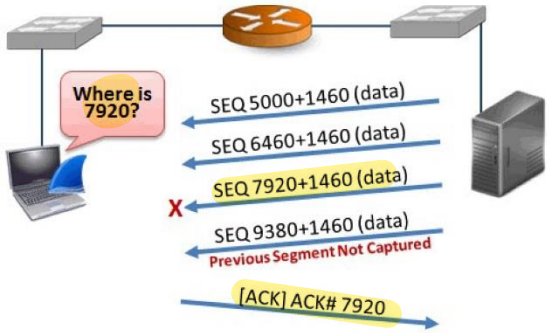
นายปัญญวัฒน์ สนหาสาคา 63010584

กิจกรรมที่ 7 : TCP Retransmission

กิจกรรมครั้งนี้จะเป็นการทำความเข้าใจกับโปรโตคอล TCP (Transmission Control Protocol) ให้มากยิ่งขึ้น โดยเน้นเรื่องของ Retransmission

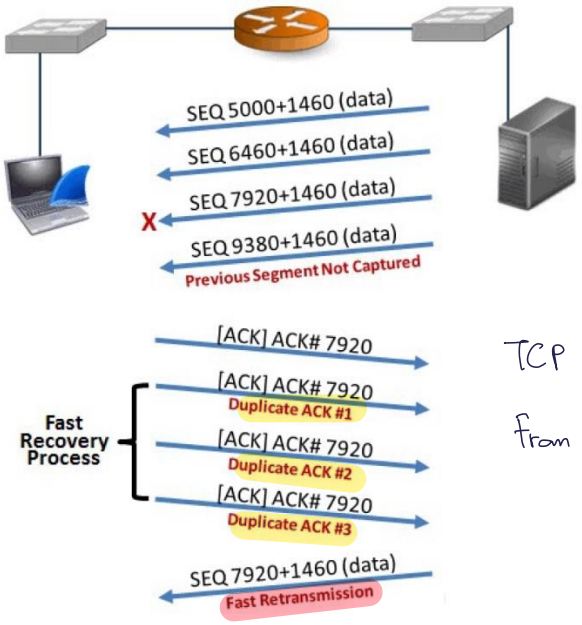
การรับข้อมูลของ TCP จะมีแนวทางการทำงาน ดังนี้

- Delayed ACK กรณีที่ฝั่งรับได้ ACK ตอบรับ packet ที่ได้รับไปทั้งหมดก่อนหน้านี้แล้ว เมื่อได้รับข้อมูลใหม่ อาจชะลอการส่ง ACK ไปก่อน เป็นระยะเวลาหนึ่งได้ หากไม่ได้รับ packet เพิ่มเติมจึงส่ง ACK ไป
- หากฝั่งรับ ยังไม่ได้ ACK ข้อมูลของ packet ล่าสุด เมื่อได้รับข้อมูลใหม่ ให้ ACK ข้อมูลล่าสุดทันที (Cumulative ACK)
- หากฝั่งรับได้รับ segment ที่ไม่เป็นไปตามลำดับ จะส่ง ACK ของ segment ล่าสุดที่ยังเป็นไปตามลำดับกลับไปทันที ซึ่งอาจทำให้เกิด *duplicate ACK* *



- ในกรณีที่เกิดการ lost segment จะมีวิธีการแก้ไข 2 รูปแบบ คือ retransmission โดยจะส่งข้อมูลใหม่ เมื่อครบเวลาของ retransmission time out (RTO) *

- อีกรูปแบบหนึ่ง คือ fast retransmission ซึ่งจะใช้ได้เฉพาะ OS ที่สนับสนุน โดยเมื่อได้รับ *duplicate ACK* ครบ 3 ครั้ง ก็จะส่งข้อมูลให้ใหม่



TCP Playload : ส่ง data เท่านั้น

From Length : ส่ง ข้อมูลทั้งหมดใน Frame นั้น
↓
header, data, อื่นๆ

1. ให้เปิดไฟล์ http-browse101d.pcapng คลิกขวาที่ Sequence Number และเลือก Apply as Column และตั้งชื่อว่า SEQ# จากนั้นคลิกขวาที่ Next Sequence Number และเลือก Apply as Column และตั้งชื่อว่า NEXTSEQ# และคลิกขวาที่ Acknowledgment Number และเลือก Apply as Column และตั้งชื่อว่า ACK# จัดรูปแบบคอลัมน์ให้เหมาะสม จะเห็นว่าเรามีข้อมูลของ SEQ#, NEXTSEQ# และ ACK# สำหรับช่วยในการวิเคราะห์
2. ใน wireshark จะมีข้อมูลที่ wireshark วิเคราะห์ขึ้น และสามารถนำมาเป็น display filter ได้ เช่น
   - tcp.analysis.duplicate_ack จะค้นหา packet ที่เกิด duplicate ACK
   - tcp.analysis.lost_segment จะค้นหา lost segment
   - tcp.analysis.retransmission จะค้นหา packet ที่เกิด retransmission
   - tcp.analysis.fast_retransmission จะค้นหา packet ที่เกิด fast retransmission

display filter

3. ให้เปิดไฟล์ tr-general101d.pcapng แล้วใช้ tcp.analysis.lost_segment กรอง จะพบว่ามี lost segment ทั้งหมด 5 แห่ง จาก Packet 10417 ให้ย้อนดู Packet 10416 แล้วตอบคำถามว่า มีข้อมูลหายไปเท่าไร มี Packet หายไปกี่ Packet บอกวิธีการหาแบบย่อๆ

มีข้อมูลหายไป 10,560 bytes. คือ มี packet หายไป 8 packet

						SEQ	NEXT SEQ	ACK	
10414	3.003858	10.9.9.9	10.10.10.10	TCP	1374	9162121	9163441	1	30000 → 1479 [ACK] Seq=9162121 Ack=1 Win=46 Len=1320
10415	3.003879	10.10.10.10	10.9.9.9	TCP	54	1	1	9163441	1479 → 30000 [ACK] Seq=1 Ack=9163441 Win=32768 Len=0
10416	3.003947	10.9.9.9	10.10.10.10	TCP	1374	9163441	9164761	1	30000 → 1479 [ACK] Seq=9163441 Ack=1 Win=46 Len=1320
10417	3.014769	10.9.9.9	10.10.10.10	TCP	1374	9175321	9176641	1	[TCP Previous segment not captured] 30000 → 1479 [ACK] Seq=9175321 Ack=1 Win=46 Len=1320
10418	3.014798	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=9175321 SRE=9176641
10419	3.014827	10.9.9.9	10.10.10.10	TCP	1374	9176641	9177961	1	30000 → 1479 [ACK] Seq=9176641 Ack=1 Win=46 Len=1320
10420	3.014836	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#1] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=9175321 SRE=9177961
10421	3.014853	10.9.9.9	10.10.10.10	TCP	1374	9177961	9179281	1	30000 → 1479 [ACK] Seq=9177961 Ack=1 Win=46 Len=1320

ให้ดูค่า SEQ ของ packet ที่ 10417 มาลบกับ NEXTSEQ packet ที่ 10416 จะได้ข้อมูลที่หายไป

คือ ขนาดของ 1320 เท่ากับ packet ที่หายไป (data 1320 byte / 1 packet)

4. จาก segment lost ใน packet 10417 หลังจากนั้นจะพบว่ามี Duplicate Ack เกิดขึ้นเป็นจำนวนมาก ให้อธิบายสาเหตุของการเกิด Duplicate Ack และเกิด Duplicate Ack กี่ครั้งในกรณีนี้

Packets: 37422 · Displayed: 808 (2.2%) · Marked: 1 (0.0%)

tcp.analysis.duplicate_ack and tcp.ack == 9164761

No.	Time	Source	Destination	Protocol	Length	SEQ#	NEXTSEQ#	ACK#	Info
10420	3.014836	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#1] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=917532
10422	3.014862	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#2] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=917532
10424	3.015338	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#3] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=917532
10426	3.015375	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#4] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=917532
10428	3.015457	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#5] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=917532
10430	3.015481	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#6] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=917532
10432	3.015505	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#7] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=917532
10434	3.015529	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#8] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=917532
10436	3.015568	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#9] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=917532
10438	3.015602	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#10] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=91753
10440	3.015698	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#11] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=91753
10442	3.015722	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#12] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=91753
10444	3.015827	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#13] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=91753
10446	3.015857	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#14] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 SLE=91753

packet ที่

เกิด Duplicate Ack : 808 ครั้ง (2.2%) $\left(\frac{12034 - 10420}{2}\right) + 2 = 808$

เกิด Duplicate Ack เพราะ ไม่ได้รับ packet ที่ต้องการจึงส่งกลับเป็น dup Ack ไปยัง ผู้ส่ง จนกว่าจะได้ Ack ที่ตนต้องการ.

5. จากข้อ 3 ข้อมูลที่หายไป ผู้ส่งทราบเมื่อใด ได้มีการส่งใหม่หรือไม่ และส่งใหม่ใน packet ใด ใช้เวลาเท่าใดในการส่งใหม่

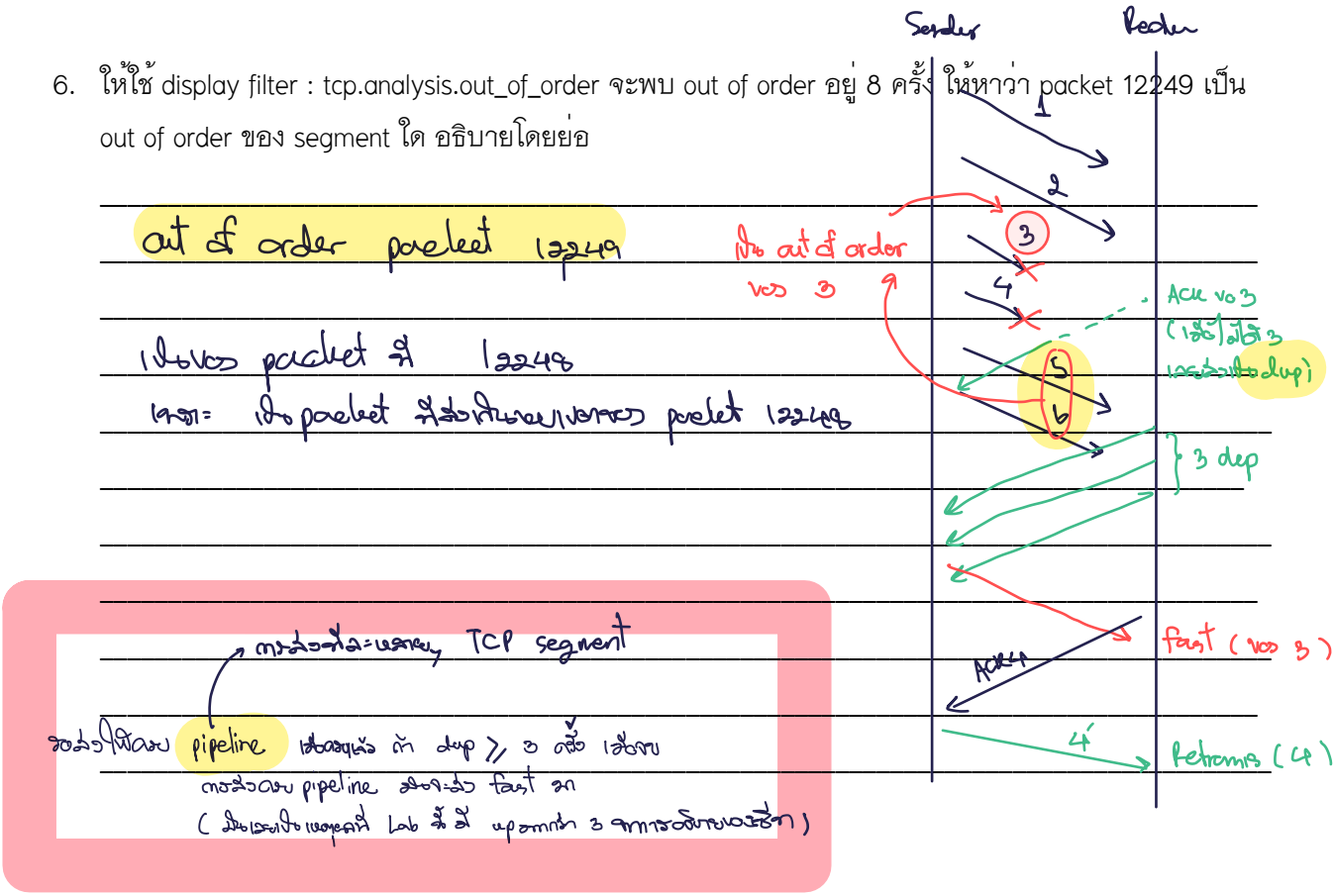
- ทราบเมื่อข้อมูลนั้นไม่ได้รับตาม SEQ# ที่ต้องการ
- มีการส่งข้อมูลใหม่อีกรอบ ส่งใน packet ที่ 12035 //

10417	3.014769	10.9.9.9	10.10.10.10	TCP	1374	9175321	9176641	1	[TCP Previous segment not captured] 30000 → 1479 [ACK]
10418	3.014798	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768 Len=0 S
10419	3.014827	10.9.9.9	10.10.10.10	TCP	1374	9176641	9177961	1	30000 → 1479 [ACK] Seq=9176641 Ack=1 Win=46 Len=1320
10420	3.014836	10.10.10.10	10.9.9.9	TCP	66	1	1	9164761	[TCP Dup ACK 10418#1] 1479 → 30000 [ACK] Seq=1 Ack=916

ใช้เวลา 3.480758 − 3.014836 = 0.465922 sec //

12035	3.480758	10.9.9.9	10.10.10.10	TCP	1374	9164761	9166081	1	[TCP Fast Retransmission] 30000 → 1479 [ACK] Seq=9164761 Ack=1 Win=46 Len=1320

6. ให้ใช้ display filter : tcp.analysis.out_of_order จะพบ out of order อยู่ 8 ครั้ง ให้หาว่า packet 12249 เป็น out of order ของ segment ใด อธิบายโดยย่อ



7. ไปที่ packet 12259 จะพบว่าเป็น retransmission ให้บอกว่าเป็น retransmission จาก RTO Timer หรือจากการได้รับ 3 Duplicate Ack พร้อมเหตุผลประกอบโดยย่อ

งานครั้งที่ 7

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งโดยเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา และ _Lab7 เช่น 63010789_Lab6.pdf
- กำหนดส่ง ภายในวันที่ 16 มีนาคม 2565