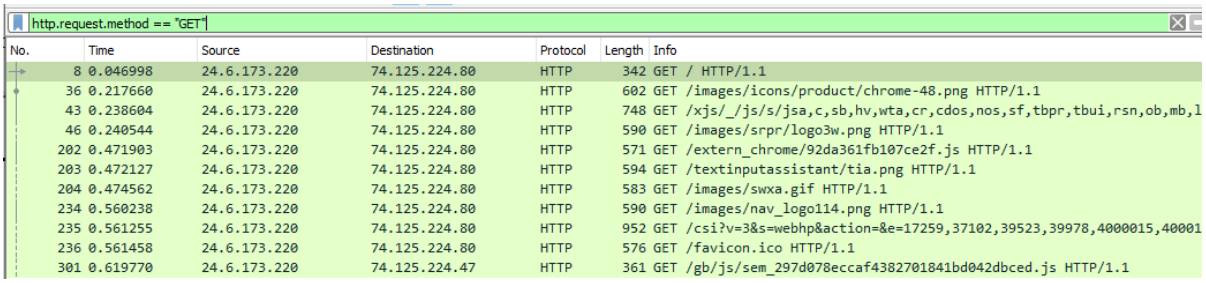
ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

กิจกรรมที่ 3 : การใช้ display filters

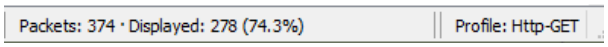
Q(3) : ให้ไปที่ display filter ให้ป้อนคำว่า http แล้วกด . จะเห็นว่า Wireshark แสดงตัวเลือกขึ้นมาให้เลือก ให้เลือก request.method ให้ป้อนให้ครบเป็น http.request.method=="GET" มีอะไรแสดงผล

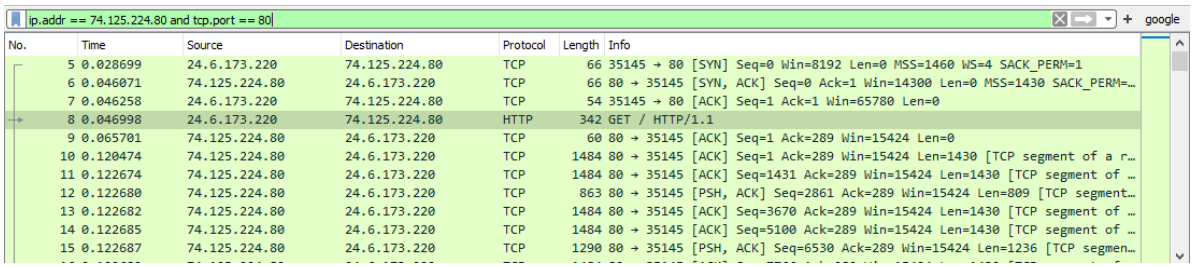
A(3) : ใน Packet List Pane จะแสดงเฉพาะ packet ที่ใช้งานโปโตคอล HTTP และมี method การใช้แบบ GET จำนวน 11 packet



Q(6) : ให้ลบ display filter (กดปุ่ม x) จากนั้นกดปุ่ม google เกิดอะไรขึ้น

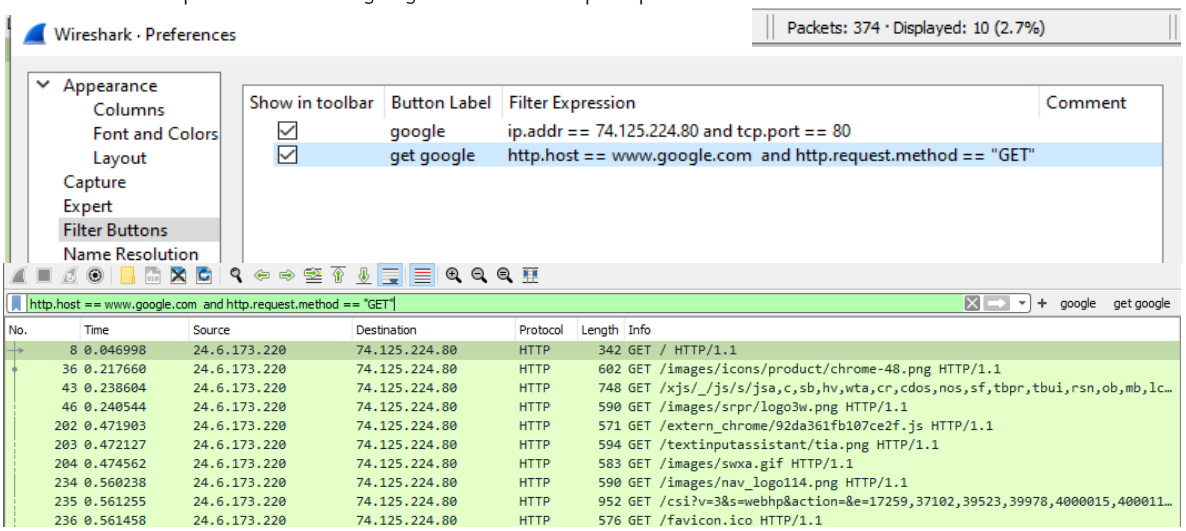
A(6) : เมื่อกดปุ่ม google ในช่อง Display filter จะปรากฏคำสั่งที่เรากรอกไว้ในตอนแรก **ip.addr == 74.125.224.80 and tcp.port == 80** ส่วนใน Packet List Pane จะแสดงเฉพาะ packet ที่มี IP Address เป็น 74.125.224.80 และมีการใช้งาน tcp port เป็น 80 จำนวน 278 packet





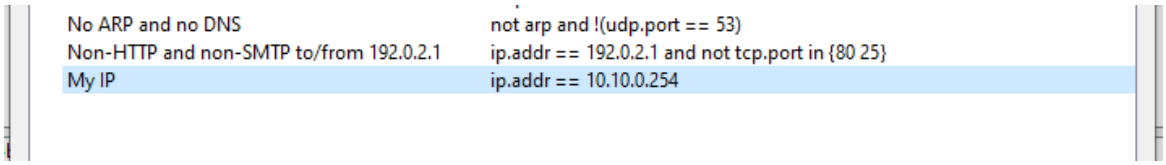
Q(7) : ให้ลบ display filter (กดปุ่ม x) จากนั้นกดปุ่ม google เกิดอะไรขึ้น

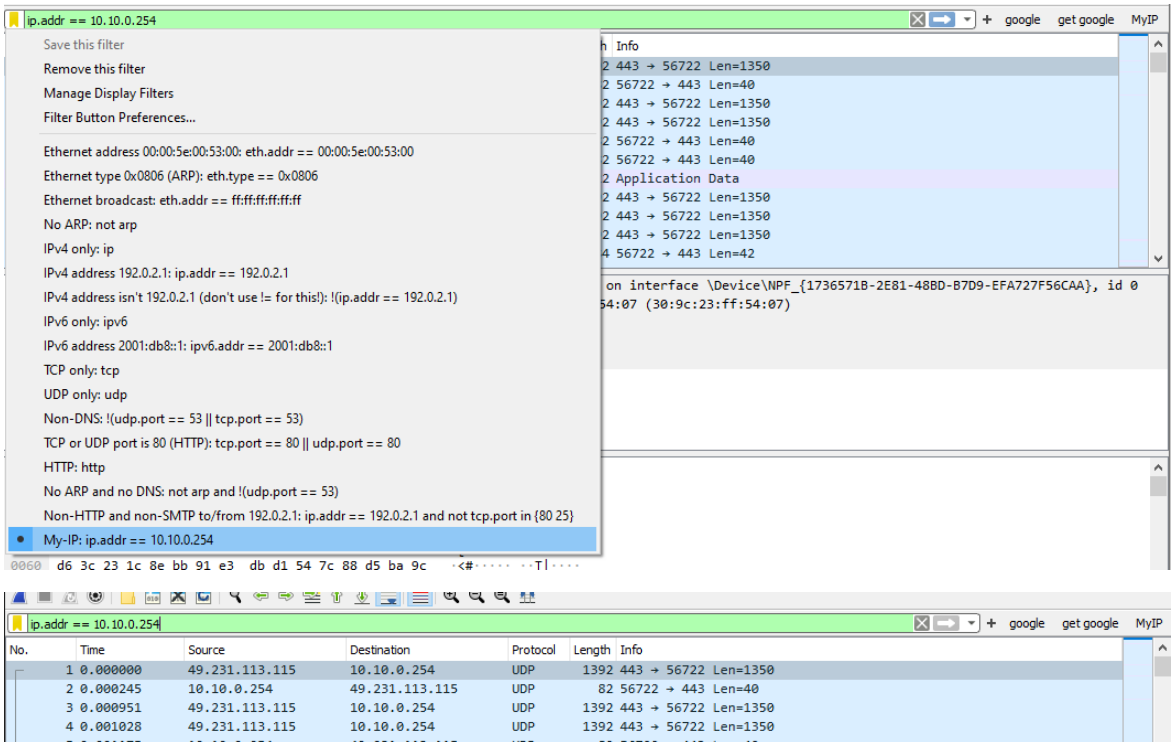
A(7) : กำหนดค่าเป็น http.host == www.google.com and http.request.method == “GET”



Q(10) : ให้เพิ่ม bookmark ของ display filter ที่เป็นการกรอง IP Address ของตัวเอง เข้าไปแล้ว capture มาแสดง ควรทดสอบโดยการ Capture แล้วกรองว่าแสดงเฉพาะ IP Address ของตัวเองจริงหรือไม่

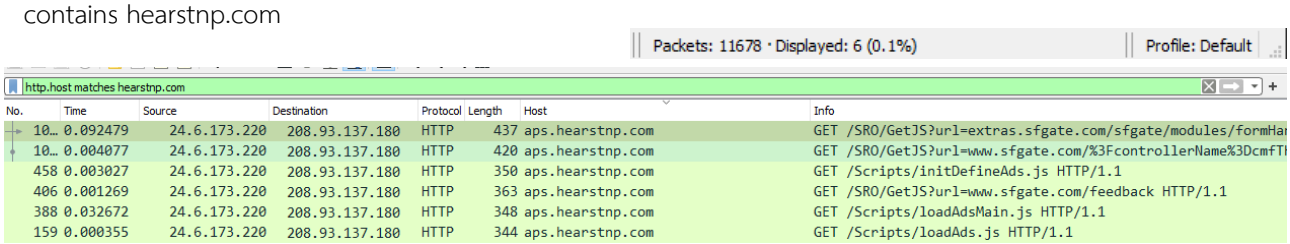
A(10) : IP Address คือ 10.10.0.254 ตั้งชื่อ bookmark คือ My-IP



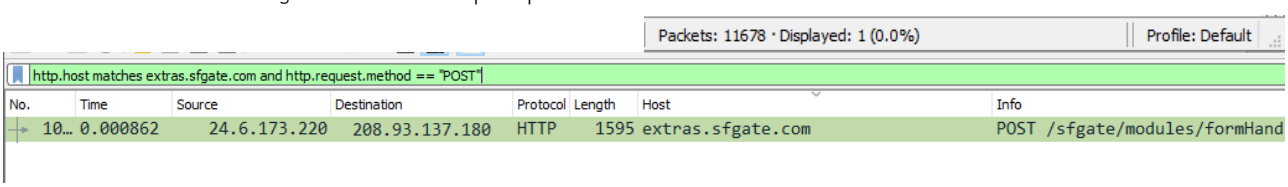


Q(12) : ให้เปิดไฟล์ http-sfgate101.pcapng และให้หา packet ที่ การ request ไปที่ hearstnp.com (มีจำนวน 6 ครั้ง) และ packet ที่ใช้ Method post ไปยัง extras.sfgate.com (มี 1 ครั้ง) ให้แสดงวิธีการ

A(12) : หา packet ที่ การ request ไปที่ hearstnp.com (มีจำนวน 6 ครั้ง) ทำได้โดยการพิมพ์ในช่อง Display filter ดังนี้ http.host contains hearstnp.com

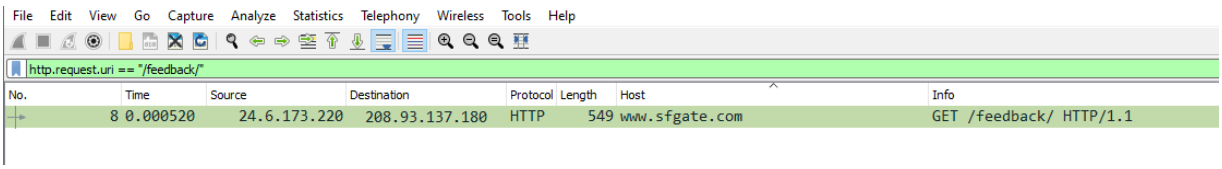


packet ที่ใช้ Method post ไปยัง extras.sfgate.com (มี 1 ครั้ง) ทำได้โดยการพิมพ์ในช่อง Display filter ดังนี้ http.host matches extras.sfgate.com and http.request.method == "POST"



Q(14) : ให้ยกเลิก display filter แล้วไปที่ packet ที่ 8 ไปที่ host แล้ว คลิกขวา แล้วเลือก Apply as Filter จากนั้นให้หาวิธีในการหา packet ที่ request ไปที่ http://www.sfgate.com/feedback

A(14) : ในช่อง Display filter ว่า http.reqest.uri == “/feedback/”



Q(16) : ให้หาว่าในไฟล์มีการโต้ตอบของ IP Address คู่ใดที่เกิดขึ้นมากที่สุด ให้สร้าง Filter ที่แสดงเฉพาะการโต้ตอบนั้น ให้บอกจำนวน Packet และ Filter ที่ปรากฏ

A(16) : ใน Conversations ในแถบเมนู IPv4 คลิกเลือกคอลัมน์ Packet ใน sort จากมากไปน้อย เราก็จะได้คู่ conversation ที่มีการใช้ปริมาณข้อมูลมากที่สุด จากนั้นคลิกขวา Apply as Filter > Selected > A <-> B จากนั้นที่ Display filter จะแสดง filter เป็น ip.addr==24.6.173.220 && ip.addr==184.84.222.144