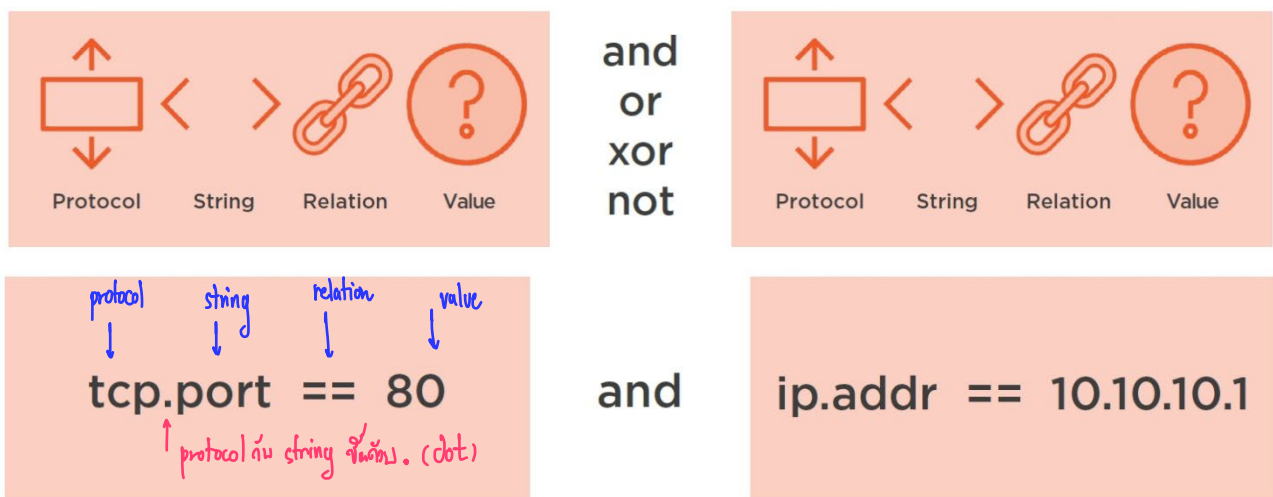


กิจกรรมที่ 3 : การใช้ display filters

ในกิจกรรมที่ผ่านมา นักศึกษาได้เรียนรู้การติดตั้งโปรแกรม และ การจัดการกับคอลัมน์ ในกิจกรรมนี้ จะทำความเข้าใจกับ 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
 - ระบุถึงข้อมูลในฟิลด์ของ 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 le 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 ได้ Hypertext Transfer Protocol แล้วขยายที่ GET ตามรูป เาเมาส์คลิกที่ Request Method ให้อยู่ที่ Status Bar จะเห็นข้อความ http.request.method ซึ่งเป็นชื่อฟิลด์ใน 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
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) C
      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 (พร้อมรูป)

filter protocol http แล้ว request method "GET" ทั้งหมดออกมา

No.	Time	Source	Destination	Protocol	Length	Info
8	0.046998	24.6.173.220	74.125.224.80	HTTP	342	GET / HTTP/1.1
36	0.217660	24.6.173.220	74.125.224.80	HTTP	602	GET /images/icons/product/chrome-48.png HTTP/1.1
43	0.238604	24.6.173.220	74.125.224.80	HTTP	748	GET /xjs/_/js/s/jsa,c,sb,hv,wta,cr,c,dos,nos,sf,tbpr,tbui,rsn,ob,mb,lc,ada,kcl,kat,aut,bihi,ifl,amcl,kp,lu,m,rtis,shb,sfa,tng,h...
46	0.240544	24.6.173.220	74.125.224.80	HTTP	590	GET /images/srpr/logo3w.png HTTP/1.1
202	0.471903	24.6.173.220	74.125.224.80	HTTP	571	GET /extern_chrome/92da361fb107ce2f.js HTTP/1.1
203	0.472127	24.6.173.220	74.125.224.80	HTTP	594	GET /textinputassistant/tia.png HTTP/1.1
204	0.474562	24.6.173.220	74.125.224.80	HTTP	583	GET /images/swxa.gif HTTP/1.1
234	0.560238	24.6.173.220	74.125.224.80	HTTP	590	GET /images/nav_logo114.png HTTP/1.1
235	0.561255	24.6.173.220	74.125.224.80	HTTP	952	GET /csi?v=3&s=webhp&action=&e=17259,37102,39523,39978,4000015,4000116,4000354,4000473,4000553,4000648,4000833,4000880,4000955...
236	0.561458	24.6.173.220	74.125.224.80	HTTP	576	GET /favicon.ico HTTP/1.1
301	0.619770	24.6.173.220	74.125.224.47	HTTP	361	GET /gb/js/sem_297d078eccaf4382701841bd042dbced.js HTTP/1.1

Display Filter Button

ในกรณีที่มันบาง 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

ip.addr==74.125.224.80 && tcp.port==80

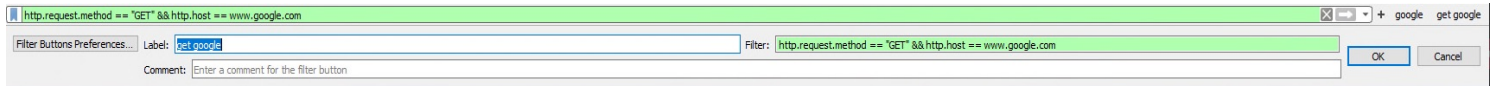
Filter Buttons Preferences... Label: Enter a description for the filter button Filter: ip.addr==74.125.224.80 && tcp.port==80 OK Cancel

Comment: Enter a comment for the filter button

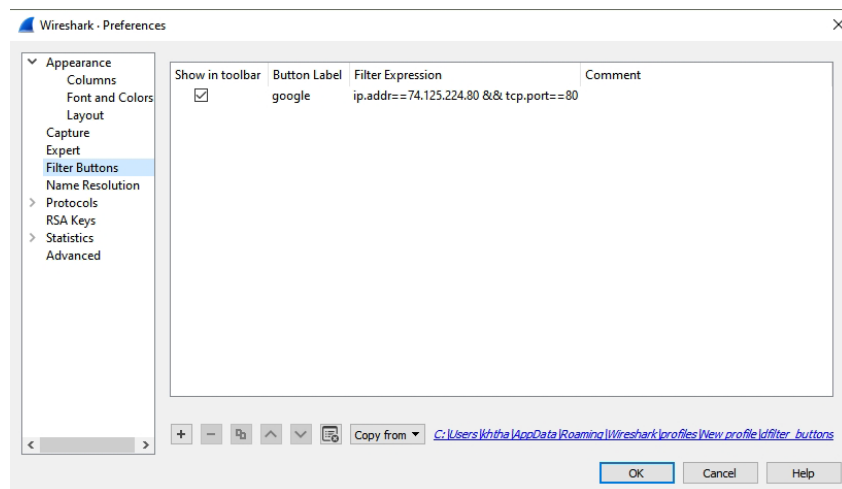
6. ให้ลบ display filter (กดปุ่ม x) จากนั้นกดปุ่ม google เกิดอะไรขึ้น

ป็นเหตุที่ filter ที่เราตั้งไว้ google (ip.addr == 74.125.224.80 & tcp.port == 80)
โดยที่เราได้ไปกดปุ่ม google ที่แถบ filter


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

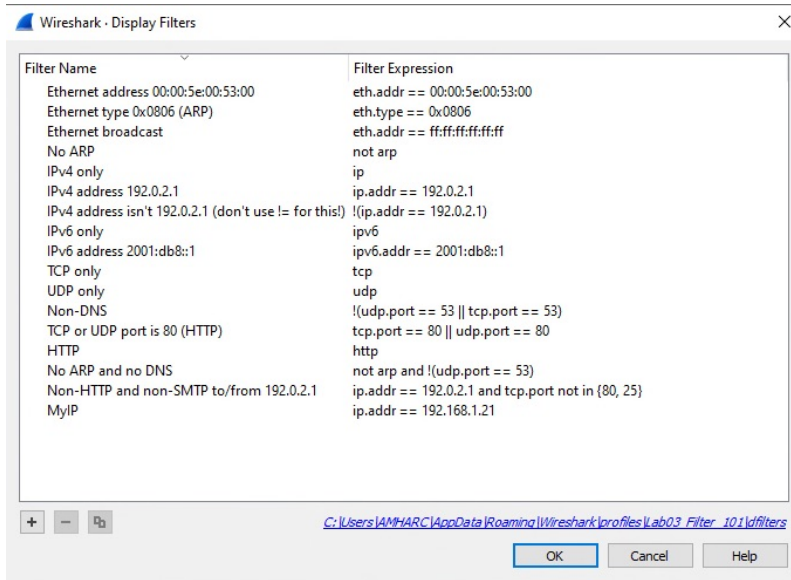


8. ให้กดปุ่ม  ที่อยู่ด้านหน้าของ display filter แล้วเลือก Filter Button Preferences.. จะปรากฏหน้าต่างต่างขึ้นมาตามรูป ซึ่งสามารถ เพิ่ม ลบ คัดลอก Filter Button ได้



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)

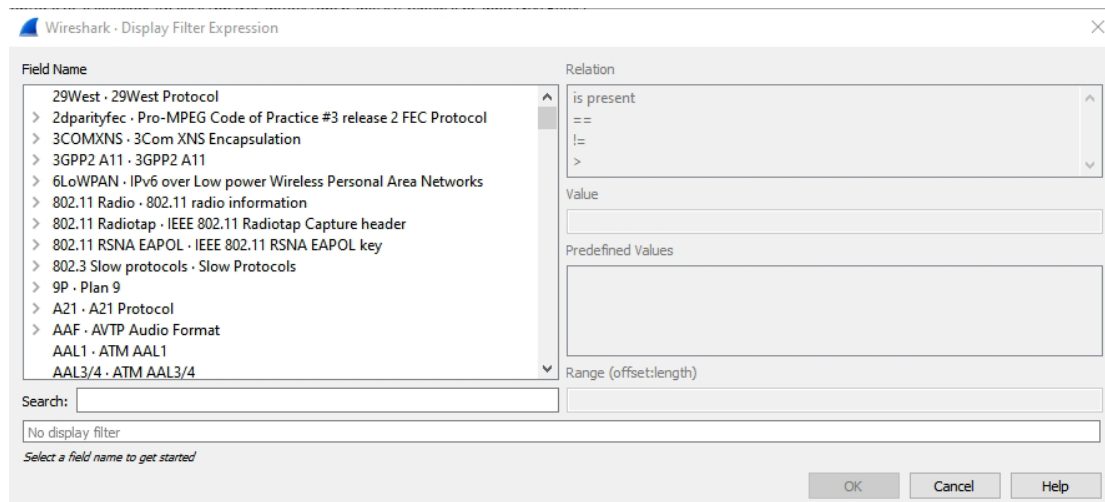


วันที่: ๒๓/๐๘/๒๕๖๓ ๑๖:๐๐-๑๖:๐๐
(พัก LAB : ๑. ๑๖.๐๐-๑๖.๐๐)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.21	213.179.200.240	UDP	146	64045 → 50003 Len=104
2	0.011491	52.112.48.32	192.168.1.21	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 171.6.133.11:50051
3	0.020124	192.168.1.21	213.179.200.240	UDP	141	64045 → 50003 Len=99
4	0.040265	192.168.1.21	213.179.200.240	UDP	138	64045 → 50003 Len=96
5	0.060222	192.168.1.21	213.179.200.240	UDP	148	64045 → 50003 Len=106
6	0.060689	192.168.1.21	147.92.165.206	TLSv...	88	Application Data
7	0.080148	192.168.1.21	213.179.200.240	UDP	150	64045 → 50003 Len=108
8	0.087004	147.92.165.206	192.168.1.21	TCP	60	443 → 53897 [ACK] Seq=1 Ack=35 Win=16138 Len=0
9	0.087161	147.92.165.206	192.168.1.21	TLSv...	88	Application Data
10	0.100175	192.168.1.21	213.179.200.240	UDP	142	64045 → 50003 Len=100
11	0.100387	192.168.1.21	52.114.54.161	STUN	264	Allocate Request bandwidth: 350 realm: :v... with nonce[Malformed Packet]
12	0.120014	192.168.1.21	213.179.200.240	UDP	140	64045 → 50003 Len=98
13	0.127956	52.114.54.161	192.168.1.21	STUN	214	Allocate Success Response lifetime: 60 MAPPED-ADDRESS: 52.114.54.161:3481 XOR-MAPPED-ADDRESS: 171.6.133.11:50048 bandwidth...
14	0.130356	192.168.1.21	147.92.165.206	TCP	54	53897 → 443 [ACK] Seq=35 Ack=35 Win=509 Len=0
15	0.140108	192.168.1.21	213.179.200.240	UDP	142	64045 → 50003 Len=100
16	0.160045	192.168.1.21	213.179.200.240	UDP	138	64045 → 50003 Len=96
17	0.165660	213.179.200.240	192.168.1.21	UDP	88	50003 → 64045 Len=46
18	0.180086	192.168.1.21	213.179.200.240	UDP	141	64045 → 50003 Len=99
19	0.200077	192.168.1.21	213.179.200.240	UDP	137	64045 → 50003 Len=95
20	0.220259	192.168.1.21	213.179.200.240	UDP	136	64045 → 50003 Len=94
21	0.238503	192.168.1.21	213.179.200.240	UDP	112	64045 → 50003 Len=70
22	0.240084	192.168.1.21	213.179.200.240	UDP	135	64045 → 50003 Len=93
23	0.260018	192.168.1.21	213.179.200.240	UDP	138	64045 → 50003 Len=96
24	0.279945	192.168.1.21	213.179.200.240	UDP	136	64045 → 50003 Len=94
25	0.299946	192.168.1.21	213.179.200.240	UDP	132	64045 → 50003 Len=90
26	0.319999	192.168.1.21	213.179.200.240	UDP	132	64045 → 50003 Len=90
27	0.339997	192.168.1.21	213.179.200.240	UDP	132	64045 → 50003 Len=90
28	0.360130	192.168.1.21	213.179.200.240	UDP	135	64045 → 50003 Len=93
29	0.380056	192.168.1.21	213.179.200.240	UDP	137	64045 → 50003 Len=95
30	0.399998	192.168.1.21	213.179.200.240	UDP	141	64045 → 50003 Len=99
31	0.420040	192.168.1.21	213.179.200.240	UDP	139	64045 → 50003 Len=97
32	0.440010	192.168.1.21	213.179.200.240	UDP	136	64045 → 50003 Len=94
33	0.459982	192.168.1.21	213.179.200.240	UDP	136	64045 → 50003 Len=94
34	0.480116	192.168.1.21	213.179.200.240	UDP	136	64045 → 50003 Len=94
35	0.500127	192.168.1.21	213.179.200.240	UDP	140	64045 → 50003 Len=98

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

Filter: `http.host == cps.hearstnp.com` (ได้ออกมาจาก packet pane details ว่า packet ที่
method get www host นั้น)

No.	Time	Source	Destination	Protocol	Length	Info
159	0.309161	24.6.173.220	208.93.137.180	HTTP	344	GET /Scripts/loadAds.js HTTP/1.1
388	0.436294	24.6.173.220	208.93.137.180	HTTP	348	GET /Scripts/loadAdsMain.js HTTP/1.1
406	0.465477	24.6.173.220	208.93.137.180	HTTP	363	GET /SRO/GetJS?url=www.sfgate.com/feedback HTTP/1.1
458	0.628832	24.6.173.220	208.93.137.180	HTTP	350	GET /Scripts/initDefineAds.js HTTP/1.1
100...	68.404262	24.6.173.220	208.93.137.180	HTTP	420	GET /SRO/GetJS?url=www.sfgate.com/%3FcontrollerName%3DcmfThirdPartyFooter HTTP/1.1
100...	69.068504	24.6.173.220	208.93.137.180	HTTP	437	GET /SRO/GetJS?url=extras.sfgate.com/sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1

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

Filter: `http.host == cps.hearstnp.com || (http.request.method == "POST" && http.host == extras.sfgate.com)`
filter: `http.request.method == "POST" && http.host == extras.sfgate.com`

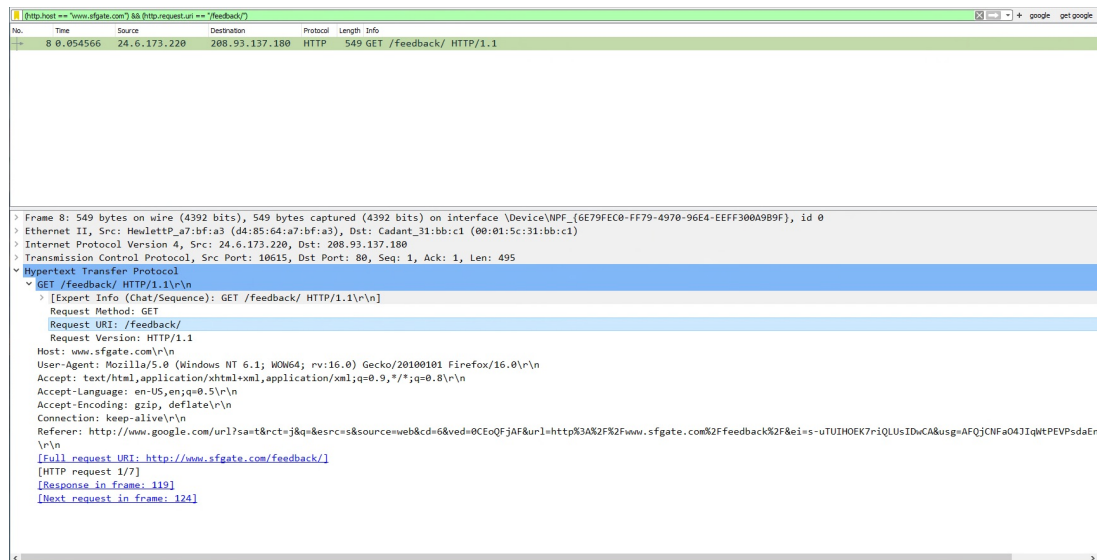
No.	Time	Source	Destination	Protocol	Length	Info
159	0.309161	24.6.173.220	208.93.137.180	HTTP	344	GET /Scripts/loadAds.js HTTP/1.1
388	0.436294	24.6.173.220	208.93.137.180	HTTP	348	GET /Scripts/loadAdsMain.js HTTP/1.1
406	0.465477	24.6.173.220	208.93.137.180	HTTP	363	GET /SRO/GetJS?url=www.sfgate.com/feedback HTTP/1.1
458	0.628832	24.6.173.220	208.93.137.180	HTTP	350	GET /Scripts/initDefineAds.js HTTP/1.1
100...	67.615441	24.6.173.220	208.93.137.180	HTTP	1595	POST /sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1 (application/x-www-form-urlencoded)
100...	68.404262	24.6.173.220	208.93.137.180	HTTP	420	GET /SRO/GetJS?url=www.sfgate.com/%3FcontrollerName%3DcmfThirdPartyFooter HTTP/1.1
100...	69.068504	24.6.173.220	208.93.137.180	HTTP	437	GET /SRO/GetJS?url=extras.sfgate.com/sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1

No.	Time	Source	Destination	Protocol	Length	Info
100...	67.615441	24.6.173.220	208.93.137.180	HTTP	1595	POST /sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1 (application/x-www-form-urlencoded)

only extrn. sfgate

- ยังมีอีกวิธีที่สามารถจะสร้าง display filter ได้ คือ การสร้างจากต้นแบบ โดยการไปที่ packet ที่จะใช้เป็นต้นแบบ และเลือกฟิลด์ที่ต้องการและ คลิกขวา แล้วเลือก Apply as Filter
- 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

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



Statistics

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

- 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

<

>

☐ Name resolution

☐ Limit to display filter

☐ Absolute start time

Conversation Types ▼

Copy ▼

Follow Stream...

Graph...

Close

Help

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

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	199.181.112.100	550	69.146 k	96	127 k	0.168701	24.5121	2332	63		
24.6.173.220	68.71.216.112	127 k	0.168701	24.5121	2332	63					
24.6.173.220	184.84.222.152	605 k	0.322923	70.0159	5024	69 k					
24.6.173.220	143.127.111.100	715	0.377829	0.1381	29 k	41 k					
24.6.173.220	70.42.13.1	675	2.433476	14.8802	1023	362					
24.6.173.220	68.71.212.1	465	2.437970	66.7377	99	55					
24.6.173.220	74.125.224.59	142	115 k	105 k	2.843065	66.3320	1162	12 k			
24.6.173.220	184.84.222.152	303	286 k	261 k	3.261301	70.9168	2865	29 k			
24.6.173.220	184.84.222.112	8	2120	1419	3.269902	65.9044	85	172			
24.6.173.220	184.84.222.137	30	19 k	17 k	3.270647	65.9042	198	2129			
24.6.173.220	68.71.220.175	7	2355	1184	3.813040	65.3609	143	144			
24.6.173.220	184.84.183.147	8	1573	874	4.950070	64.2235	87	108			
24.6.173.220	68.71.216.171	29	24 k	23 k	5.192672	65.1458	123	2929			

17. ให้อธิบายว่าในไฟล์มีการโต้ตอบของ IP Address คู่ใดที่เกิดขึ้นมากที่สุด ให้สร้าง Filter ที่แสดงเฉพาะการโต้ตอบนั้น ให้ออกจำนวน Packet และ Filter ที่ปรากฏ

filter : `ip.addr == 24.6.173.220 && ip.addr == 184.84.222.144`
 จำนวน 4468 packets (4468 / 11678 : 38.3%)

งานครั้งที่ 3

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

No.	Time	Source	Destination	Protocol	Length	Info
3546	8.844265	24.6.173.220	184.84.222.144	TCP	66	10854 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
3547	8.859388	184.84.222.144	24.6.173.220	TCP	66	80 → 10854 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=2
3548	8.859590	24.6.173.220	184.84.222.144	TCP	54	10854 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
3549	8.860909	24.6.173.220	184.84.222.144	HTTP	480	GET /static/80/92/14409/m14409_high.mp4 HTTP/1.1
3550	8.879077	184.84.222.144	24.6.173.220	TCP	60	80 → 10854 [ACK] Seq=1 Ack=427 Win=15672 Len=0
3551	8.892803	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [ACK] Seq=1 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3552	8.892807	184.84.222.144	24.6.173.220	TCP	182	80 → 10854 [PSH, ACK] Seq=1461 Ack=427 Win=15672 Len=128 [TCP segment of a reassembled PDU]
3553	8.893492	24.6.173.220	184.84.222.144	TCP	54	10854 → 80 [ACK] Seq=427 Ack=1589 Win=65700 Len=0
3554	8.894302	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [ACK] Seq=1589 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3555	8.894308	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [PSH, ACK] Seq=3049 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3556	8.894614	24.6.173.220	184.84.222.144	TCP	54	10854 → 80 [ACK] Seq=427 Ack=4509 Win=65700 Len=0
3564	8.908086	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [ACK] Seq=4509 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3565	8.908996	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [ACK] Seq=5969 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3566	8.909003	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [ACK] Seq=7429 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3567	8.909240	24.6.173.220	184.84.222.144	TCP	54	10854 → 80 [ACK] Seq=427 Ack=8889 Win=65700 Len=0
3568	8.913254	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [ACK] Seq=8889 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3569	8.914121	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [PSH, ACK] Seq=10349 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3570	8.914347	24.6.173.220	184.84.222.144	TCP	54	10854 → 80 [ACK] Seq=427 Ack=11809 Win=65700 Len=0
3575	8.917412	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [PSH, ACK] Seq=11809 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3579	8.927361	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [ACK] Seq=13269 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3580	8.927627	24.6.173.220	184.84.222.144	TCP	54	10854 → 80 [ACK] Seq=427 Ack=14729 Win=65700 Len=0
3581	8.928429	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [ACK] Seq=14729 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3582	8.928433	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [ACK] Seq=16189 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3583	8.928813	24.6.173.220	184.84.222.144	TCP	54	10854 → 80 [ACK] Seq=427 Ack=17649 Win=65700 Len=0
3584	8.929603	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [ACK] Seq=17649 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3585	8.932422	184.84.222.144	24.6.173.220	TCP	1514	80 → 10854 [ACK] Seq=19109 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]