ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

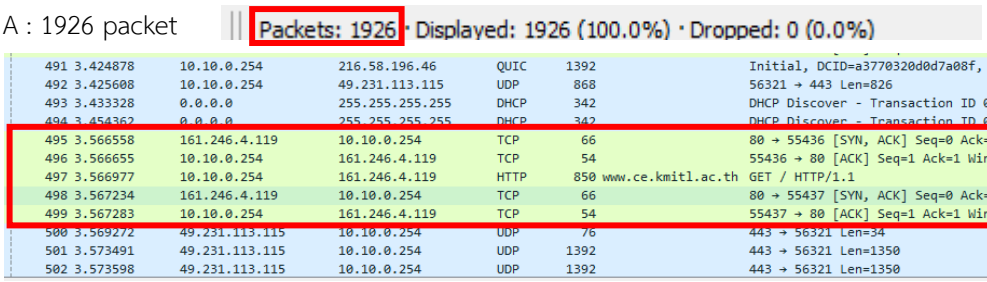
กิจกรรมที่ 2 : การ Capture ข้อมูลจากระบบเครือข่าย

Q : เปลี่ยน Profile เป็น Default คอลัมน์แสดงอย่างไร

A : คอลัมน์ใน Packet List Pane ของ Profile Default จะไม่มีคอลัมน์ Host ส่วน Profile Test_wireshark จะมีคอลัมน์ Host

Q : ได้ข้อมูลกี่ Packet

A : 1926 packet



491	3.424878	10.10.0.254	216.58.196.46	QUIC	1392	Initial, DCID=a3770320d0d7a08f, PKN: 1, CRYPTO, PADDING
492	3.425608	10.10.0.254	49.231.113.115	UDP	868	56321 → 443 Len=826
493	3.433328	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5e1b00f6
494	3.454362	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x25ca5bf2
495	3.566558	161.246.4.119	10.10.0.254	TCP	66	80 → 55436 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1400 SACK_PERM=1 WS=32
496	3.566655	10.10.0.254	161.246.4.119	TCP	54	55436 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
497	3.566977	10.10.0.254	161.246.4.119	HTTP	850 www.ce.kmitl.ac.th	GET / HTTP/1.1
498	3.567234	161.246.4.119	10.10.0.254	TCP	66	80 → 55437 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1400 SACK_PERM=1 WS=32
499	3.567283	10.10.0.254	161.246.4.119	TCP	54	55437 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
500	3.569272	49.231.113.115	10.10.0.254	UDP	76	443 → 56321 Len=34
501	3.573491	49.231.113.115	10.10.0.254	UDP	1392	443 → 56321 Len=1350
502	3.573598	49.231.113.115	10.10.0.254	UDP	1392	443 → 56321 Len=1350

Q : (5.) ...using this filter: ให้ป้อน host www.ce.kmitl.ac.th

A :

No.	Time	Source	Destination	Protocol	Length	Host	Info
1	0.000000	10.10.0.254	161.246.4.119	TCP	66		55326 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.001050	10.10.0.254	161.246.4.119	HTTP	850	www.ce.kmitl.ac.th	GET / HTTP/1.1
3	0.072954	161.246.4.119	10.10.0.254	TCP	66		80 → 55326 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1400 SACK_PERM=1 WS=32
4	0.073067	10.10.0.254	161.246.4.119	TCP	54		55326 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
5	0.084534	161.246.4.119	10.10.0.254	TCP	60		80 → 55323 [ACK] Seq=1 Ack=797 Win=233 Len=0
6	0.127087	161.246.4.119	10.10.0.254	TCP	1454		80 → 55323 [ACK] Seq=1 Ack=797 Win=233 Len=1400 [TCP segment of a reassembled PDU]
7	0.149653	161.246.4.119	10.10.0.254	TCP	1454		80 → 55323 [ACK] Seq=1401 Ack=797 Win=233 Len=1400 [TCP segment of a reassembled PDU]
8	0.149760	10.10.0.254	161.246.4.119	TCP	54		55323 → 80 [ACK] Seq=797 Ack=2801 Win=514 Len=0
9	0.196556	161.246.4.119	10.10.0.254	TCP	1454		80 → 55323 [ACK] Seq=2801 Ack=797 Win=233 Len=1400 [TCP segment of a reassembled PDU]
10	0.196556	161.246.4.119	10.10.0.254	HTTP	154		HTTP/1.1 200 OK (text/html)
11	0.196640	10.10.0.254	161.246.4.119	TCP	54		55323 → 80 [ACK] Seq=797 Ack=4301 Win=514 Len=0

Q : (6.) ...using this filter: ให้ป้อน host 161.246.4.119

A :

No.	Time	Source	Destination	Protocol	Length	Host	Info
1	0.000000	161.246.4.119	10.10.0.254	TCP	66		80 → 55349 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1400 SACK_PERM=1 WS=32
2	0.000045	10.10.0.254	161.246.4.119	TCP	66		55349 → 80 [ACK] Seq=1 Ack=1 Win=514 Len=0 SLE=0 SRE=1
3	1.020836	10.10.0.254	161.246.4.119	TCP	66		55364 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	1.037829	10.10.0.254	161.246.4.119	HTTP	824	www.ce.kmitl.ac.th	GET / HTTP/1.1
5	1.089059	161.246.4.119	10.10.0.254	TCP	66		80 → 55364 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1400 SACK_PERM=1 WS=32
6	1.089184	10.10.0.254	161.246.4.119	TCP	54		55364 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
7	1.090835	161.246.4.119	10.10.0.254	TCP	60		80 → 55349 [ACK] Seq=1 Ack=771 Win=7392 Len=0
8	1.130344	161.246.4.119	10.10.0.254	TCP	1454		80 → 55349 [ACK] Seq=1 Ack=771 Win=7392 Len=1400 [TCP segment of a reassembled PDU]
9	1.131401	161.246.4.119	10.10.0.254	TCP	1454		80 → 55349 [ACK] Seq=1401 Ack=771 Win=7392 Len=1400 [TCP segment of a reassembled PDU]
10	1.131444	10.10.0.254	161.246.4.119	TCP	54		55349 → 80 [ACK] Seq=771 Ack=2801 Win=514 Len=0
11	1.172613	161.246.4.119	10.10.0.254	TCP	1454		80 → 55349 [ACK] Seq=2801 Ack=771 Win=7392 Len=1400 [TCP segment of a reassembled PDU]
12	1.181071	161.246.4.119	10.10.0.254	HTTP	154		HTTP/1.1 200 OK (text/html)
13	1.181156	10.10.0.254	161.246.4.119	TCP	54		55349 → 80 [ACK] Seq=771 Ack=4301 Win=514 Len=0
14	1.512542	10.10.0.254	161.246.4.119	HTTP	739	www.ce.kmitl.ac.th	GET /slideshow2.css HTTP/1.1
15	1.606151	10.10.0.254	161.246.4.119	TCP	54		55334 → 80 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0
16	1.609438	161.246.4.119	10.10.0.254	HTTP	626		HTTP/1.1 404 Not Found (text/html)
17	1.652612	10.10.0.254	161.246.4.119	TCP	54		55349 → 80 [ACK] Seq=1456 Ack=4873 Win=511 Len=0

Q : ขั้นตอนในข้อ (5.) และ (6.) ต่างกันอย่างไร

A : ในขั้นตอนที่ 5 และ 6 เป็นการใช้คำสั่ง host ของ Wireshark เพื่อกรองเอาเฉพาะ packet ที่วิ่งไปหา Host ที่ต้องการ ซึ่งจะแตกต่างกันโดยในขั้นตอนที่ 5. เป็นการระบุ IP ของ Host ส่วนในขั้นตอนที่ 6. เป็นการระบุแบบเป็น URL หรือ Domain Name ที่ชี้ไปหา Host ซึ่งให้ผลลัพธ์ไม่แตกต่างกัน

ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

Q : (9.) ...using this filter: ให้ป้อน src host 161.246.4.119

A :

1	0.000000	161.246.4.119	10.10.0.254	TCP	66	80 → 55384 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1400 SACK_PERM=1 WS=32
2	0.000000	161.246.4.119	10.10.0.254	TCP	66	80 → 55383 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1400 SACK_PERM=1 WS=32
3	0.072649	161.246.4.119	10.10.0.254	TCP	60	80 → 55383 [ACK] Seq=1 Ack=761 Win=7360 Len=0
4	0.112418	161.246.4.119	10.10.0.254	TCP	1454	80 → 55383 [ACK] Seq=1 Ack=761 Win=7360 Len=1400 [TCP segment of a reassembled PDU]
5	0.113034	161.246.4.119	10.10.0.254	TCP	1454	80 → 55383 [ACK] Seq=1401 Ack=761 Win=7360 Len=1400 [TCP segment of a reassembled PDU]
6	0.138714	161.246.4.119	10.10.0.254	TCP	1454	80 → 55383 [ACK] Seq=2801 Ack=761 Win=7360 Len=1400 [TCP segment of a reassembled PDU]
7	0.138714	161.246.4.119	10.10.0.254	HTTP	154	HTTP/1.1 200 OK (text/html)
8	3.239953	161.246.4.119	10.10.0.254	HTTP	626	HTTP/1.1 404 Not Found (text/html)

Q : (10.) ...using this filter: ให้ป้อน dst host 161.246.4.119

A :

1	0.000000	10.10.0.254	161.246.4.119	TCP	54	55384 → 80 [FIN, ACK] Seq=1 Ack=1 Win=514 Len=0
2	0.000066	10.10.0.254	161.246.4.119	TCP	54	55383 → 80 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0
3	0.000510	10.10.0.254	161.246.4.119	TCP	66	55390 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	0.000637	10.10.0.254	161.246.4.119	TCP	66	55391 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	0.065262	10.10.0.254	161.246.4.119	TCP	54	55384 → 80 [ACK] Seq=2 Ack=2 Win=514 Len=0
6	0.066140	10.10.0.254	161.246.4.119	TCP	54	55390 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
7	0.066598	10.10.0.254	161.246.4.119	HTTP	850	www.ce.kmitl.ac.th GET / HTTP/1.1
8	0.066737	10.10.0.254	161.246.4.119	TCP	54	55391 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
9	0.226000	10.10.0.254	161.246.4.119	TCP	54	55390 → 80 [ACK] Seq=797 Ack=2801 Win=131584 Len=0
10	0.308537	10.10.0.254	161.246.4.119	TCP	54	55390 → 80 [ACK] Seq=797 Ack=4301 Win=131584 Len=0

Q : ขั้นตอนในข้อ (9.) และ (10.) ต่างกันอย่างไร

A : ในขั้นตอนที่ 9. จะเป็นการกรองเอาเฉพาะ packet ที่วิ่งจากเครื่อง Host (161.246.4.119) ซึ่งเป็นต้นทาง มาหาเครื่องของเราเอง (10.10.0.254) ซึ่งเป็นเครื่องปลายทาง ส่วนขั้นตอนที่ 10. เป็นการกรองเอาแค่ packet ที่เอาจากเครื่องของเรา (10.10.0.254) ที่มีปลายทางไปยังเครื่อง Host (161.246.4.119) ถ้ามองในมุม client – server คำสั่ง src host จะเป็นเสมือนว่าเราเป็นเครื่อง Host หรือ ฝั่ง server ที่วิ่งไปหา client ส่วนคำสั่ง dst host ก็จะเป็นเครื่องเรา หรือ client ที่วิ่งไปหา server

Q : ถ้าป้อน not host 161.246.4.119 คิดว่าจะหมายถึงอะไร

A : แสดงผลทุก packet ยกเว้น packet ที่มีปลายทางวิ่งไปหา Host 161.246.4.119 หรือ www.ce.kmitl.ac.th

Q : ให้นักศึกษาสรุปการใช้งานการใช้ Capture Filter เบื้องต้น

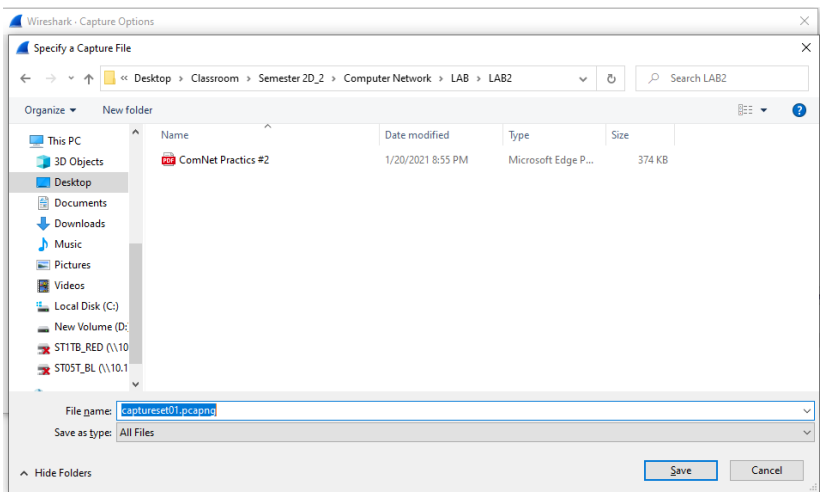
A : การใช้งาน Capture Filter เบื้องต้นสามารถทำได้โดยการใช้งานคำสั่ง host โดยมีรูปแบบดังนี้

<not> <src/dst> **host** <IP / domain name>

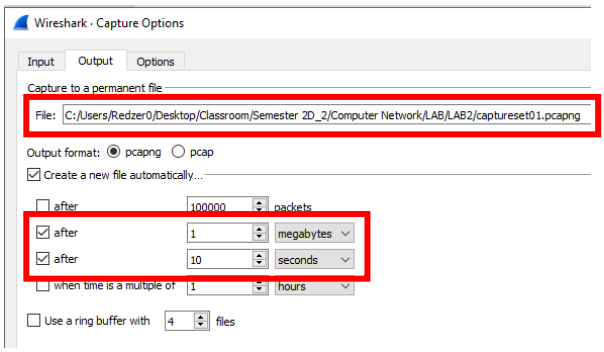
คำสั่ง **host** เป็นการกรองเอาเฉพาะ packet ที่วิ่งทั้งไป-กลับ ระหว่างเครื่องเรากับเครื่อง Host ที่ระบุโดยสามารถระบุ Host โดยใช้ IP หรือ Domain Name ก็ได้ โดยมี options เพิ่มเติม คือสามารถระบุว่าต้องการกรองเอา packet ของฝั่ง Host หรือ ฝั่งเราได้โดยการเพิ่มคำสั่ง src หรือ dst ข้างหน้าคำสั่ง **host** ส่วนคำสั่งเพิ่มเติมสุดท้ายคือ not จะเป็นการกรองเอา packet ที่มี host ปลายทางตามที่ระบุออกไป

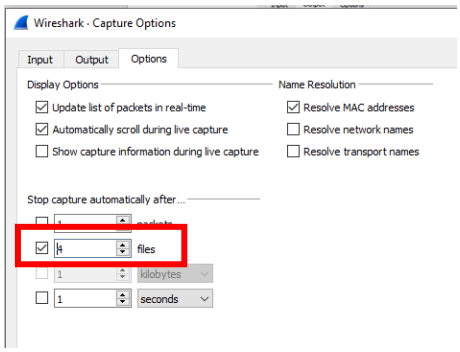
Q : ให้สร้างไฟล์ชื่อ captureset01.pcapng โดยกำหนดเงื่อนไขให้ขึ้นไฟล์ใหม่ทุก 1 MB และทุก 10 วินาที และหยุดหลังจาก 4 ไฟล์

A :

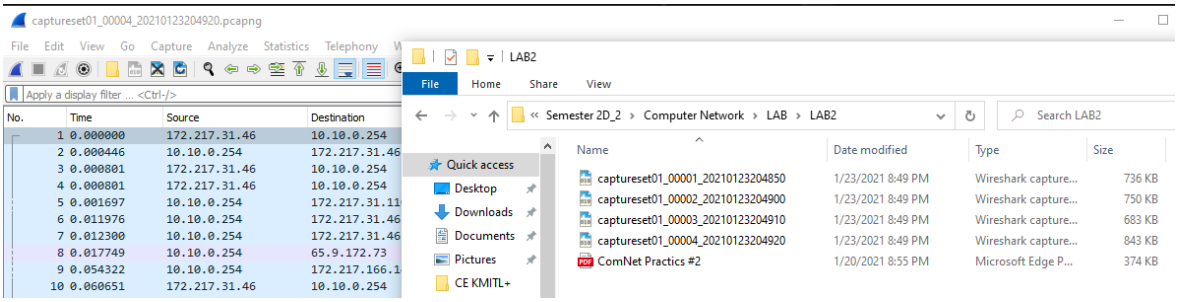


การตั้งค่า



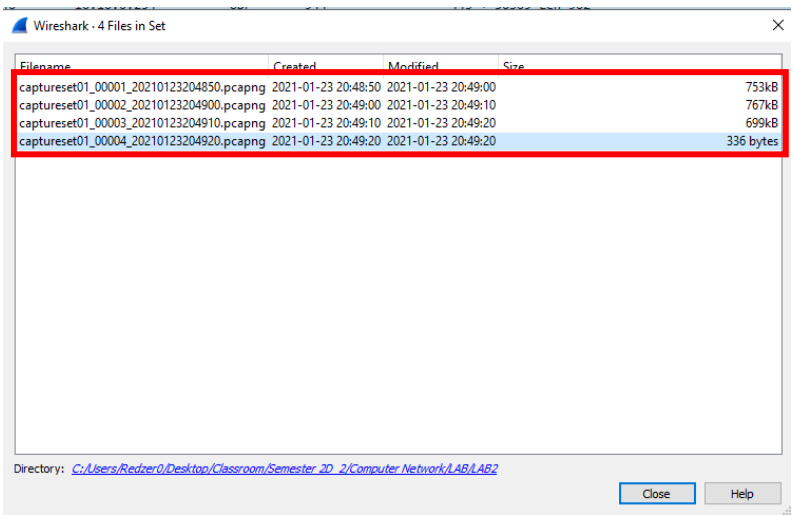


ไฟล์ Output ที่ได้



Q : ให้ไปที่ File -> File Set -> List Files มีอะไรเกิดขึ้น อธิบาย

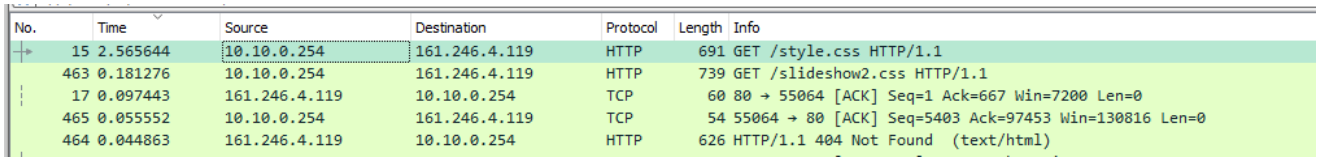
A : เกิดไฟล์ใหม่ขึ้นจำนวน 4 ไฟล์ โดยใน 1 ไฟล์จะเก็บ packet ที่เรา capture เอาไว้โดยไฟล์จะถูกสร้างเป็นไฟล์ใหม่ทุกๆ 10 วินาที หรือขนาดไฟล์เกิน 1 MB และพอครบ 4 ไฟล์ Wireshark จะหยุดการ capture packet



ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

Q : ให้หาค่าเวลาที่มากที่สุดในช่อง Time เป็น packet ที่เท่าไร และให้ถามเพื่อนอีก 3 คน พบที่ เดียวกันหรือไม่ ของเพื่อน packet ที่เท่าไร

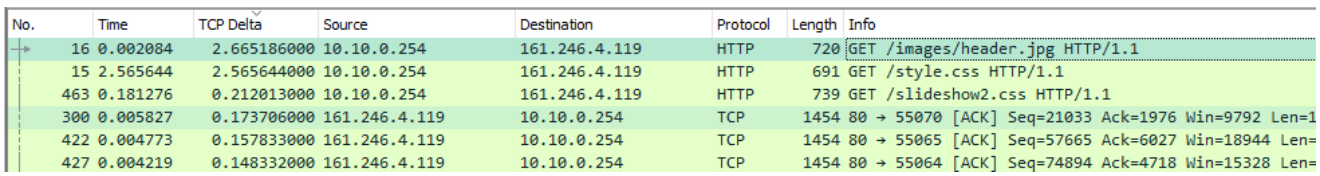
A : เป็น packet ที่ 15 ใช้เวลา 2.565 วินาที เป็นการโหลด css ของเว็บไซต์ GET /style.css HTTP/1.1 ส่วนของเพื่อนไม่ได้พบที่เดียวกัน ของเพื่อนเป็น packet ที่ 25 , 18 , 31 เป็นพวกการตอบ SYN , ACK ตามลำดับ



No.	Time	Source	Destination	Protocol	Length	Info
15	2.565644	10.10.0.254	161.246.4.119	HTTP	691	GET /style.css HTTP/1.1
463	0.181276	10.10.0.254	161.246.4.119	HTTP	739	GET /slideshow2.css HTTP/1.1
17	0.097443	161.246.4.119	10.10.0.254	TCP	60	80 → 55064 [ACK] Seq=1 Ack=667 Win=7200 Len=0
465	0.055552	10.10.0.254	161.246.4.119	TCP	54	55064 → 80 [ACK] Seq=5403 Ack=97453 Win=130816 Len=0
464	0.044863	161.246.4.119	10.10.0.254	HTTP	626	HTTP/1.1 404 Not Found (text/html)

Q : ให้หาค่าเวลาที่มากที่สุดในช่อง TCP Delta เป็น packet ที่เท่าไร และให้ถามเพื่อนอีก 3 คน พบ ที่เดียวกันหรือไม่ ของเพื่อน packet ที่เท่าไร

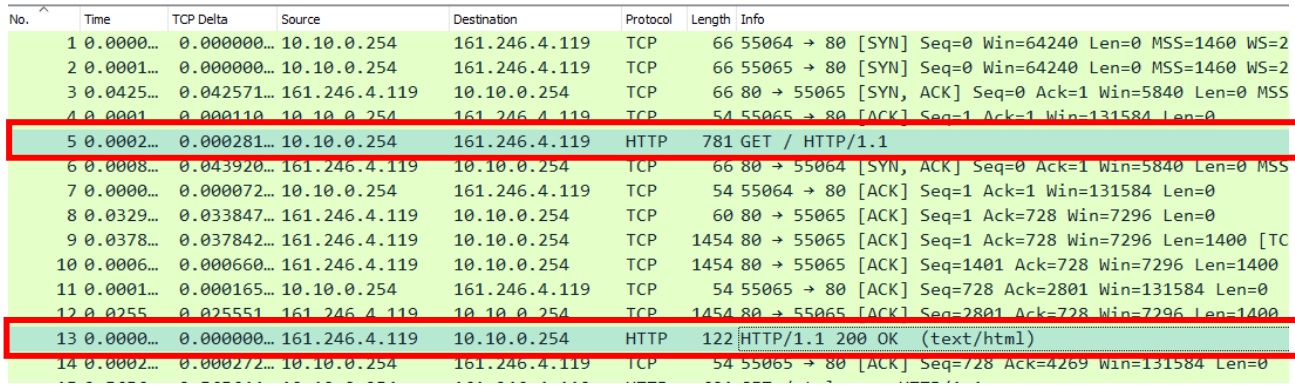
A : เป็น packet ที่ 16 ใช้เวลา 2.665 วินาที เป็นการโหลด image ของเว็บไซต์ GET /images/header.jpg HTTP/1.1
ส่วนของเพื่อนนั้นได้ใกล้เคียงกัน ของเพื่อนเป็น packet ที่ 27 , 22 , 35 เป็นการ request พวก static ไฟล์ เช่น css , ico และพวก jpg



No.	Time	TCP Delta	Source	Destination	Protocol	Length	Info
16	0.002084	2.665186000	10.10.0.254	161.246.4.119	HTTP	720	GET /images/header.jpg HTTP/1.1
15	2.565644	2.565644000	10.10.0.254	161.246.4.119	HTTP	691	GET /style.css HTTP/1.1
463	0.181276	0.212013000	10.10.0.254	161.246.4.119	HTTP	739	GET /slideshow2.css HTTP/1.1
300	0.005827	0.173706000	161.246.4.119	10.10.0.254	TCP	1454	80 → 55070 [ACK] Seq=21033 Ack=1976 Win=9792 Len=1
422	0.004773	0.157833000	161.246.4.119	10.10.0.254	TCP	1454	80 → 55065 [ACK] Seq=57665 Ack=6027 Win=18944 Len=
427	0.004219	0.148332000	161.246.4.119	10.10.0.254	TCP	1454	80 → 55064 [ACK] Seq=74894 Ack=4718 Win=15328 Len=

Q : นักศึกษาคิดว่า Packet ที่เป็นการเรียกหน้า Homepage (/) ของหน้าเว็บอยู่ที่ Packet ใด
และ Response Code ของ Packet ข้างต้นอยู่ที่ Packet ใด

A : Packet ที่เป็นการเรียกหน้า Homepage (/) อยู่ packet ที่ **5** [GET / HTTP/1.1]
Response Code ของ Packet ข้างต้นอยู่ที่ Packet ที่ **13** [HTTP/1.1 200 OK (text/html)]



No.	Time	TCP Delta	Source	Destination	Protocol	Length	Info
1	0.0000…	0.000000…	10.10.0.254	161.246.4.119	TCP	66	55064 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2
2	0.0001…	0.000000…	10.10.0.254	161.246.4.119	TCP	66	55065 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2
3	0.0425…	0.042571…	161.246.4.119	10.10.0.254	TCP	66	80 → 55065 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
4	0.0001…	0.000110…	10.10.0.254	161.246.4.119	TCP	54	55065 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
5	0.0002…	0.000281…	10.10.0.254	161.246.4.119	HTTP	781	GET / HTTP/1.1
6	0.0008…	0.043920…	161.246.4.119	10.10.0.254	TCP	66	80 → 55064 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
7	0.0000…	0.000072…	10.10.0.254	161.246.4.119	TCP	54	55064 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
8	0.0329…	0.033847…	161.246.4.119	10.10.0.254	TCP	60	80 → 55065 [ACK] Seq=1 Ack=728 Win=7296 Len=0
9	0.0378…	0.037842…	161.246.4.119	10.10.0.254	TCP	1454	80 → 55065 [ACK] Seq=1 Ack=728 Win=7296 Len=1400 [TC
10	0.0006…	0.000660…	161.246.4.119	10.10.0.254	TCP	1454	80 → 55065 [ACK] Seq=1401 Ack=728 Win=7296 Len=1400
11	0.0001…	0.000165…	10.10.0.254	161.246.4.119	TCP	54	55065 → 80 [ACK] Seq=728 Ack=2801 Win=131584 Len=0
12	0.0255…	0.025551…	161.246.4.119	10.10.0.254	TCP	1454	80 → 55065 [ACK] Seq=2801 Ack=728 Win=7296 Len=1400
13	0.0000…	0.000000…	161.246.4.119	10.10.0.254	HTTP	122	HTTP/1.1 200 OK (text/html)
14	0.0002…	0.000272…	10.10.0.254	161.246.4.119	TCP	54	55065 → 80 [ACK] Seq=728 Ack=4269 Win=131584 Len=0