กิจกรรมที่ 3 : การใช้ display filters

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

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

	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,l							
	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 0.619770	24.6.173.220	74.125.224.47	HTTP	361	GET	/gb/js/sem_297d078eccaf4382701841bd042dbced.js HTTP/1.1							

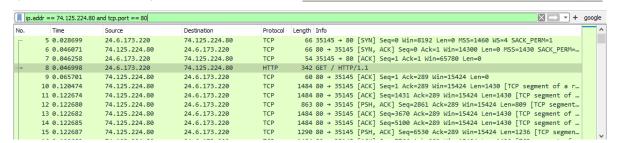
Q(6) : ให้ลบ display filter (กดปุ่ม x) จากนั้นกดปุ่ม google เกิดอะไรขึ้น

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

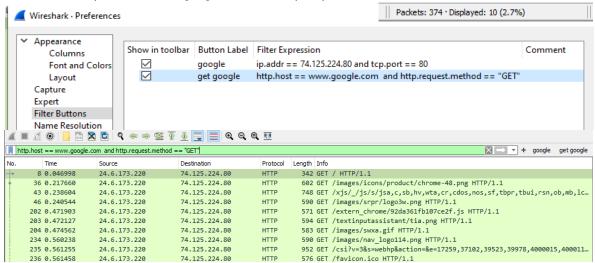
Packets: 374 · Displayed: 278 (74.3%)

Profile: Http-GET



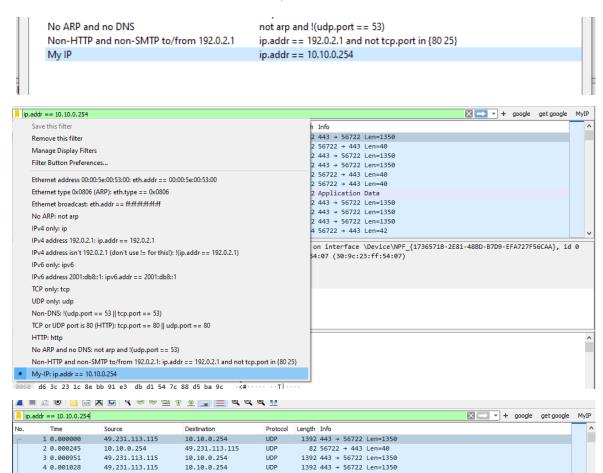
Q(7) : ให้ลบ display filter (กดปุ่ม x) จากนั้นกดปุ่ม google เกิดอะไรขึ้น

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



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



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

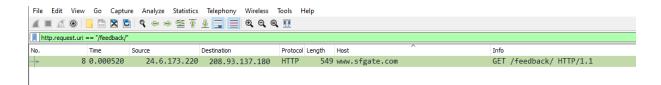


packet ที่ใช้ Method post ไปยัง extras.sfgate.com (มี 1 ครั้ง) ทำได้โดยการพิมพ์ในช่อง Display filter ดังนี้ http.host matches extras.sfgate.com and http.request.method == "POST"

						Packets: 11678 · Displayed: 1 (0.0%)		Profile: Default						
	http.host matches extras.sfgate.com and http.request.method == "POST"													
No.		Time	Source	Destination	Protocol	Length	Host	Info						
-	10	0.000862	24.6.173.220	208.93.137.180	HTTP	1595	extras.sfgate.com	POST	/sfgate/modules/formHand					

Q(14) : ให้ยกเลิก display filter แล้วไปที่ packet ที่ 8 ไปที่ host แล้ว คลิกขวา แล้วเลือก Apply as Filter จากนั้นให้ หาวิธีในการหา packet ที่ request ไปที่ http://www.sfgate.com/feedback

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



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

A(16) : ใน Conversations ในแถบเมนู IPv4 คลิกเลือกคอลัมน์ Packet ใน sort จากมากไปน้อย เราก็จะได้คู่ conversation ที่มีการใช้ ปริมาณข้อมูลมากที่สุด 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

