

01076010 เครือข่ายคอมพิวเตอร์ : 2/2564

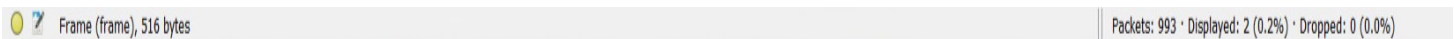
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

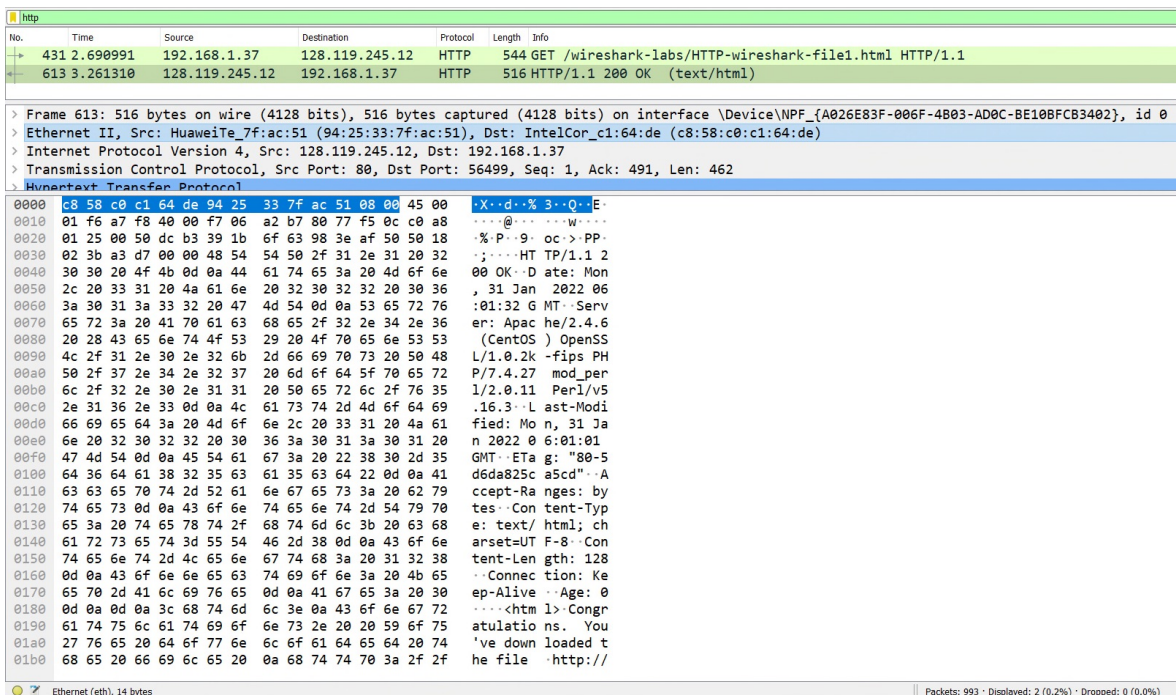
## กิจกรรมที่ 4 : HTTP

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

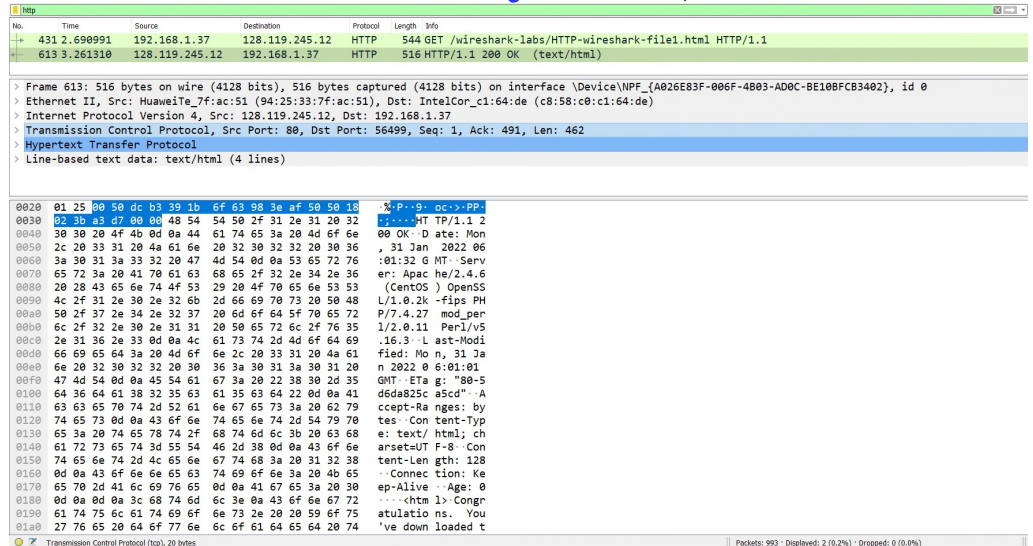


4. ใน Packet ข้อ 3 ความยาวของ Header Ethernet II เป็นเท่าไร 14 Bytes ให้ Capture หน้าจอส่วนที่แสดงความยาวประกอบ (Hint : ใช้ Packet Byte Pane)



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

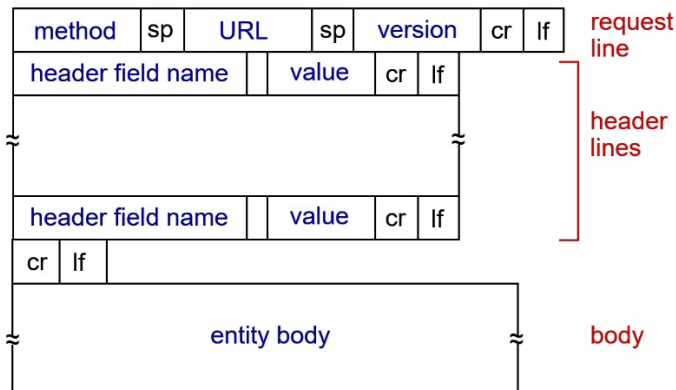
ความยาวประกอบ



6. เหตุผลที่ Header ของข้อมูลต้องซ้อนเป็นชั้นๆ คือ

เพื่อทำ encapsulation ที่ใน layer ของโหนดหนึ่งจะห่อหุ้มเป็นข้อมูล จาก L7→L1  
คือ เพิ่มหัวขั้ว Header and trailers ของมันไปเรื่อยๆ

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



- Browser และ Server ใช้ HTTP version ไດ 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 01:01:01 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]

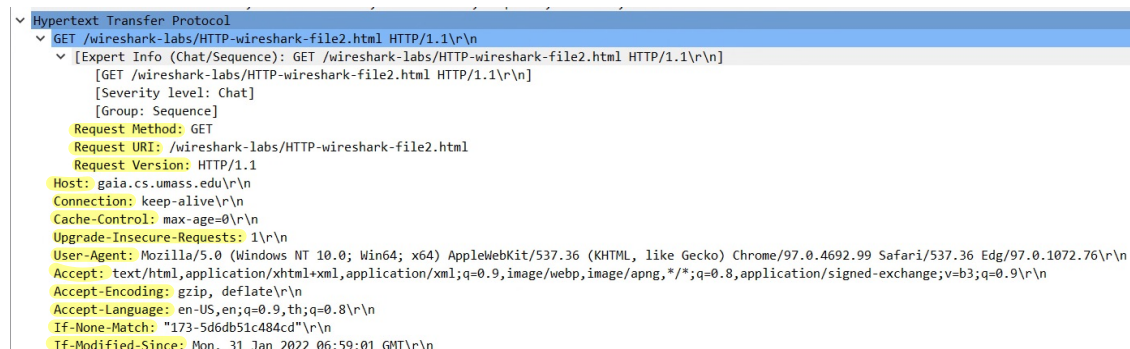
[Request in frame: 431]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

File Data: 128 bytes

วันที่: วันจันทร์ 30/01/2022 SEC 03  
(เริ่ม LAB : 9. 13.00-16.00)

- ให้สรุปว่า header field name ตาม HTTP message format ของข้อมูลที่ส่งกลับมีอะไรบ้าง

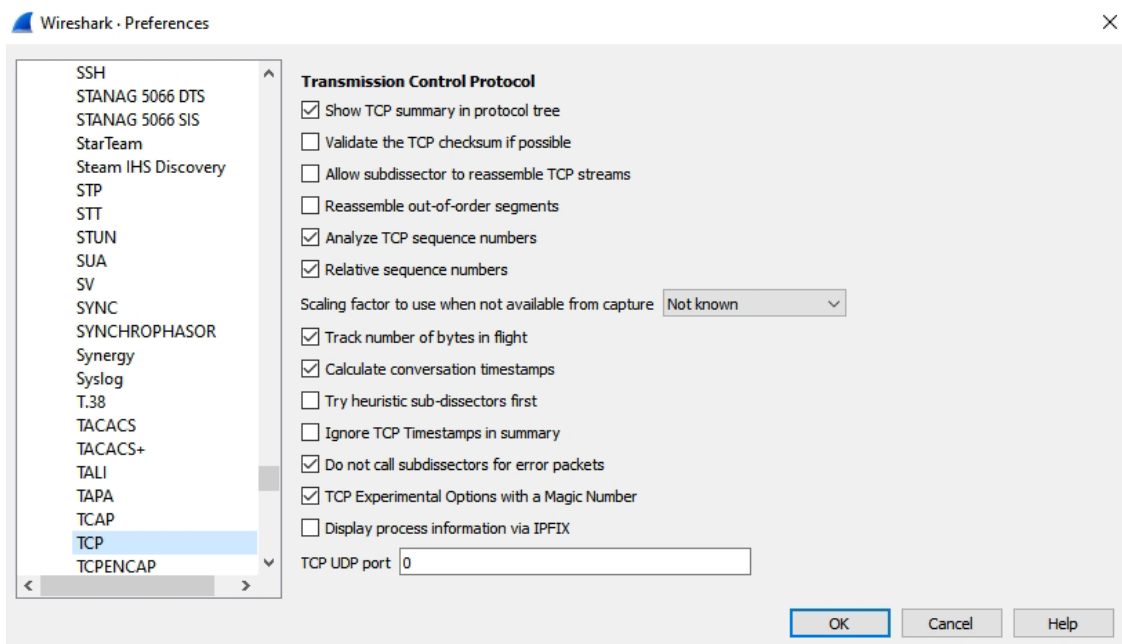


- ให้นักศึกษาหาวิธี clear cache ของ Browser ที่ตนเองใช้อยู่ แล้วจัดการ clear ให้เรียบร้อย
- เปิด Wireshark ใหม่แล้ว Capture ที่ url : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html จากนั้นให้กด Reflash เพื่อโหลดหน้าอีกครั้ง จากนั้นให้หยุด Capture

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  
ใช้บอก browser ว่าได้รับไฟล์ที่ร้องขอแล้วหรือไม่
- ในการตอบกลับของ Server ครั้งที่ 2 มีการส่งไฟล์มาด้วยหรือไม่ จะอธิบายอย่างไร  
ไม่ส่งไฟล์ เพราะ browser มี cache เก็บไว้แล้ว (แต่ไฟล์ Mod. 0.1.0 cache ใหม่) (ตัวเลขใหม่ 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



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

1 ನೇ, Status code : 200 means packet response ಸುಗಮವಾಗಿ  
 ಒಂದು data ಬಿಟ್ಟು ಇನ್ನೂ status code ಸೇರಿದ 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 และให้ตอบคำถามต่อไป

- มี HTTP GET ที่ครั้ง จาก url ไตบ้าง

3 ob : 1. /wiredshark-labs/HTTP-wireshark-file4.html

2. / pearson.py

3. / 8E\_cover\_small.jpg

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

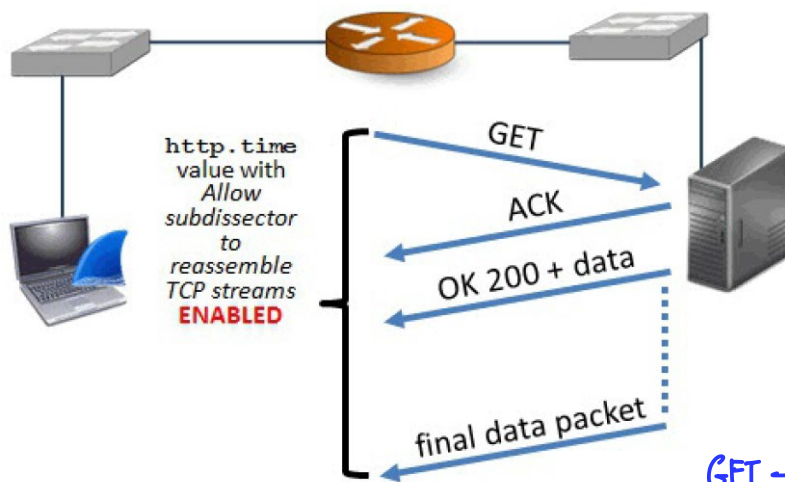
new serial  $\rightarrow$  on demand request for new communication location

also include response packet indicating location of file in hdd

## 11.2. Request to latency response interaction

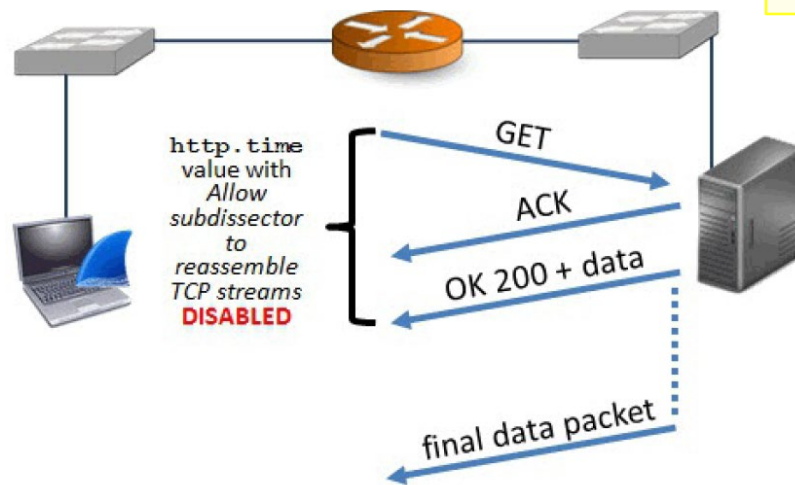
ให้คลิกขวาที่ Transmission Control Protocol | Protocol Preferences แล้วติ๊กที่ **Allow subdissector to reassemble TCP streams** เกิดอะไรขึ้น

packet stream contains more bytes than packet size } scenario  
o/g wireshark will show packet size (in continuation) } http.time



GET → OK → File Transfer

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



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

ในการตรวจสอบความล่าช้าในการทำงานของ Web Server เราจะใช้ค่า RTT (Round Trip Time) ซึ่งเป็นค่า เวลาตั้งแต่ GET จนถึงตอบกลับ (OK 200) ซึ่งจะบอกได้ถึงการตอบสนองต่อการเรียกใช้ของ Web Server ตัวนั้น ซึ่ง สำหรับ Wireshark จะมีผลกระทบจาก การกำหนดค่า Allow subdissector to reassemble TCP streams ตาม รูป คือ หาก Disable จะคิดเฉพาะ packet HTTP OK 200 แต่ถ้า Enable ก็จะเป็นเวลาที่นับรวมถึงการโหลดข้อมูล ทั้งหมด 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](http://www.ce.kmitl.ac.th), [www.reg.kmitl.ac.th](http://www.reg.kmitl.ac.th), [www.kmitl.ac.th](http://www.kmitl.ac.th) และเว็บ อื่นอีก 1 เว็บ (นักศึกษาเลือกเอง) ให้บอกว่าค่า RTT ของแต่ละเว็บมีค่าใด ให้เรียงลำดับน้อยไปมาก ให้ นักศึกษาแสดงขั้นตอนการทำงาน (เขียนอธิบายย่อๆ และ Capture รูปประกอบ) และเปรียบเทียบกับ เพื่อนอีก 1 คน ว่าลำดับเหมือนกันหรือไม่ อย่างไร

1. <a href="http://ce.kmitl.ac.th">ce.kmitl.ac.th</a>	: 0.072345 sec.	time : ce > reg > kmitl
2. <a href="http://reg.kmitl.ac.th">reg.kmitl.ac.th</a>	: 0.095651 sec.	
3. <a href="http://kmitl.ac.th">kmitl.ac.th</a>	: 0.029268 sec.	
4. <a href="http://http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html">http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html</a>	→ 0.103919 sec.	

**CE**

**Km5TL**

**REG**

วันที่ ๙ มีนาคม ๒๕๖๓ ๑๓:๐๐-๑๖:๐๐

(วัน LAB : ๙. ๑๓.๐๐-๑๖.๐๐)

#### งานครั้งที่ 4

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