



กิจกรรมที่ 3 : การใช้ display filters

Q(3) : ให้อัป display filter ให้บ่อนคำว่า http แล้วกด . จะเห็นว่า Wireshark แสดงตัวเลือกขึ้นมาให้เลือก ให้เลือก request.method ให้บ่อนให้ครบเป็น http.request.method=="GET" มีอะไรแสดงผล

A(3) : ใน Packet List Pane จะแสดงเฉพาะ packet ที่ใช้งานโปรโตคอล HTTP และมี method การใช้แบบ GET จำนวน 11 packet

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,cb,hv,wta,cr,cdos,nos,sf,tbpr,tbui,rsn,ob,mb,1
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=17259,37102,39523,39978,4000015,40001
236	0.561458	24.6.173.220	74.125.224.80	HTTP	576	GET /favicon.ico HTTP/1.1
301	0.619777	24.6.173.220	74.125.224.47	HTTP	361	GET /gb/js/sem_297d078eccaf4382701841bd042dbced.js HTTP/1.1

Q(6) : ให้ลบ display filter (กดปุ่ม x) จากนั้นกดปุ่ม google เกิดอะไรขึ้น

A(6) : เมื่อกดปุ่ม google ในช่อง Display filter จะปรากฏคำสั่งที่เรากรอกไว้ในตอนแรก ip.addr == 74.125.224.80 and tcp.port == 80 ส่วนใน Packet List Pane จะแสดงเฉพาะ packet ที่มี IP Address เป็น 74.125.224.80 และมีการใช้งาน tcp port เป็น 80 จำนวน 278 packet

No.	Time	Source	Destination	Protocol	Length	Info
5	0.028699	24.6.173.220	74.125.224.80	TCP	66	35145 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
6	0.046071	74.125.224.80	24.6.173.220	TCP	66	80 → 35145 [SYN, ACK] Seq=0 Ack=1 Win=14300 Len=0 MSS=1430 SACK_PERM=1
7	0.046258	24.6.173.220	74.125.224.80	TCP	54	35145 → 80 [ACK] Seq=1 Ack=1 Win=65780 Len=0
8	0.046998	24.6.173.220	74.125.224.80	HTTP	342	GET / HTTP/1.1
9	0.065701	74.125.224.80	24.6.173.220	TCP	60	80 → 35145 [ACK] Seq=1 Ack=289 Win=15424 Len=0
10	0.120474	74.125.224.80	24.6.173.220	TCP	1484	80 → 35145 [ACK] Seq=1 Ack=289 Win=15424 Len=1430 [TCP segment of a r...
11	0.122674	74.125.224.80	24.6.173.220	TCP	1484	80 → 35145 [ACK] Seq=1431 Ack=289 Win=15424 Len=1430 [TCP segment of ...
12	0.122680	74.125.224.80	24.6.173.220	TCP	863	80 → 35145 [PSH, ACK] Seq=2861 Ack=289 Win=15424 Len=809 [TCP segment...
13	0.122682	74.125.224.80	24.6.173.220	TCP	1484	80 → 35145 [ACK] Seq=3670 Ack=289 Win=15424 Len=1430 [TCP segment of ...
14	0.122685	74.125.224.80	24.6.173.220	TCP	1484	80 → 35145 [ACK] Seq=5100 Ack=289 Win=15424 Len=1430 [TCP segment of ...
15	0.122687	74.125.224.80	24.6.173.220	TCP	1290	80 → 35145 [PSH, ACK] Seq=6530 Ack=289 Win=15424 Len=1236 [TCP segmen...

Q(7) : ให้ลบ display filter (กดปุ่ม x) จากนั้นกดปุ่ม google เกิดอะไรขึ้น

A(7) : กำหนดค่าเป็น http.host == www.google.com and http.request.method == "GET"

Wireshark · Preferences

Packets: 374 · Displayed: 10 (2.7%)

Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution

Show in toolbar	Button Label	Filter Expression	Comment
<input checked="" type="checkbox"/>	google	ip.addr == 74.125.224.80 and tcp.port == 80	
<input checked="" type="checkbox"/>	get google	http.host == www.google.com and http.request.method == "GET"	

http.host == www.google.com and 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,cb,hv,wta,cr,cdos,nos,sf,tbpr,tbui,rsn,ob,mb,1c...
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=17259,37102,39523,39978,4000015,400011...
236	0.561458	24.6.173.220	74.125.224.80	HTTP	576	GET /favicon.ico HTTP/1.1



Q(10) : ให้เพิ่ม bookmark ของ display filter ที่เป็นการกรอง IP Address ของตัวเอง เข้าไปแล้ว capture มาแสดง
ควรทดสอบโดยการ Capture แล้วกรองว่าแสดงเฉพาะ IP Address ของตัวเองจริงหรือไม่

A(10) : IP Address คือ 10.10.0.254 ตั้งชื่อ bookmark คือ My-IP

The screenshot shows the Wireshark interface with the display filter 'My-IP: ip.addr == 10.10.0.254' applied. The packet list shows several UDP packets from 10.10.0.254 to 10.10.0.254. The packet details pane shows the structure of a UDP packet, including the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header.

Q(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

A(12) : หา packet ที่ การ request ไปที่ hearstnp.com (มีจำนวน 6 ครั้ง) ทำได้โดยการพิมพ์ในช่อง Display filter ดังนี้ http.host contains hearstnp.com

The screenshot shows the Wireshark interface with the display filter 'http.host matches hearstnp.com' applied. The packet list shows several HTTP packets from 24.6.173.220 to 208.93.137.180. The packet details pane shows the structure of an HTTP GET request to extras.sfgate.com.

packet ที่ใช้ Method post ไปยัง extras.sfgate.com (มี 1 ครั้ง) ทำได้โดยการพิมพ์ในช่อง Display filter ดังนี้ http.host matches extras.sfgate.com and http.request.method == "POST"

The screenshot shows the Wireshark interface with the display filter 'http.host matches extras.sfgate.com and http.request.method == "POST"' applied. The packet list shows a single HTTP POST packet from 24.6.173.220 to 208.93.137.180. The packet details pane shows the structure of an HTTP POST request to extras.sfgate.com.



Q(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>

A(14) : ในช่อง Display filter ว่า `http.request.uri == "/feedback/"`

No.	Time	Source	Destination	Protocol	Length	Host	Info
8	0.000520	24.6.173.220	208.93.137.180	HTTP	549	www.sfgate.com	GET /feedback/ HTTP/1.1

Q(16) : ให้หาว่าในไฟล์มีการโต้ตอบของ IP Address คู่ใดที่เกิดขึ้นมากที่สุด ให้สร้าง Filter ที่แสดงเฉพาะการโต้ตอบนั้น ให้บอกจำนวน Packet และ Filter ที่ปรากฏ

A(16) : ใน Conversations ในแถบเมนู IPv4 คลิกเลือกคอลัมน์ Packet ใน sort จากมากไปน้อย เราจะได้คู่ conversation ที่มีการใช้ปริมาณข้อมูลมากที่สุด จากนั้นคลิกขวา Apply as Filter > Selected > A <-> B จากนั้นที่ Display filter จะแสดง filter เป็น `ip.addr==24.6.173.220 && ip.addr==184.84.222.144`

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	184.84.222.144	4,468	4841k	1,314	71k	3,154	4760k	0.0.0.0/0.0.0.0	1.6491	346k	23M
24.6.173.220	96.17.110.102	1,336							26.7425	7407	417k
24.6.173.220	208.93.137.180	882							73.8462	7111	47k
24.6.173.220	75.75.75.75	536							77.6131	2178	4663
24.6.173.220	67.192.92.227	289							79.5969	2949	12k

No.	Time	Source	Destination	Protocol	Length	Host	Info
3546	0.001645	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	0.015123	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
3548	0.000202	24.6.173.220	184.84.222.144	TCP	54		10854 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
3550	0.018168	184.84.222.144	24.6.173.220	TCP	60		80 → 10854 [ACK] Seq=1 Ack=427 Win=15672 Len=0
3551	0.013726	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
3552	0.000004	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
3553	0.000685	24.6.173.220	184.84.222.144	TCP	54		10854 → 80 [ACK] Seq=427 Ack=1589 Win=65700 Len=0
3554	0.000810	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
3555	0.000006	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
3556	0.000306	24.6.173.220	184.84.222.144	TCP	54		10854 → 80 [ACK] Seq=427 Ack=4509 Win=65700 Len=0