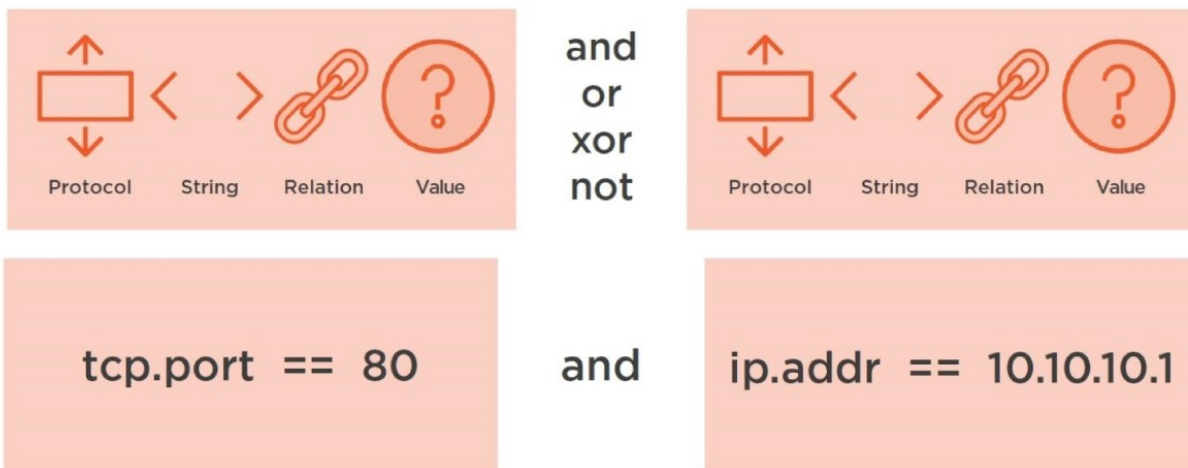


กิจกรรมที่ 3 : การใช้ display filters

ในกิจกรรมที่ผ่านมา นักศึกษาได้เรียนรู้การติดตั้งโปรแกรม และการจัดการกับคอลัมน์ 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
 - 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 เอาเมาส์คลิกที่ Request Method ใหญ่ที่ 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)

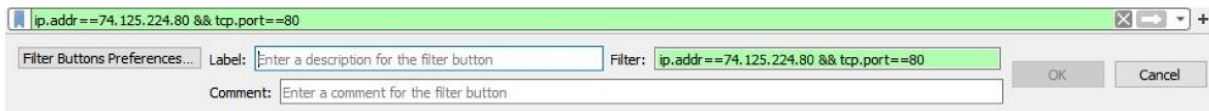
3. ให้ไปที่ display filter ให้ป้อนคำว่า http แล้วกด . จะเห็นว่า Wireshark แสดงตัวเลือกขึ้นมาให้เลือก ให้เลือก request.method ให้ป้อนให้ครบเป็น http.request.method=="GET" มีอะไรแสดงผล

แสดงผล Packet ที่มี Request method: GET ตาม Packet List Pane

Display Filter Button

ในกรณีที่สื่อบาง Display filter ที่เราใช้บ่อยๆ สามารถจะเพิ่มเข้าไปใน Toolbar ได้

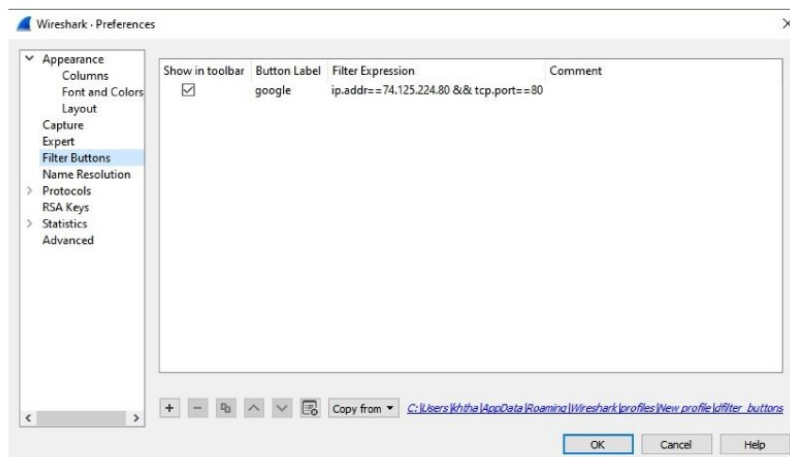
4. ให้ป้อน ip.addr==74.125.224.80 && tcp.port==80 ในช่อง display filter
5. กดปุ่ม + ที่ด้านขวาสุดของ display filter จะปรากฏตามรูป ให้ป้อน google ลงในช่อง Label แล้วกด OK



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


ช่อง Display filter จะเพิ่มค่า google ที่เคยป้อนเอาไว้

7. ให้สร้างปุ่ม get google โดยเมื่อกดแล้วให้แสดงเฉพาะเฟรมที่มี http ที่ GET ไปที่ www.google.com ให้แสดงส่วนที่ใช้ในการกำหนดค่า (คล้ายกับรูปในข้อที่ 5)



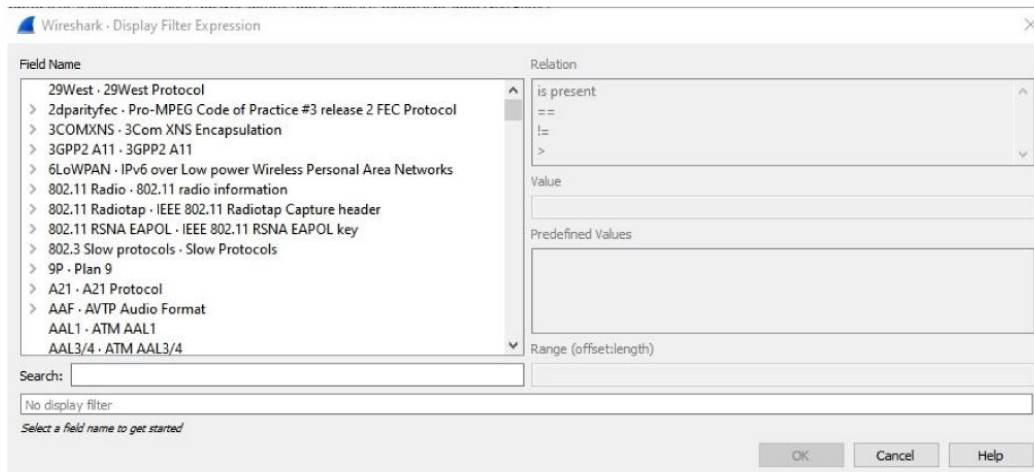
8. ให้กดปุ่ม  ที่อยู่ด้านหน้าของ display filter แล้วเลือก Filter Button Preferences.. จะปรากฏหน้าต่างขึ้นมาตามรูป ซึ่งสามารถ เพิ่ม ลบ คัดลอก Filter Button ได้

Display Filter Bookmark

9. ยังสามารถจะสร้าง Bookmark ของ Display filter ได้ โดยกดปุ่ม  และเลือก Manage Display Filters ซึ่งสามารถสร้าง ลบ หรือคัดลอกได้
10. ให้เพิ่ม bookmark ของ display filter ที่เป็นการกรอง IP Address ของตัวเอง เข้าไปแล้ว capture มาแสดง ตรวจสอบโดยการ Capture แล้วกรองว่าแสดงเฉพาะ IP Address ของตัวเองจริงหรือไม่

Display Filter Expression

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

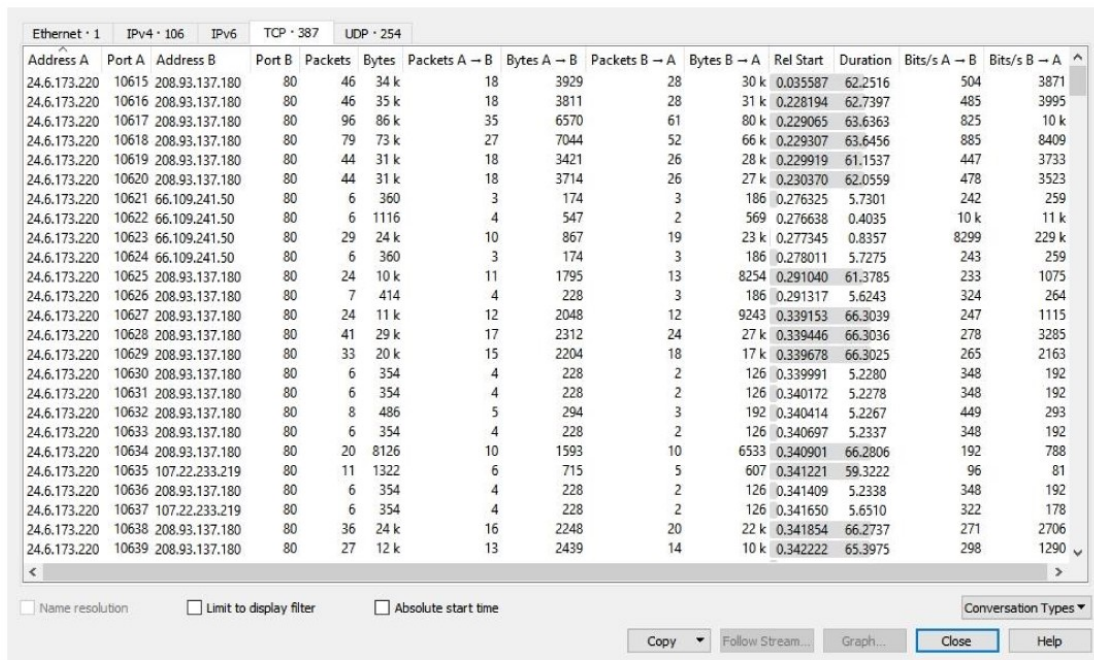


12. ให้เปิดไฟล์ <http://sfgate101.pcapng> และให้หา packet ที่ การ request ไปที่ hearstnp.com (มีจำนวน 6 ครั้ง) และ packet ที่ใช้ Method post ไปยัง extras.sfgate.com (มี 1 ครั้ง) ให้แสดงวิธีการ
13. ยังมีอีกวิธีที่สามารถจะสร้าง display filter ได้ คือ การสร้างจากต้นแบบ โดยการไปที่ packet ที่จะใช้เป็นต้นแบบ 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>

Statistics

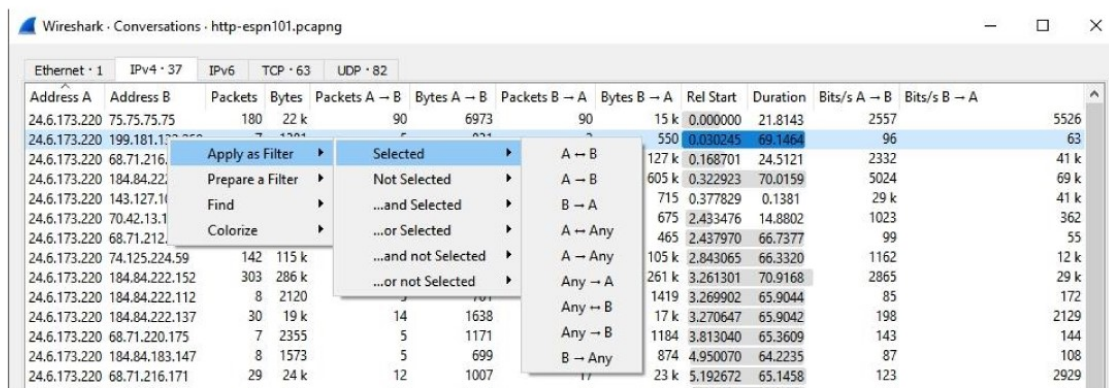
Statistics | Conversation บางครั้งเราต้องการวิเคราะห์ การสื่อสารระหว่าง Client และ Server ดังนั้นเราจะสนใจการโต้ตอบ (Conversation)

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 ซึ่งอาจจะก่อกรวนระบบเครือข่ายได้ 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	199.181.132.100	7	1344	4	634	3	550	0.030245	69.1464	96	63
24.6.173.220	68.71.216.1	127	127 k	127	127 k	0	0	0.168701	24.5121	2332	41 k
24.6.173.220	184.84.222.1	605	605 k	605	605 k	0	0	0.322923	70.0159	5024	69 k
24.6.173.220	143.127.11.1	715	715 k	715	715 k	0	0	0.377829	0.1381	29 k	41 k
24.6.173.220	70.42.13.1	675	675 k	675	675 k	0	0	2.433476	14.8802	1023	362
24.6.173.220	68.71.212.1	465	465 k	465	465 k	0	0	2.437970	66.7377	99	55
24.6.173.220	74.125.224.59	142	115 k	142	115 k	0	0	2.843065	66.3320	1162	12 k
24.6.173.220	184.84.222.152	303	286 k	303	286 k	0	0	3.261301	70.9168	2865	29 k
24.6.173.220	184.84.222.112	8	2120	8	2120	0	0	3.269902	65.9044	85	172
24.6.173.220	184.84.222.137	30	19 k	14	1638	16	17 k	3.270647	65.9042	198	2129
24.6.173.220	68.71.220.175	7	2355	5	1171	2	1184	3.813040	65.3609	143	144
24.6.173.220	184.84.183.147	8	1573	5	699	3	874	4.950070	64.2235	87	108
24.6.173.220	68.71.216.171	29	24 k	12	1007	17	23 k	5.192672	65.1458	123	2929

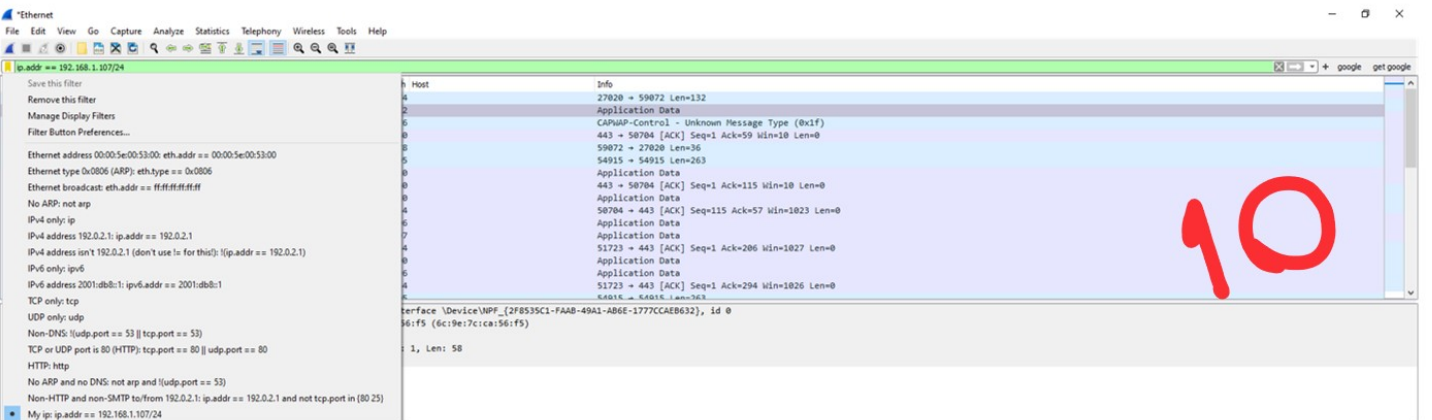
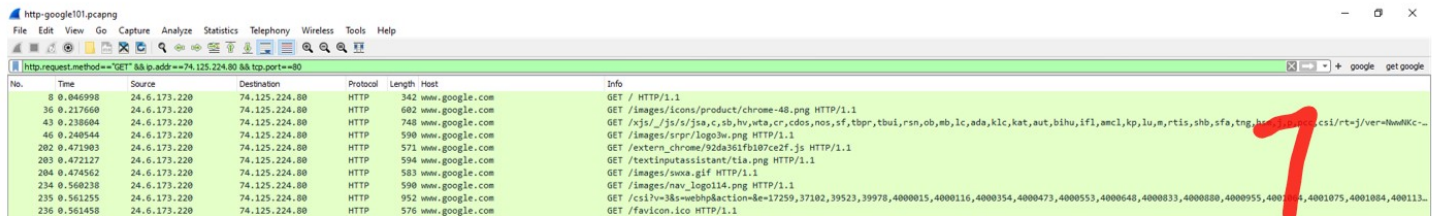
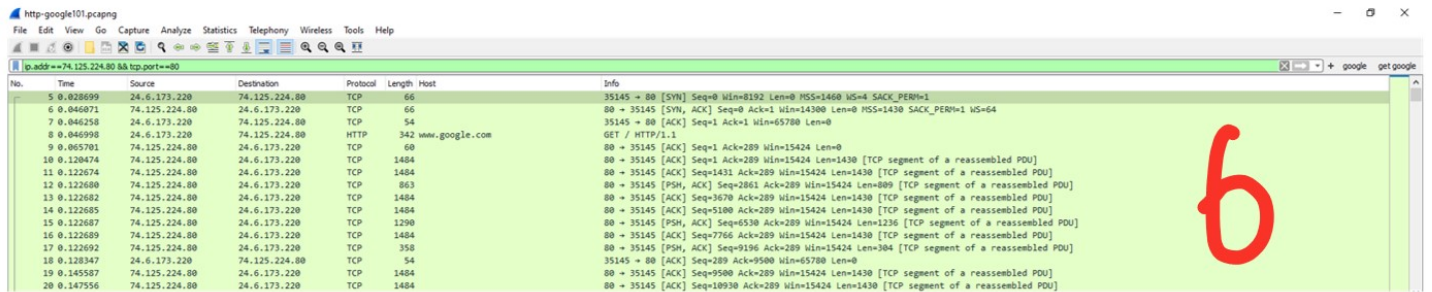
16. ให้หาว่าในไฟล์มีการโต้ตอบของ IP Address คู่ใดที่เกิดขึ้นมากที่สุด ให้สร้าง Filter ที่แสดงเฉพาะการโต้ตอบนั้น ให้บอกจำนวน Packet และ Filter ที่ปรากฏ

ระหว่าง 24.6.173.220 กับ 184.84.222.144 มี 4468 Packet

Filter ได้ดังนี้ $ip.addr == 24.6.173.220 \&\& tcp.port == 10854 \&\& ip.addr == 184.84.222.144 \&\& tcp.port == 80$

งานครั้งที่ 3

- การส่งงาน ให้เป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา
- ส่วนบนของหน้าแรกให้มี รหัสนักศึกษา และ ชื่อนักศึกษา
- ให้ส่งโดยทำเป็นคำตอบแยกออกมา โดยตอบข้อที่ 3,6,7,10,12,14,16
- กำหนดส่ง ภายในวันที่ 31 มกราคม 2563



ใช้ http.host contains และ http.request.method
ใน Display filter เพื่อกรอง

http-sfgate101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http host == "www.sfgate.com" && http contains "http://www.sfgate.com/feedback"

No.	Time	Source	Destination	Protocol	Length	Host	Info
33	0.249392	24.6.173.220	208.93.137.180	HTTP	383	www.sfgate.com	GET /external/css/global.shared.2.8.4p3.19000.css HTTP/1.1
34	0.249817	24.6.173.220	208.93.137.180	HTTP	361	www.sfgate.com	GET /external/css/global.site.2.8.4p3.19000.css HTTP/1.1
37	0.250116	24.6.173.220	208.93.137.180	HTTP	366	www.sfgate.com	GET /external/js/global.header.2.8.4p3.19000.js HTTP/1.1
42	0.251759	24.6.173.220	208.93.137.180	HTTP	370	www.sfgate.com	GET /css/pages/sections/feedback.css HTTP/1.1
43	0.252170	24.6.173.220	208.93.137.180	HTTP	363	www.sfgate.com	GET /external/js/global.top.2.8.4p3.19000.js HTTP/1.1
60	0.275990	24.6.173.220	208.93.137.180	HTTP	354	www.sfgate.com	GET /js/omiture/analyticconfig.js HTTP/1.1
83	0.278273	24.6.173.220	208.93.137.180	HTTP	349	www.sfgate.com	GET /js/hdm/omiture/s_code.js HTTP/1.1
84	0.278562	24.6.173.220	208.93.137.180	HTTP	355	www.sfgate.com	GET /js/hdm/omiture/analyticcause.js HTTP/1.1
124	0.295795	24.6.173.220	208.93.137.180	HTTP	344	www.sfgate.com	GET /js/hdm/yumwrapper.js HTTP/1.1
136	0.301020	24.6.173.220	208.93.137.180	HTTP	366	www.sfgate.com	GET /external/js/global.bottom.2.8.4p3.19000.js HTTP/1.1
143	0.303043	24.6.173.220	208.93.137.180	HTTP	395	www.sfgate.com	GET /img/modules/siteheader/chron_w_promo.gif HTTP/1.1
156	0.307355	24.6.173.220	208.93.137.180	HTTP	386	www.sfgate.com	GET /img/modules/siteheader/brand.png HTTP/1.1
181	0.316488	24.6.173.220	208.93.137.180	HTTP	393	www.sfgate.com	GET /img/modules/siteheader/wa001/arrow.gif HTTP/1.1
187	0.319475	24.6.173.220	208.93.137.180	HTTP	389	www.sfgate.com	GET /img/modules/siteheader/closeBtn.gif HTTP/1.1
191	0.320960	24.6.173.220	208.93.137.180	HTTP	403	www.sfgate.com	GET /img/partners/target/target_weekly_ad_animated.gif HTTP/1.1
197	0.330820	24.6.173.220	208.93.137.180	HTTP	376	www.sfgate.com	GET /img/utills/rss_icon.png HTTP/1.1
201	0.331854	24.6.173.220	208.93.137.180	HTTP	403	www.sfgate.com	GET /img/modules/siteheader/footer/footer_bottom.png.gif HTTP/1.1

> Frame 33: 383 bytes on wire (3064 bits), 383 bytes captured (3064 bits) on interface \Device\NPF_{6E79FEC0-F7F9-4970-96E4-EFF300A0909F}, id 0

> Ethernet II, Src: HewlettP_87:bfa3 (d4:85:64:a7:bfa3), Dst: Cadant_31:bb:c1 (08:01:5c:31:bb:c1)

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

> Transmission Control Protocol, Src Port: 80616, Dst Port: 80, Seq: 1, Ack: 1, Len: 329

> Hypertext Transfer Protocol

0000 00 01 5c 31 bb c1 d4 85 64 a7 bfa3 08 00 45 00 ... \Internet-Draft-E

0010 01 71 22 02 40 00 00 00 00 18 06 ad dc 0d 5d ... q @ - - - - -

0020 89 b4 29 78 00 50 ff 48 7a 53 49 6b 7a ab 50 18 ... :x P H z5Kz: P

0030 40 29 21 58 00 00 47 45 54 20 2f 65 78 74 65 72 ... @]X-EE T/exter

0040 66 61 6c 2f 63 73 73 2f 67 6c 6f 62 61 6c 2e 73 ... nal/css/global.s

0050 68 61 72 65 64 2e 32 2e 38 2e 34 70 33 2e 31 39 ... hared.2.8.4p3.19

0060 30 30 30 2d 63 73 73 20 48 54 54 50 2f 31 26 31 ... 0000.css HTTP/1.1

0070 0d 0a 48 6f 73 74 3a 20 77 77 72 76 67 61 61 ... Host: www.sfga

0080 74 65 2e 63 6f 6d 0a 55 73 65 72 2d 41 67 65 ... te.com User-Age

0090 66 74 3a 20 4d 4f 7a 69 6c 6c 61 2f 35 2e 30 20 ... nt: Mozilla/5.0

0100 20 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 3b ... (Windows NT 6.1;

0110 20 57 4f 57 36 34 30 20 72 76 3a 31 36 2e 30 29 ... ;MSIE6.0; rv:16.0)

0120 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 30 ... Gecko/2.0 (Ubuntu

0130 40 69 72 65 6b 6f 77 73 20 4e 54 20 36 2e 31 3b ... (Windows NT 6.1;

0140 20 57 4f 57 36 34 30 20 72 76 3a 31 36 2e 30 29 ... ;MSIE6.0; rv:16.0)

0150 2f 2a 3b 71 3d 30 2e 31 0d 0a 41 63 63 65 70 74 ... /?iq=0.1 -Accept

0160 2d 4c 61 6e 67 75 01 07 65 3a 20 65 6e 2d 55 53 ... -Language: en-US

0170 2c 65 6e 3b 71 3d 30 2e 31 0d 0a 41 63 63 65 70 ... en;q=0.5 -Accept

0180 74 2d 45 66 63 6f 64 69 6e 67 3a 20 67 69 69 70 ... t-encoding: gzip

0190 2c 2d 45 66 63 6f 64 69 6e 67 3a 20 67 69 69 70 ... , deflate - Conne

14

http-sfgate101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==24.6.173.220 && http.port==80854 && ip.addr==184.84.222.144 && http.port==80

No.	Time	Source	Destination	Protocol	Length	Host	Info
3547	8.844205	24.6.173.220	184.84.222.144	TCP	66		80 → 80854 [SYN] Seq=0 Win=0 Len=0 MSS=1460 sW=0 SACK_PERM=1
3547	8.850388	184.84.222.144	24.6.173.220	TCP	66		80854 → 80 [ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460 SACK_PERM=1 WS=2
3548	8.859590	24.6.173.220	184.84.222.144	TCP	54		80854 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
3549	8.860909	24.6.173.220	184.84.222.144	HTTP	408	vstatic.fastclick.net	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 → 80854 [ACK] Seq=1 Ack=427 Win=15672 Len=0
3551	8.892083	184.84.222.144	24.6.173.220	TCP	1514		80 → 80854 [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	102		80 → 80854 [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		80854 → 80 [ACK] Seq=427 Ack=1589 Win=65700 Len=0
3554	8.894302	184.84.222.144	24.6.173.220	TCP	1514		80 → 80854 [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 → 80854 [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		80854 → 80 [ACK] Seq=427 Ack=4589 Win=65700 Len=0
3564	8.900806	184.84.222.144	24.6.173.220	TCP	1514		80 → 80854 [ACK] Seq=4589 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3565	8.900996	184.84.222.144	24.6.173.220	TCP	1514		80 → 80854 [ACK] Seq=5969 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3566	8.900903	184.84.222.144	24.6.173.220	TCP	1514		80 → 80854 [ACK] Seq=7429 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3567	8.900240	24.6.173.220	184.84.222.144	TCP	54		80854 → 80 [ACK] Seq=427 Ack=6889 Win=65700 Len=0
3568	8.912554	184.84.222.144	24.6.173.220	TCP	1514		80 → 80854 [ACK] Seq=8889 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]
3648	8.914131	184.84.222.144	24.6.173.220	TCP	1514		80 → 80854 [ACK] Seq=13340 Ack=427 Win=15672 Len=1460 [TCP segment of a reassembled PDU]

> Frame 3546: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-F7F9-4970-96E4-EFF300A0909F}, id 0

> Ethernet II, Src: HewlettP_87:bfa3 (d4:85:64:a7:bfa3), Dst: Cadant_31:bb:c1 (08:01:5c:31:bb:c1)

> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 184.84.222.144

> Transmission Control Protocol, Src Port: 80854, Dst Port: 80, Seq: 0, Len: 0

0000 00 01 5c 31 bb c1 d4 85 64 a7 bfa3 08 00 45 00 ... \Internet-Draft-E

0010 00 34 28 bd 00 00 00 00 00 18 06 ad dc b8 54 ... 4 @ - - - - -T

0020 de 90 2a 66 00 50 b6 d9 f0 06 00 00 00 00 80 02 ... :f P - - - - -

0030 20 80 5c 4e 00 00 02 04 05 b4 01 03 02 01 01 ... : - - - - -

0040 04 02

16