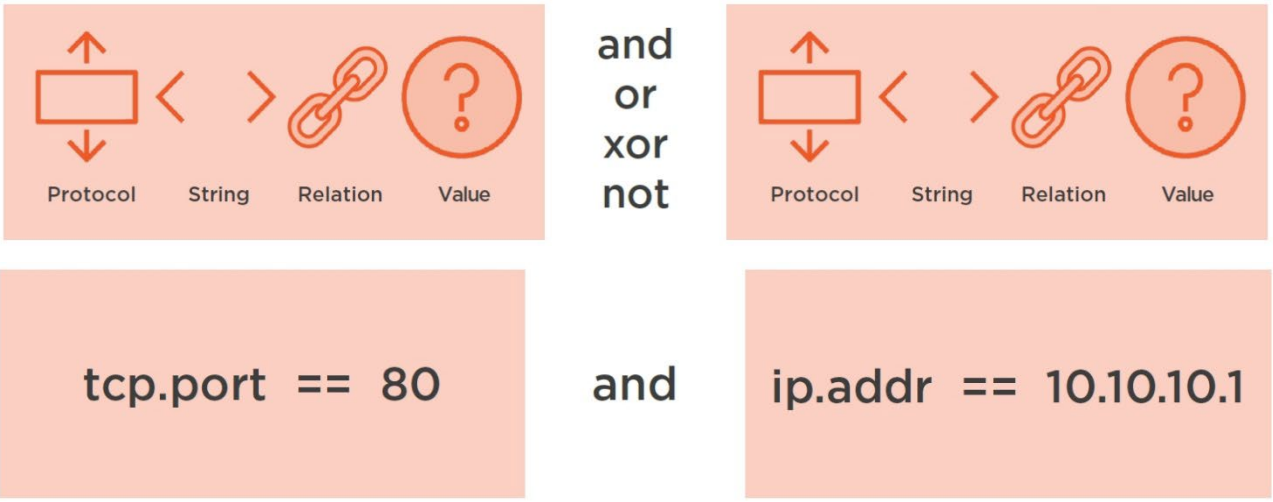
กิจกรรมที่ 3 : การใช้ display filters

ในกิจกรรมที่ผ่านมา นักศึกษาได้เรียนรู้การติดตั้งโปรแกรม และ การจัดการกับคอลัมน์ ในกิจกรรมนี้ จะทำความรู้จักกับ display filters

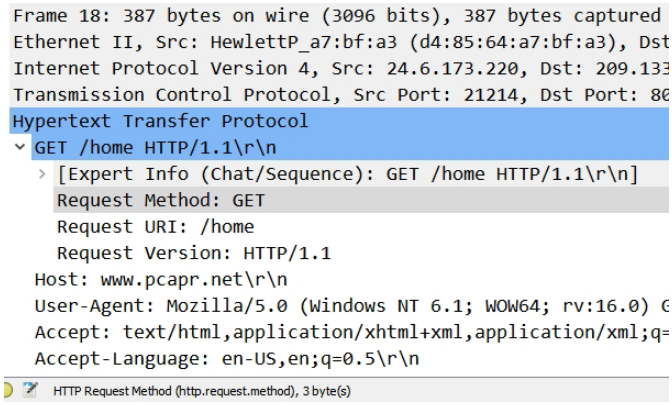
Display filters

เป็น filter ที่ใช้กรอง packet ที่แสดงผล เพื่อหา packet หรือ event ที่ต้องการ โดยรูปแบบการใช้งาน display filter มีรูปแบบดังนี้ (การใช้ display filter จะต่างจาก capture filter)



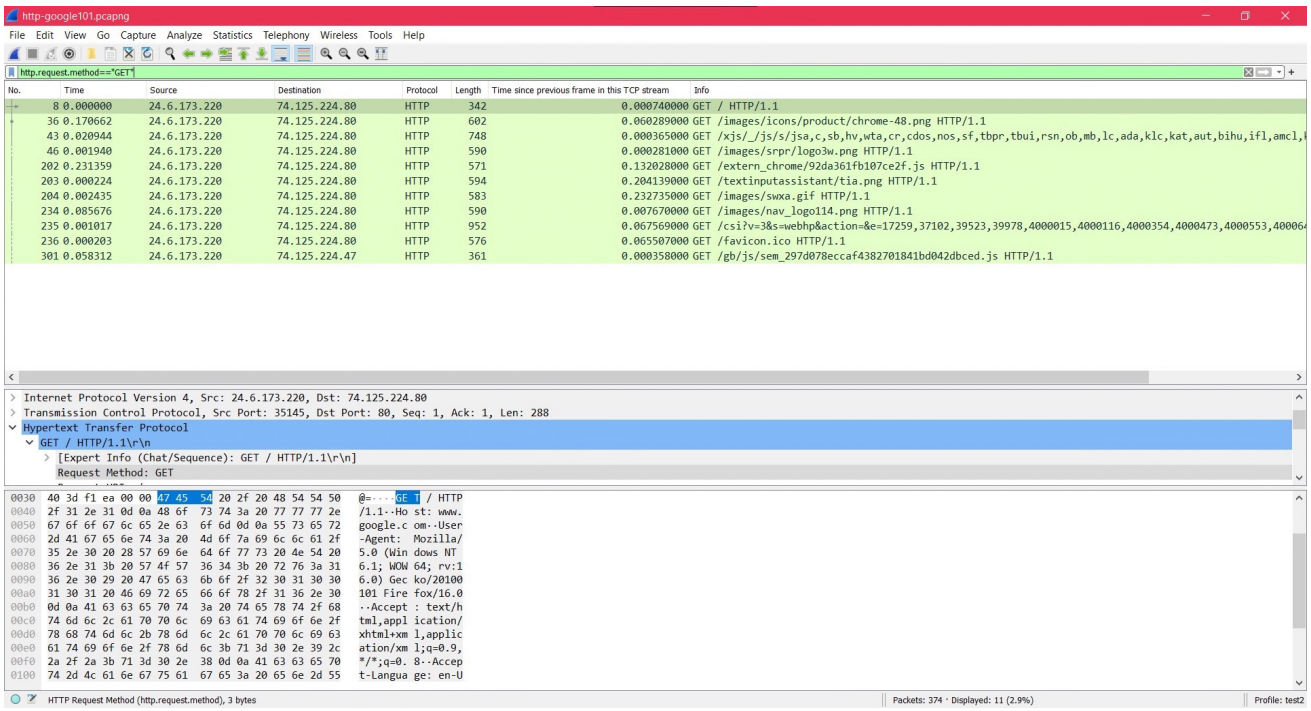
- Protocol สามารถใช้ได้ 3 แบบ
  - ใช้เฉพาะ protocol เช่น arp, ip, tcp, dns, http, icmp
  - ระบุลงถึงข้อมูลในฟิลด์ของ protocol เช่น http.host, ftp.request.command
  - ระบุโดยใช้คุณลักษณะที่ Wireshark สร้างขึ้น เช่น tcp.analysis.flags
- Relation คล้ายกับภาษาโปรแกรม ได้แก่ == หรือ eq, != หรือ ne, > หรือ gt, < หรือ lt, >= หรือ ge, <= หรือ lt และ Contains
- ตัวอย่าง
  - ip.src == 10.2.2.2
  - frame.time_relative > 1 (แสดง packet ที่มาเกิน 1 วินาทีจาก packet ก่อนหน้า)
  - http contains "GET"

1. เปิดไฟล์ http-google101.pcapng และสร้าง Configuration Profile ใหม่
2. ไปที่ frame ที่ 8 ใต้ Hypertext Transfer Protocol แล้วขยายที่ GET ตามรูป เอาเมาส์คลิกที่ Request Method ให้ดูที่ Status Bar จะเห็นข้อความ http.request.method ซึ่งเป็นชื่อฟิลด์ใน protocol HTTP



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

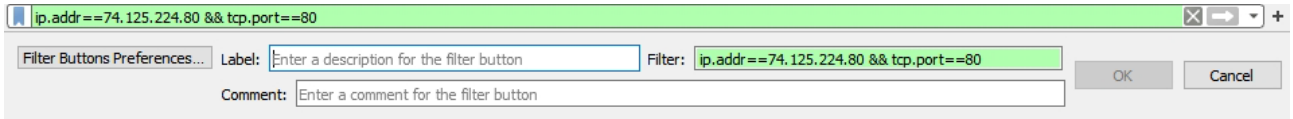
แสดงแค่ packet ที่มี GET



Display Filter Button

ในกรณีที่มีบาง Display filter ที่เราใช้บ่อยๆ สามารถจะเพิ่มเข้าไปใน Toolbar ได้

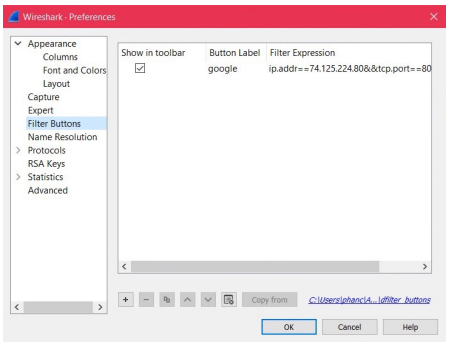
4. ให้ป้อน ip.addr==74.125.224.80 && tcp.port==80 ในช่อง display filter
5. กดปุ่ม + ที่ด้านขวาสุดของ display filter จะปรากฏตามรูป ให้ป้อน google ลงในช่อง Label แล้วกด OK



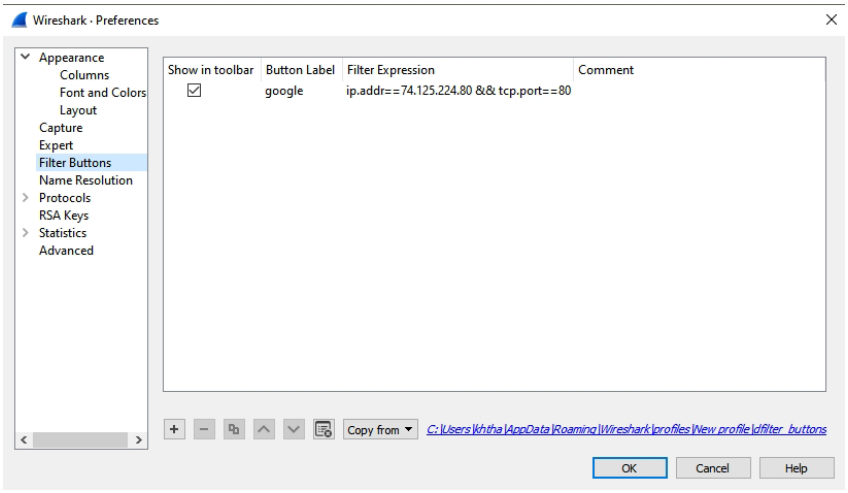
6. ให้ลบ display filter (กดปุ่ม x) จากนั้นกดปุ่ม google เกิดอะไรขึ้น

สร้าง ตัวแปร ชื่อ Label คือ google เมื่อเลือกปุ่ม google จะแสดง packet ข้อมูลที่พิมพ์ใน display fliter

7. ให้สร้างปุ่ม get google โดยเมื่อกดแล้วให้แสดงเฉพาะเฟรมที่มี http ที่ GET ไปที่ www.google.com ให้แสดงส่วนที่ใช้ในการกำหนดค่า (ให้ Capture เฉพาะส่วนกำหนดค่าคล้ายกับรูปในข้อที่ 5 มาแปะ)

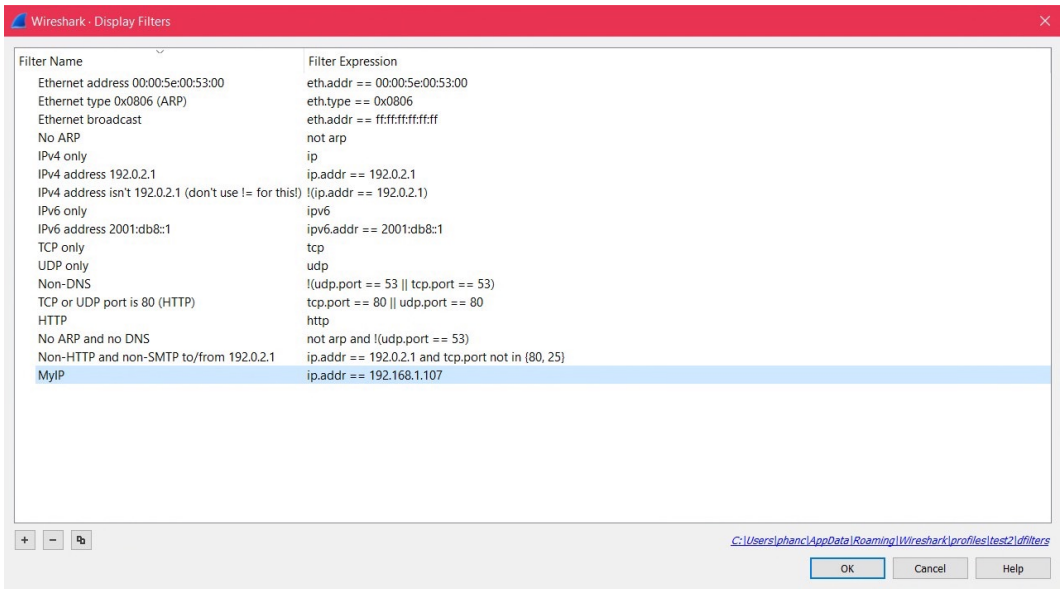


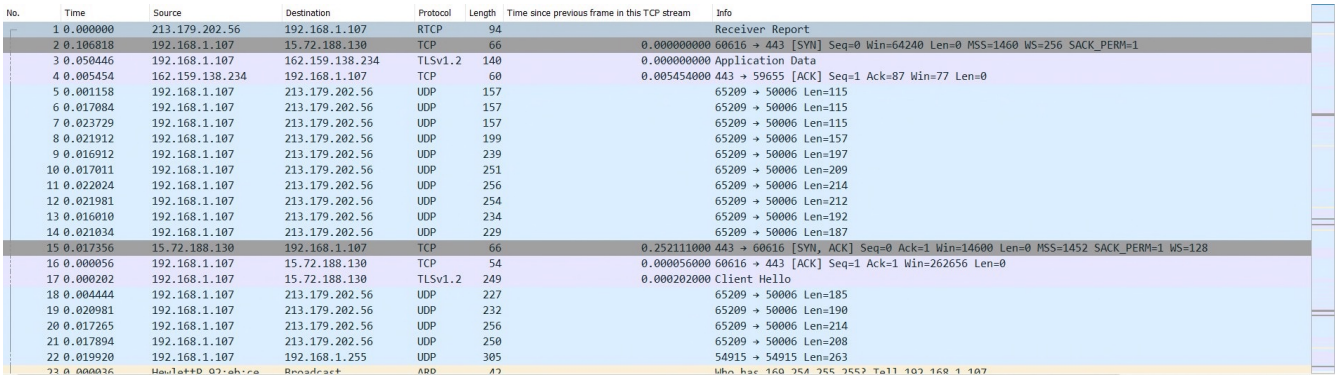
8. ให้กดปุ่ม ที่อยู่ด้านหน้าของ display filter แล้วเลือก Filter Button Preferences.. จะปรากฏหน้าต่างขึ้นมาตามรูป ซึ่งสามารถ เพิ่ม ลบ คัดลอก Filter Button ได้



Display Filter Bookmark

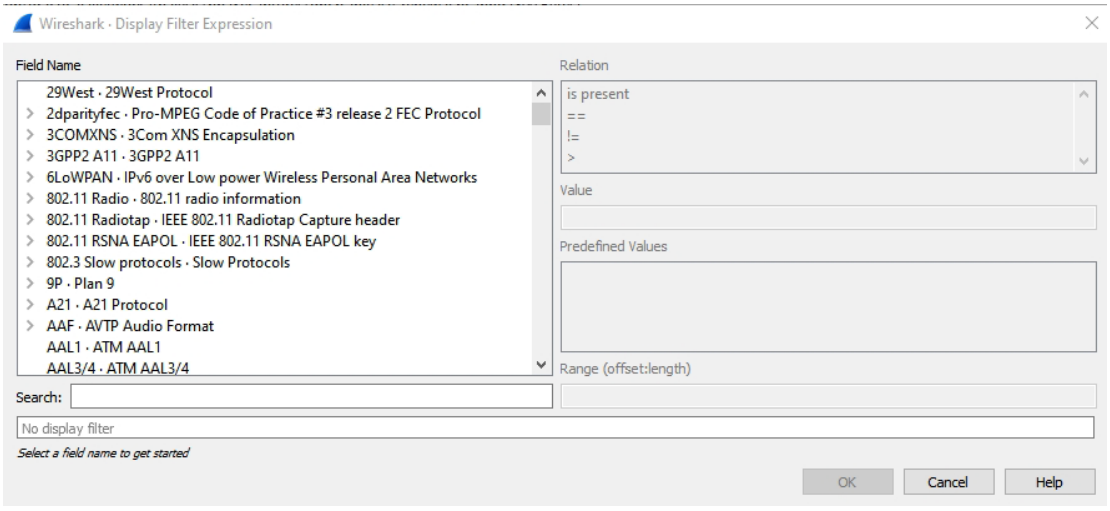
9. ยังสามารถจะสร้าง Bookmark ของ Display filter ได้ โดยกดปุ่ม และเลือก Manage Display Filters ซึ่งสามารถสร้าง ลบ หรือคัดลอกได้
10. ให้เพิ่ม bookmark ของ display filter ชื่อ MyIP โดยเป็นการกรองเฉพาะ IP Address ของตัวเอง (ไปที่ cmd แล้วใช้คำสั่ง ipconfig เพื่อดู IP Address ของเครื่องตนเอง) จากนั้นให้ทดลอง capture Packet และเข้าเว็บต่างๆ ว่าแสดงเฉพาะ IP Address ของตัวเองจริงหรือไม่ (ให้ capture หน้าต่าง Manage Display Filters ที่มีการกรองเฉพาะ IP ตัวเองมาแสดง และ Capture หน้าผลการทำงานของ Filter)





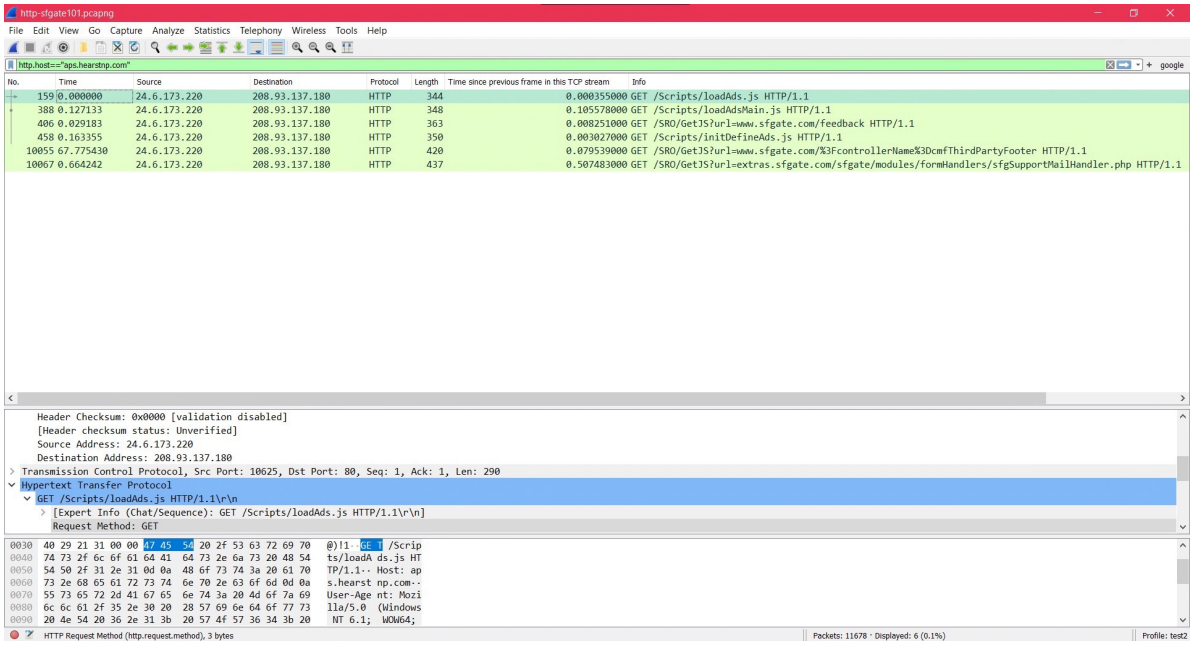
Display Filter Expression

11. คลิกขวาที่ช่อง display filter แล้วเลือก Display Filter Expression จะปรากฏหน้าต่างตามรูป ซึ่งสามารถใช้ในการช่วยสร้าง display filter ได้



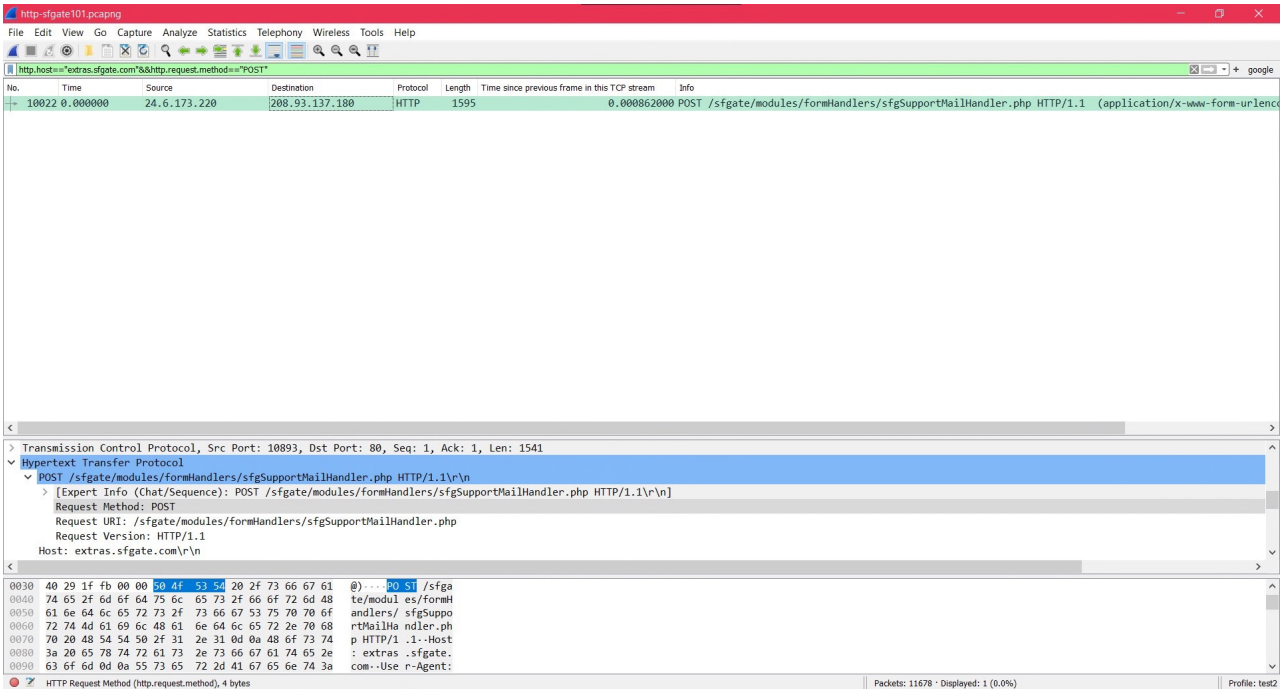
12. ให้เปิดไฟล์ http-sfgate101.pcapng และให้หา packet ที่ การ request ไปที่ hearstnp.com (มีจำนวน 6 ครั้ง) ให้แสดงวิธีการที่สั้นที่สุด และ ผลการทำงาน

พิมพ์ในช่อง display fliter ว่า http.host=="aps.heartnp.com"
จะได้ packet ที่ request ไปที่ heartnp.com



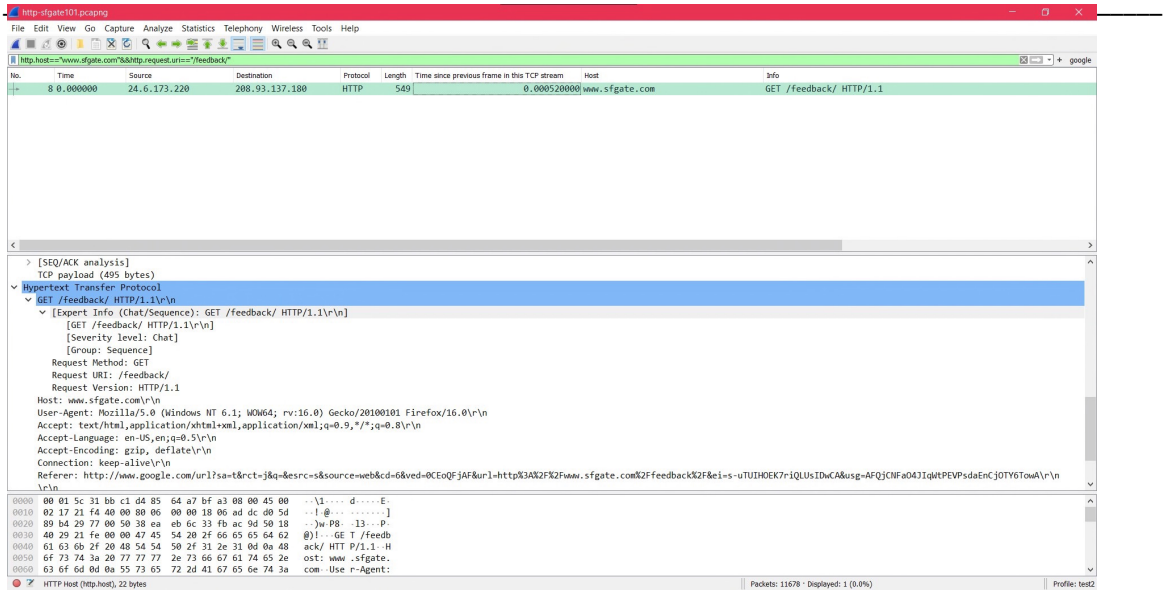
13. ให้หา packet ที่ การ request ไปที่ hearstnp.com (มีจำนวน 6 ครั้ง) และ packet ที่ใช้ Method post ไปยัง extras.sfgate.com (มี 1 ครั้ง) ให้แสดงวิธีการที่สั้นที่สุด และ ผลการทำงาน

พิมพ์ในช่อง display fiter ว่า
http.host=="extras.sfgate.com" && http.request.method=="POST"



14. ยังมีอีกวิธีที่สามารถจะสร้าง display filter ได้ คือ การสร้างจากต้นแบบ โดยการไปที่ packet ที่จะใช้เป็นต้นแบบ และเลือกฟิลด์ที่ต้องการและ คลิกขวา แล้วเลือก Apply as Filter
15. 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 ที่สั้นที่สุด

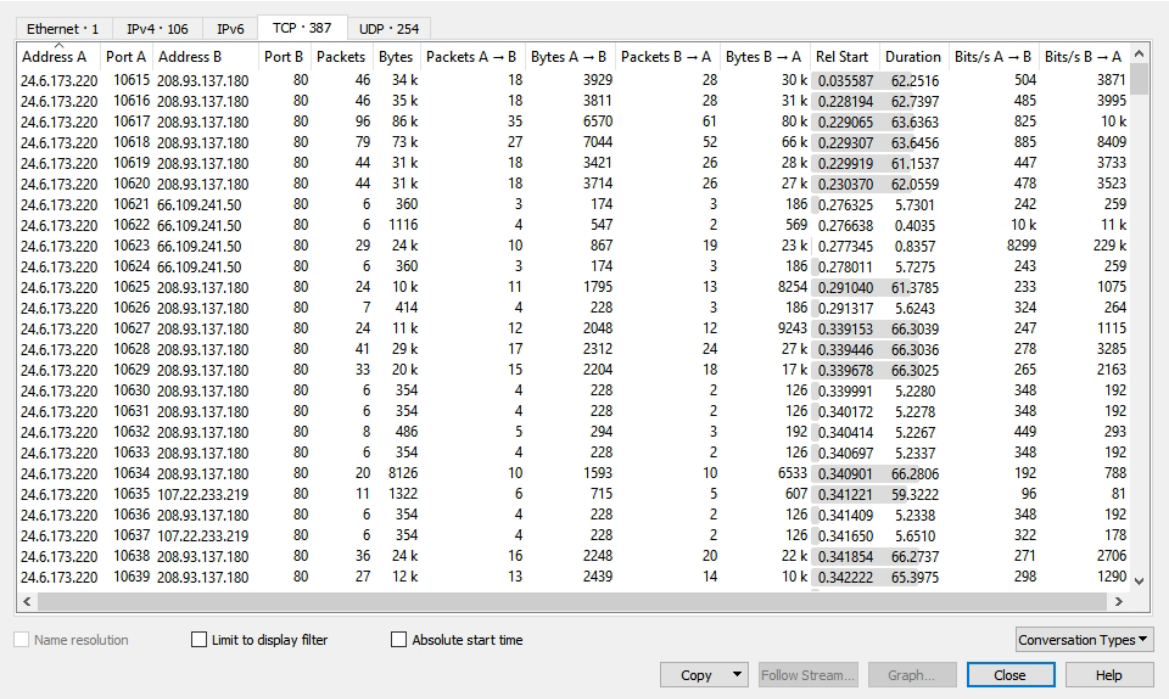
http.host == "www.sfgate.com" && http.request.uri == "/feedback/"



Statistics

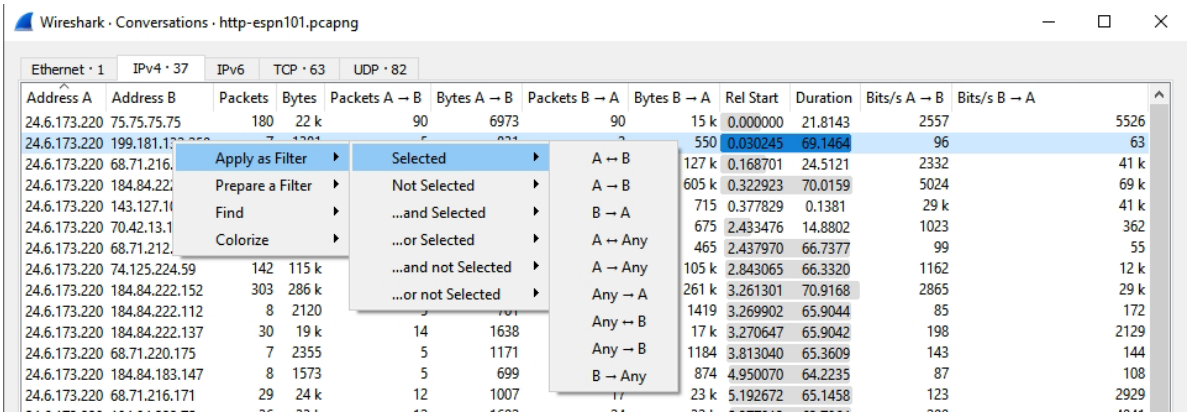
Statistics | Conversation บางครั้งเราต้องการวิเคราะห์ การสื่อสารระหว่าง Client และ Server ดังนั้นเราจะสนใจการโต้ตอบ (Conversation)

16. ให้เลือก Statistics | Conversations จะแสดงหน้าต่างดังรูป



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
24.6.173.220	10615	208.93.137.180	80	46	34 k	18	3929	28	30 k	0.035587	62.2516	504	3871
24.6.173.220	10616	208.93.137.180	80	46	35 k	18	3811	28	31 k	0.228194	62.7397	485	3995
24.6.173.220	10617	208.93.137.180	80	96	86 k	35	6570	61	80 k	0.229065	63.6363	825	10 k
24.6.173.220	10618	208.93.137.180	80	79	73 k	27	7044	52	66 k	0.229307	63.6456	885	8409
24.6.173.220	10619	208.93.137.180	80	44	31 k	18	3421	26	28 k	0.229919	61.1537	447	3733
24.6.173.220	10620	208.93.137.180	80	44	31 k	18	3714	26	27 k	0.230370	62.0559	478	3523
24.6.173.220	10621	66.109.241.50	80	6	360	3	174	3	186	0.276325	5.7301	242	259
24.6.173.220	10622	66.109.241.50	80	6	1116	4	547	2	569	0.276638	0.4035	10 k	11 k
24.6.173.220	10623	66.109.241.50	80	29	24 k	10	867	19	23 k	0.277345	0.8357	8299	229 k
24.6.173.220	10624	66.109.241.50	80	6	360	3	174	3	186	0.278011	5.7275	243	259
24.6.173.220	10625	208.93.137.180	80	24	10 k	11	1795	13	8254	0.291040	61.3785	233	1075
24.6.173.220	10626	208.93.137.180	80	7	414	4	228	3	186	0.291317	5.6243	324	264
24.6.173.220	10627	208.93.137.180	80	24	11 k	12	2048	12	9243	0.339153	66.3039	247	1115
24.6.173.220	10628	208.93.137.180	80	41	29 k	17	2312	24	27 k	0.339446	66.3036	278	3285
24.6.173.220	10629	208.93.137.180	80	33	20 k	15	2204	18	17 k	0.339678	66.3025	265	2163
24.6.173.220	10630	208.93.137.180	80	6	354	4	228	2	126	0.339991	5.2280	348	192
24.6.173.220	10631	208.93.137.180	80	6	354	4	228	2	126	0.340172	5.2278	348	192
24.6.173.220	10632	208.93.137.180	80	8	486	5	294	3	192	0.340414	5.2267	449	293
24.6.173.220	10633	208.93.137.180	80	6	354	4	228	2	126	0.340697	5.2337	348	192
24.6.173.220	10634	208.93.137.180	80	20	8126	10	1593	10	6533	0.340901	66.2806	192	788
24.6.173.220	10635	107.22.233.219	80	11	1322	6	715	5	607	0.341221	59.3222	96	81
24.6.173.220	10636	208.93.137.180	80	6	354	4	228	2	126	0.341409	5.2338	348	192
24.6.173.220	10637	107.22.233.219	80	6	354	4	228	2	126	0.341650	5.6510	322	178
24.6.173.220	10638	208.93.137.180	80	36	24 k	16	2248	20	22 k	0.341854	66.2737	271	2706
24.6.173.220	10639	208.93.137.180	80	27	12 k	13	2439	14	10 k	0.342222	65.3975	298	1290

- ซึ่งแสดงการโต้ตอบที่เกิดขึ้นในไฟล์ ทำให้เห็นว่าเครื่องคู่ไหนที่สร้าง traffic จำนวนมาก ซึ่งอาจจะก่อกวนระบบเครือข่ายได้ จากนั้นเราสามารถเลือกให้ Wireshark แสดงเฉพาะ traffic จาก Conversation นั้นๆ โดยการคลิกขวาที่ Conversation ที่เลือก แล้วเลือก Apply as Filter



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

4468 Packet ระหว่าง 24.6.173.220 กับ 184.84.222.144 เป็น A↔B

Fliter ใช้ ip.addr == 24.6.173.220 && ip.addr == 184.84.222.144

งานครั้งที่ 3

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งโดยเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา และ _Lab3 เช่น 63010789_Lab3.pdf
- กำหนดส่ง ภายในวันที่ 2 กุมภาพันธ์ 2563