

### 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 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 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)
      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)

แสดง method ที่เป็น Get ออกมาเท่านั้น (Packet HTTP Protocol)

http.request.method=="GET"						
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,cdos,nos,sf,tbpr,tbui,rsn,ob,mb
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/swx.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=17259,37102,39523,39978,4000015,400
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

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

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

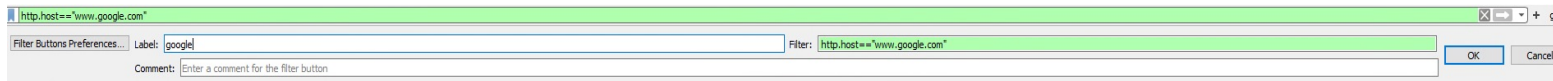
Filter Buttons Preferences... Label:  Filter:  OK Cancel

Comment:

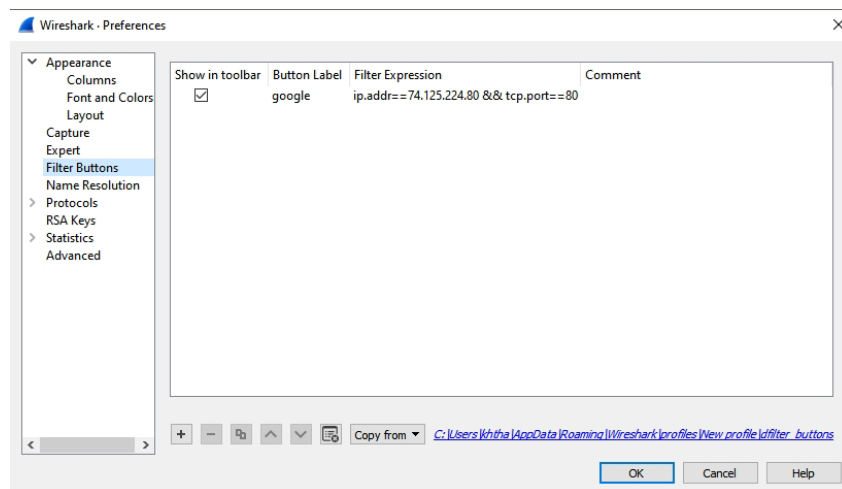
6. ให้ลบ display filter (กดปุ่ม x) จากนั้นกดปุ่ม google เกิดอะไรขึ้น

การกดของปุ่ม ip address เป็น 72.125.224.80 & tcp port คือ 80 มาแสดง


7. ให้สร้างปุ่ม get google โดยเมื่อกดแล้วให้แสดงเฉพาะเฟรมที่มี http ที่ GET ไปที่ [www.google.com](http://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

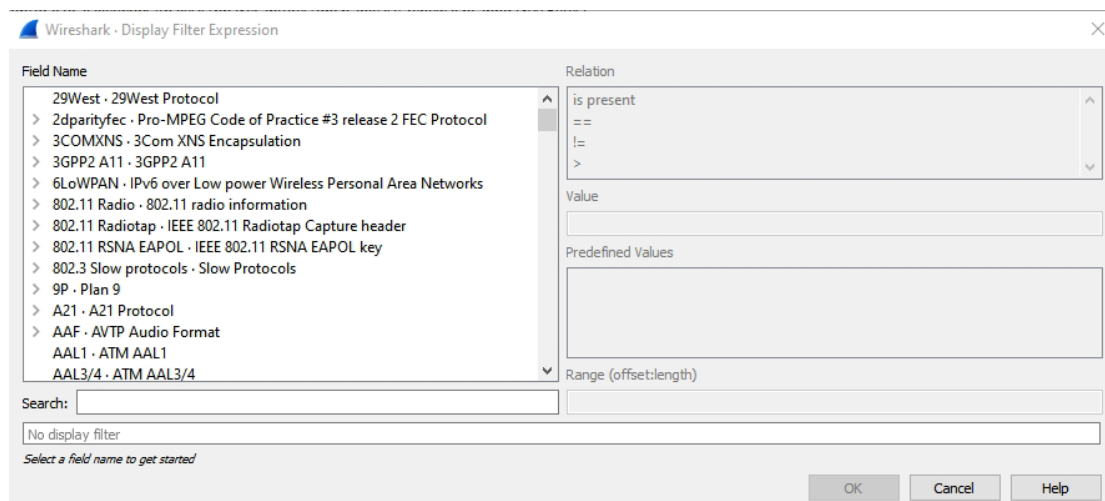
9. ยังสามารถจะสร้าง Bookmark ของ Display filter ได้ โดยกดปุ่ม  และเลือก Manage Display Filters ซึ่งสามารถสร้าง ลบ หรือคัดลอกได้
10. ให้เพิ่ม bookmark ของ display filter ชื่อ MyIP โดยเป็นการกรองเฉพาะ IP Address ของตัวเอง (ไปที่ cmd แล้วใช้คำสั่ง ipconfig เพื่อดู IP Address ของเครื่องตนเอง) จากนั้นให้ทดลอง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

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!)	!(ip.addr == 192.0.2.1)
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	!(udp.port == 53    tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80    udp.port == 80
HTTP	http
No ARP and no DNS	not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and tcp.port not in {80, 25}
MyIP	ip.addr == 192.168.1.68

ip.addr == 192.168.1.68						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	213.179.202.37	192.168.1.68	UDP	323	50004 → 64814 Len=281
2	0.015961	192.168.1.68	213.179.202.28	UDP	314	64813 → 50004 Len=272
3	0.016008	192.168.1.68	213.179.202.28	UDP	778	64813 → 50004 Len=736
4	0.016020	192.168.1.68	213.179.202.28	UDP	778	64813 → 50004 Len=736
5	0.016024	192.168.1.68	213.179.202.28	UDP	780	64813 → 50004 Len=738
6	0.016041	192.168.1.68	213.179.202.28	UDP	780	64813 → 50004 Len=738
7	0.019064	192.168.1.68	213.179.202.28	UDP	877	64813 → 50004 Len=835
8	0.019074	192.168.1.68	213.179.202.28	UDP	876	64813 → 50004 Len=834
9	0.019078	192.168.1.68	213.179.202.28	UDP	910	64813 → 50004 Len=868
10	0.019082	192.168.1.68	213.179.202.28	UDP	910	64813 → 50004 Len=868
11	0.019396	213.179.202.28	192.168.1.68	UDP	94	50004 → 64813 Len=52
12	0.021964	192.168.1.68	213.179.202.28	UDP	780	64813 → 50004 Len=738
13	0.021973	192.168.1.68	213.179.202.28	UDP	780	64813 → 50004 Len=738
14	0.021978	192.168.1.68	213.179.202.28	UDP	877	64813 → 50004 Len=835
15	0.021981	192.168.1.68	213.179.202.28	UDP	780	64813 → 50004 Len=738

## Display Filter Expression

- 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

ระบุ Display Filter เป็น http.host == "aps.hearstnp.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
10055	68.404262	24.6.173.220	208.93.137.180	HTTP	420	GET /SRO/GetJS?url=www.sfgate.com/%3FcontrollerName%3DcmfThirdPartyFooter HTTP/1.1
10067	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

ใส่ Filter เป็น http.request.method == "POST" && http.host == "extras.sfgate.com"

คำสั่งกรอง packet ให้เปลี่ยนเป็น http.host == "aps.hearstnp.com" || http.request.method == "POST" && http.host == "extras.sfgate.com"

No.	Time	Source	Destination	Protocol	Length	Info
10022	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)

> Frame 10022: 1595 bytes on wire (12760 bits), 1595 bytes captured (12760 bits) on interface \Device\NPF\_{6E79FECB-FF79-4970-96E4-EEF300A089F}, id 0

> Ethernet II, Src: HewlettP\_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant\_31:bb:c1 (00:01:5c:31:bb:c1)

> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 208.93.137.180

> Transmission Control Protocol, Src Port: 10093, Dst Port: 80, Seq: 1, Ack: 1, Len: 1541

> Hypertext Transfer Protocol

POST /sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1\r\n

> [Expert Info (Chat/Sequence): POST /sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1.1\r\n]

Request Method: POST

Request URI: /sfgate/modules/formHandlers/sfgSupportMailHandler.php

Request Version: HTTP/1.1

Host: extras.sfgate.com\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

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
10022	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)
10055	68.404262	24.6.173.220	208.93.137.180	HTTP	420	GET /SRO/GetJS?url=www.sfgate.com/%3FcontrollerName%3DcmfThirdPartyFooter HTTP/1.1
10067	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



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

วิธี Display filter เจน `http.host == "www.sfgate.com" && http.request.uri == "/feedback/"`

No.	Time	Source	Destination	Protocol	Length	Info
8	0.054566	24.6.173.220	208.93.137.180	HTTP	549	GET /feedback/ HTTP/1.1

```
> Frame 8: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A989F}, Id 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 208.93.137.180
> Transmission Control Protocol, Src Port: 10615, Dst Port: 80, Seq: 1, Ack: 1, Len: 495
> Hypertext Transfer Protocol
  GET /feedback/ HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /feedback/ HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /feedback/
    Request Version: HTTP/1.1
Host: www.sfgate.com\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
```

## Statistics

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

16. ให้เลือก Statistics | Conversations จะแสดงหน้าต่างดังรูป

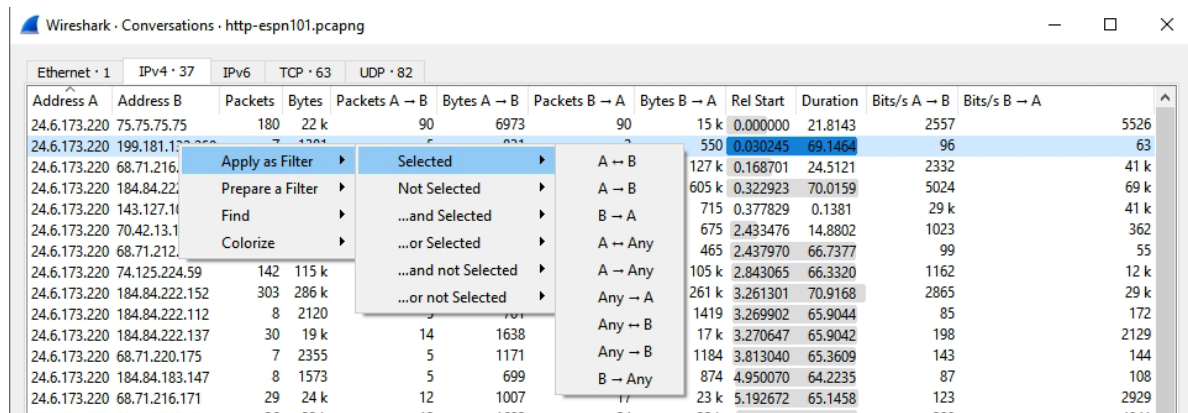
Ethernet • 1		IPv4 • 106		IPv6	TCP • 387		UDP • 254						
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
24.6.173.220	10615	208.93.137.180	80	46	34 k	18	3929	28	30 k	0.035587	62.2516	504	3871
24.6.173.220	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

☐ 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



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

คู่ IP Address ที่โต้ตอบกันมากที่สุดคือ 24.6.173.220 & 184.84.222.144 โดยจำนวน 4463 Packets (33.3%)  
& Display Filter เป็น 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