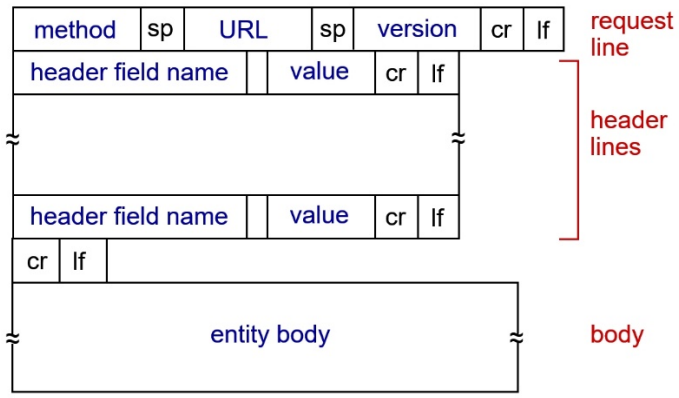
<u>กิจกรรมที่ 4 : HTTP</u>

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 ติดมาไม่ต้องไปสนใจ)
   (กรณีบรรทัดที่ 2 (Response) เป็น 304 Not Modified ให้ปิด Browser แล้วทำใหม่)
3. ให้ใช้ข้อมูลจาก Packet Bytes Pane เพื่อหาความยาวของข้อมูล และตอบคำถามต่อไปนี้
   - ความยาวเฟรมทั้งหมด _____
   - ความยาวของ Header Ethernet II _____
   - ความยาวของ TCP Header _____
   - เหตุผลที่ Header ของข้อมูลต้องซ้อนเป็นชั้นๆ คือ
     _____
     _____
4. จากรูปแบบของ HTTP Message ตามรูป และ HTTP Request และ Response ที่ดักจับได้ ให้ตอบคำถามต่อไปนี้ (สามารถใช้วิธี Capture แล้ว Highlight ข้อมูลเพื่อตอบคำถามได้)



   - Browser และ Server ใช้ HTTP version ใด _____
   - Browser เป็นโปรแกรมอะไร _____
   - Server เป็นโปรแกรมอะไร _____

- ภาษาที่ Browser ระบุว่าสามารถรับจาก Server ได้

  _____

- Status Code ที่ส่งกลับมาจาก Server มายัง Browser
- ค่าของ Last-Modified ของไฟล์ที่ Server _____
- มีข้อมูลกี่ไบต์ที่ส่งมายัง Browser _____
- ให้สรุปว่า header field name ตาม HTTP message format ของข้อมูลที่ส่งกลับมีอะไรบ้าง

  _____

  _____

5. ให้นักศึกษาหาวิธี clear cache ของ Browser ที่ตนเองใช้อยู่ แล้วจัดการ clear ให้เรียบร้อย
6. เปิด Wireshark ใหม่แล้ว Capture ที่ url http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html จากนั้นให้กด Reflash เพื่อโหลดหน้าอีกครั้ง จากนั้นให้หยุด Capture
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 _____
   - ใน HTTP GET ครั้งที่ 2 มีคำว่า IF-MODIFIED-SINCE หรือไม่ _____
   - **(ถ้ามี) ข้อมูลที่ต่อจาก** IF-MODIFIED-SINCE มีความหมายอย่างไร _____

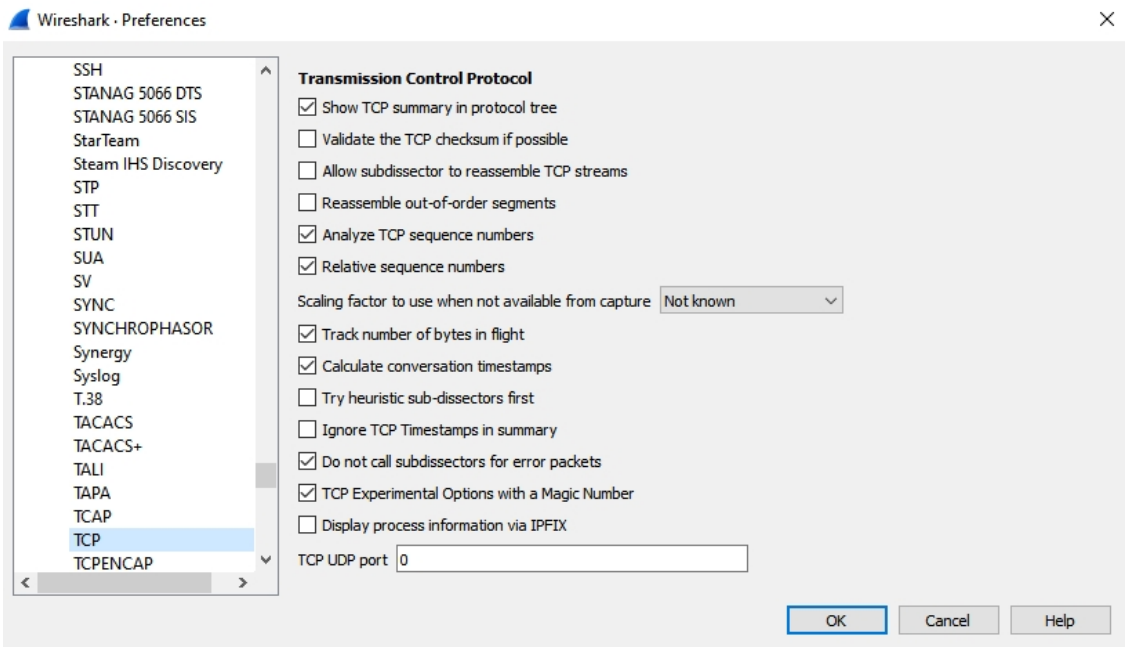
     _____

   - ในการตอบกลับของ Server ครั้งที่ 2 มีการส่งไฟล์มาด้วยหรือไม่ จะอธิบายอย่างไร

     _____

     _____

8. ให้ปที่ Edit | Preference... | Protocol | TCP ตามรูป



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

9. ให้ทำตามข้อ 5 อีกครั้ง และเปิด Wireshark ใหม่แล้ว Capture ที่ url http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html จากนั้นให้หยุด Capture
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

    _____

11. ให้ทำตามข้อ 5 อีกครั้ง และเปิด Wireshark ใหม่แล้ว Capture ที่ url http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html จากนั้นให้หยุด Capture
12. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP และให้ตอบคำถามต่อไปนี้
    - มี HTTP GET กี่ครั้ง จาก url ใดบ้าง

    _____

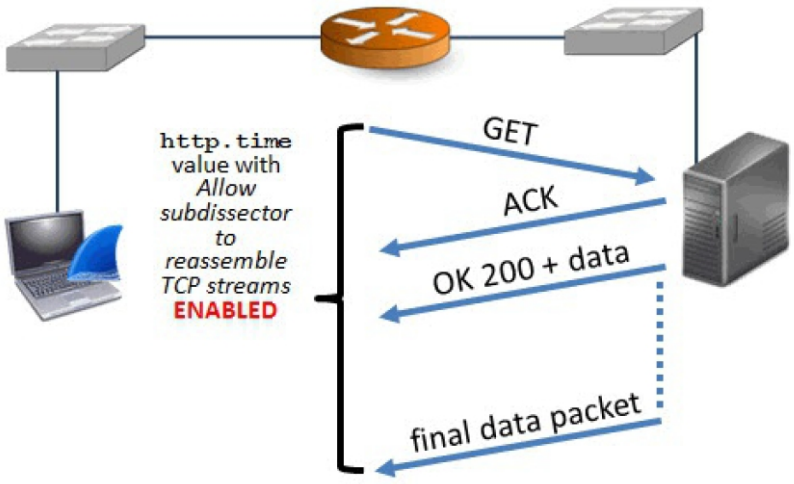
    - นักศึกษาคิดว่า ภาพทั้ง 2 ภาพในไฟล์ มีการ download ทีละไฟล์ (serial) หรือทำพร้อมๆ กัน (parallel) ให้อธิบาย

    _____

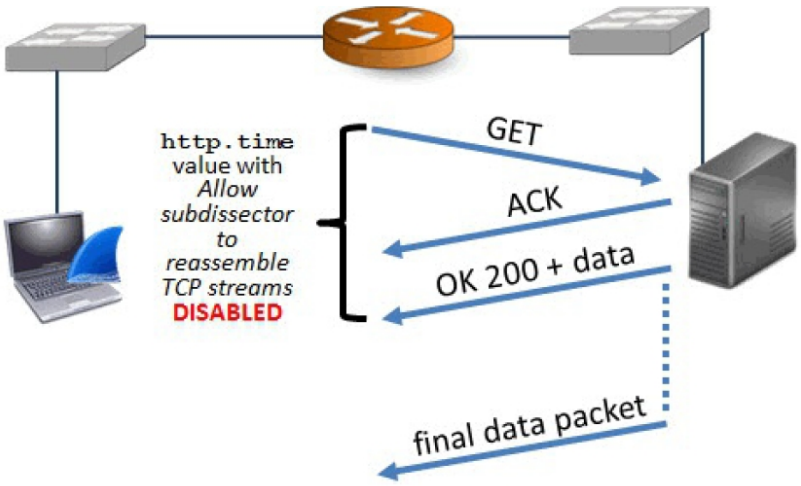
13. ให้คลิ๊กขวาที่ Transmission Control Protocol | Protocol Preferences แล้วติ๊กที่ **Allow subdissector to reassemble TCP streams** เกิดอะไรขึ้น

    _____

    _____



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 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

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

งานครั้งที่ 4

- การส่งงาน ให้ส่งเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา
- ส่วนบนของหน้าแรกให้มี รหัสนักศึกษา และ ชื่อนักศึกษา
- ให้ส่งโดยทำเป็นคำตอบแยกออกมา อาจมีรูปประกอบคำตอบเพื่อความชัดเจน
- กำหนดส่ง ภายในวันที่ 7 กุมภาพันธ์ 2564