

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)

```

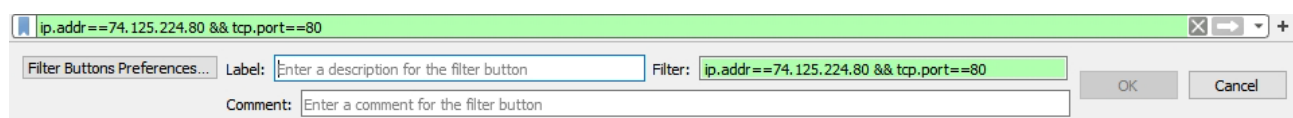
3. ให้ไปที่ display filter ให้ป้อนคำว่า http แล้วกด . จะเห็นว่า Wireshark แสดงตัวเลือกขึ้นมาให้เลือก ให้เลือก request.method ให้ป้อนให้ครบเป็น http.request.method=="GET" มีอะไรแสดงผล แสดงเฉพาะ packet ที่มีการ GET มีจำนวน 11 packet ตามรูป

No.	Time	Time since request	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/
43	0.238604		24.6.173.220	74.125.224.80	HTTP	748	GET /xjs/_/js/s/jsa,c,sb,h
46	0.240544		24.6.173.220	74.125.224.80	HTTP	590	GET /images/srpr/logo3w.png
202	0.471903		24.6.173.220	74.125.224.80	HTTP	571	GET /extern_chrome/92da361-
203	0.472127		24.6.173.220	74.125.224.80	HTTP	594	GET /textinputassistant/ti
204	0.474562		24.6.173.220	74.125.224.80	HTTP	583	GET /images/swxa.gif HTTP/
234	0.560238		24.6.173.220	74.125.224.80	HTTP	590	GET /images/nav_logo114.png
235	0.561255		24.6.173.220	74.125.224.80	HTTP	952	GET /csi?v=3&s=webhp&action
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_297d078eccar

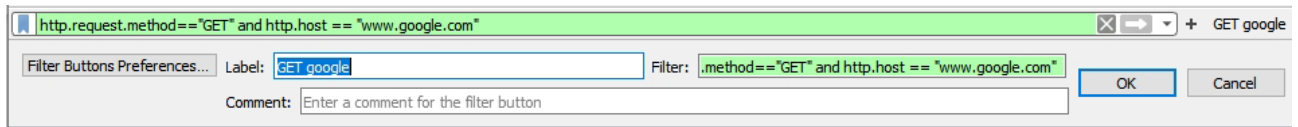
Display Filter Button

ในกรณีที่บาง 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
ในช่อง display filter จะมี filter `ip.addr==74.125.224.80 && tcp.port==80` แสดง
และมีการใช้การกรองที่กำหนดไว้ในปุ่ม google
7. ให้สร้างปุ่ม get google โดยเมื่อกดแล้วให้แสดงเฉพาะเฟรมที่มี http ที่ GET ไปที่ www.google.com ให้แสดง
ส่วนที่ใช้ในการกำหนดค่า (คล้ายกับรูปในข้อที่ 5)

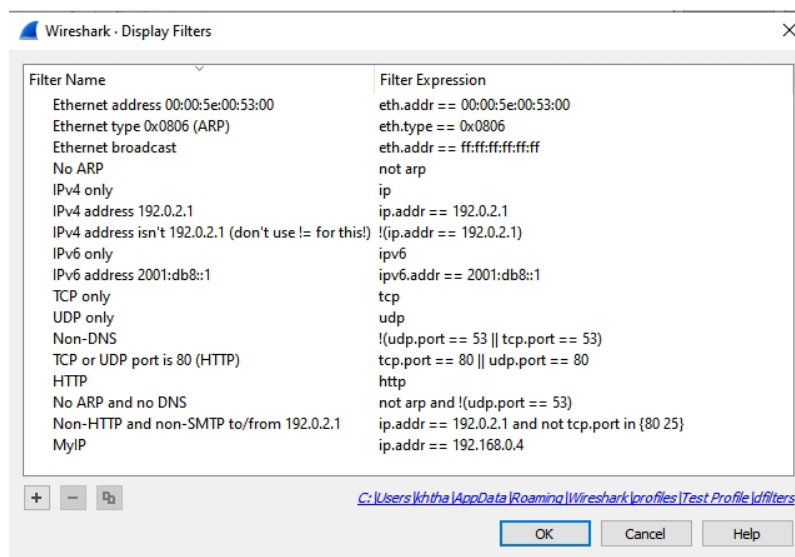


- มีหลักฐานการสร้างปุ่ม get google โดยมี Filter เป็น `http.host == "www.google.com"` and `http.request.method=="GET"` หรือแบบอื่นๆ ที่ได้ผลการทำงานเดียวกัน
8. ให้กดปุ่ม  ที่อยู่ด้านหน้าของ display filter แล้วเลือก Filter Button Preferences.. จะปรากฏหน้าต่างต่างขึ้นมาตามรูป ซึ่งสามารถ เพิ่ม ลบ คัดลอก 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 ที่เป็นการกรอง IP Address ของตัวเองเข้าไป (ไปที่ cmd แล้วใช้คำสั่ง `ipconfig` เพื่อดู IP Address) จากนั้นให้ capture และเข้าเว็บต่างๆ ว่าแสดงเฉพาะ IP Address ของตัวเองจริงหรือไม่

แสดงการกำหนดค่าตามตัวอย่าง และรูปแสดงผลการ Capture เฉพาะ IP ของเครื่องตนเอง



```

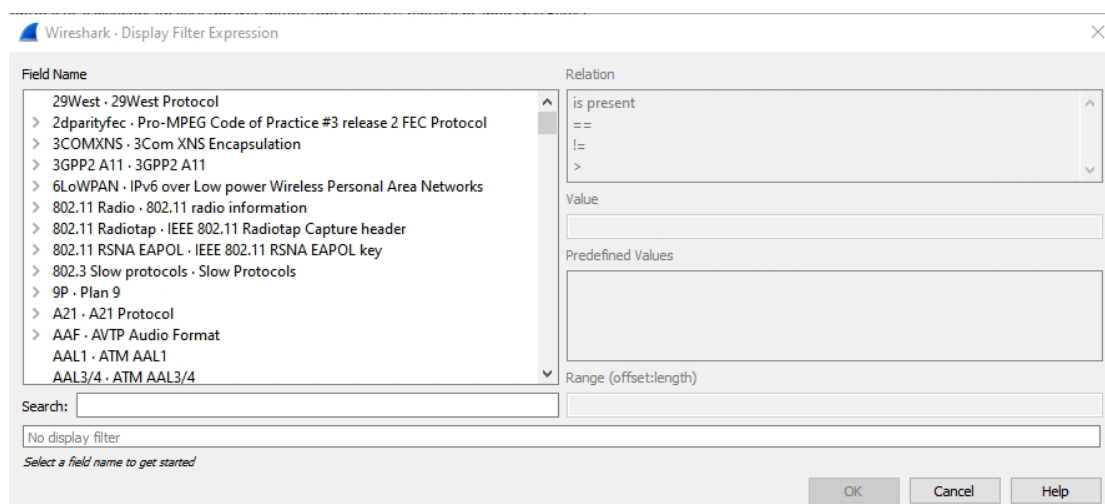
Ethernet address 00:00:5e:00:53:00: eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP): eth.type == 0x0806
Ethernet broadcast: eth.addr == ff:ff:ff:ff:ff:ff
No ARP: not arp
IPv4 only: ip
IPv4 address 192.0.2.1: ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!): !(ip.addr == 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 not tcp.port in {80 25}
MyIP: ip.addr == 192.168.0.4

```

ip.addr == 192.168.1.4					
No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.4	161.246.4.119	TCP	9101 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
2	0.000519	192.168.1.4	161.246.4.119	TCP	9102 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
3	0.018554	161.246.4.119	192.168.1.4	TCP	80 → 9102 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1412 S
4	0.000091	192.168.1.4	161.246.4.119	TCP	9102 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
5	0.000253	192.168.1.4	161.246.4.119	HTTP	GET / HTTP/1.1
6	0.008919	161.246.4.119	192.168.1.4	TCP	80 → 9101 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1412 S
7	0.000064	192.168.1.4	161.246.4.119	TCP	9101 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
8	0.001948	161.246.4.119	192.168.1.4	TCP	80 → 9102 [ACK] Seq=1 Ack=646 Win=7136 Len=0
9	0.045910	161.246.4.119	192.168.1.4	HTTP	HTTP/1.1 200 OK (text/html)
10	0.000000	161.246.4.119	192.168.1.4	HTTP	Continuation
11	0.000044	192.168.1.4	161.246.4.119	TCP	9102 → 80 [ACK] Seq=646 Ack=2825 Win=262400 Len=0
12	0.018815	161.246.4.119	192.168.1.4	HTTP	Continuation
13	0.041197	192.168.1.4	161.246.4.119	TCP	9102 → 80 [ACK] Seq=646 Ack=4141 Win=261120 Len=0
14	0.420318	192.168.1.4	161.246.4.119	HTTP	GET /slideshow2.css HTTP/1.1
15	0.018950	161.246.4.119	192.168.1.4	TCP	80 → 9101 [ACK] Seq=1 Ack=646 Win=7136 Len=0

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) และ packet ที่ใช้ Method post ไปยัง extras.sfgate.com (มี 1 ครั้ง) ให้แสดงวิธีการ

การทำงานอาจทำได้หลายวิธีแต่วิธีการที่เหมาะสม คือ ใช้ filter : http.host contains "hearstnp.com"

วิธีการอาจใช้ display filter expression

No.	Time	Time since request	Source	Destination	Protocol	Length	Info
159	0.309161		24.6.173.220	208.93.137.180	HTTP	344	GET /Scripts/loadAds.js HTTP/1
388	0.436294		24.6.173.220	208.93.137.180	HTTP	348	GET /Scripts/loadAdsMain.js HT
406	0.465477		24.6.173.220	208.93.137.180	HTTP	363	GET /SRO/GetJS?url=www.sfgate.
458	0.628832		24.6.173.220	208.93.137.180	HTTP	350	GET /Scripts/initDefineAds.js
10055	68.404262		24.6.173.220	208.93.137.180	HTTP	420	GET /SRO/GetJS?url=www.sfgate.
10067	69.068504		24.6.173.220	208.93.137.180	HTTP	437	GET /SRO/GetJS?url=extras.sfga

การทำงานอาจทำได้หลายวิธีแต่วิธีการที่เหมาะสม คือ ใช้ filter : http.request.method == "POST" and

http.host contains "sfgate.com" โดยอาจใช้ display filter expression

http.request.method == "POST" and http.host contains "sfgate.com" ✕ ➡ + GET google					
No.	Time	Source	Destination	Protocol	Info
10022	0.000000	24.6.173.220	208.93.137.180	HTTP	POST /sfgate/modules/fo

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

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

การทำงานอาจทำได้หลายวิธีแต่วิธีการที่เหมาะสม คือ ใช้ filter

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

โดยอาจเริ่มจากใช้ filter : http.host contains "sfgate.com" จากนั้นหา packet ต้องการ

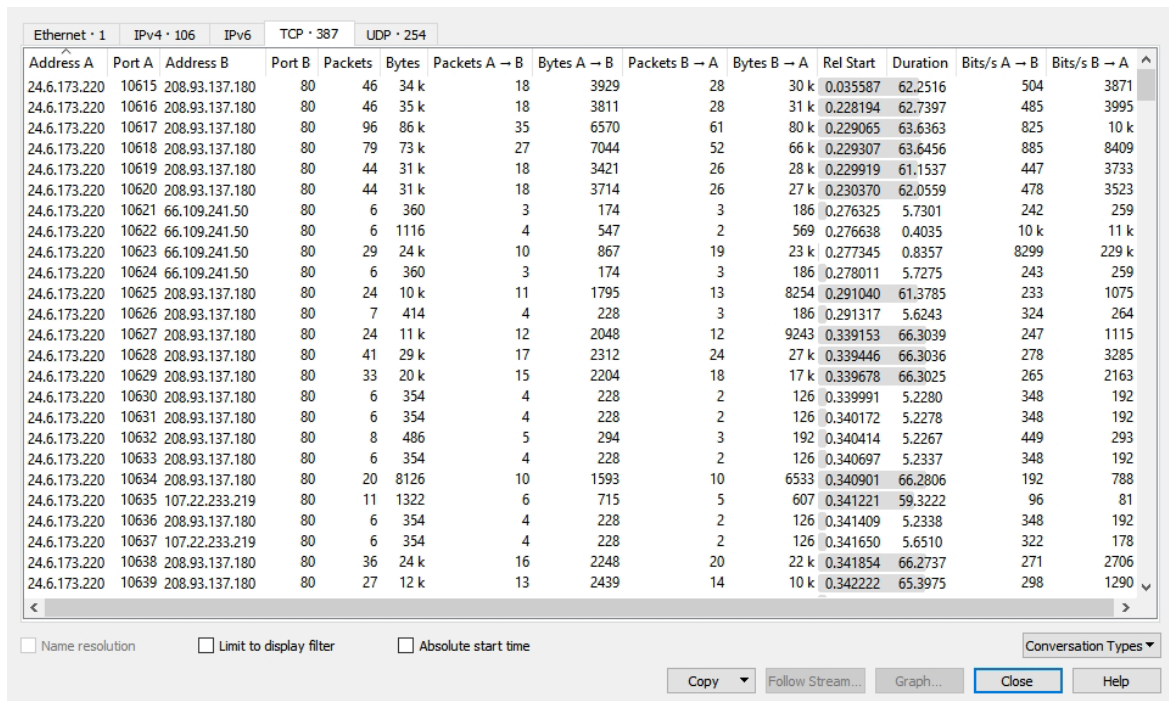
คลิกขวา Prepare as Filter ที่ Host และ ที่ Request URI

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

Statistics

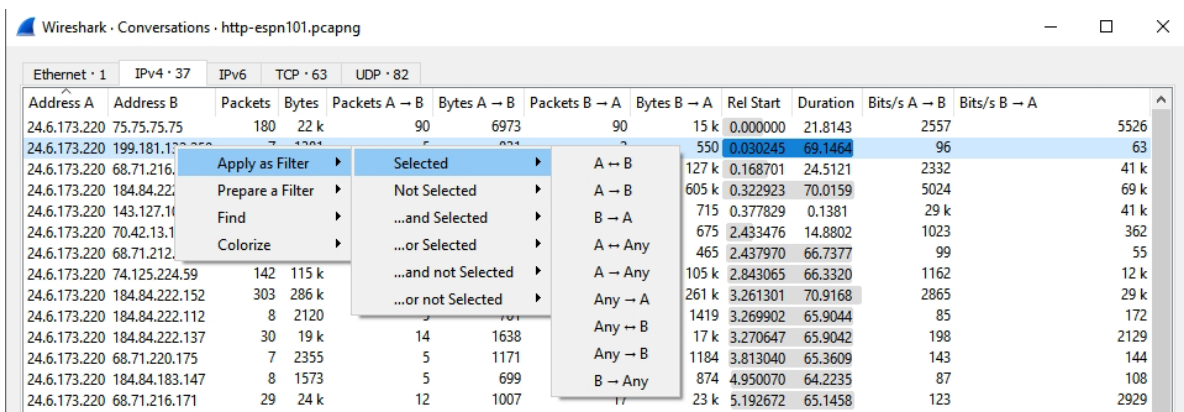
Statistics | Conversation บางครั้งเราต้องการวิเคราะห์ การสื่อสารระหว่าง Client และ Server ดังนั้นเราจะสนใจการโต้ตอบ (Conversation)

15. 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 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	199.181.128.222	7	1264	5	623	2	550	0.030245	69.1464	96	63
24.6.173.220	68.71.216.14	1	126	1	126	0	127 k	0.168701	24.5121	2332	41 k
24.6.173.220	184.84.222.112	8	2120	4	1060	4	605 k	0.322923	70.0159	5024	69 k
24.6.173.220	143.127.14.14	1	126	1	126	0	715	0.377829	0.1381	29 k	41 k
24.6.173.220	70.42.13.1	1	126	1	126	0	675	2.433476	14.8802	1023	362
24.6.173.220	68.71.212.1	1	126	1	126	0	465	2.437970	66.7377	99	55
24.6.173.220	74.125.224.59	142	115 k	71	57500	71	105 k	2.843065	66.3320	1162	12 k
24.6.173.220	184.84.222.152	303	286 k	151	143000	152	261 k	3.261301	70.9168	2865	29 k
24.6.173.220	184.84.222.112	8	2120	4	1060	4	1419	3.269902	65.9044	85	172
24.6.173.220	184.84.222.137	30	19 k	15	1638	15	17 k	3.270647	65.9042	198	2129
24.6.173.220	68.71.220.175	7	2355	4	1171	3	1184	3.813040	65.3609	143	144
24.6.173.220	184.84.183.147	8	1573	4	699	4	874	4.950070	64.2235	87	108
24.6.173.220	68.71.216.171	29	24 k	14	1007	15	23 k	5.192672	65.1458	123	2929

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

ip.addr==24.6.173.220 && tcp.port==10854 && ip.addr==184.84.222.144 && tcp.port==80

จำนวน 4468 Packet

