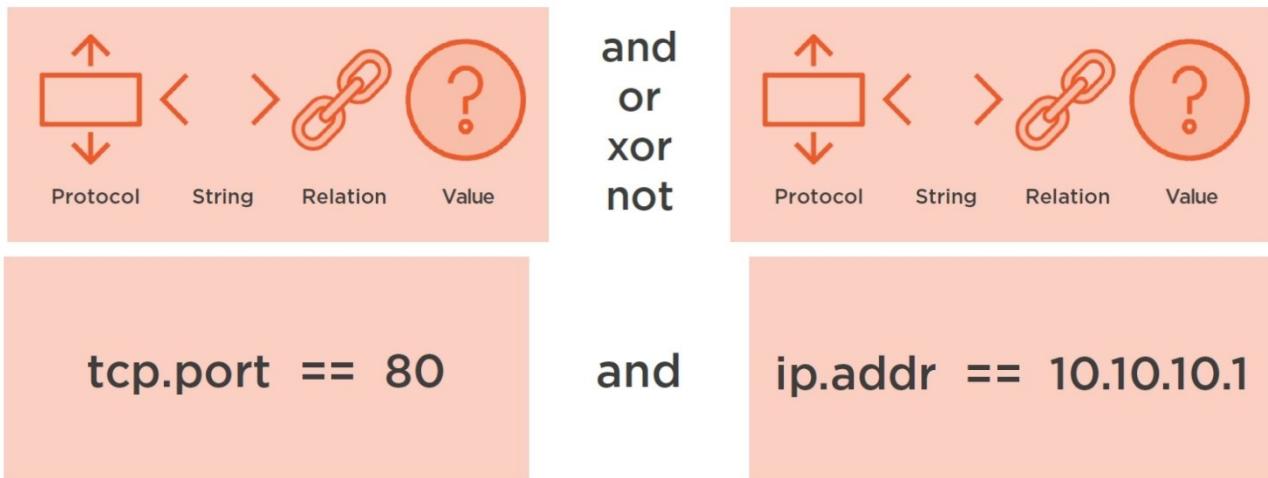


กิจกรรมที่ 3 : การใช้ display filters

ในกิจกรรมที่ผ่านมา นักศึกษาได้เรียนรู้การติดตั้งโปรแกรม และ การจัดการกับคอมมาน์ดในกิจกรรมนี้ 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
 - ระบุลงถึงช้อมูลในฟิลด์ของ 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 ที่มากิน 1 วินาทีจาก packet ก่อนหน้า)
 - http contains "GET"

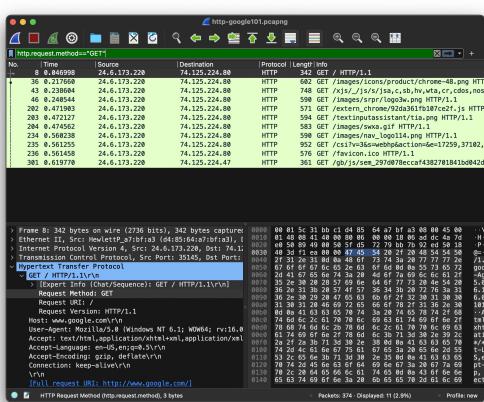
1. เปิดไฟล์ http-google101.pcapng และสร้าง Configuration Profile ใหม่
2. ไปที่ frame ที่ 8 ให้ Hypertext Transfer Protocol แล้วขยายที่ GET ตามรูป เอามาสีคลิกที่ Request Method ให้ดูที่ Status Bar จะเห็นข้อความ http.request.method ซึ่งเป็นชื่อฟิล์ดใน protocol HTTP

```
Frame 18: 387 bytes on wire (3096 bits), 387 bytes captured
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: 209.133
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 209.133
Transmission Control Protocol, Src Port: 21214, Dst Port: 80
Hypertext Transfer Protocol
  GET /home HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /home HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /home
    Request Version: HTTP/1.1
    Host: www.pcapr.net\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) G
    Accept: text/html,application/xhtml+xml,application/xml;q=
    Accept-Language: en-US,en;q=0.5\r\n

```

HTTP Request Method (http.request.method), 3 byte(s)

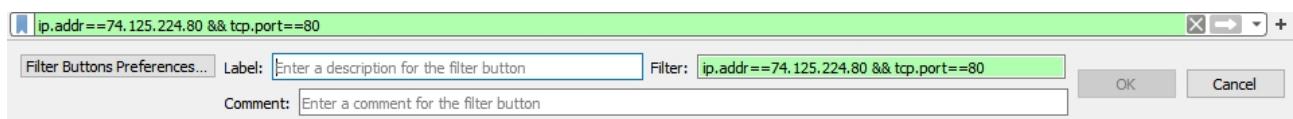
3. ให้ไปที่ display filter ให้ป้อนคำว่า http แล้วกด . จะเห็นว่า Wireshark แสดงตัวเลือกขึ้นมาให้เลือก ให้เลือก request.method ให้ป้อนให้ครบเป็น http.request.method=="GET" มีอะไรแสดงผล จงเขียนขอรับรายละเอียดบันทึก screenshot ผลลัพธ์นำมาแสดง



เมื่อกดปุ่ม google จะขึ้น filter ที่เราตั้งไว้ คือ ip.addr และบันทึกที่ปุ่มการ GET

Display Filter Button

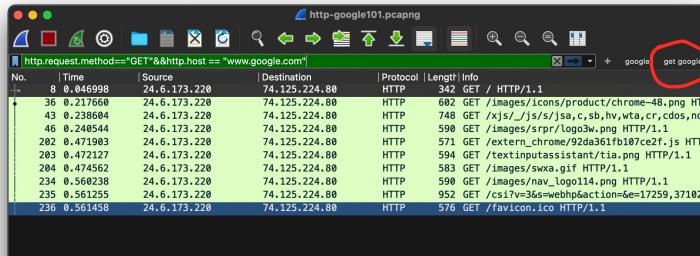
- ในการถ้าที่มีบาง Display filter ที่เราใช้บ่อยๆ สามารถเพิ่มเข้าไปใน Toolbar ได้
4. ให้ป้อน ip.addr==74.125.224.80 && tcp.port==80 ในช่อง display filter
 5. กดปุ่ม + ที่ด้านขวาสุดของ display filter จะปรากฏตามรูป ให้ป้อน google ลงในช่อง Label และกด OK



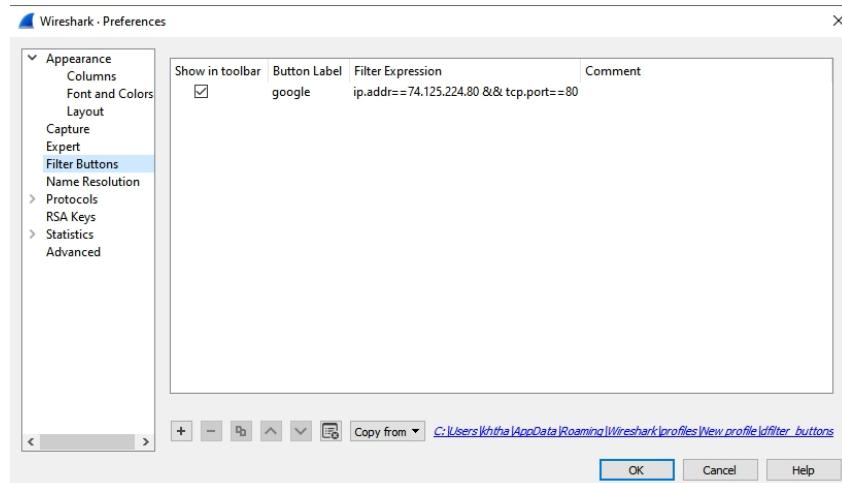
6. ให้ลบ display filter (กดปุ่ม x) จากนั้นกดปุ่ม google เกิดอะไรขึ้น

เมื่อกดปุ่ม google จะขึ้น filter ที่เราตั้งไว้ คือ ip.addr และบันทึกที่ปุ่มการ GET

7. ให้สร้างปุ่ม get google โดยเมื่อกดแล้วให้แสดงเฉพาะเฟรมที่มี http ที่ GET ไปที่ www.google.com ให้บันทึก screenshot ของส่วนที่ใช้ในการกำหนดค่าการแสดง

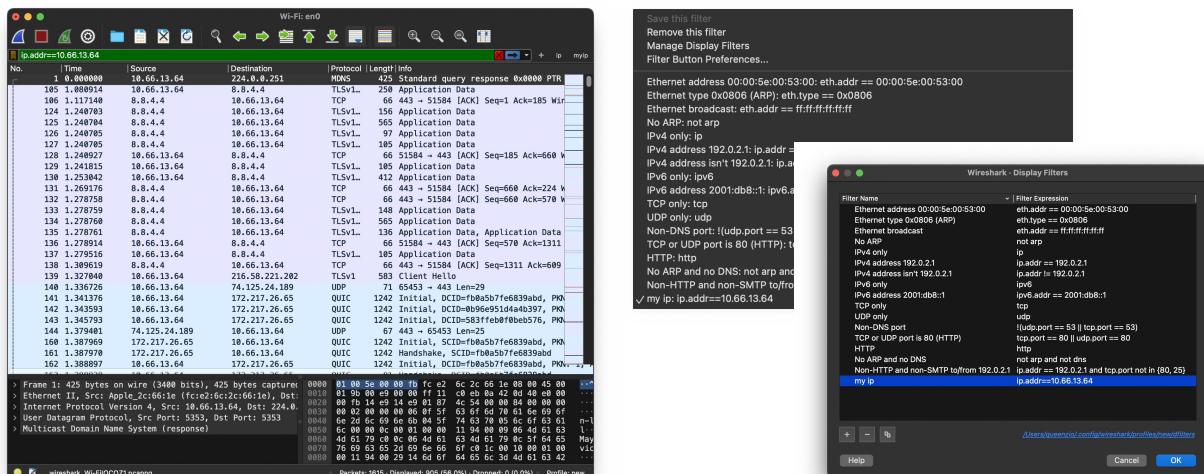


8. ให้กดปุ่ม ที่อยู่ด้านหน้าของ display filter และเลือก Filter Button Preferences.. จะปรากฏหน้าต่างขึ้นมาตามรูป ซึ่งสามารถเพิ่ม ลบ คัดลอก Filter Button ได้



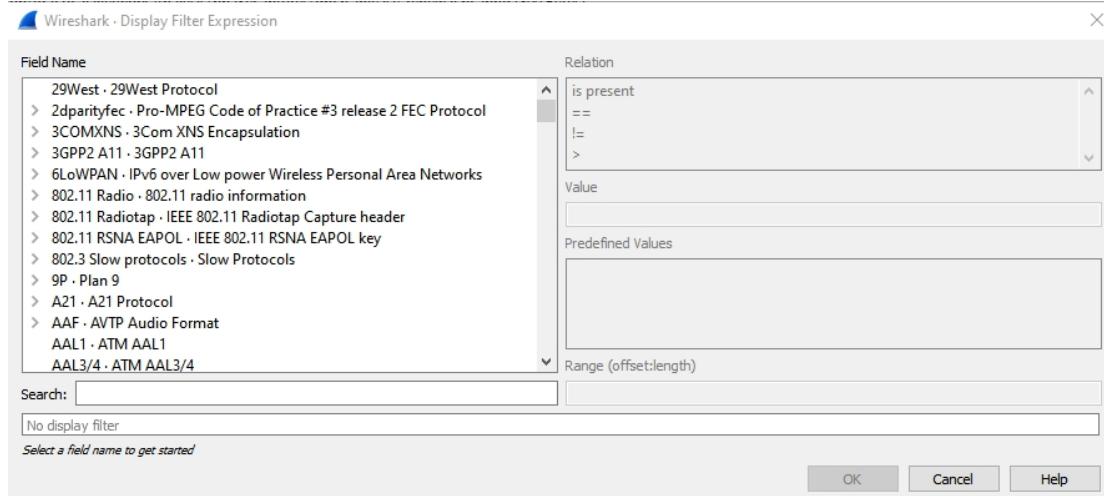
Display Filter Bookmark

9. สามารถสร้าง Bookmark ของ Display filter ได้ โดยกดปุ่ม และเลือก Manage Display Filters ซึ่งสามารถสร้าง ลบ หรือคัดลอกได้
10. ให้เพิ่ม bookmark ของ display filter ที่เป็นการกรอง IP Address ของตัวเองเข้าไป (ไปที่ cmd และใช้คำสั่ง ipconfig เพื่อดู IP Address) จากนั้นให้ capture และเข้าเว็บต่างๆ ว่าแสดงเฉพาะ IP Address ของตัวเองจริงหรือไม่ ให้บันทึก screenshot หน้าต่าง Manage Display Filters ที่มีการกรองเฉพาะ IP ตัวเองมาแสดงรวมถึงบันทึก screenshot ผลลัพธ์ใน Packet List Pane จากการใช้ Filter ดังกล่าวมาแสดงด้วย



Display Filter Expression

11. คลิกขวาที่ช่อง display filter และเลือก Display Filter Expression จะปรากฏหน้าต่างตามรูป ซึ่งสามารถใช้ในการสร้าง display filter ได้



12. เปิดไฟล์ http-sfgate101.pcapng สร้าง display filter เพื่อค้นหาและแสดง packet ที่ส่ง request ไปยัง host ที่อยู่ภายใต้โดเมนชื่อ hearstnp.com (มีจำนวน 6 ครั้ง) เขียนขอรับ display filter ที่ใช้พร้อมทั้งบันทึก screenshot ผลลัพธ์นำมาแสดง

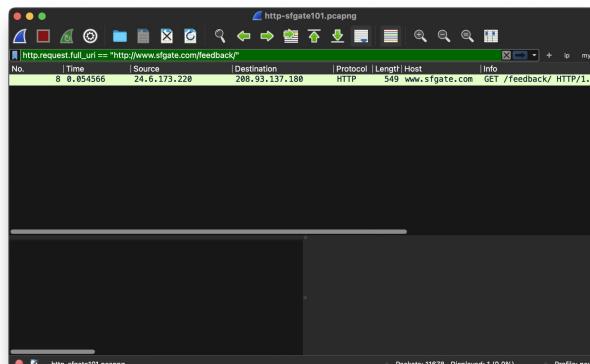
No.	Time	Source	Destination	Protocol	Length	Host	Info
152	0.436241	24.6.173.220	208.93.137.180	HTTP	344	http://hearstnp.com	GET /index.php?route=common/footer&language_id=1
388	0.436294	24.6.173.220	208.93.137.180	HTTP	348	http://hearstnp.com	GET /script/loader/main.js
486	0.465477	24.6.173.220	208.93.137.180	HTTP	363	http://hearstnp.com	GET /SR0/GetJSUrl/www.js
458	0.628832	24.6.173.220	208.93.137.180	HTTP	358	http://hearstnp.com	GET /Scripts/initDefineA
18855	68.484262	24.6.173.220	208.93.137.180	HTTP	420	http://hearstnp.com	GET /SR0/GetJSUrl/www.js
18867	69.868584	24.6.173.220	208.93.137.180	HTTP	437	http://hearstnp.com	GET /SR0/GetJSUrl/extr

13. จากไฟล์ http-sfgate101.pcapng สร้าง display filter เพื่อค้นหาและแสดง packet ที่ใช้ Method POST ไปยัง extras.sfgate.com เขียนขอรับ display filter ที่ใช้พร้อมทั้งบันทึก screenshot ผลลัพธ์นำมาแสดง

No.	Time	Source	Destination	Protocol	Length	Host	Info
10022	67.615441	24.6.173.220	208.93.137.180	HTTP	1595	extras.sfgate.com	POST /sfgate/modules/for

14. ยังมีอิควิรีที่สามารถสร้าง display filter ได้ คือ การสร้างจากต้นแบบ โดยการไปที่ packet ที่จะใช้เป็นต้นแบบ และเลือกฟิลเตอร์ที่ต้องการและ คลิกขวา แล้วเลือก Apply as Filter
15. ให้ยกเลิก display filter และไปที่ packet ที่ 8 ไปที่ host และ คลิกขวา และเลือก Apply as Filter จากนั้นให้หัวรีในการหา packet ที่ request ไปที่ <http://www.sfgate.com/feedback> เขียนอันนี้บายรีที่ใช้พร้อมทั้งบันทึก screenshot นำมาแสดง

เลือก packet ที่ 8 กดขวา [Full request URI: http://www.sfgate.com/feedback/] เลือก Apply as filter > เลือก selectet



Statistics

Statistics | Conversations บันทึกครั้งเราต้องการวิเคราะห์ การสื่อสารระหว่าง Client และ Server ดังนั้นเราจะสนใจการโต้ตอบ (Conversation)

16. ให้เลือก Statistics | Conversations จะแสดงหน้าต่างดังรูป

Ethernet • 1		IPv4 • 106		IPv6		TCP • 387		UDP • 254									
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 ทำให้เห็นว่าเครื่องคุ้นเคยที่สร้าง traffic จำนวนมาก ซึ่งอาจก่อภัยระบบเครือข่ายได้ จากนั้นเราสามารถเลือกให้ Wireshark แสดงเฉพาะ traffic จาก Conversation นั้นๆ โดยการคลิกขวาที่ Conversation ที่เลือก และเลือก Apply as Filter

Wireshark - Conversations - http-esp101.pcapng

Ethernet • 1 IPv4 • 37 IPv6 TCP • 63 UDP • 82											
Address A	Address 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	75.75.75.75	180	22 k	90	6973	90	15 k	0.000000	21.8143	2557	5526
24.6.173.220	199.181.172.250	7	1201	2	221	2	550	0.030245	59.1464	96	63
24.6.173.220	68.71.216.							127 k	0.168701	24.5121	2332
24.6.173.220	184.84.22.							605 k	0.322923	70.0159	5024
24.6.173.220	143.127.11							715	0.377829	0.1381	29 k
24.6.173.220	70.42.13.1							675	2.433476	14.8802	1023
24.6.173.220	68.71.212.							465	2.437970	66.7377	99
24.6.173.220	74.125.224.59	142	115 k					105 k	2.843065	66.3320	1162
24.6.173.220	184.84.222.152	303	286 k					261 k	3.261301	70.9168	2865
24.6.173.220	184.84.222.112	8	2120					1419	3.269902	65.9044	85
24.6.173.220	184.84.222.137	30	19 k	14	1638			17 k	3.270647	65.9042	198
24.6.173.220	68.71.220.175	7	2355	5	1171			1184	3.813040	65.3609	143
24.6.173.220	184.84.183.147	8	1573	5	699			874	4.950070	64.2235	87
24.6.173.220	68.71.216.171	29	24 k	12	1007			23 k	5.192672	65.1458	123
		26	221	12	1000						2929

17. ให้หาว่าในไฟล์มีการต่อตัวของ IP Address คู่ใดที่เกิดขึ้นมากที่สุด ให้สร้าง Filter ที่แสดงเฉพาะการต่อตัวนั้น ให้นับกองจำนวน Packet และ Filter ที่ปรากฏ

หากไฟล์ที่มีการต่อตัวของ IP Address คู่ใดก็ต้อง column นำเข้ามาจาก Flow → มาก มาก เกิน ก็คุ้มครอง

หาก หดลง 00000 7 ๖ filter ip.addr == 24.6.173.220 & ip.addr == 184.84.222.144

