

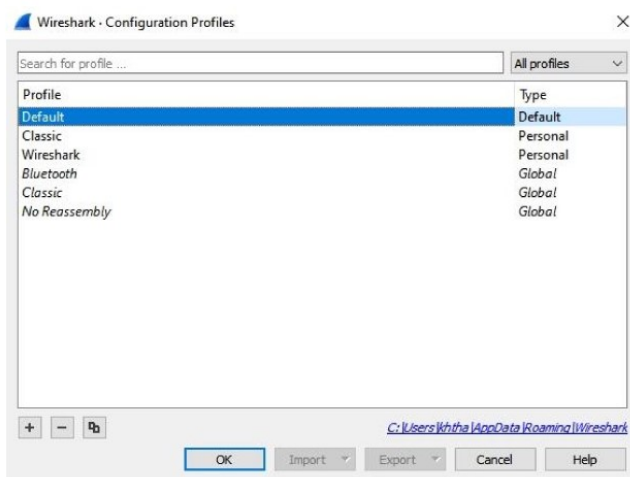
### กิจกรรมที่ 2 : การ Capture ข้อมูลจากระบบเครือข่าย

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

#### Configuration Profile

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

โปรแกรม Wireshark จึงได้สร้าง Configuration Profile มาให้ โดยหากต้องการเปลี่ยนแปลงรูปแบบการใช้งานก็เพียงแค่เปลี่ยน Profile ใหม่เท่านั้น รูปแบบการใช้งานก็จะเปลี่ยนไปตามที่ต้องการทันที



ในหน้าโปรแกรม Wireshark ให้เลือก Edit -> Configuration Profiles... จะปรากฏหน้าต่างดังรูปด้านบน ซึ่งจะ มี 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 คลิกขวาตรงมุมขวาล่างของหน้าต่าง ตรงคำว่า 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

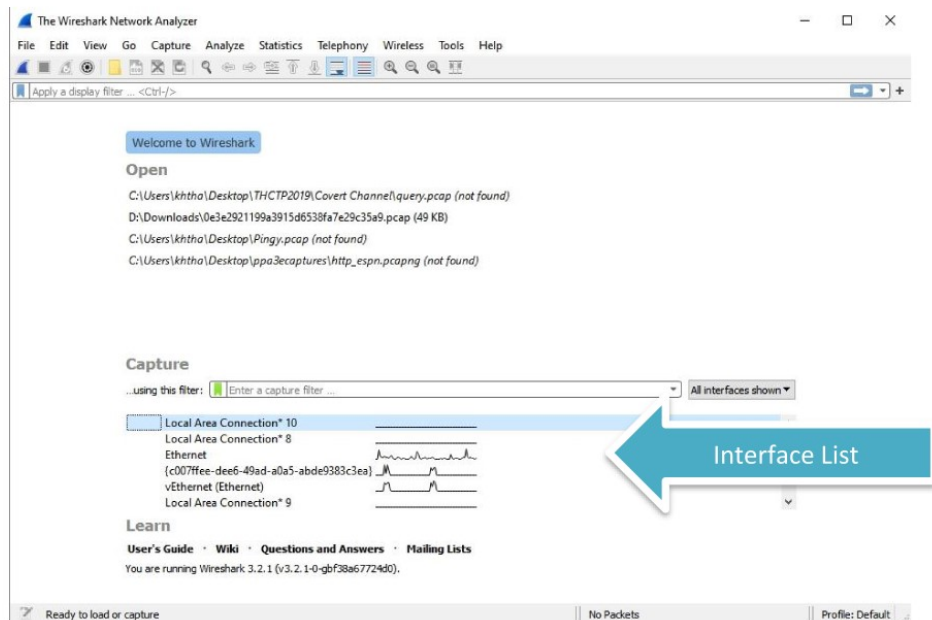
การสร้าง Profile ใหม่ จะเป็นการ copy มาจาก Default Profile

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 ไม่ใช่ Column Host
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](http://www.ce.kmitl.ac.th) (ถ้าเข้าไม่ได้ให้ใช้ Link อื่นได้)
3. แล้วสั่งให้หยุด Capture
4. ได้ข้อมูลที่ Packet 266

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

กรองด้วยชื่อ (Host name) กรองด้วย 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](http://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

เหมือนกัน

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

Source Address คือ IPv4 ต้นทาง , Destination Address คือ IPv4 ปลายทาง

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

Packet ที่ดักมาได้นั้น ไม่เหมือนกัน เพราะ Capture filter ไม่เหมือน

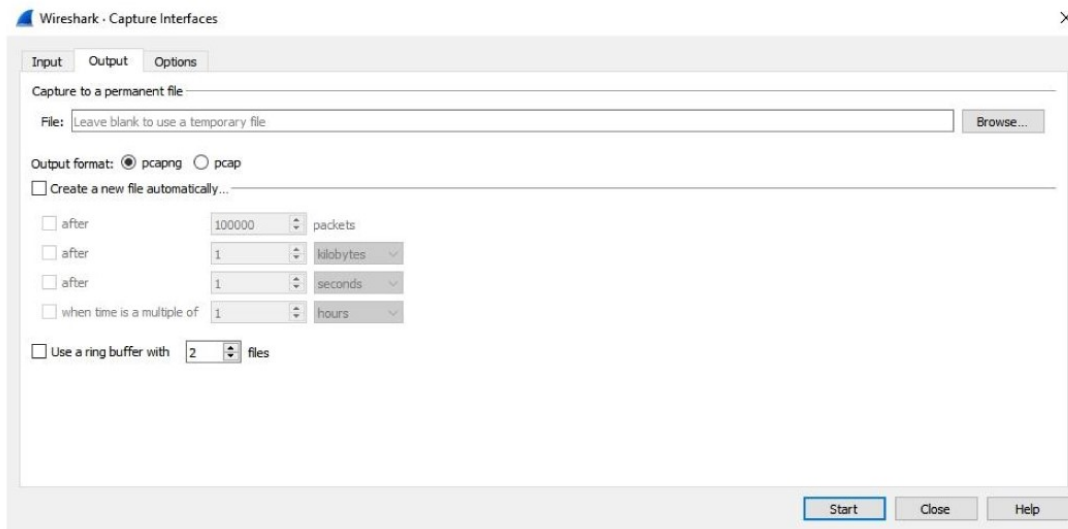
12. ถ้าป้อน not host 161.246.4.119 คิดว่าจะหมายถึงอะไร

Packet ที่ไม่ได้มีต้นทางมาจาก 161.246.4.119

13. ให้นักศึกษาสรุปการใช้งานการใส่ Capture Filter เบื้องต้น

ที่เราใส่ตัวแปรใน packet ที่เราสนใจลงไปในช่วง packet filter ได้ แล้ว Wire shark จะทำการกรอง packet ออกมา

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 เพื่อป้องกันไม่ให้พื้นที่ในฮาร์ดดิสก์ มากเกินไป



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



14. ให้สร้างไฟล์ชื่อ captures01.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

ไฟล์ captures01 จะรันขึ้น 4 ไฟล์ โดยเวลาที่ถูกรับต่างกัน 10 วินาทีพอดี

## 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

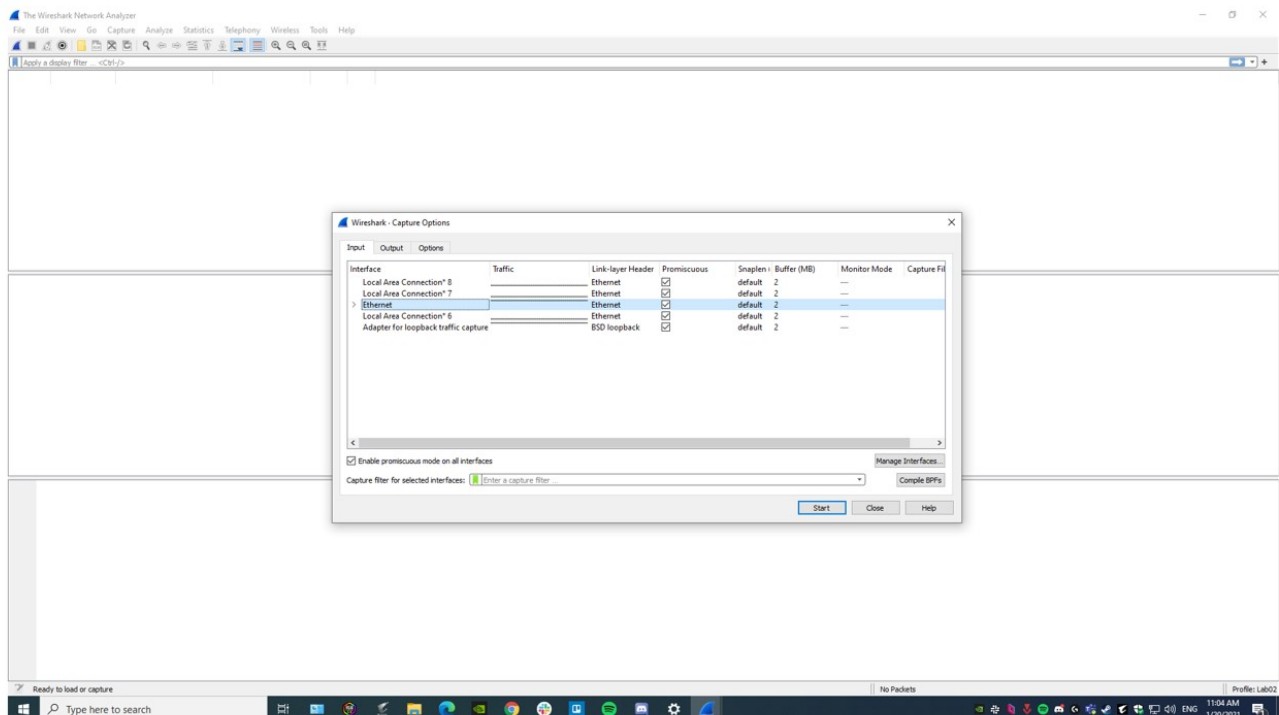
1. ให้สร้างและใช้ Profile ใหม่ เพื่อไม่กระทบกับ Default Profile
2. ให้ capture ข้อมูลจากเครื่องนักศึกษาไปที่ [www.ce.kmitl.ac.th](http://www.ce.kmitl.ac.th)
3. ตั้งการแสดงผล Time เป็น Seconds Since Previous Displayed Packet
4. ให้หาค่าเวลาที่มากที่สุดในช่อง Time เป็น packet ที่เท่าไร 8 และให้ถามเพื่อนอีก 3 คน พบที่เดียวกันหรือไม่ ของเพื่อน packet ที่เท่าไร พบที่ packet 8 เช่นเดียวกัน
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

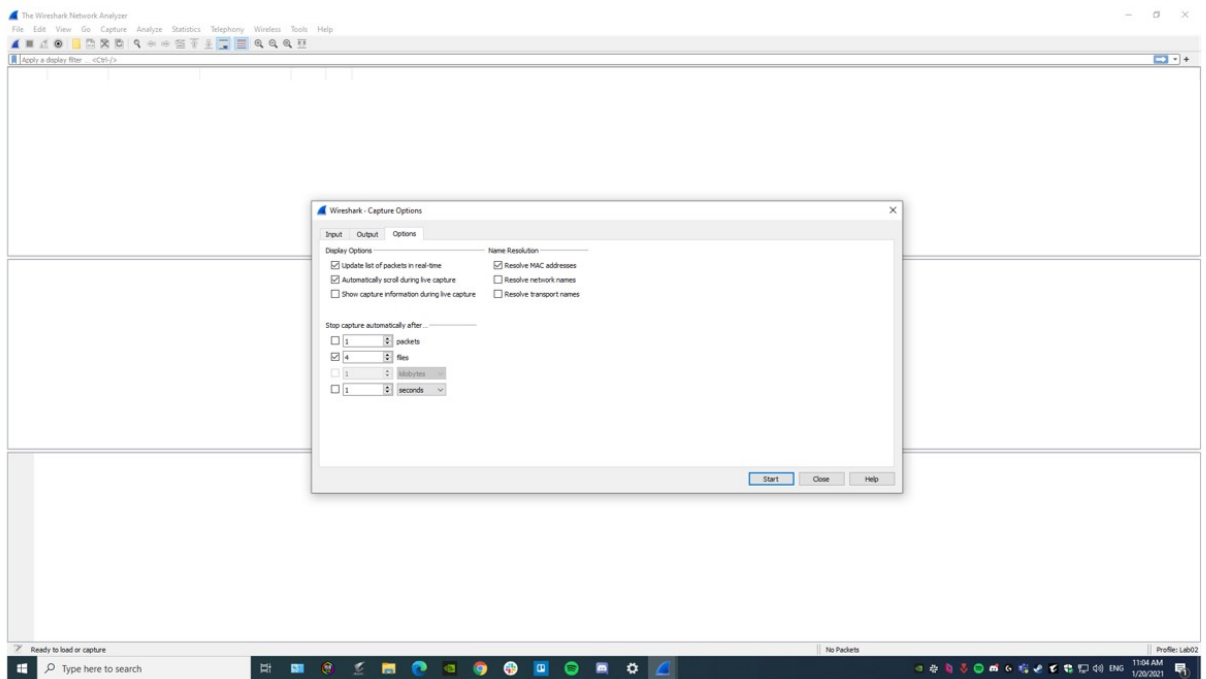
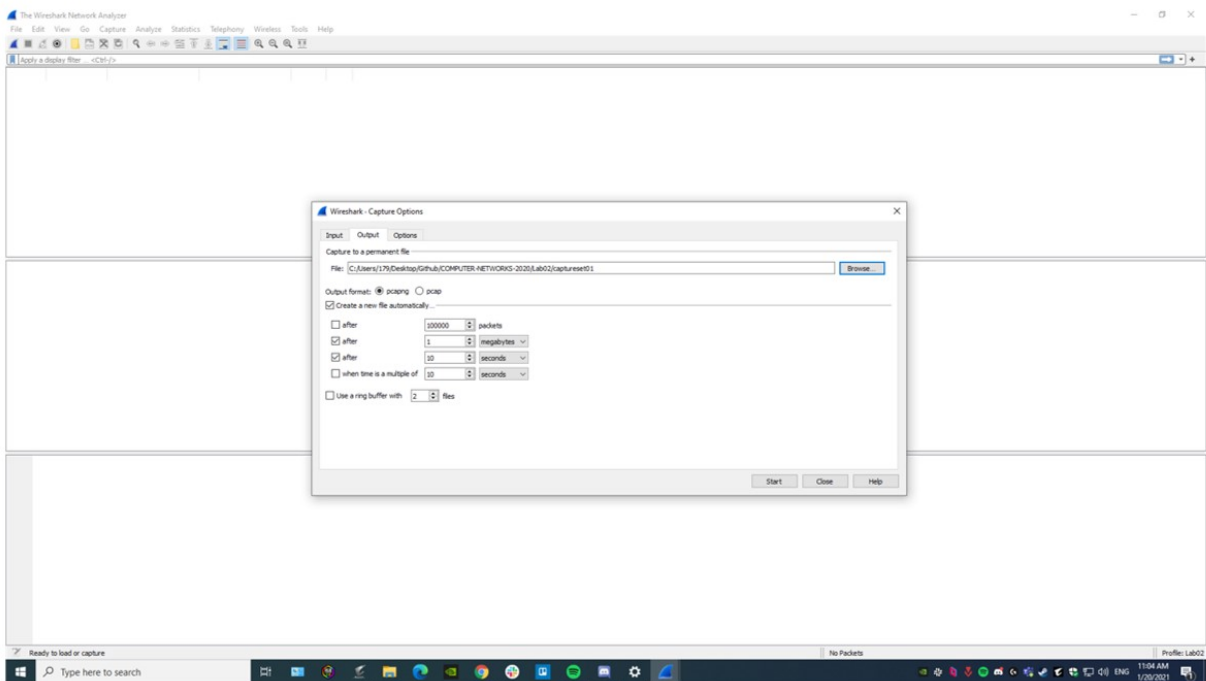
```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{D6DB428C-ACA3-4424-A94A-D43F6A65603F}, id 0
> Ethernet II, Src: Dell_02:eb:60 (18:66:da:02:eb:60), Dst: HuaweiTe_fb:24:d5 (c4:b8:b4:fb:24:d5)
> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 161.246.4.119
< Transmission Control Protocol, Src Port: 1847, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 1847
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Sequence number (raw): 1546021792
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 64240
    [Calculated window size: 64240]
    Checksum: 0x6840 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  < [Timestamps]
    [Time since first frame in this TCP stream: 0.000000000 seconds]
    [Time since previous frame in this TCP stream: 0.000000000 seconds]
```

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 8 และให้ถามเพื่อนอีก 3 คน พบที่เดียวกันหรือไม่ ของเพื่อน packet ที่เท่าไร พบที่ packet 8 เหมือนกัน เป็นการทำงานอะไร GET /slideshow2.css HTTP/1.1 (HTTP)
8. ให้นักศึกษาตอบคำถามต่อไปนี้  
 นักศึกษาคิดว่า Packet ที่เป็นการเรียกหน้า Homepage (/) ของหน้าเว็บอยู่ที่ Packet ไດ 4 และ Response Code ของ Packet ข้างต้นอยู่ที่ Packet ไດ 8

## งานครั้งที่ 2

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





Wireshark interface showing a packet capture of network traffic. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 1) is a TCP segment from 192.168.1.100 to 192.168.1.101, Seq=13449, Ack=1902, Win=65532, Len=1452, [TCP segment of a reassembled PDU].

The packet details pane shows the structure of the selected packet:

- Frame 1: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on 0
- Ethernet II, Src: Microsoft\_Office65 (28:16:ad:08:ee:63), Dst: d8ackn3n\_fa
- Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.101
- Transmission Control Protocol, Src Port: 63466, Dst Port: 27836, Seq: 1,
- Transport Layer Security

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 70 85 c2 f0 7a 3c 28 16 a8 60 ee 63 00 00 45 00 p-z[...]-c-E-
0010 00 66 50 17 40 00 00 16 52 c0 20 01 60 c0 a8 47 00 -A-k-
0020 01 66 f7 ea 69 9c 03 05 fc 64 a7 2e 7a ee 50 18 f-1-...-d-z-P-
0030 fa 21 88 6f 00 00 17 03 03 00 40 5a 18 ff 2e -1-o-...-Bv-..
0040 2a 45 00 92 3c ee 36 0e a1 71 0e 1a 0d 3e 25 45 *A-...-e-08-
0050 25 7e 70 99 33 36 46 f7 2c cf b8 37 c8 c2 90 c8 <w-36P-...-?...
0060 2b 45 1a 4c 03 02 95 e1 1f 55 94 77 0c 4d 46 af +...-E-w3P-
0070 ba 17 2f 6f 46 bb 34 bb a6 0f a1 -/f-A-...
```

A "WireShark - Filter in Set" dialog box is open, showing a table of filters:

Filename	Created	Modified	Size
captures01_00001_20210120110514	2021-01-20 11:05:14	2021-01-20 11:05:20	12268
captures01_00002_20210120110520	2021-01-20 11:05:20	2021-01-20 11:05:30	23488
captures01_00003_20210120110530	2021-01-20 11:05:30	2021-01-20 11:05:40	6168
captures01_00004_20210120110540	2021-01-20 11:05:40	2021-01-20 11:05:40	328 bytes

The directory path is C:\Users\77\Desktop\Github\COMPS\08-07-2020\JAN Lab02.

Wireshark status bar: Packets: 209 - Displayed: 209 (100.0%) Profile: Lab02