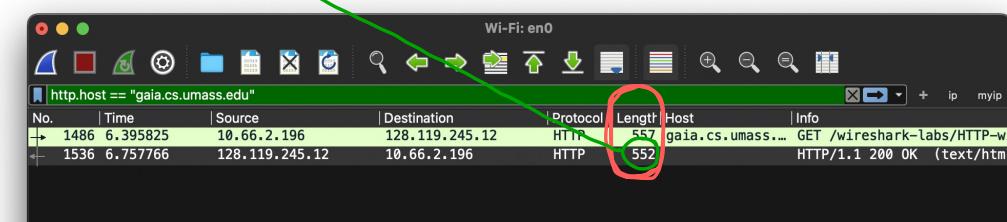


01076117 ปฏิบัติการเครือข่ายคอมพิวเตอร์ 2/2565
 ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
 สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

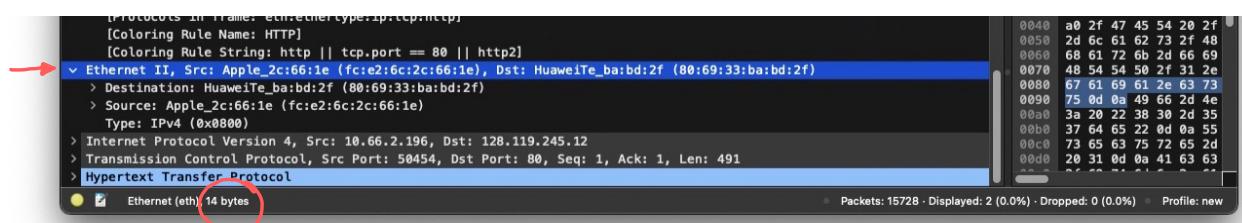
กิจกรรมที่ 4 : HTTP

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

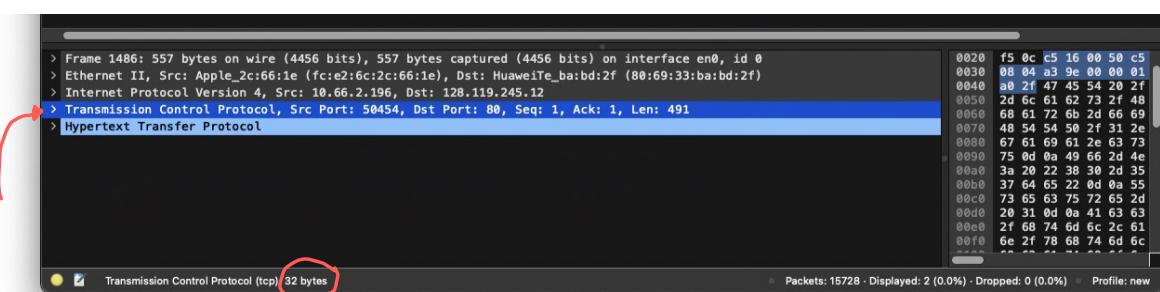
- ให้ใช้ Wireshark เริ่มทำการ Capture และป้อน url : <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html> เสร็จแล้วให้หยุด
- ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ HTTP (ที่ถูกต้องควรจะมีแค่ 2 แพ็กเกต ในกรณีที่มีเกิน 2 แพ็คเกต อาจมาจากกรณี favicon ติดมาด้วย แต่ไม่ต้องไปสนใจแพ็คเกตที่เกินมา)
 (กรณีบรรทัดที่ 2 (Response) เป็น 304 Not Modified ให้เคลียร์ cache ของ browser และทำใหม่)
- ใน Packet List Pane ให้เลือก packet ที่เป็น HTTP Response และหัวข้อความยาวของทั้ง frame เป็นเท่าไร 552 ให้บันทึก screenshot หน้าจอส่วนที่แสดงความยาวมาแสดง



- ใน packet ตามข้อ 3 ความยาวเฉพาะส่วน header ของ Ethernet II เป็นเท่าไร 14 byte ให้บันทึก screenshot หน้าจอส่วนที่แสดงความยาวมาแสดง (Hint: หัวข้อมูลจาก Packet Byte Pane)



- ใน packet ตามข้อ 3 ความยาวเฉพาะส่วน header ของ Transmission Control Protocol เป็นเท่าไร 32 byte ให้บันทึก screenshot หน้าจอส่วนที่แสดงความยาวมาแสดง

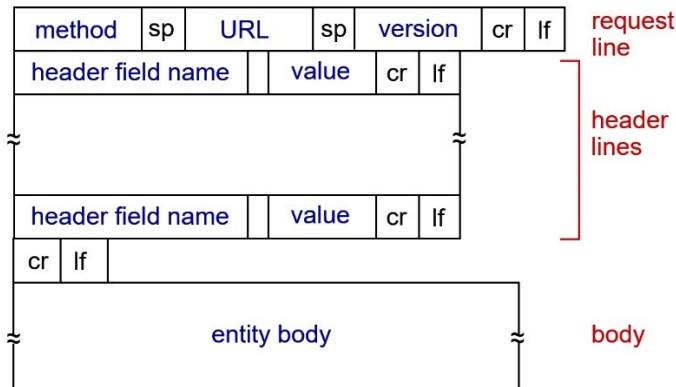


6.

- เพราะเหตุใด header ของ packet ต้องซ้อนเป็นชั้นๆ จึงอธิบายเหตุผล

เพราะการสื่อสาร กันใน ISO model การส่งรับข้อมูลต้องใช้ลักษณะ encapsulate
 ชั้นๆ นำ header มารวมกับ data เพื่อไม่ผู้รับเข้าใจว่า กำลัง ข้อมูลอะไร

7. จากรูปแบบของ HTTP Message ตามรูป และ HTTP Request และ Response ที่ดักจับได้ ให้ตอบคำถามต่อไปนี้ (สามารถใช้วิธี capture และ highlight ข้อมูลเพื่อตอบคำถามได้)



- browser และ server ใช้ HTTP version ได้ version 1.1
- browser เป็นโปรแกรมอะไร safari
- server เป็นโปรแกรมอะไร Apache / 2.4.6
- ภาษาที่ browser ระบุว่าสามารถรับจาก server ได้ th-TH
- status code ที่ส่งกลับมาจาก server นายัง browser 200 OK
- ค่าของ Last-Modified ของไฟล์ที่ server Thu, 09 Feb 2023 06:52:02 GMT\n
- มีข้อมูลกิ๊บเด็ตที่ส่งมายัง browser 128 bytes

- ให้สรุปว่า header field name ตาม HTTP message format ของข้อมูลที่ส่งกลับมีอะไรบ้าง
status code , server , last-modified , Etag , Accept-Ranges
content-Length , keep-Alive , connection , content-type

8. ให้นักศึกษาหาวิธี clear cache ของ browser ที่ตนเองใช้อยู่ และจัดการ clear ให้เรียบร้อย

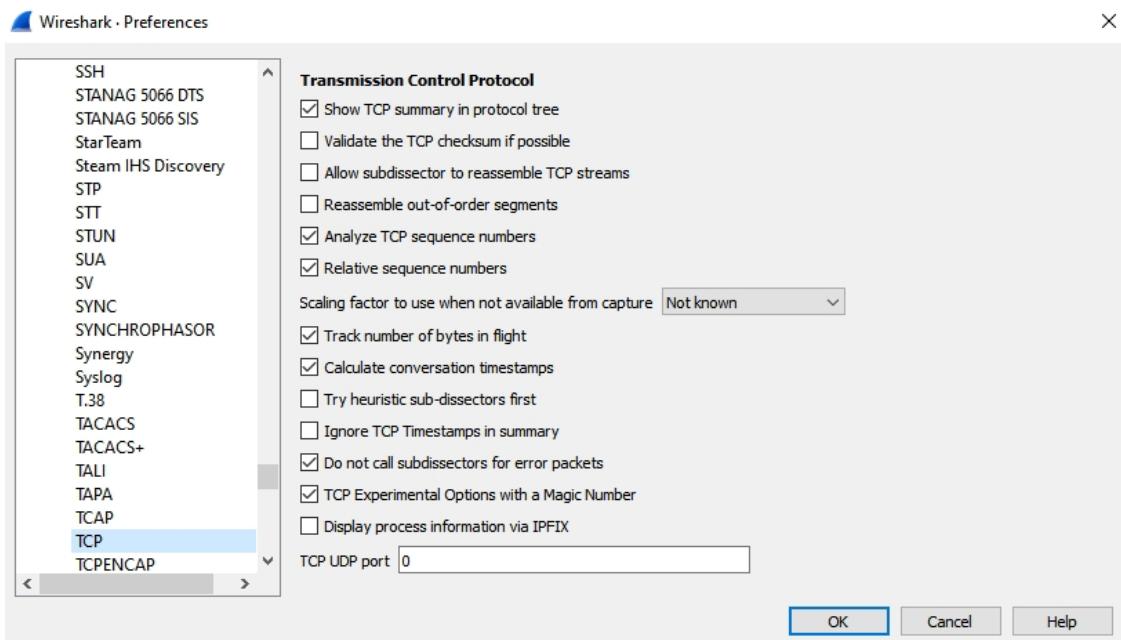
9. เปิด Wireshark ใหม่แล้ว capture การเรียกหน้าเว็บเพจไปยัง url <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html> จากนั้นให้กด refresh เพื่อโหลดหน้าอีกครั้ง จากนั้นให้หยุด capture
10. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ HTTP (ที่ถูกต้องควรจะมีแค่ 4 แพ็คเกต ในกรณีที่มีเกิน 4 แพ็คเกต อาจมาจากการ์นิ favicon ติดมาด้วย แต่ไม่ต้องไปสนใจแพ็คเกตที่เกินมา) 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

ถ้า ร่องว่าง ไม่ระบุ ข้อมูล ล่าสุดจาก server

- ในการตอบกลับของ server ครั้งที่ 2 มีการส่งไฟล์มาด้วยหรือไม่ สามารถอธิบายได้ว่าอย่างไร
ไม่ เพราะ การตอบกลับครั้งที่ 2 ของ server ไม่ได้ส่งตรรกะข้อมูล
ก็คงจะไม่เป็นค่อสั่ง file สำหรับ

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



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

12. ให้ทำตามข้อ 8 อีกครั้ง และเปิด Wireshark ใหม่แล้ว capture การเรียกหน้าเว็บเพจไปยัง url <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html> จากนั้นให้หยุด capture
13. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ 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 กี่ครั้ง และมี packet ใดบ้างที่มี Status Code และเป็น Status Code ใด
1 ครั้ง : ณ packet แรก ที่มี status code คือ 200 ok
-

14. ให้ทำการข้อ 8 อีกครั้ง และเปิด Wireshark ใหม่แล้ว capture การเรียกหน้าเว็บเพจไปยัง url
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html> จากนั้นให้หยุด capture

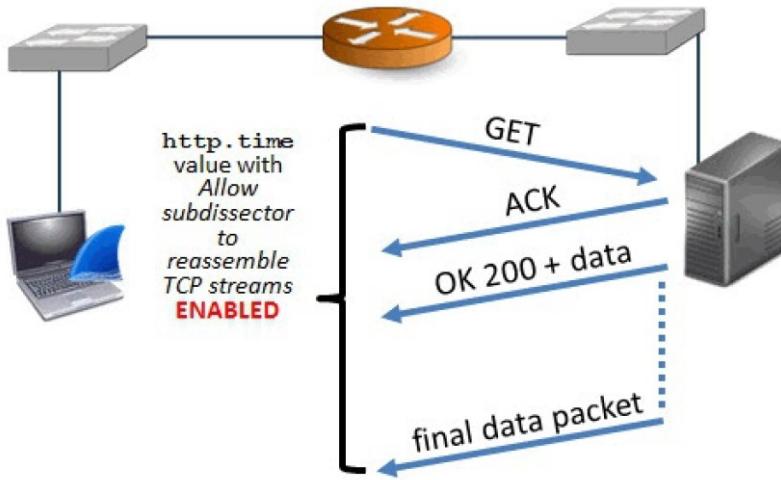
- ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ HTTP และให้ตอบคำถามต่อไปนี้
- มี HTTP GET กี่ครั้ง และไปยัง url ใดบ้าง

3 ครั้ง ไปยัง gaia.cs.umass.edu
kurose.csslash.net\r\n

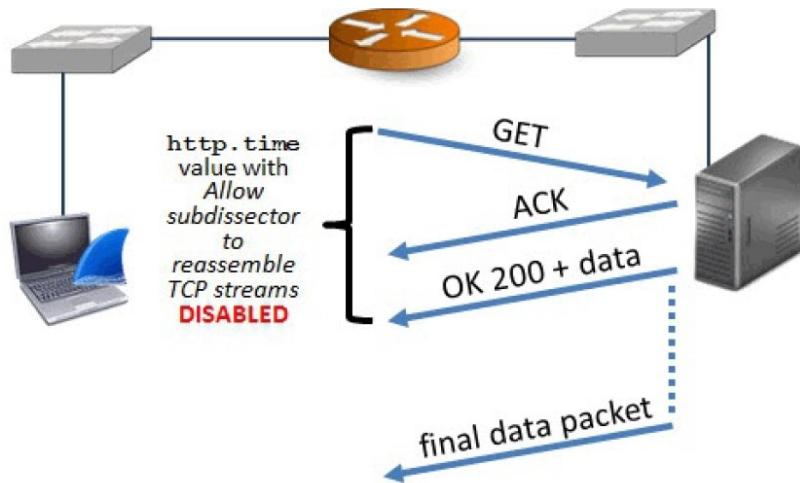
- ผู้เรียนคิดว่า ภาพทั้ง 2 ภาพในไฟล์ ถูกทำการ download ทีละไฟล์ (serialize) หรือถูก download ไปพร้อมๆ กัน (parallelize) ให้อธิบาย

download ทีละ file เห็นจากเป็น http 1.1 ที่ parallelize
จะเป็น http 2.0

- ให้คลิกขวาที่ Transmission Control Protocol | Protocol Preferences และติ๊กที่ **Allow subdissector to reassemble TCP streams** เกิดอะไรขึ้น
ติ๊ก Allow subdissector จะดูว่า ตอน packet continuation
-



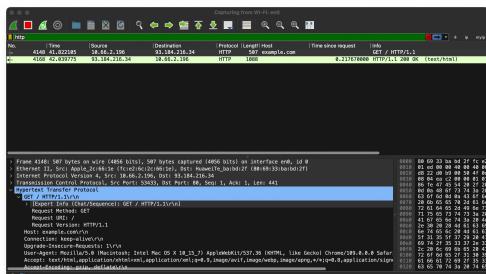
ค่า http.time เมื่อ Enable Allow subdissector to reassemble TCP streams



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

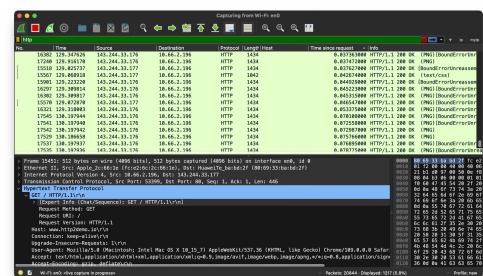
ในการตรวจสอบความล่าช้าในการทำงานของ Web Server เราจะใช้ค่า RTT (Round Trip Time) ซึ่งเป็นค่าเวลาตั้งแต่ GET จนถึงตอบกลับ (OK 200) ซึ่งจะบอกได้ถึงการตอบสนองต่อการเรียกใช้ของ Web Server ตัวนั้น ซึ่งสำหรับ Wireshark จะมีผลกระทบจากการกำหนดค่า **Allow subdissector to reassemble TCP streams** ตามรูป คือ หาก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

15. ให้ไปที่ บรรทัดที่เป็น 200 OK และไปที่ Hypertext Transfer Protocol และขยาย subtrees ออกมาก้างหมด และไปที่บรรทัด **Time since request** และเลือก **Apply as Column** ให้ตั้งชื่อว่า HTTP Delta จากนั้นให้ sort เพื่อหา packet ที่มีเวลา HTTP Delta มากที่สุด **packet ที่ 5 (HTTP/1.1 200 OK)**
16. ให้นักศึกษาตรวจสอบ RTT ของ 3 เว็บดังนี้ 1) <http://example.com/> 2) <http://www.http2demo.io/> 0.079775000
0.33062400
3) <http://www.vulnweb.com/> และเว็บอื่นอีก 1 เว็บ (ผู้เรียนเลือกเอง) ให้บันกอกว่าค่า RTT ของแต่ละเว็บมีค่าได้ 0.021494000 com.pro.ce.KMITL.ac.th
ให้เรียงลำดับน้อยไปมาก ให้นักศึกษาแสดงขั้นตอนการทำงาน (เขียนขอรับใบอนุญาต และบันทึก screenshot ประกอบ) และเปรียบเทียบค่ากันเพื่อนอก 1 คน ว่าลำดับเหมือนกันหรือไม่ อย่างไร
เว็บที่ล็อกดาวน์, 2, 1, 3)
clear cache กด capture เพิ่ง url ใหม่
คลิกที่ column แล้วดู packet ที่ Time มากที่สุด
เนมอันกัน โดย Time ต่างกัน แต่ลำดับเนมอันกัน บนล็อกดาวน์



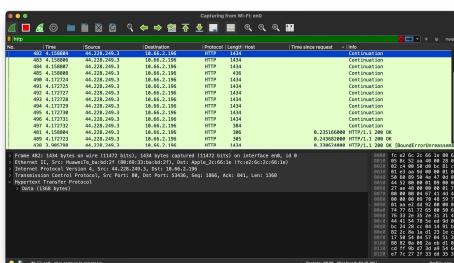
→ http://example.com |
Time : 0.2

ព័ត៌មាន ទៅអ្នក



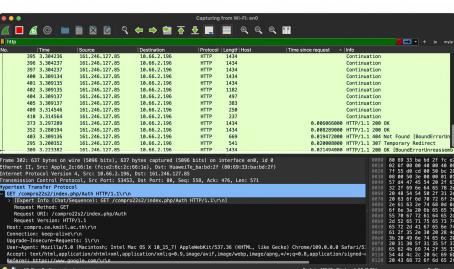
→ <http://www.http2demo.io/>

កំចុង ទរាង ពីរ



→ <http://www.vulnweb.com>

ព័ត៌មាន ទំនាក់ទំនង



→ <http://compro.ce.kmitl.ac.th>

ព័ត៌មាន គ្រប់គ្រង

งานครั้งที่ 4

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งเป็นไฟล์ PDF เท่านั้น
 - ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา ตามด้วย section และ _lab04 ตามตัวอย่างต่อไปนี้
64019999_sec20_lab04.pdf
 - กำหนดส่ง ภายในวันที่ 10 กุมภาพันธ์ 2566 โดยให้ส่งใน Microsoft Teams ของรายวิชา