นายปัญญาวัฒน์ สนหาสาคา 63010584

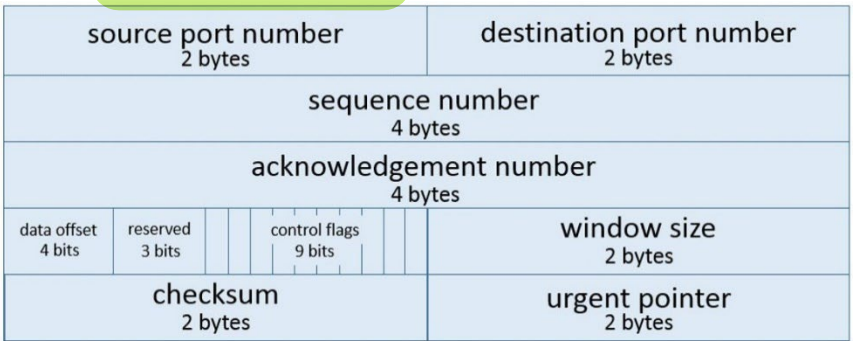
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

กิจกรรมที่ 6 : TCP Connection

กิจกรรมครั้งนี้จะเป็นการทำความเข้าใจกับโปรโตคอล TCP (Transmission Control Protocol) ซึ่ง TCP มีคุณสมบัติในการทำงานอยู่ 5 ประการได้แก่

- Reliable, in-order delivery คือ การส่งไม่ผิดพลาดโดยข้อมูลมีการเรียงตามลำดับ
- Connection Oriented คือ ต้องมีการสร้างการเชื่อมต่อก่อน และมีการแลกเปลี่ยนข้อมูลควบคุม
- Flow Control ควบคุมการไหลของข้อมูลระหว่าง Process ทั้ง 2 ด้าน
- Congestion Control ควบคุมการไหลของข้อมูลผ่านอุปกรณ์เครือข่าย
- Full Duplex data สามารถส่งได้ทั้ง 2 ทาง ในการเชื่อมต่อเดียวกัน

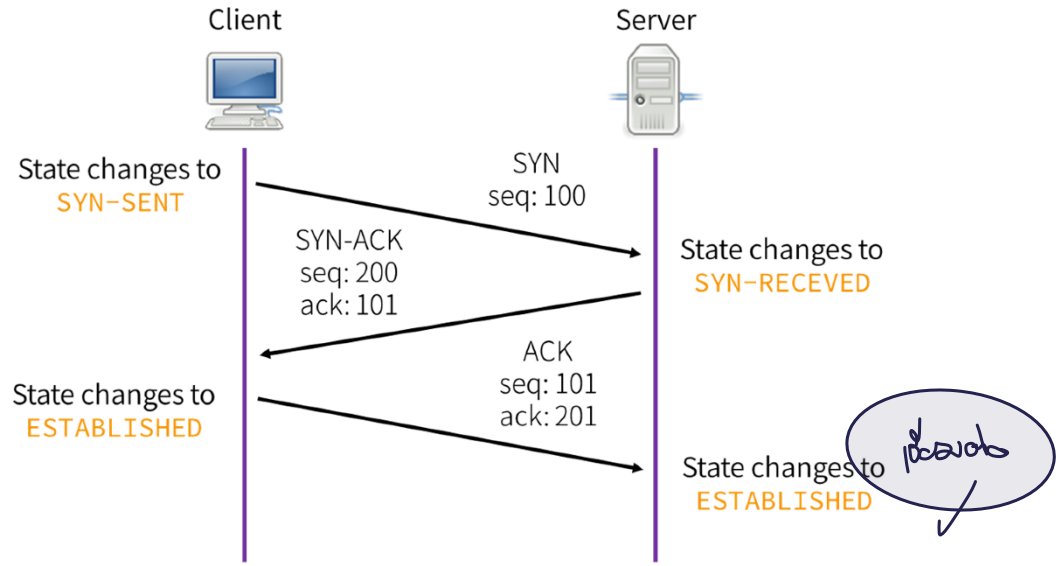
Connection Setup



รูปแสดง TCP Header

ก่อนเริ่มการส่งข้อมูลทุกครั้งของ TCP จะต้องมีการสร้าง Connection ขึ้นมาก่อนโดย Client จะเริ่มสร้างการเชื่อมต่อไปที่ Server ซึ่งประกอบด้วย 3 ขั้นตอน

- Client การส่ง packet SYN ไปที่ Server โดย Client จะมีการสร้างหมายเลข Sequence Number เรียกว่า ISN : Initial Sequence Number ขึ้นมา (ในรูปสมมติว่า 100) ใส่ใน SEQ# แล้วส่ง
- เมื่อ Server ได้รับ packet SYN จะตอบกลับโดย packet SYN-ACK โดย Server จะมีการสร้างหมายเลข ISN ของตนเองขึ้นมาเช่นกัน โดยใส่ใน SEQ# และนำหมายเลข SN:Client+1 แล้วใส่ใน ACK# แล้วส่ง
- เมื่อ Client ได้รับ packet SYN-ACK ก็จะตอบกลับโดย packet ACK สุดท้าย โดย Client จะนำ SN:Client+1 ใส่ใน SEQ# และนำ SN:Server+1 ใส่ใน ACK# แล้วส่ง เมื่อถึงตรงนี้จะถือว่าฝั่ง Client สร้างการเชื่อมต่อสำเร็จแล้ว ซึ่ง Client สามารถจะเริ่มส่งข้อมูลได้
- เมื่อ Server ได้รับ packet ACK สุดท้าย จะถือว่าฝั่ง Server สร้างการเชื่อมต่อสำเร็จแล้วเช่นกัน



1. ให้เปิดไฟล์ http-browse101d.pcapng ค้นหา 3 way handshake แรกในไฟล์แล้ว บันทึกข้อมูลลงในตารางด้านล่าง (ทั้ง Seq# และ Ack# ให้ใช้แบบ raw ในช่อง Flag ให้บอกว่ามี Flag ใดที่ Set บ้าง

SYN

Src Port : 61598	Dest Port : 80
Seq # : 610997682	
Ack # : 0	
Flags : 0x002	SYN

SYN-ACK

Src Port : 80	Dest Port : 61598
Seq # : 4134094401	
Ack # : 610997683	
Flags : 0x012	SYN, ACK

ACK

Src Port : 61598	Dest Port : 80
Seq # : 610997683	
Ack # : 4134094402	
Flags : 0x010	ACK

- ค่าความยาวข้อมูลของ packet ทั้ง 3 เท่ากับเท่าไรบ้าง SYN 66 bytes, SYN/ACK 66 bytes, ACK 54 bytes
- ใน packet SYN มีข้อมูลอื่นๆ ส่งมาด้วยหรือไม่ อะไรบ้าง (ดูในคอลัมน์ info) และข้อมูลต่างๆ เหล่านั้นมีความหมายอะไรหรือนำไปใช้อะไร (ให้ค้นหาข้อมูลเพิ่มเติมจากหนังสือ)

ขนาดหน้าต่างสูงสุด

ค่า (win = 8192) (1460) (4)

ข้อมูล	ความหมาย
window	เป็นการสื่อสารข้อมูลระหว่าง Client กับ Server ว่าจะรับปริมาณเท่าใดถึงจะตอบกลับ.
Sack_Perm	เลือกรับได้ว่าจะรับสิ่งไหนหรือข้อมูลได้ส่วนไหนถึงไหน ช่วงไหนไม่ได้อยู่ในเงื่อนไขที่ได้รับ
MSS (Maximum segment size)	ระบุขนาด packet ที่สูงสุดที่ server ทั้ง 2 รู้ เพื่อป้องกันไม่ให้ส่ง packet ที่ขนาดใหญ่เกิน (เกิน = หาย) drop
WS (window scale)	เป็นตัวเลือกขยายขนาดหน้าต่าง

- ใน packet SYN-ACK มีข้อมูลอื่นๆ ส่งมาด้วยหรือไม่ อะไรบ้าง (ดูในคอลัมน์ info) และข้อมูลต่างๆ เหล่านั้นมีความหมายอะไรหรือนำไปใช้อะไร

ค่า (14600) (1430) (64)

ข้อมูล	ความหมาย
window	เป็นการสื่อสารข้อมูลระหว่าง Client กับ Server ว่าจะรับปริมาณเท่าใดถึงจะตอบกลับ.
Sack_Perm	เลือกรับได้ว่าจะรับสิ่งไหนหรือข้อมูลได้ส่วนไหนถึงไหน ช่วงไหนไม่ได้อยู่ในเงื่อนไขที่ได้รับ
MSS	ระบุขนาด packet ที่สูงสุดที่ server ทั้ง 2 รู้ เพื่อป้องกันไม่ให้ส่ง packet ที่ขนาดใหญ่เกิน
WS	เป็นตัวเลือกขยายขนาดหน้าต่าง

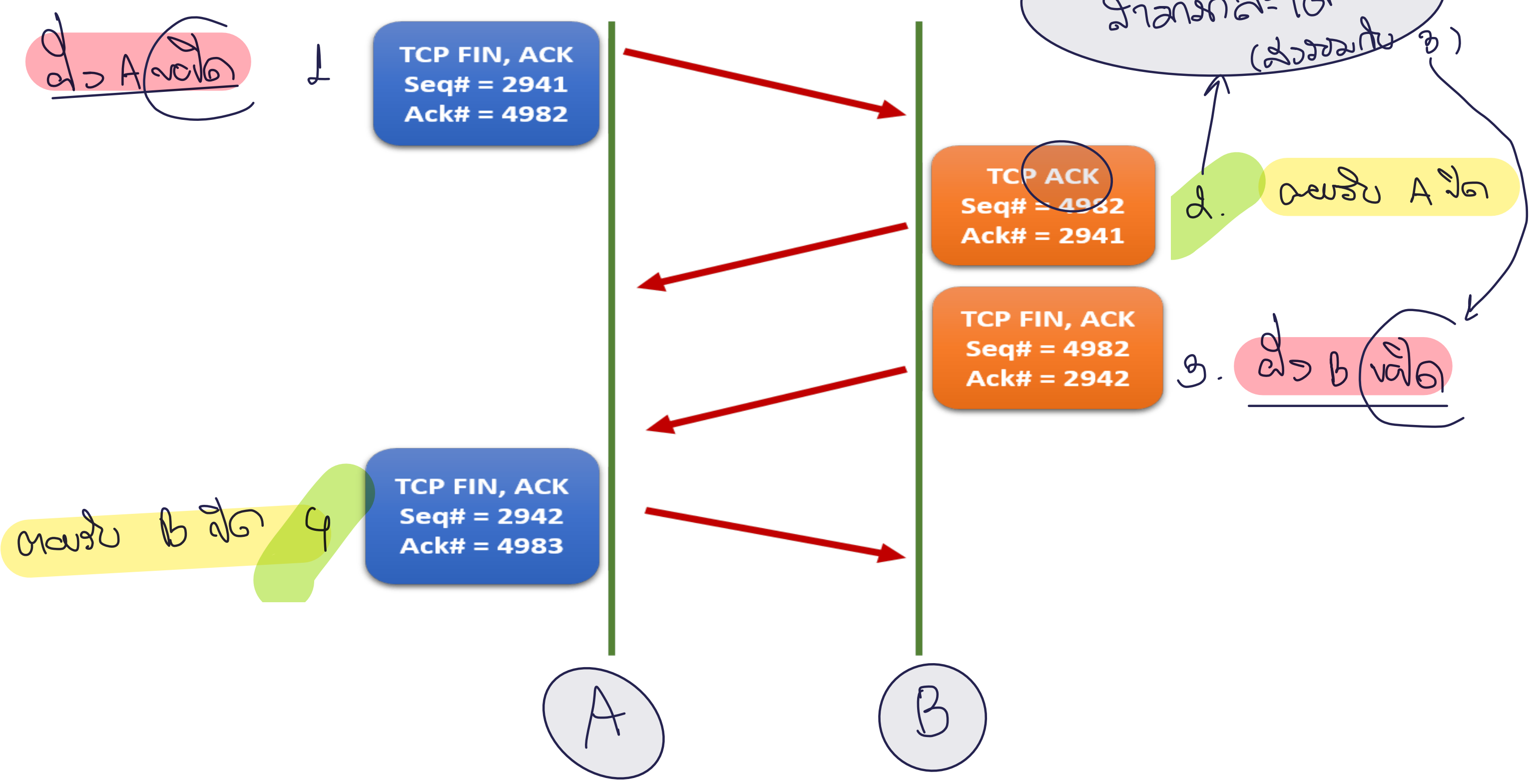
รับได้แค่ 1430

- ให้ดู packet ที่ส่งข้อมูล packet แรก (หรือ packet อื่นก็ได้) ให้ตอบว่าในข้อมูลที่ไม่เท่ากันของ Client กับ Server ในการเลือกใช้ข้อมูลหนึ่ง (เนื่องจากทั้ง 2 ด้านต้องใช้พารามิเตอร์เดียวกันในการส่งข้อมูล) คิดว่ามีหลักในการเลือกอย่างไร

ใช้ window size ในการเลือก เพราะในแต่ละ packet จะส่งข้อมูล window size ของคู่สื่อ ต่างไม่เท่ากัน ขึ้นอยู่กับ packet ตัวอื่น.

Connection Terminated จบการเชื่อมต่อ

เมื่อสิ้นสุดการส่งข้อมูลแล้ว ใน TCP จะมีการปิด Connection ซึ่งประกอบด้วย 4 ขั้นตอน



1 - ฝ่ายใดฝ่ายหนึ่งที่ต้องการปิด Connection (ต่อไปจะเรียก A และเรียกอีกฝั่งว่า B) จะส่ง packet ที่มี FIN/ACK flag มา โดยใช้ SEQ# และ ACK# เท่ากับ packet สุดท้ายก่อนจะปิด connection

2- ฝั่ง B จะตอบด้วย packet ที่มี ACK flag โดยใช้ SEQ# เท่ากับ ACK# ของ FIN/ACK ก่อนหน้า และใช้ ACK# เท่ากับของ SYN# ของ packet ล่าสุด โดยเมื่อ A ได้รับ packet นี้ จะถือว่าเป็นการสิ้นสุด connection ของฝั่ง A (**หมายเหตุ** บางครั้งอาจไม่มีการส่ง packet นี้ โดยอาจรวมไปกับ packet ที่ 3

3 - ฝั่ง B จะเริ่มปิด Connection บ้าง โดยจะส่ง packet ที่มี FIN/ACK flag โดยใช้ SEQ# เท่ากับ ACK# ของ FIN/ACK ก่อนหน้า และใช้ ACK# เท่ากับของ SYN# ของ packet ล่าสุด +1

4 - ฝั่ง A จะตอบกลับการปิด Connection โดยจะส่ง packet ที่มี FIN/ACK flag โดยใช้ SEQ# เท่ากับ ACK# ของ FIN/ACK ก่อนหน้า และใช้ ACK# เท่ากับของ SYN# ของ packet ล่าสุด +1 เมื่อถึงจุดนี้จะถือว่าเป็นการสิ้นสุด Connection ของ B

2. ให้หา Packet ที่ปิด Connection ของ Connection ในข้อ 1 โดยให้บอกขั้นตอนการหาและป้อนรายละเอียดลงในตาราง (ข้อมูล Seq# และ Ack # ให้ใช้แบบ Relative)

Packet#	1663		
Src Port :	61598	Dest Port :	80
Seq # :	6109978005		
Ack # :	4134095528		
Flags :	0x011		FIN , ACK

Packet#	1664		
Src Port :	80	Dest Port :	61598
Seq # :	4134095528		
Ack # :	6109978006		
Flags :	0x011		FIN, ACK

Packet#	1665		
Src Port :	61598	Dest Port :	80
Seq # :	6109978006		
Ack # :	4134095529		
Flags :	0x010		ACK

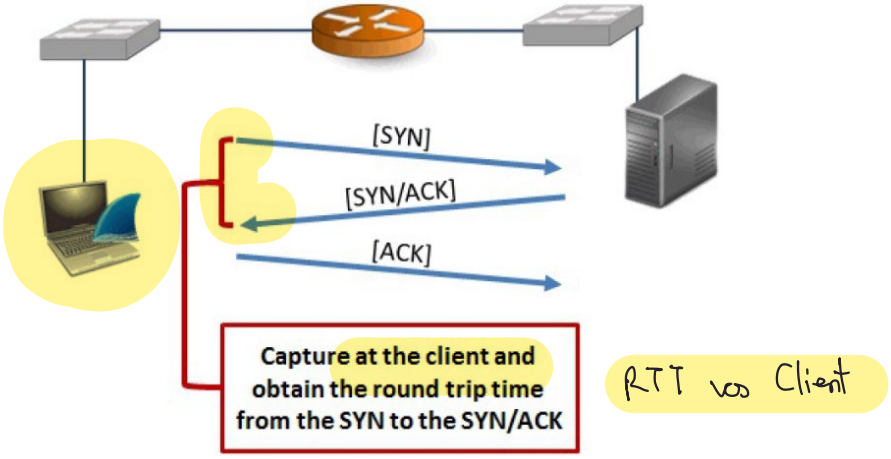
วิธีค้นหา

ใช้ filter ใน

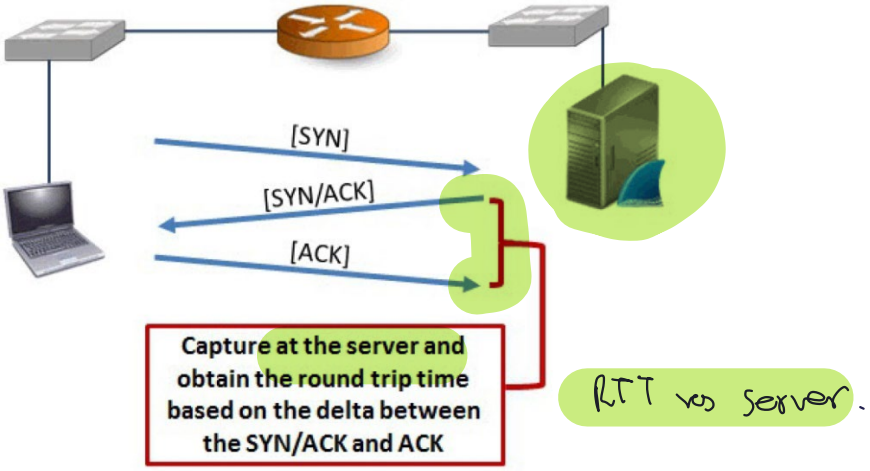
```
( tcp.srcport == 61598 and tcp.dstport == 80) or (tcp.srcport == 80 and tcp.dstport == 61598)
```

ดูที่ลำดับที่เป็นลำดับการสิ้นสุดการเชื่อมต่อ (FIN)

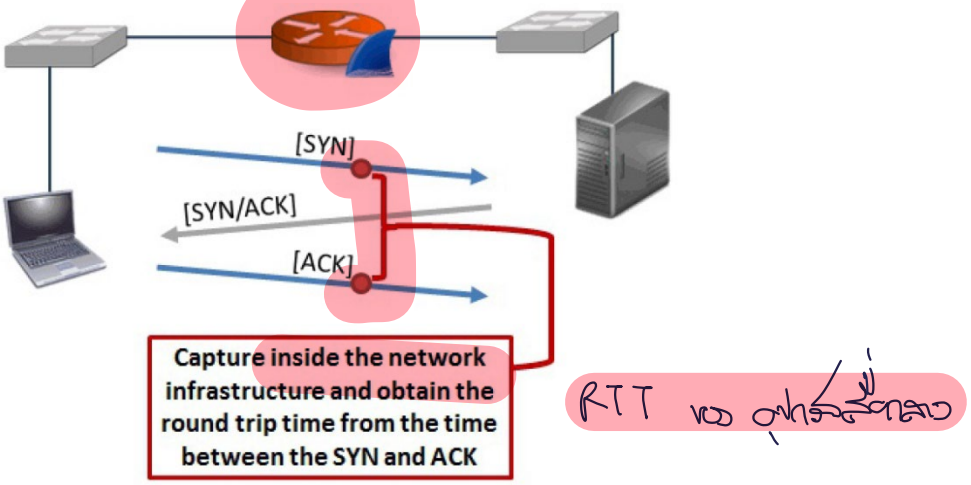
3. ใน Wireshark เราสามารถจะหา packet ที่มีคุณลักษณะของ flags เฉพาะได้ โดยใช้ display filter tcp.flags เช่น **tcp.flags.syn==1** หรือ **tcp.flags.ack==1** ซึ่งเราสามารถใช้หา RTT ของ TCP handshake ได้ โดยการหา RTT ของ TCP handshake มี 3 แบบ คือ วัดจากฝั่ง Client จะใช้เวลาระหว่าง SYN และ SYN-ACK



และวัดจากฝั่ง Server จะใช้เวลาระหว่าง SYN/ACK กับ ACK



แต่ในกรณีที่วัดจากอุปกรณ์ ควรใช้ระหว่าง SYN และ ACK ตามรูป



4. จากไฟล์ http-browse101d.pcapng ให้สร้าง display filter ที่สามารถแสดงเฉพาะ packet ที่เป็น Open Connection (3 way handshake) คู่ที่กำหนด ของทุกๆ TCP Stream โดยไม่มี packet อื่นๆ มาปน (<u>นักศึกษาพยายามคิดด้วยตนเอง</u>) ให้เขียนวิธีการหา และ display filter ของแต่ละอัน

   (1) – packet SYN และ SYN/ACK ของ 3 way handshake (packet ที่ 1 และ 2)

   (2) – packet SYN/ACK และ ACK ของ 3 way handshake (packet ที่ 2 และ 3)

   (3) – packet SYN และ ACK 3 way handshake (packet ที่ 1 และ 3)

(1)

(tcp.flags == 0x012 or tcp.flags.syn==1) and ((tcp.dstport == 80 and tcp.srcport == 61598) or (tcp.srcport == 80 and tcp.dstport == 61598))

No.	Time	Source	Destination	Protocol	Length	Host	DNS Delta	Info
1	0.000000	24.6.173.220	173.194.79.121	TCP	66			61598 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.035945	173.194.79.121	24.6.173.220	TCP	66			80 → 61598 [SYN, ACK] Seq=0 Ack=1 Win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64

(2)

(tcp.flags == 0x012 or tcp.flags == 0x010) and ((tcp.dstport == 80 and tcp.srcport == 61598) or (tcp.srcport == 80 and tcp.dstport == 61598)) and (tcp.window_size == 14300 or tcp.window_size == 65780)

No.	Time	TCP Delta	Source	Destination	Protocol	Length	Info
2	0.035945	0.035945000	173.194.79.121	24.6.173.220	TCP	66	80 → 61598 [SYN, ACK] Seq=0 Ack=1 Win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64
3	0.036067	0.000122000	24.6.173.220	173.194.79.121	TCP	54	61598 → 80 [ACK] Seq=1 Ack=1 Win=65780 Len=0

(3)

(tcp.flags == 0x010 or tcp.flags == 0x002) and ((tcp.dstport == 80 and tcp.srcport == 61598) or (tcp.srcport == 80 and tcp.dstport == 61598)) and tcp.time_delta <0.0002 and tcp.seq != 324

No.	Time	TCP Delta	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000000	24.6.173.220	173.194.79.121	TCP	66	61598 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
3	0.036067	0.000122000	24.6.173.220	173.194.79.121	TCP	54	61598 → 80 [ACK] Seq=1 Ack=1 Win=65780 Len=0

5. เราสามารถใช้ค่า RTT ของ TCP handshaking ตามข้อ 4 มาใช้วัดประสิทธิภาพของ Web Server ได้เช่นกัน โดย Server ที่มีค่า RTT น้อย แสดงถึงการตอบสนองที่รวดเร็ว ดังนั้นให้ capture ข้อมูลจากเว็บและใช้ display filter ตามข้อ 4 (ให้นักศึกษาเลือกใช้ตัวที่เหมาะสม) เพื่อหาค่า RTT ของเว็บต่างๆ จำนวน 3 เว็บ แล้วนำค่ามาใส่ตาราง

URL	เวลา
KMITL	0.020126
CE.KMITL	0.02264
DATASTRUC.CE.KMITL	0.020652

- ให้ตอบว่าระหว่าง RTT ที่วัดในครั้งนี้ กับ HTTP RTT ที่วัดในครั้งก่อนหน้านี้ บอกถึงอะไร และแตกต่างกันอย่างไร

RTT ของ TCP เป็นช่วงเวลาในการ Handshake เท่านั้น (ส่งการร้องขอ) แต่ RTT ของ HTTP เป็นช่วงเวลาในการตอบสนองจาก server ณ ช่วงที่ website สมบูรณ์.

งานครั้งที่ 6

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งโดยเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา และ _Lab6 เช่น 63010789_Lab6.pdf
- กำหนดส่ง ภายในวันที่ 23 กุมภาพันธ์ 2565