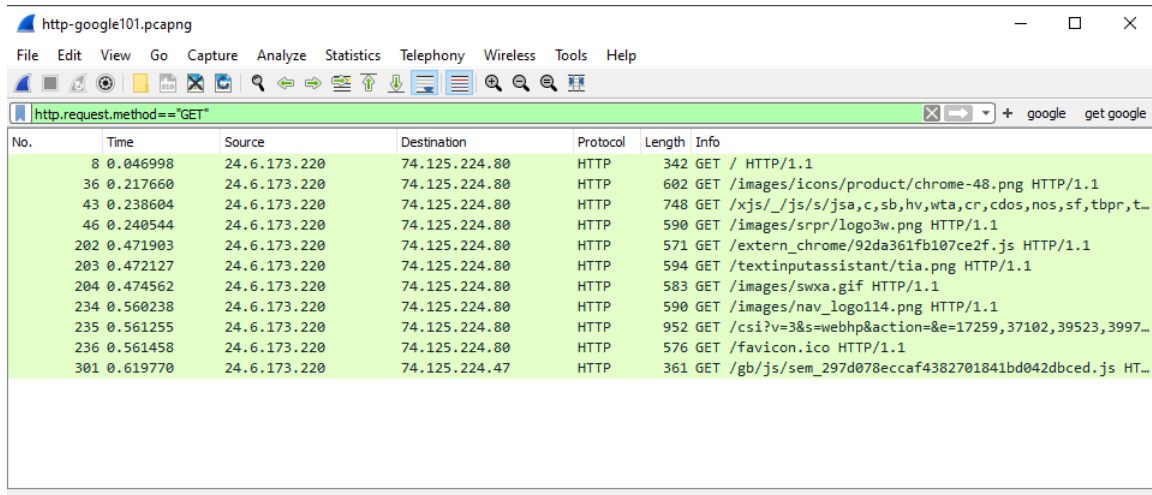


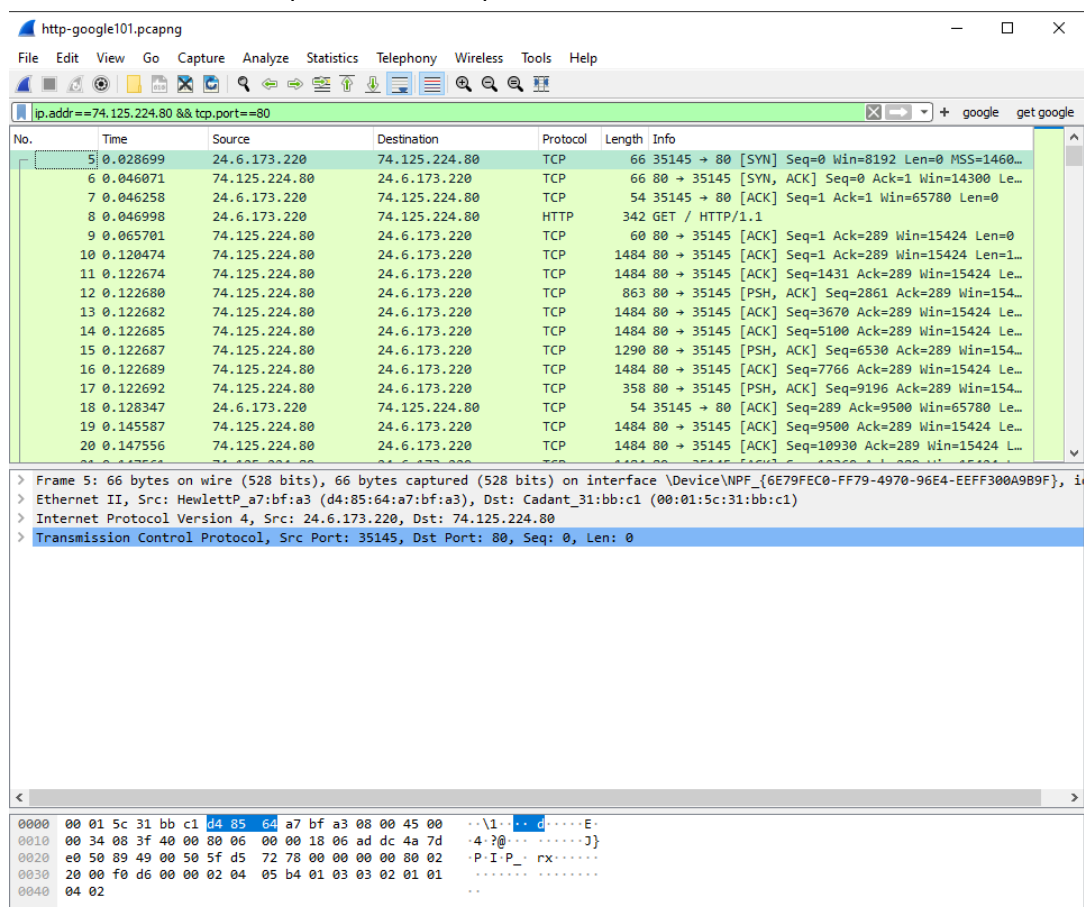
3. ให้ไปที่ display filter ให้ป้อนคำว่า http แล้วกด . จะเห็นว่า Wireshark แสดงตัวเลือกขึ้นมาให้เลือก ให้เลือก request.method ให้ป้อนให้ครบเป็น http.request.method=="GET" มีอะไรแสดงผล



Wireshark interface showing a display filter of `http.request.method=="GET"`. The packet list shows several HTTP GET requests to various resources on 74.125.224.80.

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,t...
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=17259,37102,39523,3997...
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_297d078eccaf4382701841bd042dbcd.js HT...

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



Wireshark interface showing a display filter of `ip.addr==74.125.224.80 && tcp.port==80`. The packet list shows a series of TCP and HTTP packets. The packet details pane shows the selected packet (No. 5) as a SYN packet from 24.6.173.220 to 74.125.224.80 on port 80.

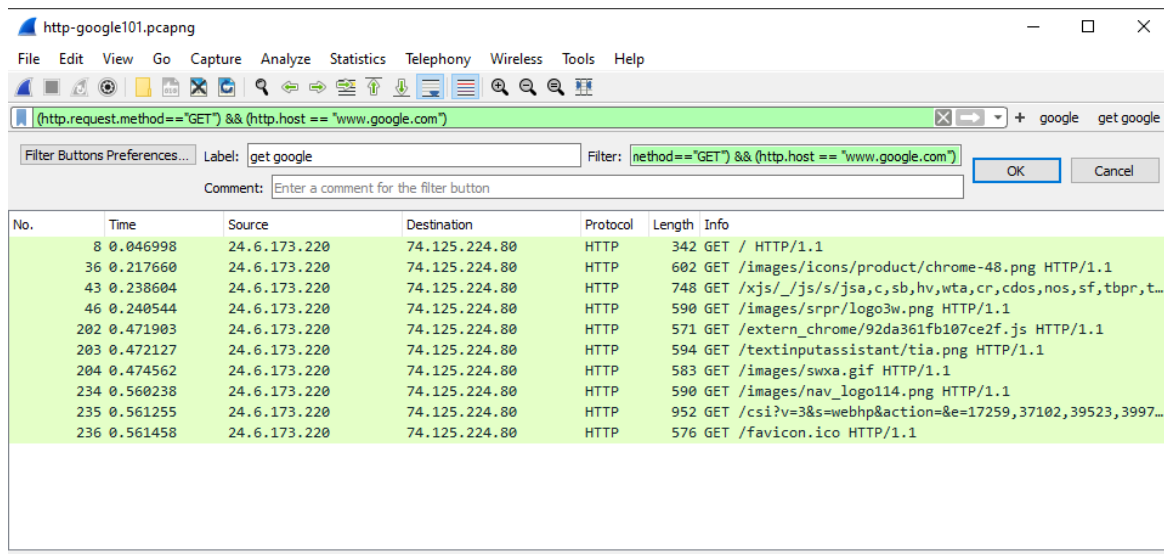
No.	Time	Source	Destination	Protocol	Length	Info
5	0.028699	24.6.173.220	74.125.224.80	TCP	66	35145 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460...
6	0.046071	74.125.224.80	24.6.173.220	TCP	66	80 → 35145 [SYN, ACK] Seq=0 Ack=1 Win=14300 Le...
7	0.046258	24.6.173.220	74.125.224.80	TCP	54	35145 → 80 [ACK] 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=1...
11	0.122674	74.125.224.80	24.6.173.220	TCP	1484	80 → 35145 [ACK] Seq=1431 Ack=289 Win=15424 Le...
12	0.122680	74.125.224.80	24.6.173.220	TCP	863	80 → 35145 [PSH, ACK] Seq=2861 Ack=289 Win=154...
13	0.122682	74.125.224.80	24.6.173.220	TCP	1484	80 → 35145 [ACK] Seq=3670 Ack=289 Win=15424 Le...
14	0.122685	74.125.224.80	24.6.173.220	TCP	1484	80 → 35145 [ACK] Seq=5100 Ack=289 Win=15424 Le...
15	0.122687	74.125.224.80	24.6.173.220	TCP	1290	80 → 35145 [PSH, ACK] Seq=6530 Ack=289 Win=154...
16	0.122689	74.125.224.80	24.6.173.220	TCP	1484	80 → 35145 [ACK] Seq=7766 Ack=289 Win=15424 Le...
17	0.122692	74.125.224.80	24.6.173.220	TCP	358	80 → 35145 [PSH, ACK] Seq=9196 Ack=289 Win=154...
18	0.128347	24.6.173.220	74.125.224.80	TCP	54	35145 → 80 [ACK] Seq=289 Ack=9500 Win=65780 Le...
19	0.145587	74.125.224.80	24.6.173.220	TCP	1484	80 → 35145 [ACK] Seq=9500 Ack=289 Win=15424 Le...
20	0.147556	74.125.224.80	24.6.173.220	TCP	1484	80 → 35145 [ACK] Seq=10930 Ack=289 Win=15424 L...

Packet Details for Frame 5:

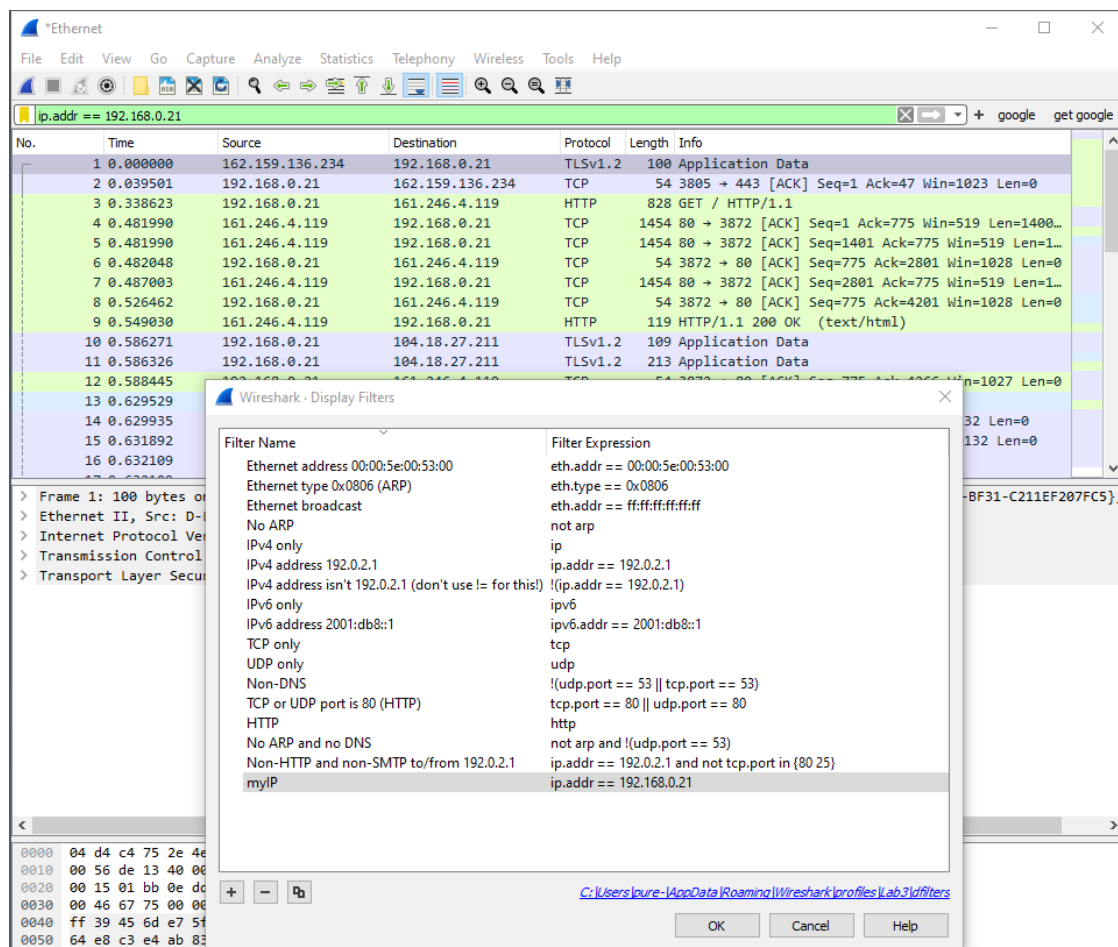
- Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, in
- Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
- Internet Protocol Version 4, Src: 24.6.173.220, Dst: 74.125.224.80
- Transmission Control Protocol, Src Port: 35145, Dst Port: 80, Seq: 0, Len: 0

ในช่อง display filter จะขึ้นตามที่ตั้งไว้

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



10. ให้เพิ่ม bookmark ของ display filter ที่เป็นการกรอง IP Address ของตัวเอง เข้าไปแล้ว capture มาแสดง ควรทดสอบโดยการ Capture แล้วกรองว่าแสดงเฉพาะ IP Address ของตัวเองจริงหรือไม่



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

- 1.ไปที่ display filter ให้ป้อนคำว่า http.request.method=="GET"
- 2.เพิ่มคอลัมน์ http.host
- 3.แล้วหา hearstnp.com ในคอลัมน์ host จะเจอ aps.hearstnp.com
- 4.ไปที่ display filter ให้ป้อนคำว่า http.host == aps.hearstnp.com จะได้ 6 packet
- 5.ไปที่ display filter ให้ป้อนคำว่า http.request.method == "POST" && http.host == extras.sfgate.com จะได้ 1 packet
- 6.ไปที่ display filter ให้ป้อนคำว่า http.host == aps.hearstnp.com || (http.request.method == "POST" && http.host == extras.sfgate.com) จะได้ 6+1 packet ดังนี้

No.	Time	Source	Destination	Protocol	Length	Host	Info
159	0.309161	24.6.173.220	208.93.137.180	HTTP	344	aps.hearstnp.com	GET /Scripts/loadAc
388	0.436294	24.6.173.220	208.93.137.180	HTTP	348	aps.hearstnp.com	GET /Scripts/loadAc
406	0.465477	24.6.173.220	208.93.137.180	HTTP	363	aps.hearstnp.com	GET /SRO/GetJS?url=
458	0.628832	24.6.173.220	208.93.137.180	HTTP	350	aps.hearstnp.com	GET /Scripts/initDe
10055	68.404262	24.6.173.220	208.93.137.180	HTTP	420	aps.hearstnp.com	GET /SRO/GetJS?url=
10067	69.068504	24.6.173.220	208.93.137.180	HTTP	437	aps.hearstnp.com	GET /SRO/GetJS?url=
10022	67.615441	24.6.173.220	208.93.137.180	HTTP	1595	extras.sfgate.com	POST /sfgate/module

14. ให้ยกเลิก display filter แล้วไปที่ packet ที่ 8 ไปที่ host แล้ว คลิกขวา แล้วเลือก Apply as Filter จากนั้นให้หา
 วิธีในการหา packet ที่ request ไปที่ <http://www.sfgate.com/feedback>
 ไปที่ request uri คลิกขวา แล้วเลือก Apply as Filter เลือก selected

No.	Time	Source	Destination	Protocol	Length	Host	Info
8	0.054566	24.6.173.220	208.93.137.180	HTTP	549	www.sfgate.com	GET /feedback/ HTTP

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

The image shows a Wireshark capture of a network packet. The packet list at the top shows a series of TCP connections between 24.6.173.220 and 184.84.222.144. The packet details pane shows the structure of a TCP reset (RST) packet, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header.

No.	Time	Source	Destination	Protocol	Length	Host	Info
8080	10.488375	184.84.222.144	24.6.173.220	TCP	1514		80 → 10854 [RST] Seq=10854
8081	10.489140	184.84.222.144	24.6.173.220	TCP	1514		80 → 10854 [RST] Seq=10854
8082	10.489142	184.84.222.144	24.6.173.220	TCP	1514		80 → 10854 [RST] Seq=10854
8083	10.489144	184.84.222.144	24.6.173.220	TCP	1514		80 → 10854 [RST] Seq=10854
8084	10.489213	24.6.173.220	184.84.222.144	TCP	54		10854 → 80 [RST] Seq=10854
8085	10.489959	184.84.222.144	24.6.173.220	TCP	1514		80 → 10854 [RST] Seq=10854
8086	10.490749	184.84.222.144	24.6.173.220	TCP	1514		80 → 10854 [RST] Seq=10854
8087	10.490752	184.84.222.144	24.6.173.220	TCP	1514		80 → 10854 [RST] Seq=10854
8088	10.490809	24.6.173.220	184.84.222.144	TCP	54		10854 → 80 [RST] Seq=10854
8089	10.491578	184.84.222.144	24.6.173.220	TCP	1514		80 → 10854 [RST] Seq=10854
8090	10.491580	184.84.222.144	24.6.173.220	TCP	1514		80 → 10854 [RST] Seq=10854
8091	10.491634	24.6.173.220	184.84.222.144	TCP	54		10854 → 80 [RST] Seq=10854
8092	10.492383	184.84.222.144	24.6.173.220	TCP	1514		80 → 10854 [RST] Seq=10854
8093	10.493154	184.84.222.144	24.6.173.220	TCP	1514		80 → 10854 [RST] Seq=10854
8094	10.493158	184.84.222.144	24.6.173.220	TCP	508		80 → 10854 [RST] Seq=10854

Frame 8096: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}

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: 184.84.222.144

Transmission Control Protocol, Src Port: 10854, Dst Port: 80, Seq: 427, Ack: 4622943, Len: 0

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ..1...d.....E.

0010 00 28 2e 11 40 00 80 06 00 00 18 06 ad dc b8 54 ..(.@.....T

0020 de 90 2a 66 00 50 b6 d9 f1 b1 41 af fe dc 50 10 ...*fP...A...P.

0030 b0 cc 5c e2 00 00 \...

การโต้ตอบของ IP Address 24.6.173.220 และ 184.84.222.144 เยอะที่สุด มี 4468 packets และ filter ที่ปรากฏ ip.addr==24.6.173.220 && ip.addr==184.84.222.144