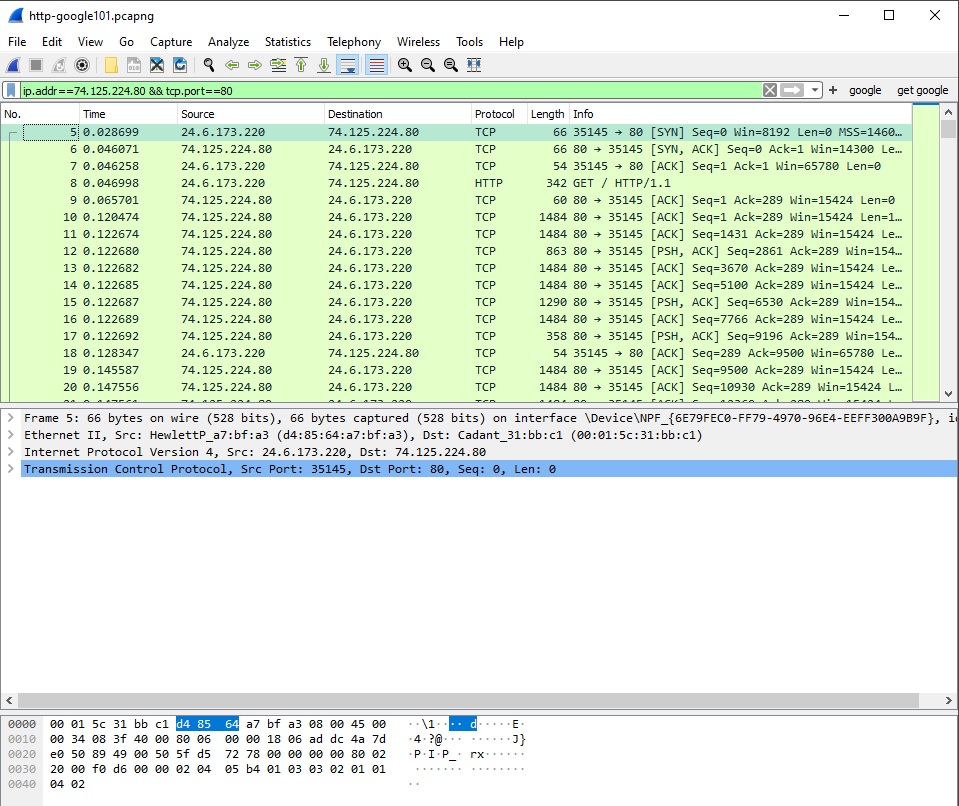
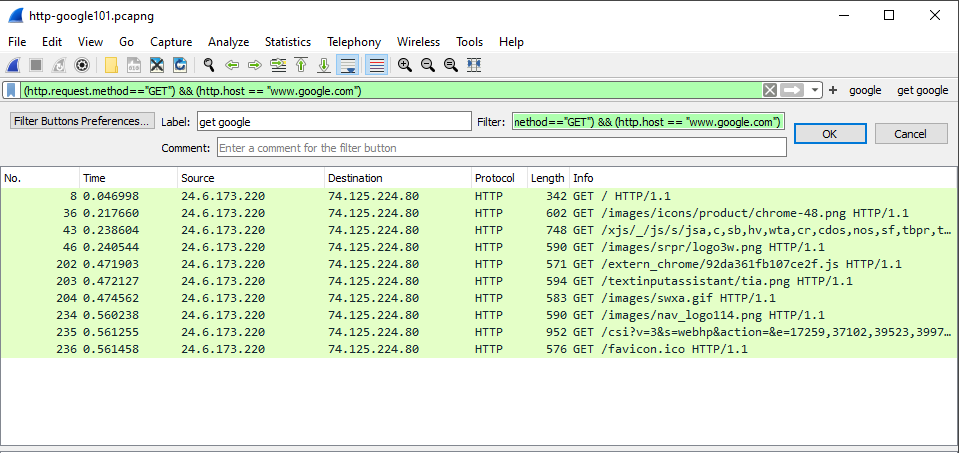
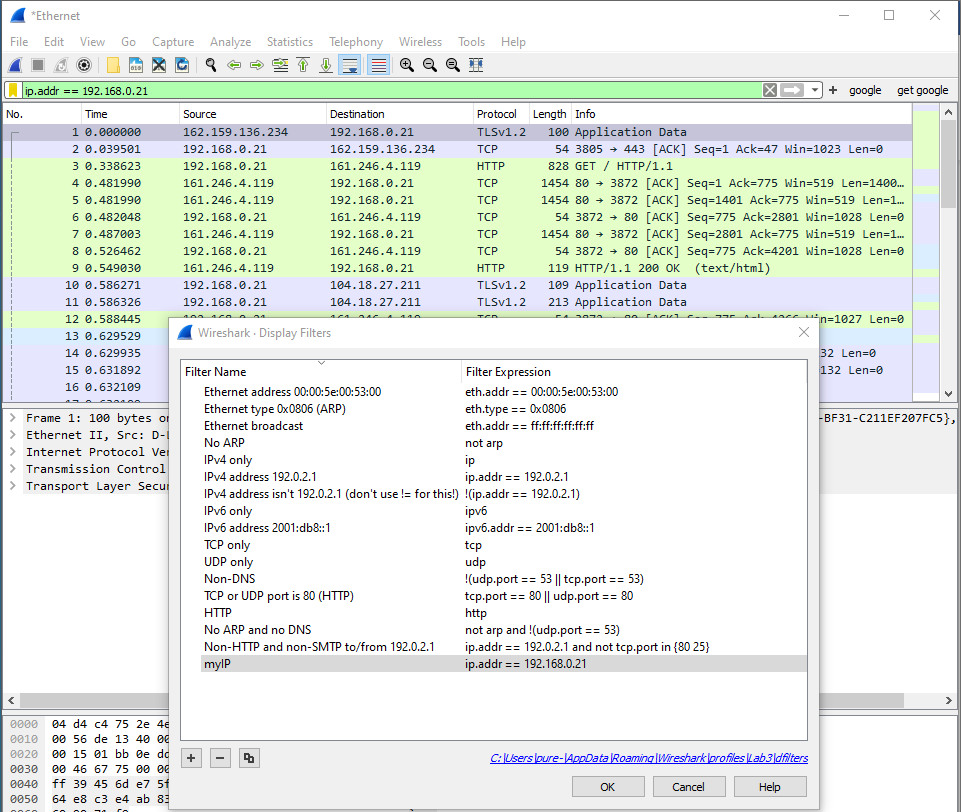
3. ให้ไปที่ display filter ให้ป้อนคำว่า http แล้วกด . จะเห็นว่า Wireshark แสดงตัวเลือกขึ้นมาให้เลือก ให้เลือก request.method ให้ป้อนให้ครบเป็น http.request.method=="GET" มีอะไรแสดงผล

6. ให้ลบ display filter (กดปุ่ม x) จากนั้นกดปุ่ม google เกิดอะไรขึ้น

ในช่อง display filter จะขึ้นตามที่ตั้งไว้

7. ให้สร้างปุ่ม get google โดยเมื่อกดแล้วให้แสดงเฉพาะเฟรมที่มี http ที่ GET ไปที่ www.google.com ให้แสดงส่วนที่ใช้ในการกำหนดค่า (คล้ายกับรูปในข้อที่ 5)



10. ให้เพิ่ม bookmark ของ display filter ที่เป็นการกรอง IP Address ของตัวเอง เข้าไปแล้ว capture มาแสดง ควรทดสอบโดยการ Capture แล้วกรองว่าแสดงเฉพาะ IP Address ของตัวเองจริงหรือไม่

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

1.ไปที่ display filter ให้ป้อนคำว่า http.request.method=="GET"

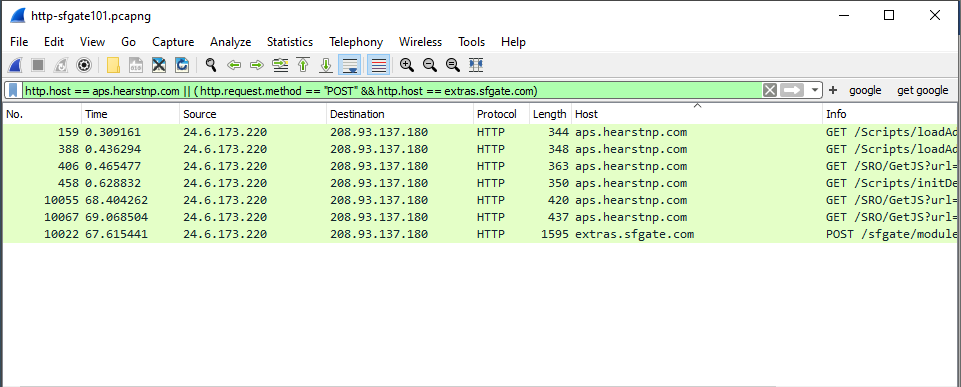
2.เพิ่มคอลัมน์ http.host

3.แล้วหา hearstnp.com ในคอลัมน์ host จะเจอ aps.hearstnp.com

4.ไปที่ display filter ให้ป้อนคำว่า http.host == aps.hearstnp.com จะได้ 6 packet

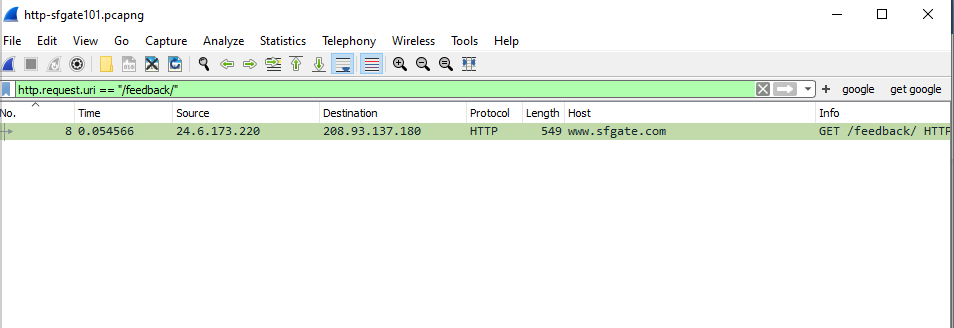
5.ไปที่ display filter ให้ป้อนคำว่า http.request.method == "POST" && http.host == extras.sfgate.com จะได้ 1 packet

6.ไปที่ display filter ให้ป้อนคำว่า http.host == aps.hearstnp.com || ( http.request.method == "POST" && http.host ==

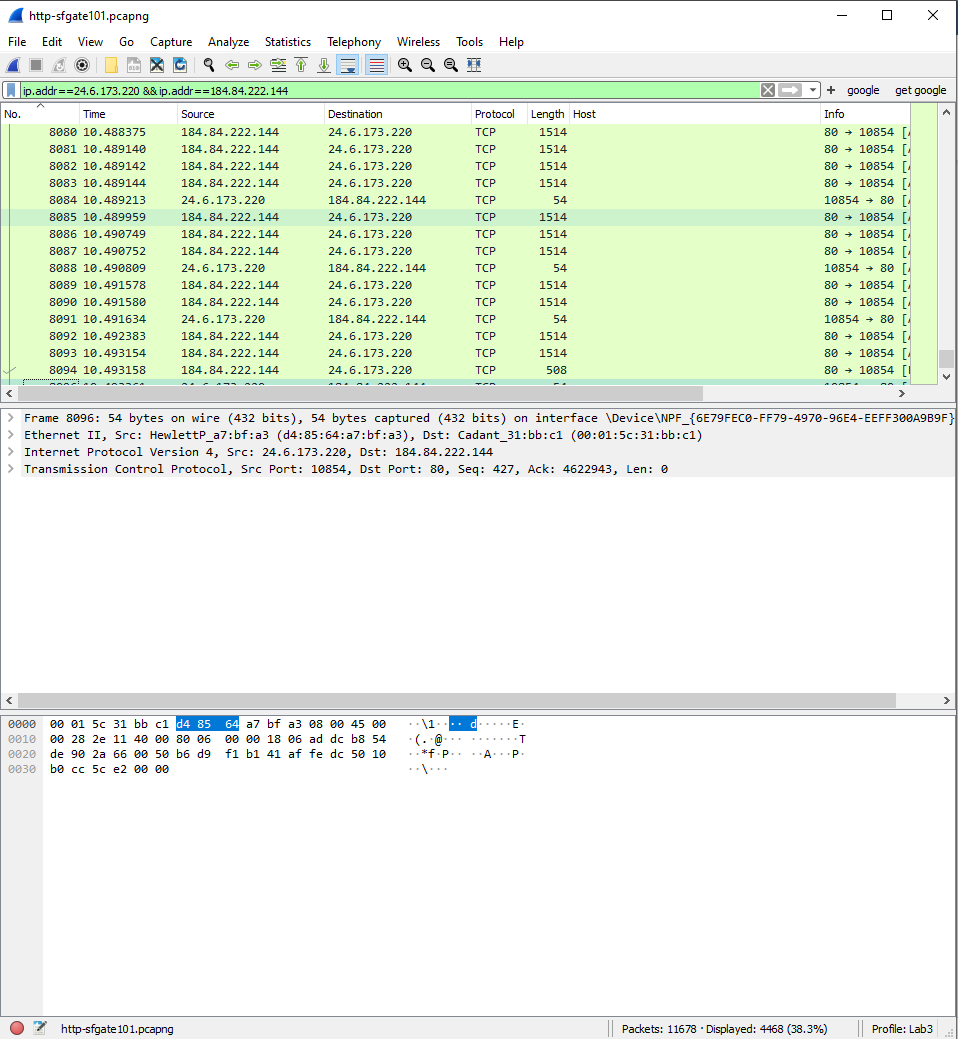
extras.sfgate.com) จะได้ 6+1 packet ดังนี้

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>

ไปที่ request uri คลิกขวา แล้วเลือก Apply as Filter เลือก selected



16. ให้หาว่าในไฟล์มีการโต้ตอบของ IP Address คู่ใดที่เกิดขึ้นมากที่สุด ให้สร้าง Filter ที่แสดงเฉพาะการโต้ตอบนั้น ให้บอกจำนวน Packet และ Filter ที่ปรากฏ



การโต้ตอบของ IP Address 24.6.173.220 และ 184.84.222.144 เยอะที่สุด มี 4468 packets และ filter

ที่ปรากฏ ip.addr==24.6.173.220 && ip.addr==184.84.222.144