นกสร ชาลพุมมศ 63010492



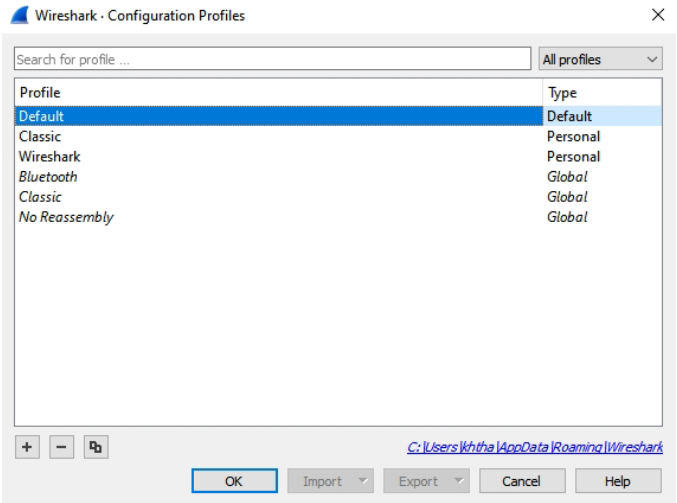
## กิจกรรมที่ 2 : การ Capture ข้อมูลจากระบบเครือข่าย

ในกิจกรรมที่ผ่านมา นักศึกษาได้เรียนรู้การติดตั้งโปรแกรม และ การจัดการกับคอลัมน์ ในกิจกรรมนี้ จะทำความรู้จักกับ Configuration Profiles, การ Capture ข้อมูล และ TCP Delta

### Configuration Profile

Configuration Profile คือ รูปแบบการกำหนดค่าการใช้งาน เนื่องจากโปรแกรม Wireshark สามารถนำไปใช้งานได้หลายรูปแบบ ดังนั้นการนำไปใช้งานในแต่ละเรื่องก็อาจจะมีการตั้งค่าไม่เหมือนกัน เช่น การเพิ่มคอลัมน์จากครั้งที่ผ่านมา ถือเป็นการเปลี่ยนแปลงโปรแกรม (Configuration) อย่างหนึ่ง การเพิ่มคอลัมน์ Host เข้าไป ทำให้รูปแบบของโปรแกรมเปลี่ยนแปลง หากเปิดไฟล์อื่นที่ไม่จำเป็นจะต้องดูคอลัมน์ Host ก็ต้องลบคอลัมน์นี้ออกไป ทำให้ผู้ใช้งานต้องลำบากในการคอยปรับรูปแบบการแสดงผล (และการกำหนดอื่นๆ)

โปรแกรม Wireshark จึงได้สร้าง Configuration Profile มาให้ โดยหากต้องการเปลี่ยนแปลงรูปแบบการใช้งานก็เพียงแต่เปลี่ยน Profile ใหม่เท่านั้น รูปแบบการใช้งานก็จะเปลี่ยนไปตามที่ต้องการทันที




ในหน้าโปรแกรม Wireshark ให้เลือก Edit –> Configuration Profiles... จะปรากฏหน้าต่างดังรูปด้านบน ซึ่งจะมี 2 Profiles ที่เป็นของ Wireshark แต่เดิม คือ Classic กับ Default โดย Default จะเป็น Config. ดั้งเดิม ดังนั้นเราไม่ควรใช้ Default Profiles เพราะหากเราปรับเปลี่ยนโปรแกรม เราจะจำไม่ได้ว่า Profile แรกเริ่มเป็นแบบไหนกันแน่ ดังนั้นควรใช้การสร้าง Profile ใหม่ ซึ่งทำได้ 2 วิธี คือ กด + จากรูปด้านบน หรือ คลิกขวาตรงมุมขวาล่างของหน้าต่างตรงคำว่า Profile แล้วเลือก New...

วิธีปฏิบัติที่เหมาะสม คือ ใช้ 1 Profile ต่องาน 1 แบบ เพื่อที่เมื่อเจองานลักษณะเดิม จะได้นำ Profile ที่เคยสร้างไว้มาใช้ได้ทันที ไม่ต้องมาปรับแต่ง Wireshark ใหม่

โดยสิ่งที่จะเก็บใน Profile ประกอบด้วย

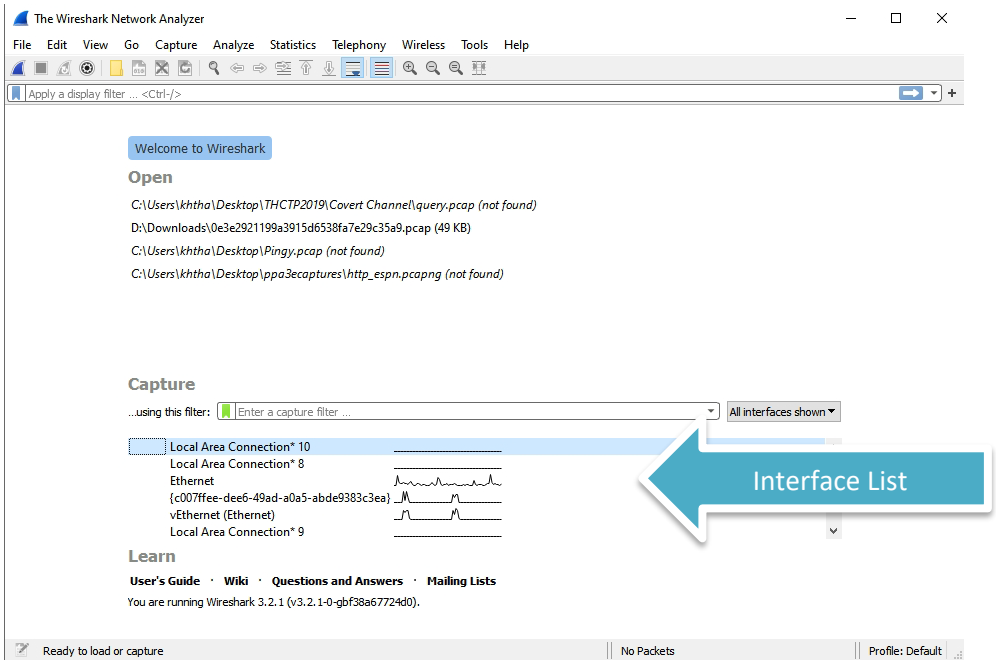
- Preference
- Capture Filters
- Display Filters
- Coloring Rules
- Disable Protocols
- ข้อมูลการแสดงผล เช่น คอลัมน์ หรือ ความกว้างของคอลัมน์

การสร้าง Profile ใหม่นี้ จะเป็นการ copy มาจาก Default Profile
ให้ทดลองดังนี้

1. Edit -> Configuration Profiles...
2. กด New (+) แล้วตั้งชื่อว่า Test_Wireshark
3. ทดลองเปิดไฟล์ http-google101.pcapng เพิ่มคอลัมน์ Host เหมือนครั้งที่ผ่านมา
4. เปลี่ยน Profile เป็น Default คอลัมน์แสดงอย่างไร คอลัมน์มีเพิ่มขึ้น จากข้อ 3
5. ให้เปลี่ยน Profile เป็น Test_Wireshark แล้วปิดไฟล์

## การดักจับข้อมูล

ในการดักจับข้อมูล สามารถดักจับได้หลาย Interface ตาม Interface ที่มีในแต่ละเครื่อง โดย Interface ที่มีข้อมูลจะแสดงเป็นรูปกราฟท้าย Interface นั้น




ให้ทดลองดังนี้

6. เอาเมาส์ไปคลิกที่ Interface ที่มีข้อมูล และ คลิกปุ่ม Start Capture ที่อยู่ใน Toolbar
7. ให้เปิด Browser ใดๆ ก็ได้ แล้วป้อน URL www.ce.kmitl.ac.th (ถ้าเข้าไม่ได้ให้ใช้ Link อื่นได้)
8. เมื่อแสดงผลครบหน้าแล้วสั่งให้หยุด Capture
9. ได้ข้อมูลกี่ Packet 5747

ในการ Capture ในลักษณะข้างต้น จะเห็นว่าจะได้ข้อมูลจำนวนมาก โดยมีข้อมูลที่เราไม่สนใจติดเข้ามาด้วยจำนวนมาก (เรียกว่า Background Data) หากเราต้องการจะสั่งให้ Wireshark ดักจับข้อมูลเฉพาะที่เราสนใจ เราจะต้องใช้เครื่องมือที่เรียกว่า Capture Filter โดย Capture Filter คือ ตัวกรองที่จะใช้ในขณะที่ทำการ Capture โดยสามารถกรองได้ดังนี้

กรองด้วยชื่อ (Host name) กรอบด้วย Network Address (โดยทั่วไปคือ IP Address) และ Port Number ให้ทดลองดังนี้

10. ทำตามขั้นตอนในข้อ 6-8 อีกครั้ง แต่ในช่อง ...using this filter: ให้ป้อน **host www.ce.kmitl.ac.th** 21
11. ทำตามขั้นตอนในข้อ 6-8 อีกครั้ง แต่ในช่อง ...using this filter: ให้ป้อน **host 161.246.4.119** 21
12. ขั้นตอนในข้อ ~~7~~ 10 และ ~~8~~ 11 ให้ผลต่างกันอย่างไร

10) ใช้ URL ในการกรอง filter } ทั้งสองมีจำนวน packet เท่ากัน
11) ใช้ IP Address ในการกรอง filter

13. ใน Packet Details Pane หัวข้อ Internet Protocol Version 4 ให้หาส่วนที่เขียนว่า Source และ Destination ให้นักศึกษาลองเดาความหมายว่าหมายถึงอะไร

Source : IP ของต้นทาง (ผู้ส่ง)
Destination : IP ของปลายทาง (ผู้รับ)

14. ทำตามขั้นตอนในข้อ 6-8 อีกครั้ง แต่ในช่อง ...using this filter: ให้ป้อน src host **161.246.4.119**
15. ทำตามขั้นตอนในข้อ 6-8 อีกครั้ง แต่ในช่อง ...using this filter: ให้ป้อน dst host **161.246.4.119**
16. จากข้อ 14 และข้อ 15 การทำงานแตกต่างกันอย่างไร เพราะอะไร

14) จะแสดงผลเฉพาะ packet ที่มี source (ต้นทาง) เป็น 161.246.4.119
15) จะแสดงผลเฉพาะ packet ที่มี destination (ปลายทาง) เป็น 161.246.4.119

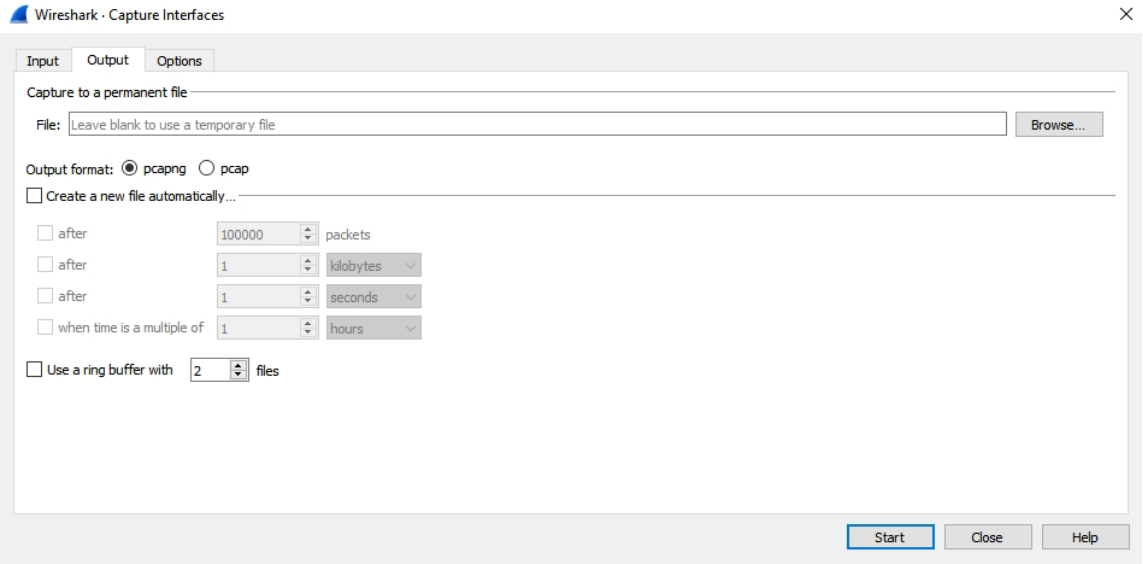
17. ถ้าป้อน **not host 161.246.4.119** คิดว่าจะหมายถึงอะไร

คัดกรองข้อมูลโดยไม่แสดงผล packet ที่มี 161.246.4.119

18. ให้นักศึกษาสรุปการใช้งานการใช้ Capture Filter เบื้องต้น

ใช้ในการเลือก Capture หรือ เลือกแสดงผลตาม filters ต่างๆ ตามที่ต้องการ หรือไม่ต้องการได้ เช่น protocol, ip เป็นต้น

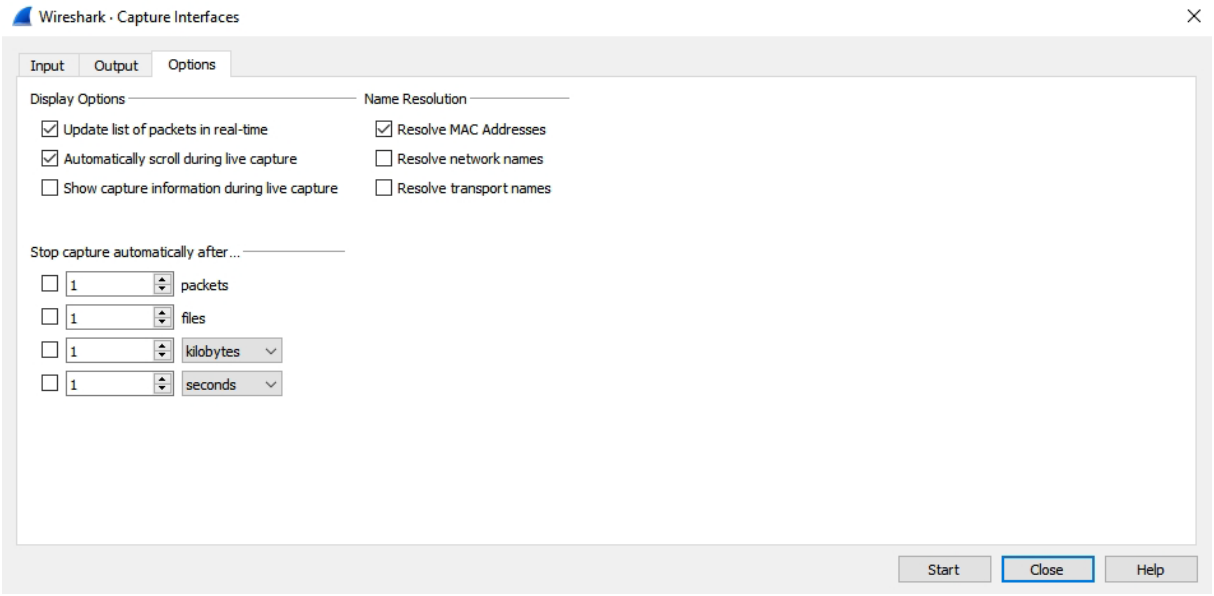
ใน Wireshark สามารถกำหนดเงื่อนไขของการดักจับข้อมูลได้ หากเลือก Capture Option จาก Toolbar




ใน Tab Output เราสามารถกำหนดให้ save ข้อมูลที่ capture เป็นไฟล์ได้ โดยอัตโนมัติ โดยไม่ต้องคอย save เอง นอกจากนั้นยังสามารถกำหนดเงื่อนไขได้

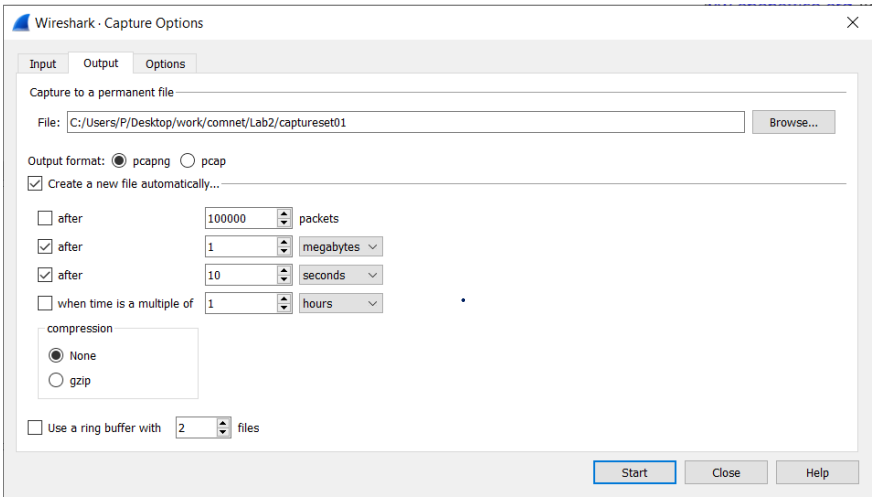
- สร้างไฟล์ใหม่ทุก จำนวน packet ที่กำหนด
- สร้างไฟล์ใหม่ เมื่อไฟล์มีขนาดถึงขนาดที่กำหนด ซึ่งจะทำให้ 1 ไฟล์ไม่ใหญ่มากเกินไป
- สร้างไฟล์ใหม่ ทุกช่วงเวลาที่ระบุ

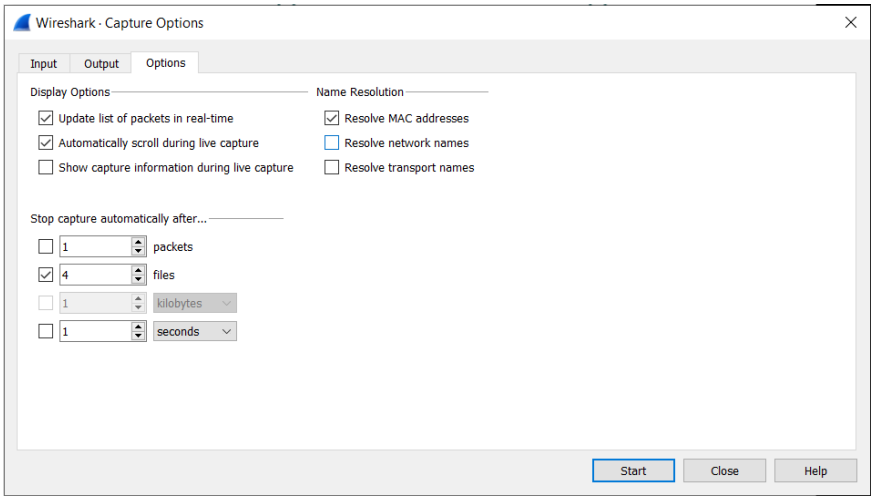
สามารถกำหนดให้ทำงานแบบ Ring Buffer คือ ย้อนกลับไปใช้ไฟล์เดิม เพื่อป้องกันไม่ให้ใช้พื้นที่ในฮาร์ดดิสก์มากเกินไปได้อีกด้วย

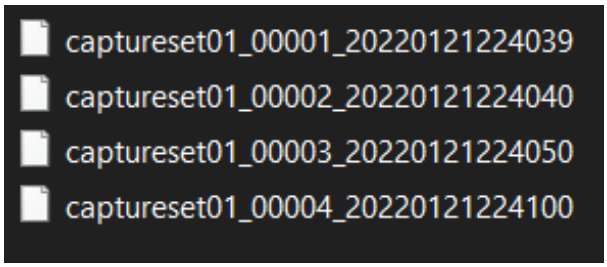



ใน Tab Options ยังสามารถกำหนดการหยุด Capture ได้ด้วย โดยสามารถกำหนดได้ว่าให้หยุดเมื่อ Capture ครบกี่ Packet หรือ ครบกี่ไฟล์ หรือ ครบขนาดที่ต้องการ หรือ ครบเวลาที่ต้องการ

19. ให้สร้างไฟล์ชื่อ captureset01.pcapng โดยกำหนดเงื่อนไขให้ขึ้นไฟล์ใหม่ทุก 1 MB และทุก 10 วินาที และหยุดหลังจาก 4 ไฟล์ หลังจากกด start ให้ไปที่ไซต์ http://www.openoffice.org และกดดูไปเรื่อยๆ ไม่น้อยกว่า 40 วินาที ให้ Capture ภาพหน้าของการตั้งค่า และภาพไฟล์ Output ลงในที่ว่างด้านล่างนี้




20. ให้ไปที่ File -> File Set -> List Files มีอะไรเกิดขึ้น อธิบาย

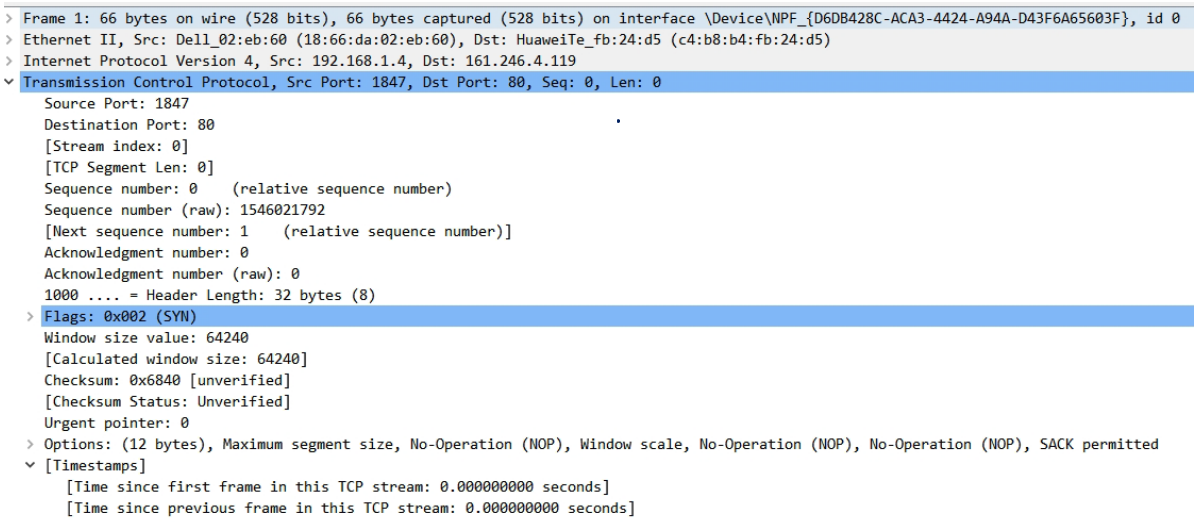
แสดง List File ที่ทำการ capture จากข้อ 19 ซึ่งมีทั้งหมด 4 ไฟล์ ตามการตั้งค่าที่กำหนดไว้

**ข้อมูลเวลา**

ปัญหาเกี่ยวกับเวลาเป็นปัญหาสำคัญในระบบเครือข่าย เช่น ความล่าช้าในการทำงาน โดยความล่าช้าหรือเวลาที่เสียไปในการทำงานในการทำงานของระบบเครือข่ายจะเรียกว่า Latency ซึ่งโดยทั่วไปจะวัดตั้งแต่เวลาที่ Host ส่ง Request ออกไป จนถึงเวลาที่ Reply กลับมา โดยทั่วไป

การพิจารณาเกี่ยวกับเวลาใน Wireshark จะดูที่คอลัมน์ Time เป็นหลัก ปกติคอลัมน์ Time จะแสดงข้อมูล Seconds Since Beginning of Capture โดยเริ่มจาก 0.000000000 ซึ่งจะใช้พิจารณา แต่เพื่อให้เห็นค่าระหว่าง Packet (เรียกว่า delta time) ให้เปลี่ยนการแสดงผลในช่อง Time เป็น **View | Time Display Format | Seconds Since Previous Displayed Packet**

21. ให้สร้างและใช้ Profile ใหม่ เพื่อไม่กระทบกับ Default Profile
22. ให้ capture ข้อมูลระหว่างเครื่องนักศึกษากับ **www.ce.kmitl.ac.th** เท่านั้น
23. ตั้งการแสดงผล Time เป็น Seconds Since Previous Displayed Packet
24. ให้หาค่าเวลาที่มากที่สุดในช่อง Time เป็น packet ที่เท่าไร 23 และให้ถามเพื่อนอีก 2 คน พบที่เดียวกันหรือไม่ ของเพื่อน packet ที่เท่าไร พบคนละที่กับเพื่อน
เพื่อนพบที่ packet 29 และ 22
25. ใน Packet Details Pane หัวข้อ Transmission Control Protocol (จะเรียนในบทที่ 3) คลิกขวาที่ Time since previous frame in this TCP stream แล้วเลือก Apply as Column ให้ตั้งชื่อคอลัมน์ว่า TCP Delta และเลื่อนมาใกล้ๆ Time




26. ค่า TCP Delta นี้เป็นระยะเวลาของ Latency ที่คิดเฉพาะใน TCP Stream เดียวกัน เนื่องจากในการขอข้อมูล 1 หน้าเว็บ อาจมีการขอข้อมูลหลายครั้ง สำหรับแต่ละส่วนของเว็บ ซึ่งอาจขอไปพร้อมๆ กันก็ได้ (หลาย Stream) ดังนั้นค่าเวลาในช่อง Time ที่เป็น Seconds Since Previous Displayed Packet จึงอาจไม่สะท้อน ความล่าช้าที่เกิดขึ้นจริง ค่า TCP Delta นี้ จึงสามารถตรวจสอบความล่าช้าได้ชัดเจนกว่า

27. ให้หาค่าเวลาที่มากที่สุดในช่อง TCP Delta เป็น packet ที่เท่าไร 25 และให้ถามเพื่อนอีก 2 คน พบที่เดียวกันหรือไม่ ของเพื่อน packet ที่เท่าไร พบคนละที่ ของเพื่อน packet ที่ 29, 22 เป็นการทำงานอะไร protocol TCP ส่งข้อมูลจากเว็บ → เครื่องเรา

Capture ภาพของ packet list pane ลงในที่ว่างด้านล่าง

| No. | Time | TCP Delta | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | 0.000000000 | 192.168.10.109 | 161.246.4.119 | TCP | 66 | 53743 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 2 | 0.000961 | 0.000000000 | 192.168.10.109 | 161.246.4.119 | TCP | 66 | 53744 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 3 | 0.009684 | 0.010645000 | 161.246.4.119 | 192.168.10.109 | TCP | 66 | 80 → 53743 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 SACK_PERM=1 WS=32 |
| 4 | 0.000060 | 0.000060000 | 192.168.10.109 | 161.246.4.119 | TCP | 54 | 53743 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0 |
| 5 | 0.000166 | 0.009910000 | 161.246.4.119 | 192.168.10.109 | TCP | 66 | 80 → 53744 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 SACK_PERM=1 WS=32 |
| 6 | 0.000012 | 0.000178000 | 192.168.10.109 | 161.246.4.119 | HTTP | 820 | GET / HTTP/1.1 |
| 7 | 0.000003 | 0.000015000 | 192.168.10.109 | 161.246.4.119 | TCP | 54 | 53744 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0 |
| 8 | 0.012350 | 0.012353000 | 161.246.4.119 | 192.168.10.109 | TCP | 54 | 80 → 53743 [ACK] Seq=1 Ack=767 Win=7392 Len=0 |
| 9 | 0.039320 | 0.039320000 | 161.246.4.119 | 192.168.10.109 | TCP | 1506 | 80 → 53743 [ACK] Seq=1 Ack=767 Win=7392 Len=1452 [TCP segment of a reassembled PDU] |
| 10 | 0.000225 | 0.000225000 | 161.246.4.119 | 192.168.10.109 | TCP | 1506 | 80 → 53743 [ACK] Seq=1453 Ack=767 Win=7392 Len=1452 [TCP segment of a reassembled PDU] |
| 11 | 0.000021 | 0.000021000 | 192.168.10.109 | 161.246.4.119 | TCP | 54 | 53743 → 80 [ACK] Seq=767 Ack=2905 Win=132096 Len=0 |
| 12 | 0.009847 | 0.009847000 | 161.246.4.119 | 192.168.10.109 | TCP | 1506 | 80 → 53743 [ACK] Seq=2905 Ack=767 Win=7392 Len=1452 [TCP segment of a reassembled PDU] |
| 13 | 0.000000 | 0.000000000 | 161.246.4.119 | 192.168.10.109 | HTTP | 83 | HTTP/1.1 200 OK (text/html) |
| 14 | 0.000060 | 0.000060000 | 192.168.10.109 | 161.246.4.119 | TCP | 54 | 53743 → 80 [ACK] Seq=767 Ack=4386 Win=132096 Len=0 |
| 15 | 0.390475 | 0.390475000 | 192.168.10.109 | 161.246.4.119 | HTTP | 840 | GET /slideshow2.css HTTP/1.1 |
| 16 | 0.005085 | 0.457383000 | 192.168.10.109 | 161.246.4.119 | HTTP | 872 | GET /favicon.ico HTTP/1.1 |
| 17 | 0.013254 | 0.018339000 | 161.246.4.119 | 192.168.10.109 | TCP | 54 | 80 → 53743 [ACK] Seq=4386 Ack=1553 Win=8960 Len=0 |
| 18 | 0.000000 | 0.000000000 | 161.246.4.119 | 192.168.10.109 | HTTP | 625 | HTTP/1.1 404 Not Found (text/html) |
| 19 | 0.024195 | 0.037449000 | 161.246.4.119 | 192.168.10.109 | TCP | 54 | 80 → 53744 [ACK] Seq=1 Ack=819 Win=7488 Len=0 |
| 20 | 0.000000 | 0.000000000 | 161.246.4.119 | 192.168.10.109 | HTTP | 624 | HTTP/1.1 404 Not Found (text/html) |
| 21 | 0.029670 | 0.053865000 | 192.168.10.109 | 161.246.4.119 | TCP | 54 | 53743 → 80 [ACK] Seq=1553 Ack=4957 Win=131328 Len=0 |
| 22 | 0.015034 | 0.044704000 | 192.168.10.109 | 161.246.4.119 | TCP | 54 | 53744 → 80 [ACK] Seq=819 Ack=571 Win=131328 Len=0 |
| 23 | 14.919937 | 14.934971000 | 161.246.4.119 | 192.168.10.109 | TCP | 54 | 80 → 53743 [FIN, ACK] Seq=4957 Ack=1553 Win=8960 Len=0 |
| 24 | 0.000072 | 0.000072000 | 192.168.10.109 | 161.246.4.119 | TCP | 54 | 53743 → 80 [ACK] Seq=1553 Ack=4958 Win=131328 Len=0 |
| 25 | 0.027906 | 14.947915000 | 161.246.4.119 | 192.168.10.109 | TCP | 54 | 80 → 53744 [FIN, ACK] Seq=571 Ack=819 Win=7488 Len=0 |
| 26 | 0.000074 | 0.000074000 | 192.168.10.109 | 161.246.4.119 | TCP | 54 | 53744 → 80 [ACK] Seq=819 Ack=572 Win=131328 Len=0 |
| 27 | 0.677899 | 0.705879000 | 192.168.10.109 | 161.246.4.119 | TCP | 54 | 53743 → 80 [FIN, ACK] Seq=1553 Ack=4958 Win=131328 Len=0 |
| 28 | 0.000085 | 0.677984000 | 192.168.10.109 | 161.246.4.119 | TCP | 54 | 53744 → 80 [FIN, ACK] Seq=819 Ack=572 Win=131328 Len=0 |
| 29 | 0.013122 | 0.013207000 | 161.246.4.119 | 192.168.10.109 | TCP | 54 | 80 → 53743 [ACK] Seq=4958 Ack=1554 Win=8960 Len=0 |
| 30 | 0.000000 | 0.013122000 | 161.246.4.119 | 192.168.10.109 | TCP | 54 | 80 → 53744 [ACK] Seq=572 Ack=820 Win=7488 Len=0 |

28. ให้นักศึกษาตอบคำถามต่อไปนี้

นักศึกษาคิดว่า Packet ที่เป็นการเรียกหน้า Homepage (/) ของหน้าเว็บอยู่ที่ Packet ใด 6

และ Response Code ของ Packet ข้างต้นอยู่ที่ Packet ใด 13

**งานครั้งที่ 2**

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งโดยเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา และ _Lab2 เช่น 63010789_Lab2.pdf
- กำหนดส่ง ภายในวันที่ 26 มกราคม 2564