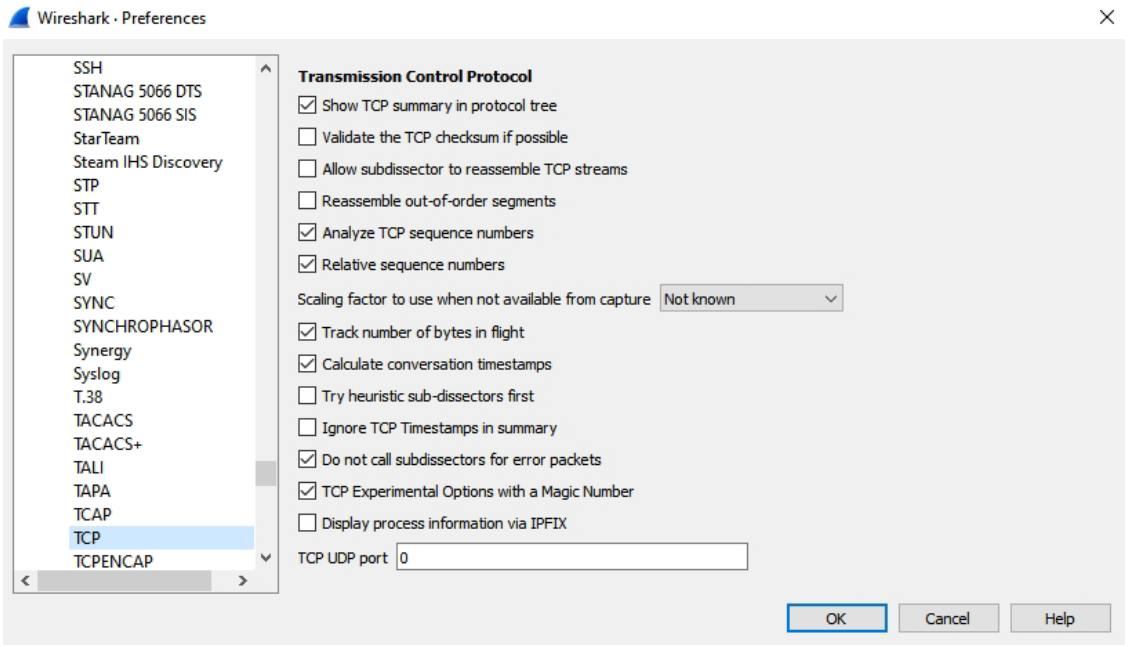
```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.html
    Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\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/97.0.4692.99 Safari/537.36 Edg/97.0.1072.76\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: en-US,en;q=0.9,th;q=0.8\r\n
  If-None-Match: "173-5d6db51c484cd"\r\n
  If-Modified-Since: Mon, 31 Jan 2022 06:59:01 GMT\r\n
```

8. ให้นักศึกษาหาวิธี clear cache ของ Browser ที่ตนเองใช้อยู่ แล้วจัดการ clear ให้เรียบร้อย
9. เปิด Wireshark ใหม่แล้ว Capture ที่ url : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html จากนั้นให้กด Reflash เพื่อโหลดหน้าอีกครั้ง จากนั้นให้หยุด Capture

ปีระ วิริยะกุล 63010871 SEC 03
(เรียน LAB : ศ. 13.00-16.00)

10. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP (ถ้าทำถูกจะมีแค่ 4 บรรทัด บรรทัด แต่อาจมี favicon ติดมาไม่ต้องไปสนใจ) และตอบคำถามต่อไปนี้
    - ใน HTTP GET ครั้งที่ 1 มีคำว่า IF-MODIFIED-SINCE หรือไม่ ไม่
    - ใน HTTP GET ครั้งที่ 2 มีคำว่า IF-MODIFIED-SINCE หรือไม่ มี
    - **(ถ้ามี) ข้อมูลที่ต่อจาก** IF-MODIFIED-SINCE มีความหมายอย่างไร
      ใช้เก็บเวลาที่ browser ได้รับข้อมูลครั้งล่าสุด
    - ในการตอบกลับของ Server ครั้งที่ 2 มีการส่งไฟล์มาด้วยหรือไม่ จะอธิบายอย่างไร
      ไม่มีการส่งไฟล์ เพราะ browser มี cache เก็บไว้อยู่แล้ว (แสดงว่าไม่มีการ Mod. อะไร cache เพิ่ม)
      (ตัวเลขเพิ่มมา 371 Bytes)

11. ให้ไปที่ Edit | Preference... | Protocol | TCP ตามรูป



ให้แน่ใจว่า ไม่ติ๊กที่ **Allow subdissector to reassemble TCP streams**

12. ให้ทำตามข้อ 8 อีกครั้ง และเปิด Wireshark ใหม่แล้ว Capture ที่ url http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html จากนั้นให้หยุด Capture
13. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP (ถ้าทำถูกจะมี 5 บรรทัด) ซึ่งจะเห็นว่าหลังจากข้อมูล HTTP/1.1 200 OK แล้ว ยังมีข้อมูลตามมาอีก เนื่องจากไฟล์ html มีความยาวมาก (มากกว่า 4000 ไบต์) ทำให้ไม่สามารถส่งมาใน 1 packet ได้ จึงมีการแบ่งเป็นหลายๆ ส่วน (โดย TCP) ดังนั้นใน Wireshark จึงแสดงคำว่า Continuation ให้นักศึกษาตอบคำถามต่อไปนี้

ปิยะ วิริยะกุล 63010871 SEC 03
(เรียน LAB : จ. 13.00-16.00)

- มี HTTP GET กี่ครั้ง และมี packet ใดบ้างที่มี Status Code และเป็น Status Code ใด

1 ครั้ง , Status code : 200 มีแค่ packet response เท่านั้น
ส่วน data ที่มีๆ ก็ไฟล์ status code มีแค่ file data

14. ให้ทำตามข้อ 5 อีกครั้ง และเปิด Wireshark ใหม่แล้ว Capture ที่ url http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html จากนั้นให้หยุด Capture

- ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP และให้ตอบคำถามต่อไปนี้
- มี HTTP GET กี่ครั้ง จาก url ใดบ้าง

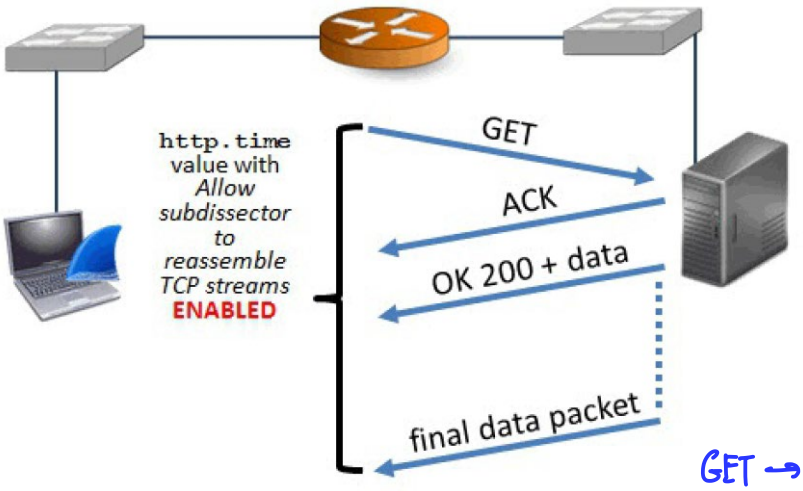
3 ครั้ง : 1. /wireshark-labs/HTTP-wireshark-file4.html
2. /pearson.png
3. /8E_cover_small.jpg

- นักศึกษาคิดว่า ภาพทั้ง 2 ภาพในไฟล์ มีการ download ทีละไฟล์ (serial) หรือทำพร้อมๆ กัน (parallel) ให้อธิบาย

แบบ serial เพราะต้องส่ง request ทีละ ภาพ ได้ภาพแรกมาแล้วถึงจะมีข้อมูล location
ของภาพที่สองจาก response packet ที่มีข้อมูลของ location ของ file ภาพแรก
แต่ถ้าเป็น request ก็ต้องได้รับ response ของภาพแรกก่อน

ให้คลิ๊กขวาที่ Transmission Control Protocol | Protocol Preferences แล้วติ๊กที่ **Allow subdissector to reassemble TCP streams** เกิดอะไรขึ้น

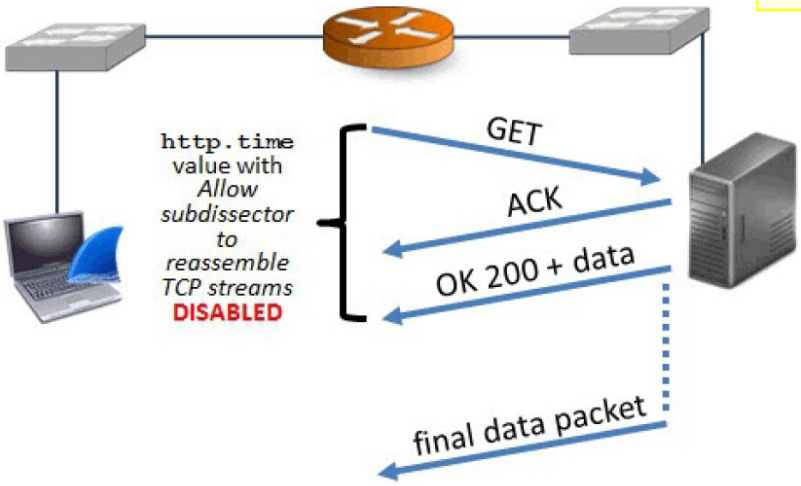
packet ที่ถูกแบ่งออกมาจากข้อมูล ตามขนาด byte ที่ตั้งค่าไว้ packet แรก } ส่งผลต่อ
จะถูก wireshark ตีความไปพร้อมกับ packet หลัก (ไม่มี continuation) } http.time



GET → OK → File Transfer

ค่า http.time เมื่อ Enable Allow subdissector to reassemble TCP streams

ศิริระ ศิริมะยุล 63010871 SEC 03
(เรียน LAB : จ. 13.00-16.00)

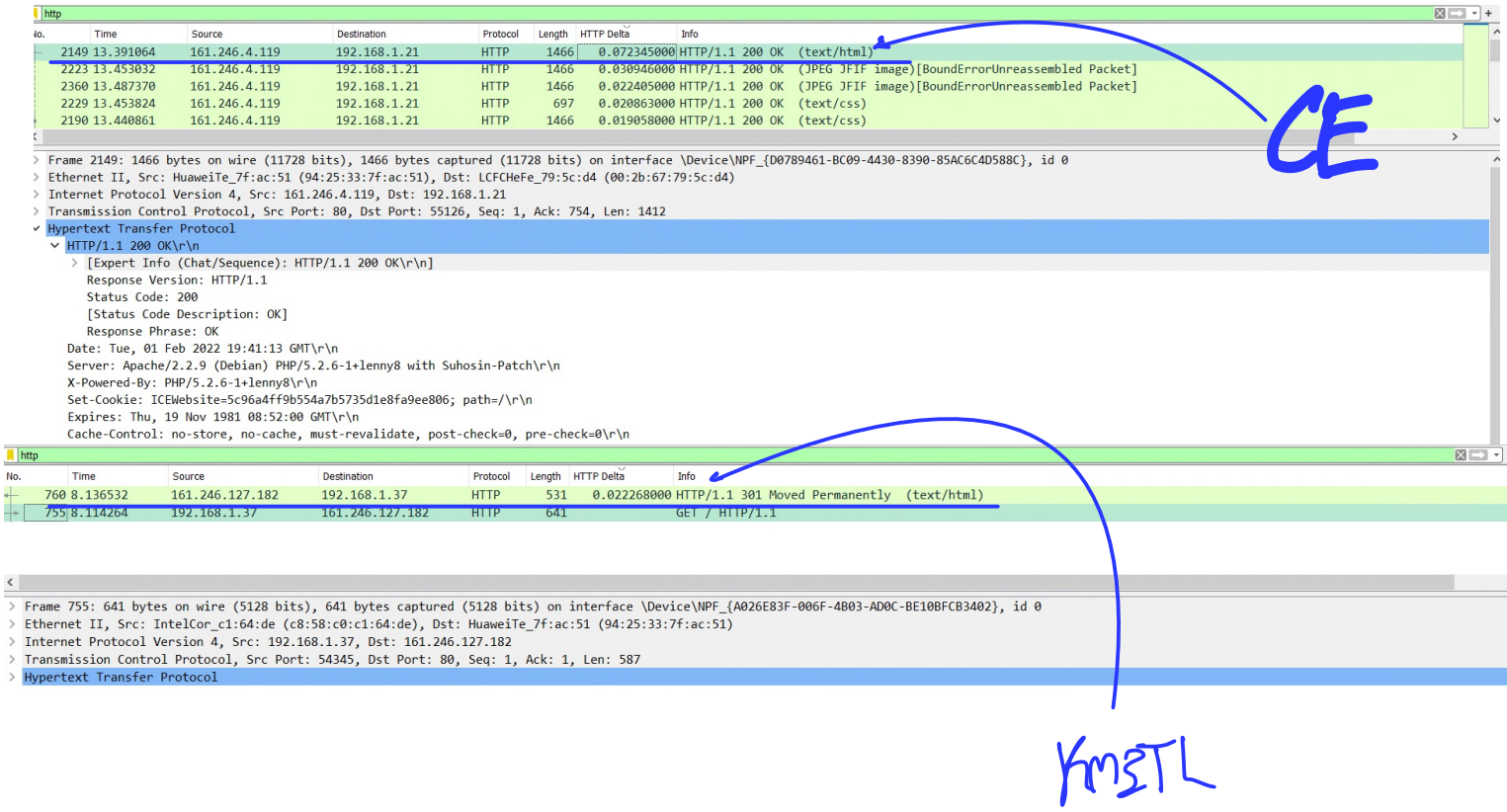


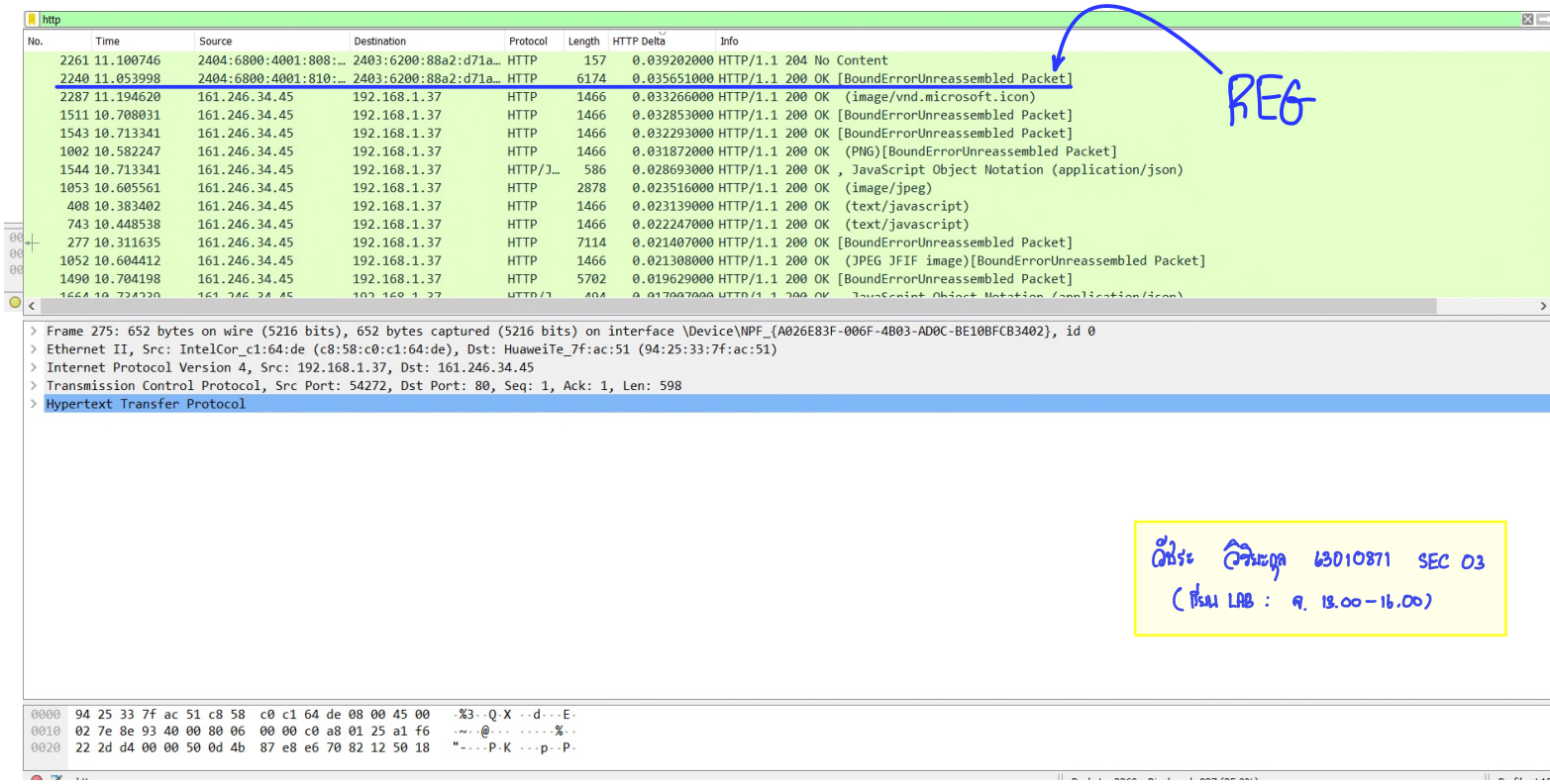
ค่า http.time เมื่อ Disable Allow subdissector to reassemble TCP streams

ในการตรวจสอบความล่าช้าในการทำงานของ Web Server เราจะใช้ค่า RTT (Round Trip Time) ซึ่งเป็นค่าเวลาตั้งแต่ GET จนถึงตอบกลับ (OK 200) ซึ่งจะบอกได้ถึงการตอบสนองต่อการเรียกใช้ของ Web Server ตัวนั้น ซึ่งสำหรับ Wireshark จะมีผลกระทบจาก การกำหนดค่า **Allow subdissector to reassemble TCP streams** ตามรูป คือ หาก Disable จะคิดเฉพาะ packet HTTP OK 200 แต่ถ้า Enable ก็จะเป็นเวลาที่นับรวมถึงการโหลดข้อมูลทั้งหมด ดังนั้นให้ disable **Allow subdissector to reassemble TCP streams** ก่อน

15. ให้ไปที่ บรรทัดที่เป็น 200 OK แล้วไปที่ Hypertext Transfer Protocol แล้ว Expand Subtrees ออกมาทั้งหมด แล้วไปที่บรรทัด **Time since request** แล้วเลือก **Apply as Column** ให้ตั้งชื่อว่า **HTTP Delta** จากนั้นให้ Sort จะพบ packet ที่ใช้เวลามากที่สุด
16. ให้นักศึกษาตรวจสอบ RTT ของเว็บ www.ce.kmitl.ac.th, www.reg.kmitl.ac.th, www.kmitl.ac.th และเว็บอื่นอีก 1 เว็บ (นักศึกษาเลือกเอง) ให้บอกว่าค่า RTT ของแต่ละเว็บมีค่าใด ให้เรียงลำดับน้อยไปมาก ให้นักศึกษาแสดงขั้นตอนการทำงาน (เขียนอธิบายย่อๆ และ Capture รูปประกอบ) และเปรียบเทียบค่ากับเพื่อนอีก 1 คน ว่าลำดับเหมือนกันหรือไม่ อย่างไร

1. ce.kmitl.ac.th : 0.072345 sec. | time : ce > reg > kmitl
2. reg.kmitl.ac.th : 0.095051 sec.
3. kmitl.ac.th : 0.022268 sec.
4. http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html
   → 0.603919 sec.





ศิริรัช วิริยะกุล 63010871 SEC 03
(เรียน LAB : จ. 13.00-16.00)

งานครั้งที่ 4

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งโดยเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา และ _Lab4 เช่น 63010789_Lab4.pdf
- กำหนดส่ง ภายในวันที่ 9 กุมภาพันธ์ 2565