3. ให้ใช้ข้อมูลจาก Packet Bytes Pane เพื่อหาความยาวของข้อมูล และตอบคำถามต่อไปนี้

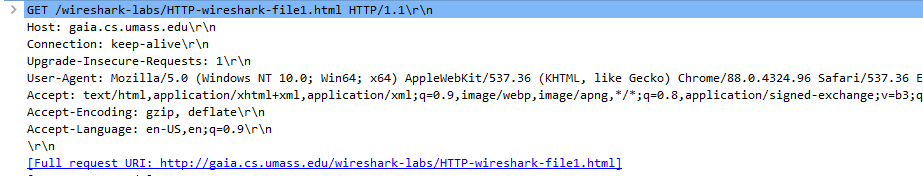
- ความยาวเฟรมทั้งหมด 534 bytes

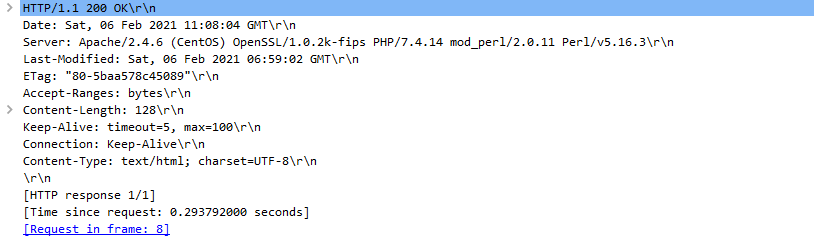
- ความยาวของ Header Ethernet II 14 bytes

- ความยาวของ TCP Header 20 bytes

- เหตุผลที่ Header ของข้อมูลต้องซ้อนเป็นชั้นๆ คือ เพื่อความเป็นระเบียบและง่ายต่อการหา

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





- Browser และ Server ใช้ HTTP version ใด HTTP/1.1

- Browser เป็นโปรแกรมอะไร Microsoft edge

- Server เป็นโปรแกรมอะไร Apache/2.4.6

-ภาษาที่ Browserระบุว่าสามารถรับจากServerได้ en-US

- Status Code ที่ส่งกลับมาจากServer มายัง Browser 200

-ค่าของ Last-Modified ของไฟล์ที่ Sat, 06 Feb 2021 06:59:02 GMT

- มีข้อมูลกี่ไบต์ที่ส่งมายัง Browser 128 bytes

- ให้สรุปว่า header field name ตาม HTTP message format ของข้อมูลที่ส่งกลับมีอะไรบ้าง

Date, Sever ,Last-Modified, Etag, Accept-Ranges, Content-Length, Keep-Alive, Connection, Content-Type

7. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP (ถ้าทำถูกจะมีแค่ 4 บรรทัด บรรทัด แต่อาจมี favicon ติดมาไม่ต้องไปสนใจ) และตอบคำถามต่อไปนี้

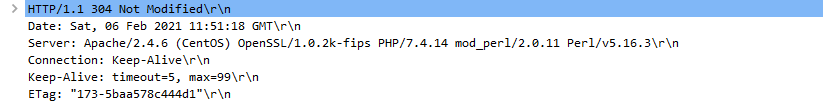
- ใน HTTP GET ครั้งที่ 1 มีคำว่า IF-MODIFIED-SINCE หรือไม่ ไม่มี

- ใน HTTP GET ครั้งที่ 2 มีคำว่า IF-MODIFIED-SINCE หรือไม่ มี

- (ถ้ามี) ข้อมูลที่ต่อจาก IF-MODIFIED-SINCE มีความหมายอย่างไร

Server จะตอบ 304 Not Modified ถ้าทรัพยากรไม่มีการเปลี่ยนแปลงตั้งแต่เวลาที่ระบุ

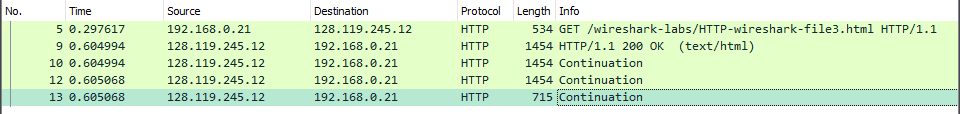
- ในการตอบกลับของ Server ครั้งที่ 2 มีการส่งไฟล์มาด้วยหรือไม่ จะอธิบายอย่างไร



ไม่ เพราะ header field name ไม่มี Content-Length

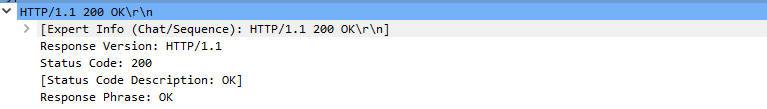
10. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP (ถ้าทำถูกจะมี 5 บรรทัด) ซึ่งจะเห็นว่าหลังจากข้อมูล HTTP/1.1 200 OK แล้ว ยังมีข้อมูลตามมาอีก เนื่องจากไฟล์ html มีความยาวมาก (มากกว่า 4000 ไบต์) ทำให้ไม่สามารถส่งมาใน 1 packet ได้ จึงมีการแบ่งเป็นหลายๆ ส่วน (โดย TCP) ดังนั้นใน Wireshark จึงแสดงคำว่า Continuation ให้นักศึกษาตอบคำถามต่อไปนี้

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



มี GET 1 ครั้ง

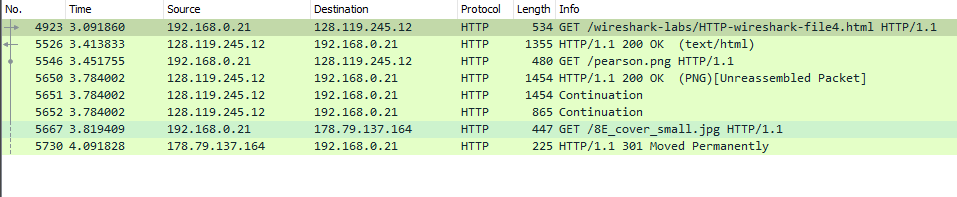




มี 1 packet ตามรูปด้านบนที่มี status code และมี status code : 200

12. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP และให้ตอบคำถามต่อไปนี้

- มี HTTP GET กี่ครั้ง จาก url ใดบ้าง



มี HTTP GET 2 ครั้ง

จาก url : <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>

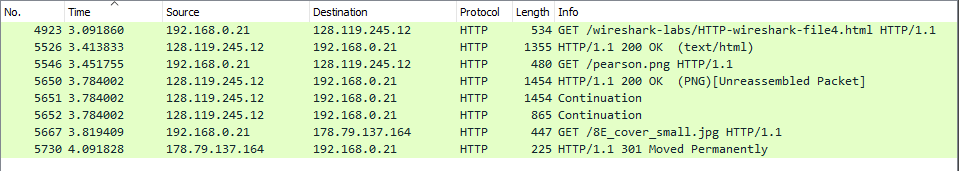
<http://gaia.cs.umass.edu/pearson.png>

http://kurose.cslash.net/8E\_cover\_small.jpg

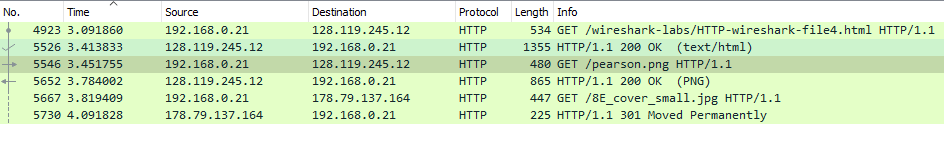
- นักศึกษาคิดว่า ภาพทั้ง 2 ภาพในไฟล์ มีการ download ทีละไฟล์ (serial) หรือทำพร้อมๆ กัน (parallel) ให้อธิบาย

มีการ download ทีละไฟล์ เนื่องจากตอนเปิดเว็บจะ download ภาพ pearson.png ก่อนแล้วโหลดภาพ cover\_small.jpg ทีหลัง หรือดูได้จากคอลัมน์ Time ใน wireshark

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

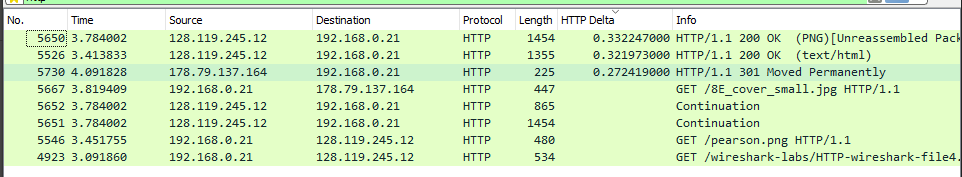
ก่อน

หลัง



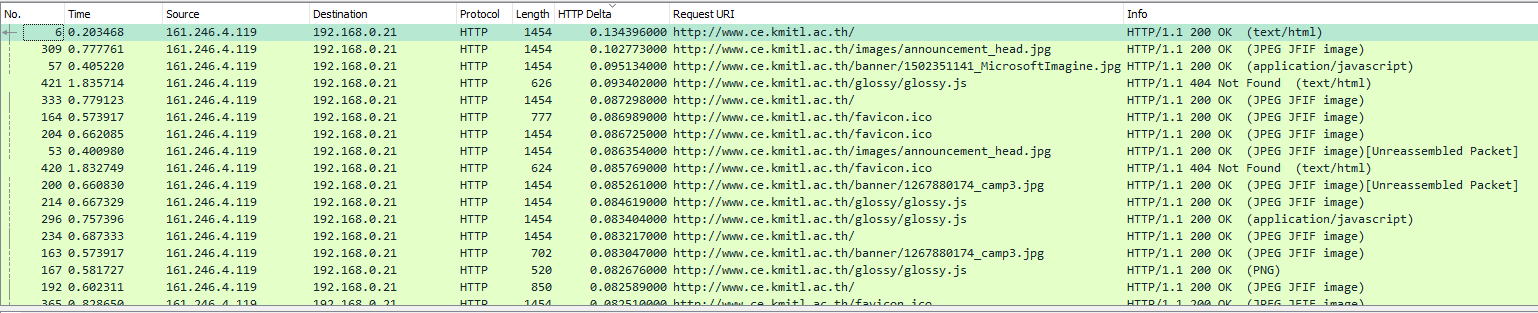
ไม่มี packet continuation

14. 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

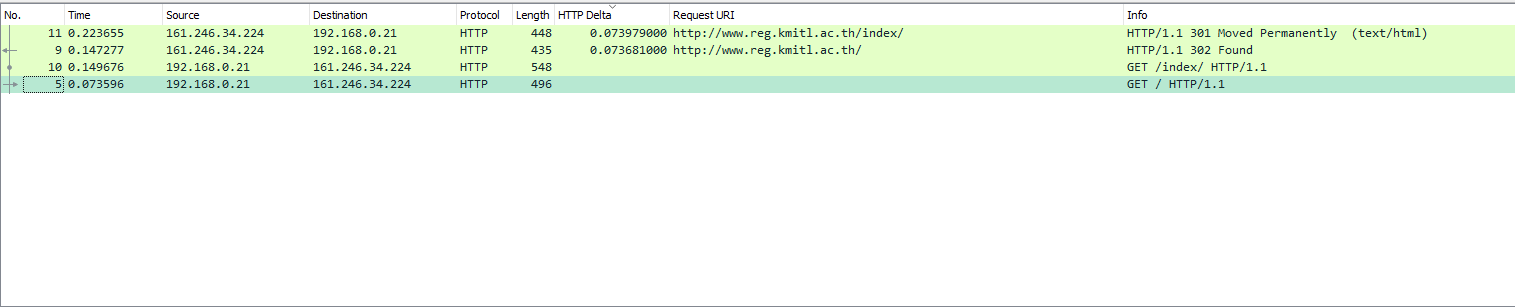


15. ให้นักศึกษาตรวจสอบ RTT ของเว็บ www.ce.kmitl.ac.th, www.reg.kmitl.ac.th, www.kmitl.ac.th และเว็บอื่นอีก 1 เว็บ (นักศึกษาเลือกเอง) ให้บอกว่าค่า RTT ของแต่ละเว็บมีค่าใด ให้เรียงลำดับน้อยไปมาก ให้นักศึกษาแสดงขั้นตอนการทำงาน (เขียนอธิบายย่อๆ และ Capture รูปประกอบ) และเปรียบเทียบค่ากับเพื่อนอีก 1 คน

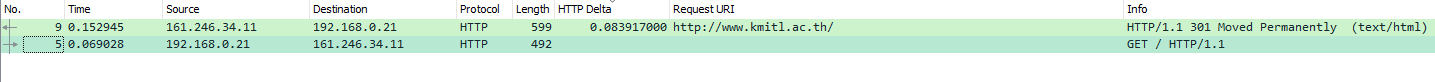
www.ce.kmitl.ac.th



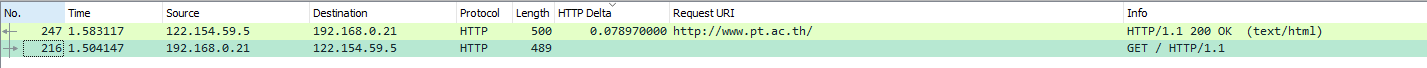
www.reg.kmitl.ac.th



www.kmitl.ac.th



www.pt.ac.th



ขั้นตอนการทำงาน

1.กด capture แล้วเข้าเว็บตามด้านบน

2.ใช้ display filter : http

3.กด sort คอลัมน์ HTTP Delta

เรียงลำดับจากน้อยไปมาก

1. [www.reg.kmitl.ac.th](http://www.reg.kmitl.ac.th) (0.73979000)

2. [www.pt.ac.th](http://www.pt.ac.th) (0.78970000)

3. [www.kmitl.ac.th](http://www.kmitl.ac.th) (0.83917000)

4. [www.ce.kmitl.ac.th](http://www.ce.kmitl.ac.th) (0.134396000)

เปรียบเทียบกับเพื่อน

1. www.reg.kmitl.ac.th (0.019618000)

2. www.kmitl.ac.th (0.030770000)

3. www.ce.kmitl.ac.th (0.05982000)

4. www.bangkok.go.th (0.150547000)