*จงตอบคำถามดังต่อไปนี้แล้วบันทึกไฟล์นี้โดยใช้ชื่อว่า CS433\_LAB1\_[รหัสนักศึกษา] เช่น*

*“CS433\_LAB1\_567890123.docx” แล้วส่งอีเมล์ไปยัง csmjuko@gmail.com*

*โดยให้ใช้ Subject เป็นชื่อเดียวกันกับชื่อ file ซึ่งก็คือ CS433\_LAB1\_567890123*

*ส่งช้าเลย deadline คะแนนเต็มเหลือ 50% ไม่ส่ง คะแนนเป็น 0 สำหรับ Lab นั้นๆ*

**Lab 1: Wireshark**

**1. เริ่มต้นใช้งาน Wireshark**

1.1 ให้ List รายการ Network Interface ที่โปรแกรม Wireshark มองเห็น

ตอบ Wi-Fi , Local Area Connection\*2 , Bluetooth Network Connect , Ethernet

1.2 Network Interface ที่ใช้งานต่อ Internet นั้นมีชื่อว่าอะไร

ตอบ Ethernet

1.3 ให้ List รายชื่อโปรโตคอลที่โปรแกรม Wireshark สามารถดัก Packet มาได้ (ไม่เกิน 10 โปรโตคอล)

ตอบ HTTP FTP DNS TCP NBNS SSDP LLMNR

**2. โปรโตคอล HTTP**

- เปิดโปรแกรม Web browser ขึ้นมา

- เปิดโปรแกรม Wireshark ขึ้นมา แต่ยังไม่ต้องเริ่มดัก Packet

- ตรงช่อง Apply a display filter ให้พิมพ์คำว่า “http && tcp” แล้วกด Enter โดยที่ไม่ต้องมีฟันหนูลงไปเพื่อเราจะดูเพียง Packet ที่ใช้งานโปรโตคอล HTTP เท่านั้น

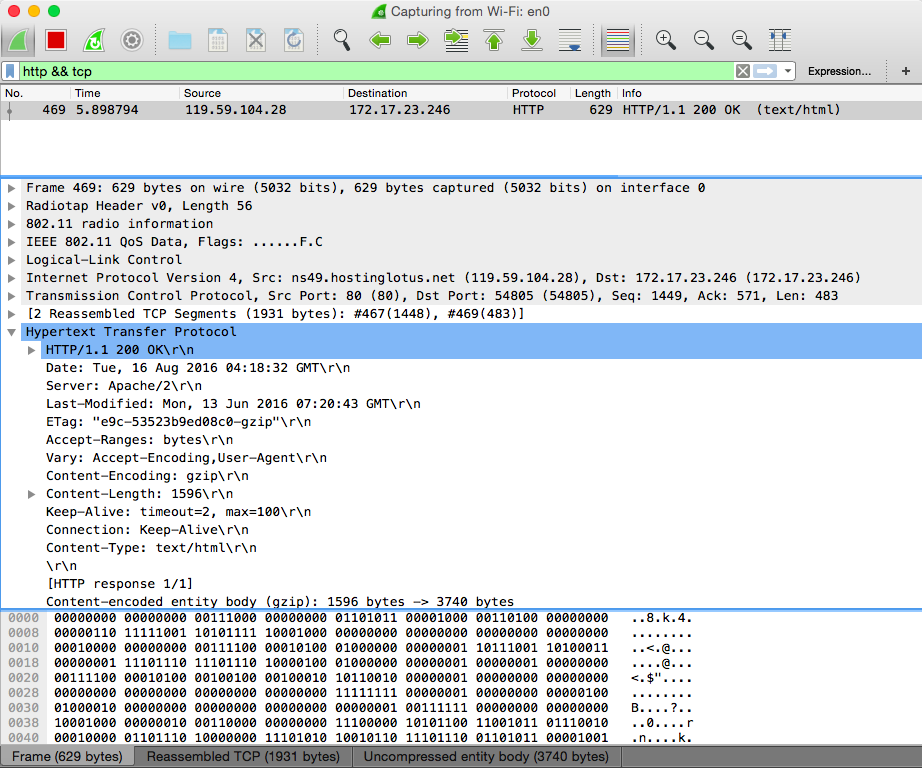
\\Mac\Dropbox\Screenshots\Screenshot 2016-08-16 11.09.57.png

- รอประมาณ 1 นาที แล้วจึงเริ่มดัก Packet ในโปรแกรม Wireshark จาก Interface ที่เราใช้งาน Internet (ปกติจะเป็น eth0 หรือ wlan0)

- กลับมายัง Web browser แล้วเปิดหน้าเวป csmju.jowave.com

- หยุดดัก Packet ในโปรแกรม Wireshark

การใช้งานโปรโตคอล HTTP นั้นจะมีการส่ง HTTP GET ไปยัง Web server เพื่อร้องขอหน้าเวปเพจที่Client ต้องการ เมื่อ Server ได้รับ HTTP GET จาก Client แล้วก็จะตอบกลับมาด้วย HTTP Response ซึ่งอาจจะเป็นหน้าเวปที่ Client ร้องขอ หรืออาจจะแจ้งมาให้ Client ทราบว่าไม่มีหน้าเวปนี้อยู่ก็ได้



รูปที่ 1. Packet ที่ดักมาได้จากการร้องขอเวป csmju.jowave.com ใน Web browser

ตัวอย่างผลลัพธ์ของ Packet ที่ใช้งานโปรโตคอล HTTP ที่ดักมาได้ สามารถดูได้ดังรูปที่ 1 ซึ่ง Header ในส่วนที่เป็น HTTP หรือ Hypertext Transfer Protocol นั้นจะมีรายละเอียดต่างๆ ที่ใช้ในการสื่อสารระหว่าง Web browser และ Web server อยู่

จงตอบคำถามดังต่อไปนี้ โดยใช้ Packet HTTP GET ที่ดักมาได้

2.1 โปรแกรม Web browser ที่ใช้งานนั้นมีชื่อว่าอะไร (User Agents)

ตอบ Mozilla

2.2 Web Browser ที่ใช้งานอยู่นั้น ใช้งาน HTTP เวอร์ชั่นใด

ตอบ version 1.1

2.3 ภาษาที่ Web Browser นั้นรองรับมีภาษาอะไรบ้าง

ตอบ th-TH,th;q=0.8

2.4 IP Address ของเครื่องคอมพิวเตอร์เราคืออะไร

ตอบ 172.17.1.180

จงใช้ Packet ที่ดักมาได้จากการตอบกลับของ Server ตอบคำถามดังต่อไปนี้

2.5 เมื่อได้รับข้อความตอบกลับจาก Web Server เราจะได้ Status Code หรือรหัสการทำงานอะไรบ้าง

ตอบ HTTP/1.1 200 OK

2.6 โปรแกรม Web Server เป็นที่ใช้งานอยู่นั้นมีชื่อว่าอะไร

ตอบ Apache/2

2.7 ไฟล์ HTML ที่ได้รับมาจาก Web Server นั้นถูกแก้ไขครั้งล่าสุดเมื่อใด

ตอบ Tue, 24 Jan 2017 08:00:52 GMT

2.8 จงบอกขนาด (Bytes) ของ Object ที่ได้รับมาจาก Web Server (Content-Length)

ตอบ 384

ให้ลองเข้า Web Browser แล้วพิมพ์ URL ดังนี้ www.mju.ac.th

2.9 ให้ตรวจสอบว่าในข้อความ HTTP GET Request ที่ส่งจาก Web Browser ไปถึง Web Server มี Header Line ที่ชื่อว่า “IF-MODIFIED-SINCE” อยู่หรือไม่

ตอบ ไม่มี

2.10 ตรวจสอบว่า Web Server ส่งอะไรมาให้เรา

ตอบ 200K

2.11 จากนั้นให้ลองกด Refresh ที่ Web Browser แล้วดูว่าในข้อความ HTTP GET Request ส่งไปถึง Web Server เป็นครั้งที่ 2 นั้นมี Header Line ที่ชื่อว่า “IF-MODIFIED-SINCE” อยู่หรือไม่

ตอบ HTTP/1.1 304 Not Modified

2.12 หลังจากส่งข้อความ HTTP GET Request เป็นครั้งที่ 2 นั้นเราจะได้ข้อความ ตอบกลับจาก Web Server มา จงหา Status Code ของ Web Server จากข้อความที่ตอบกลับมาให้เรา

ตอบ HTTP/1.1 304 Not Modified

จากนั้นให้ลองเข้าเว็ปไซต์เช่น [www.sanook.com](http://www.sanook.com)

2.13 Web Browser ของเราส่งข้อความ HTTP GET Request มากกว่า 1 ครั้งใช่หรือไม่

ตอบ มากกว่า 1ครั้ง

2.14 ถ้าคำตอบของข้อที่ผ่านมา (2.12) คือใช่ ถามว่าเพราะอะไรจึงเป็นเช่นนั้น

ตอบ มีการ request มากกว่า 1Object

2.15 ระหว่างที่ส่งข้อมูลเป็นจำนวนมากเพื่อดาวโหลดหน้าเวปนี้ ได้เกิดการสูญหายของ Packet บ้างหรือไม่ ถ้าใช้เราจะรู้ได้อย่างไร

ตอบ เกิดการเสียหาย ดูจากแถบสีดำ