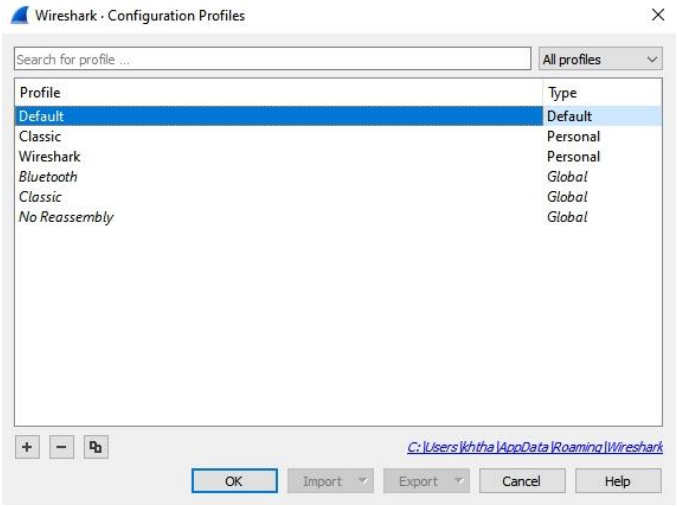
กิจกรรมที่ 2 : การ Capture ข้อมูลจากระบบเครือข่าย

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

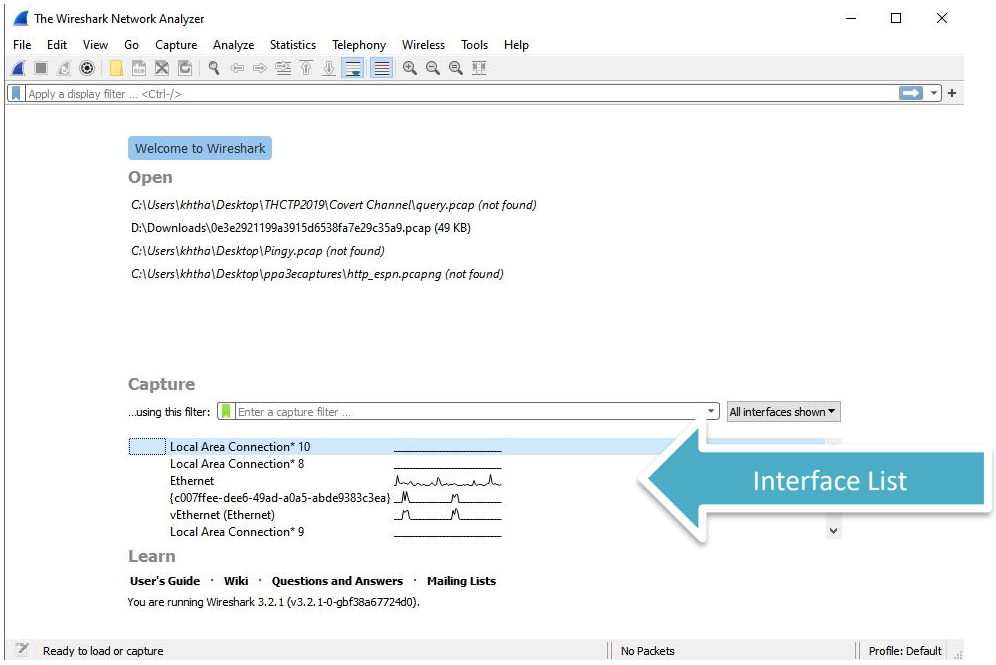
- Preference
- Capture Filters
- Display Filters
- Coloring Rules
- Disable Protocols
- ข้อมูลการแสดงผล เช่น คอลัมน์ หรือ ความกว้างของคอลัมน์

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 ม่ column text item + Host เพิ่ม.
5. ให้เปลี่ยน Profile เป็น Test_Wireshark แล้วปิดไฟล์

การดักจับข้อมูล

ในการดักจับข้อมูล สามารถดักจับได้หลาย Interface ตาม Interface ที่มีในแต่ละเครื่อง โดย Interface ที่มีข้อมูลจะแสดงเป็นรูปกราฟท้าย Interface นั้น



ให้ทดลองดังนี้

1. เอาเมาส์ไปคลิกที่ Interface ที่มีข้อมูล และ คลิกปุ่ม Start Capture ที่อยู่ใน Toolbar
2. ให้เปิด Browser ใดๆ ก็ได้ แล้วป้อน URL www.ce.kmitl.ac.th (ถ้าเข้าไม่ได้ให้ใช้ Link อื่นได้)
3. แล้วสั่งให้หยุด Capture
4. ได้ข้อมูลกี่ Packet 4255 packets

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

5. ทำตามขั้นตอนในข้อ 1-3 อีกครั้ง แต่ในช่อง ...using this filter: ให้ป้อน **host www.ce.kmitl.ac.th**
6. ทำตามขั้นตอนในข้อ 1-3 อีกครั้ง แต่ในช่อง ...using this filter: ให้ป้อน **host 161.246.4.119**
7. ขั้นตอนในข้อ 5 และ 6 ต่างกันอย่างไร

   หาก capture พร้อมกัน packet ของทั้ง 2 จะมีขนาดเท่ากัน.
   หาก capture ที่ละครั้ง packet ของทั้ง 2 จะมีขนาดต่างกัน
8. ใน Packet Details Pane หัวข้อ Internet Protocol Version 4 ให้หาส่วนที่เขียนว่า Source และ Destination ให้นักศึกษาลองเดาความหมายว่าหมายถึงอะไร

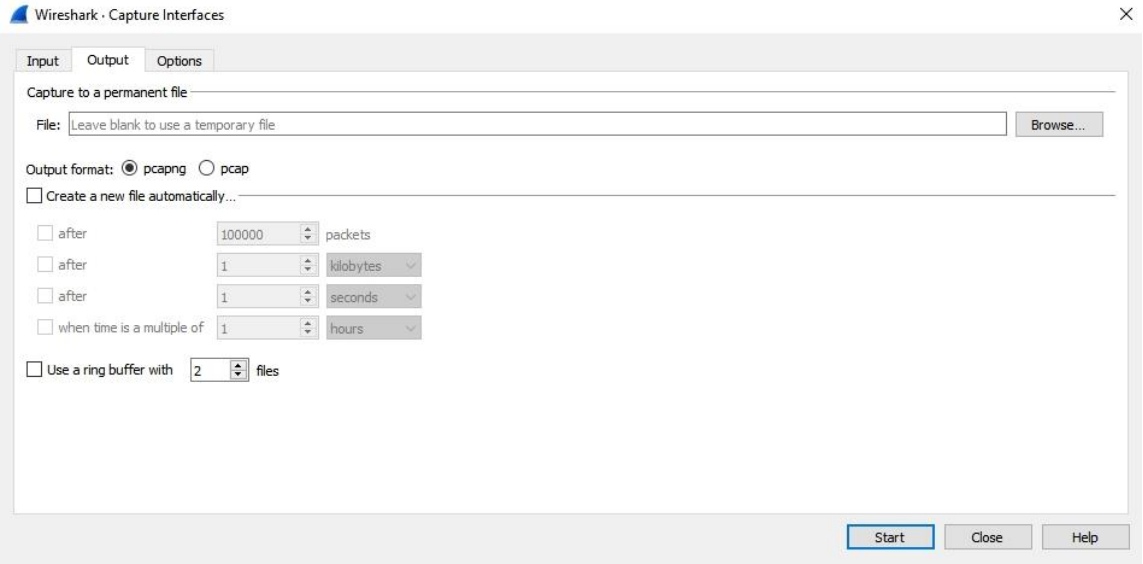
   Source หมายถึง IP ของผู้ใช้.
   Destination หมายถึง IP ของ www.kmitl.ac.th
9. ทำตามขั้นตอนในข้อ 1-3 Capture Filter แต่ในช่อง ...using this filter: ให้ป้อน src host **161.246.4.119**
10. ทำตามขั้นตอนในข้อ 1-3 Capture Filter แต่ในช่อง ...using this filter: ให้ป้อน dst host **161.246.4.119**
11. จากข้อ 9 และข้อ 10 การทำงานแตกต่างกันอย่างไร เพราะอะไร

    ต่างกัน ตรงที่ packets ของการร้องขอ time request ถึง www.kmitl.ac.th
    และ time sent ถึง PC ต่างกัน PC → kmitl.ac.th (rv) ← (sent.)
12. ถ้าป้อน **not host 161.246.4.119** คิดว่าจะหมายถึงอะไร

    ไม่ดักกรองข้อมูลของตัวเว็บ www.kmitl.ac.th หรือ 161.246.4.119
13. ให้นักศึกษาสรุปการใช้งานการใช้ Capture Filter เบื้องต้น

    Capture Filter เป็น Configuration ส่วนหนึ่งของโปรแกรมซึ่งทำหน้าที่ packet ของ host หนึ่งๆ เช่น ถ้าเราใส่ filter ของ KMITL website เราก็จะได้แต่ packet ของเว็บ kmitl เป็นต้น.

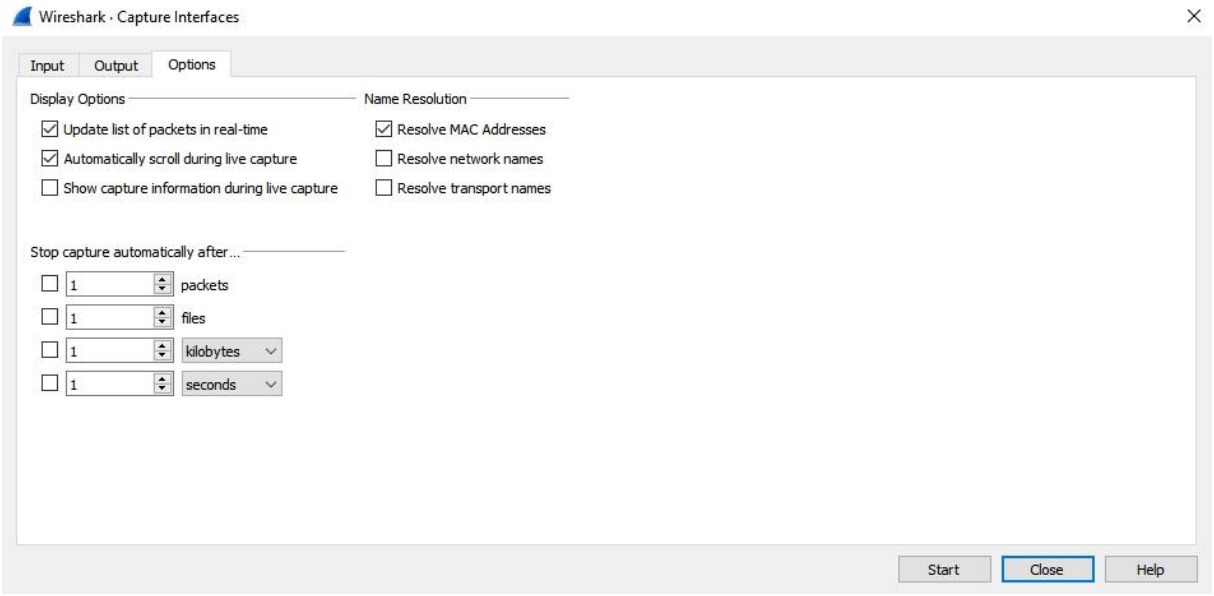
ใน Wireshark สามารถกำหนดเงื่อนไขของการดักจับข้อมูลได้ หากเลือก Capture Option จาก Toolbar



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

- สร้างไฟล์ใหม่ทุก จำนวน packet ที่กำหนด
- สร้างไฟล์ใหม่ เมื่อถึงขนาดที่กำหนด
- สร้างไฟล์ใหม่ ทุกช่วงเวลา

สามารถกำหนดให้ทำงานแบบ Ring Buffer คือ ย้อนกลับไปใช้ไฟล์เดิม เพื่อป้องกันไม่ให้ใช้พื้นที่ในฮาร์ดดิสก์มากเกินไป



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

14. 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 และไฟล์ Output
15. ให้ไปที่ File –> File Set –> List Files มีอะไรเกิดขึ้น อธิบาย

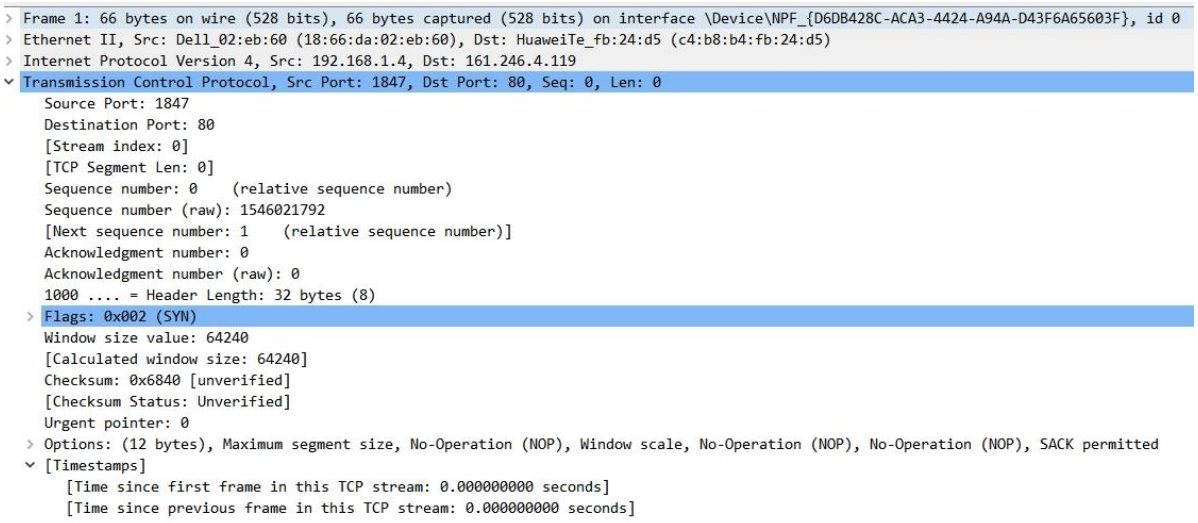
แสดง Filename , Created (สร้างไฟล์ตอนไหน) , Modified , Size (ขนาดของไฟล์)

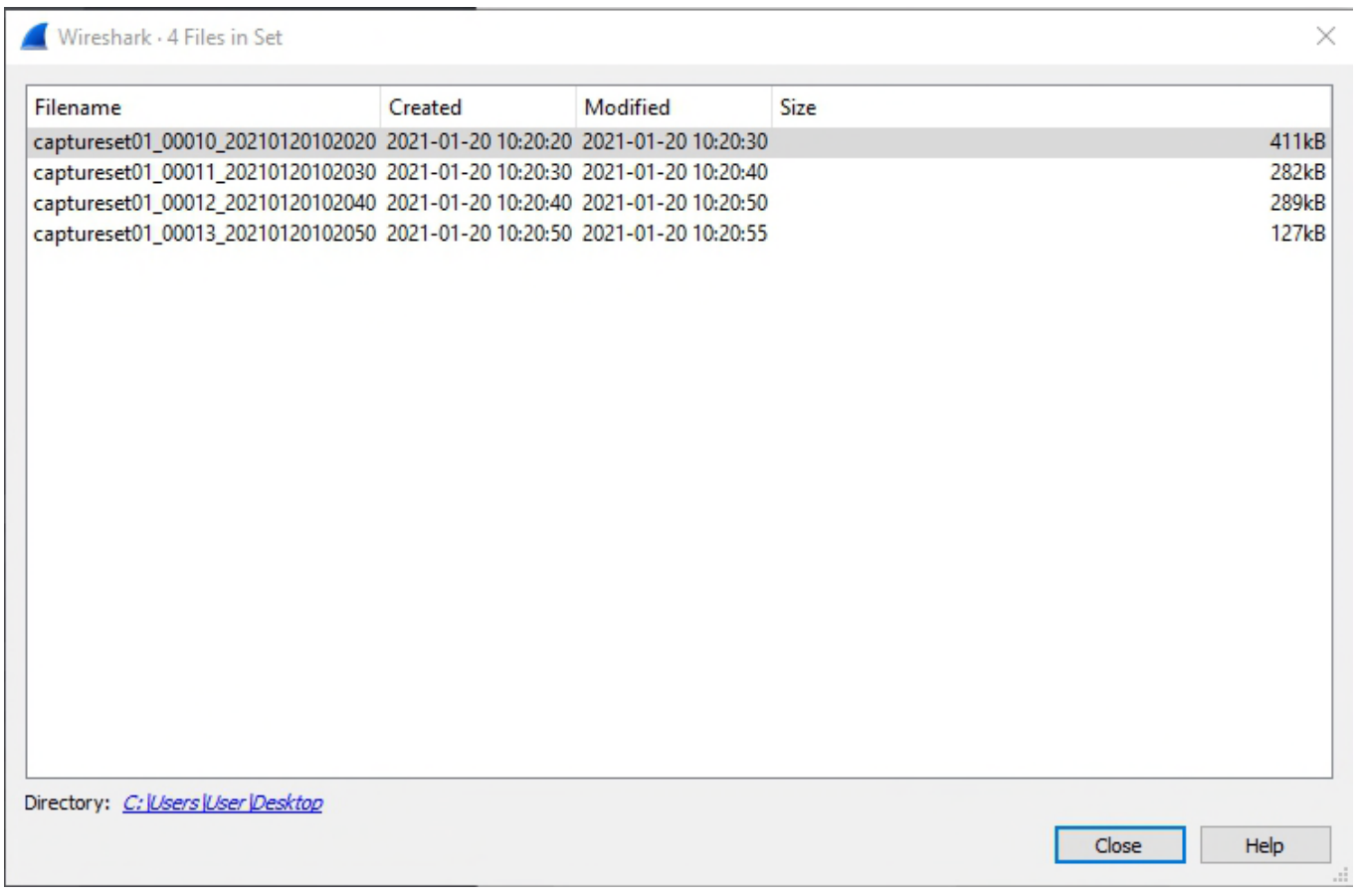
ข้อมูลเวลา

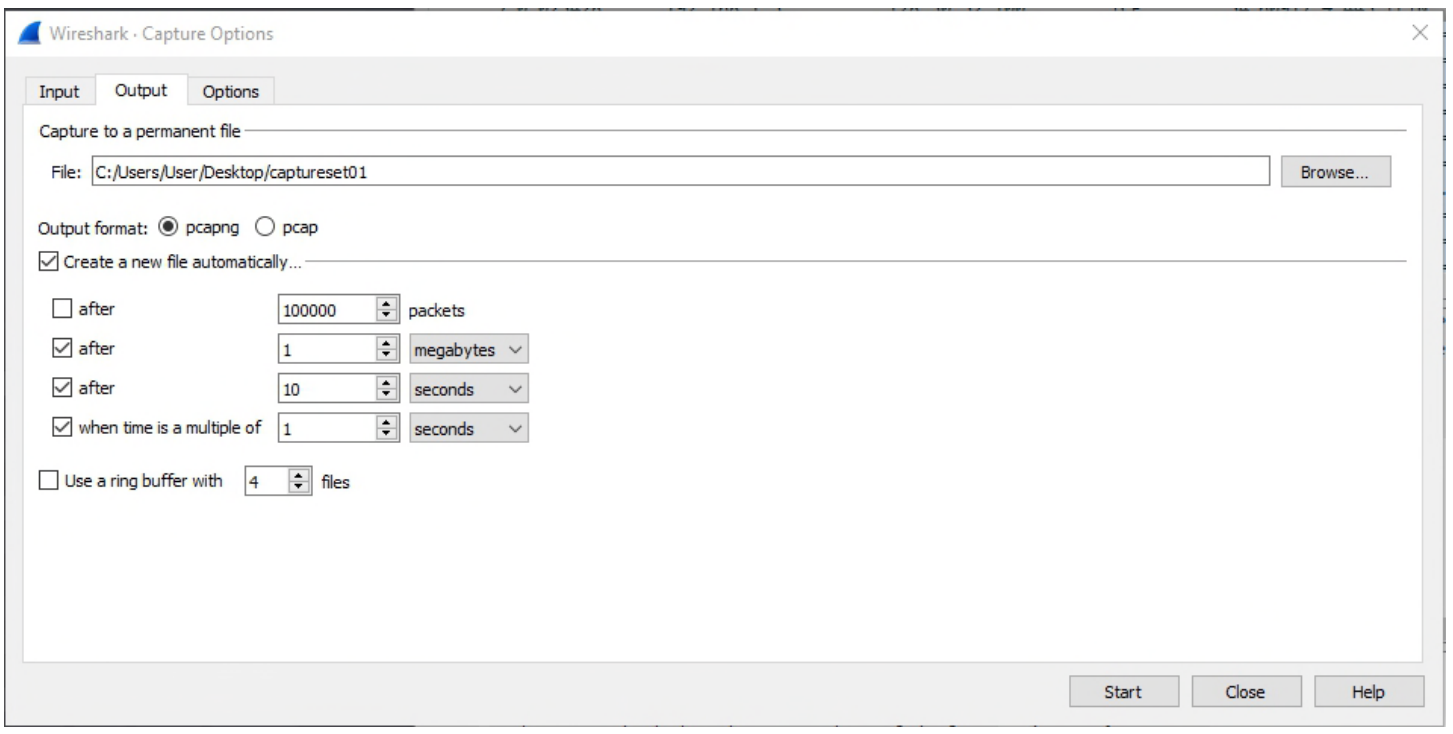
ปัญหาเกี่ยวกับเวลาเป็นปัญหาสำคัญในระบบเครือข่าย เช่น ความล่าช้าในการทำงาน โดยความล่าช้าหรือเวลาที่เสียไปในการทำงานในการทำงานของระบบเครือข่ายจะเรียกว่า Latency ซึ่งโดยทั่วไปจะวัดตั้งแต่เวลาที่ Host ส่ง Request ออกไป จนถึงเวลาที่ Reply กลับมา โดยทั่วไป

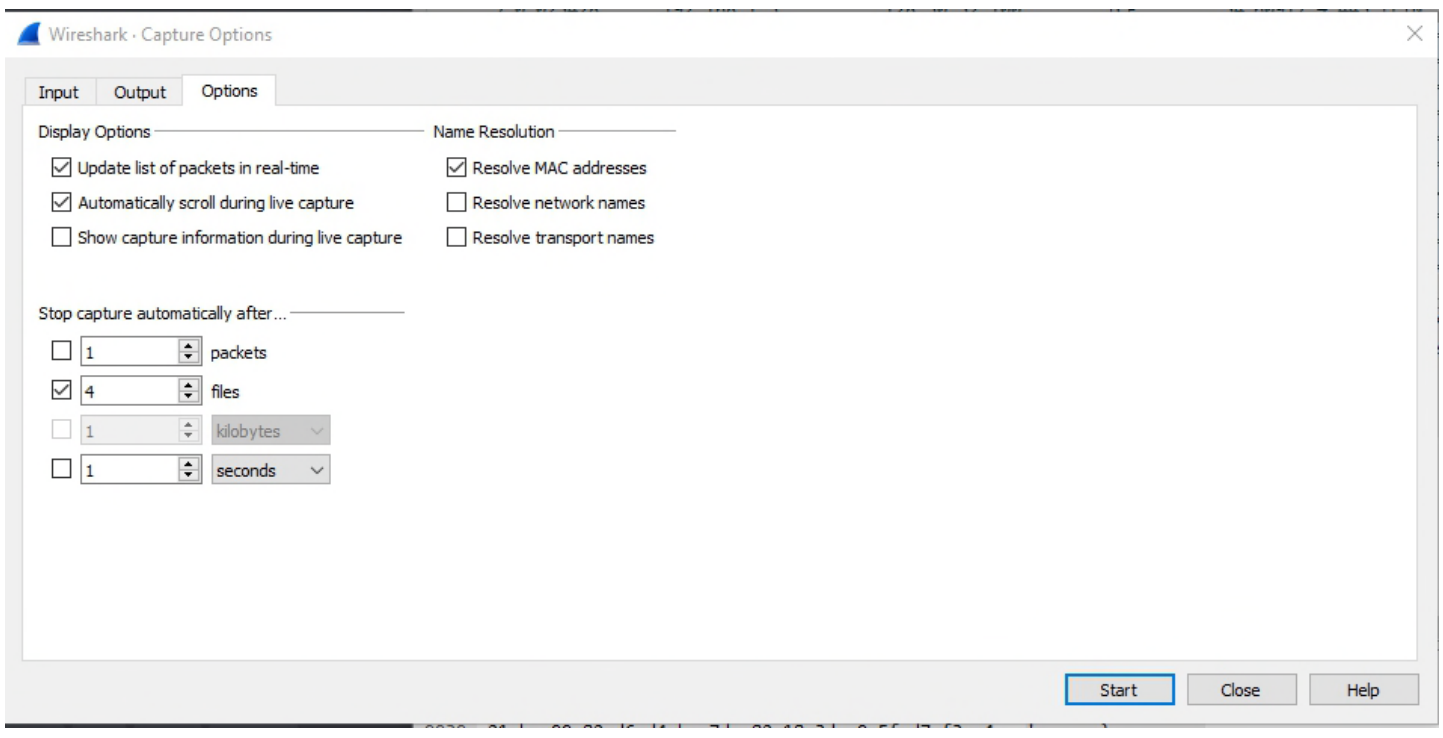
การพิจารณาเกี่ยวกับเวลาใน Wireshark จะดูที่คอลัมน์ Time เป็นหลัก ปกติคอลัมน์ Time จะแสดงข้อมูล Seconds Since Beginning of Capture โดยเริ่มจาก 0.000000000 ซึ่งจะใช้พิจารณา แต่เพื่อให้เห็นค่าระหว่าง Packet (เรียกว่า delta time) ให้เปลี่ยนการแสดงผลในช่อง Time เป็น **View I Time Display Format I Seconds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

1. ให้สร้างและใช้ Profile ใหม่ เพื่อไม่กระทบกับ Default Profile
2. ให้ capture ข้อมูลจากเครื่องนักศึกษาไปที่ **www.ce.kmitl.ac.th**
3. ตั้งการแสดงผล Time เป็น Seconds Since Previous Displayed Packet
4. ให้หาค่าเวลาที่มากที่สุดในช่อง Time เป็น packet ที่เท่าไร 19 และให้ถามเพื่อนอีก 3 คน พบที่เดียวกันหรือไม่ ของเพื่อน packet ที่เท่าไร 3, 17, 4
5. 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




Wireshark · 4 Files in Set
Filename
Created
Modified
Size
captureset01_00010_20210120102020 2021-01-20 10:20:20 2021-01-20 10:20:30 411kB
captureset01_00011_20210120102030 2021-01-20 10:20:30 2021-01-20 10:20:40 282kB
captureset01_00012_20210120102040 2021-01-20 10:20:40 2021-01-20 10:20:50 289kB
captureset01_00013_20210120102050 2021-01-20 10:20:50 2021-01-20 10:20:55 127kB
Directory: C:\Users\User\Desktop
Close
Help


Wireshark · Capture Options
Input
Output
Options
Capture to a permanent file
File: C:/Users/User/Desktop/captureset01
Browse...
Output format: pcapng pcap
Create a new file automatically...
after 100000 packets
after 1 megabytes
after 10 seconds
when time is a multiple of 1 seconds
Use a ring buffer with 4 files
Start
Close
Help


Wireshark · Capture Options
Input
Output
Options
Display Options
Update list of packets in real-time
Automatically scroll during live capture
Show capture information during live capture
Name Resolution
Resolve MAC addresses
Resolve network names
Resolve transport names
Stop capture automatically after...
1 packets
4 files
1 kilobytes
1 seconds
Start
Close
Help

6. ค่า TCP Delta นี้เป็นระยะเวลาของ Latency ที่คิดเฉพาะใน TCP Stream เดียวกัน เนื่องจากในการขอข้อมูล 1 หน้าเว็บ อาจมีการขอข้อมูลหลายครั้ง สำหรับแต่ละส่วนของเว็บ ซึ่งอาจขอไปพร้อมๆ กันก็ได้ ดังนั้นค่าเวลาในช่อง Time ที่เป็น Seconds Since Previous Displayed Packet จึงอาจไม่สะท้อน ความล่าช้าที่เกิดขึ้นจริง ค่า TCP Delta นี้ จึงสามารถตรวจสอบความล่าช้าได้ชัดเจนกว่า
7. ให้หาค่าเวลาที่มากที่สุดในช่อง TCP Delta เป็น packet ที่เท่าไร 19 และให้ถามเพื่อนอีก 3 คน พบที่เดียวกันหรือไม่ ของเพื่อน packet ที่เท่าไร 3,17,4
   เป็นการทำงานอะไร TCP
8. ให้นักศึกษาตอบคำถามต่อไปนี้
   นักศึกษาคิดว่า Packet ที่เป็นการเรียกหน้า Homepage (/) ของหน้าเว็บอยู่ที่ Packet ใด 5,15
   และ Response Code ของ Packet ข้างต้นอยู่ที่ Packet ใด 5

งานครั้งที่ 2

- การส่งงาน ให้ส่งเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา
- ส่วนบนของหน้าแรกให้มี รหัสนักศึกษา และ ชื่อนักศึกษา
- งานที่ส่งทำได้ 2 รูปแบบ คือ 1) เขียนเพิ่มเติมลงใน Sheet นี้ หรือ 2) ทำเป็นคำตอบแยกออกมา โดยให้มีหัวข้อเรื่อง และ ข้อด้วย เพื่อให้ทราบว่าเป็นคำตอบของส่วนไหน
- กำหนดส่ง ภายในวันที่ 24 มกราคม 2563