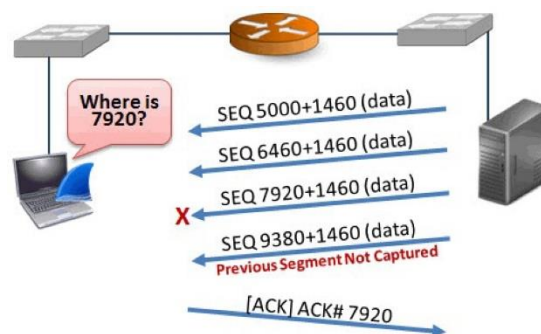


กิจกรรมที่ 7 : TCP Retransmission

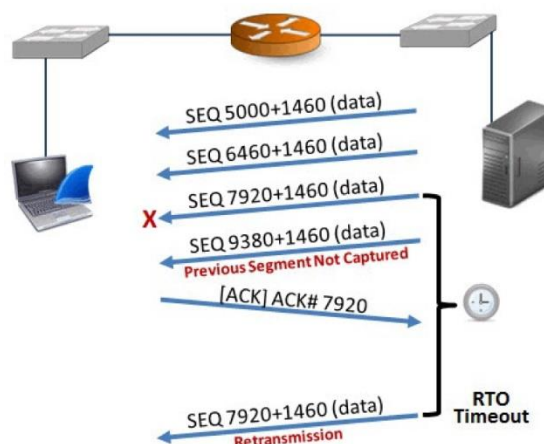
กิจกรรมครั้งนี้จะเป็นการทำความเข้าใจกับโปรโตคอล TCP (Transmission Control Protocol) ให้มากยิ่งขึ้น โดยเน้นเรื่องของ Retransmission

การรับข้อมูลของ TCP จะมีแนวทางการทำงาน ดังนี้

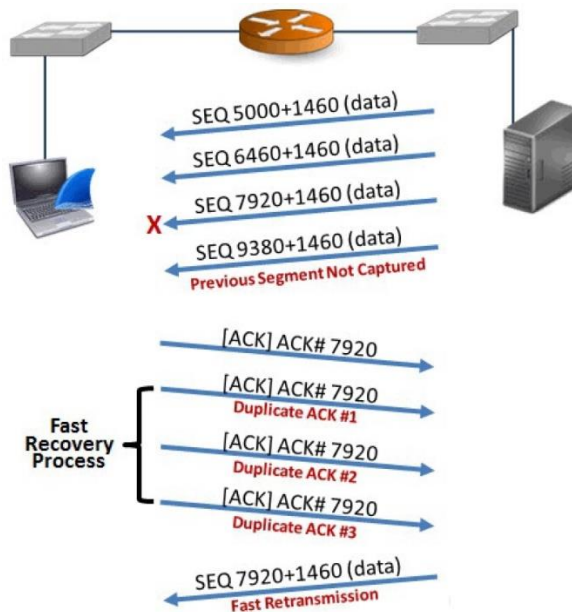
- Delayed ACK กรณีที่ฝั่งรับได้ ACK ตอบรับ packet ที่ได้รับไปทั้งหมดก่อนหน้านี้แล้ว เมื่อได้รับข้อมูลใหม่ อาจชะลอการส่ง ACK ไปก่อน เป็นระยะเวลาหนึ่งได้ หากไม่ได้รับ packet เพิ่มเติมจึงส่ง ACK ไป
- หากฝั่งรับ ยังไม่ได้ ACK ข้อมูลของ packet ล่าสุด เมื่อได้รับข้อมูลใหม่ ให้ ACK ข้อมูลล่าสุดทันที (Cumulative 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



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

packet ขนาด 1320 byte

ต้องนำก่อนหน้าไปก็ byte โทว

packet ที่ 10416 next seq = 9164761

packet ที่ 10417 seq = 9175921

นำไป 9175921 - 9164761 = 10560 byte

คิดเป็น $\frac{10560}{1320} = 8 \text{ packet}$

10416	3.003947	10.9.9.9	10.10.10.10	TCP	1374
10417	3.014769	10.9.9.9	10.10.10.10	TCP	1374
10418	3.014798	10.10.10.10	10.9.9.9	TCP	66

Frame 10416: 1374 bytes on wire (10992 bits), 1374 bytes captured (10992 bits) on interface unknown, id 0 Ethernet II, Src: Cisco_00:00:00:00:00:00, Dst: Cisco_00:00:00:00:00:00 Internet Protocol Version 4, Src: 10.9.9.9, Dst: 10.10.10.10 Transmission Control Protocol, Src Port: 30000, Dst Port: 1479, Seq: 9163441, Ack: 1, Len: 1320 Source Port: 30000 Destination Port: 1479 [Stream index: 0] [Conversation completeness: Incomplete (28)] [TCP Segment Len: 1320] Sequence Number: 9163441 (relative sequence number) Sequence Number (raw): 916318888 [Next Sequence Number: 9164761 (relative sequence number)]					
--	--	--	--	--	--

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Questions	Answer RRs	DNS Delta	SEC
4204	1.053731	10.9.9.9	10.10.10.10	TCP	1374					
10417	3.014769	10.9.9.9	10.10.10.10	TCP	1374					
11499	3.375988	10.9.9.9	10.10.10.10	TCP	1374					
15699	5.715885	10.9.9.9	10.10.10.10	TCP	1374					
22816	95.274599	10.9.9.9	10.10.10.10	TCP	1374					

Frame 10417: 1374 bytes on wire (10992 bits), 1374 bytes captured (10992 bits) on interface unknown, id 0 Ethernet II, Src: Cisco_00:00:00:00:00:00, Dst: Cisco_00:00:00:00:00:00 Internet Protocol Version 4, Src: 10.9.9.9, Dst: 10.10.10.10 Transmission Control Protocol, Src Port: 30000, Dst Port: 1479, Seq: 9175321, Ack: 1, Len: 1320					
---	--	--	--	--	--

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

เกิดจากที่ส่ง ACK แล้วมีการตอบกลับ

จึงมีการส่ง ACK ซ้ำทำให้เกิดการ duplicate

9 packet ตามทบทวน จึงได้ว่า 808 + 105 =

913 packet ที่เกิด duplicate ack

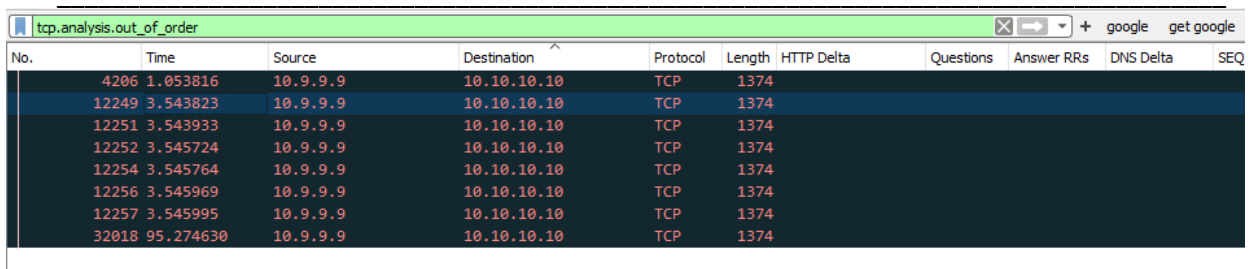
5. จากข้อ 3 ข้อมูลที่หายไป ผู้ส่งทราบเมื่อใด ได้มีการส่งใหม่หรือไม่ และส่งใหม่ใน packet ใด ใช้เวลาเท่าใดในการส่งใหม่

① ทราบเมื่อได้รับ duplicate ack กลับมาทบทวน = seq ไม่ตรง

② ค้นหาถึง packet packet แรก = 12035 packet ที่หายไป = 12257

③ ใช้เวลา 0.591226 วินาที

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



No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Questions	Answer RRs	DNS Delta	SEQ
4206	1.053816	10.9.9.9	10.10.10.10	TCP	1374					
12249	3.543823	10.9.9.9	10.10.10.10	TCP	1374					
12251	3.543933	10.9.9.9	10.10.10.10	TCP	1374					
12252	3.545724	10.9.9.9	10.10.10.10	TCP	1374					
12254	3.545764	10.9.9.9	10.10.10.10	TCP	1374					
12256	3.545969	10.9.9.9	10.10.10.10	TCP	1374					
12257	3.545995	10.9.9.9	10.10.10.10	TCP	1374					
32018	95.274630	10.9.9.9	10.10.10.10	TCP	1374					

packet 12249 เป็น out of order ของ segment 12246
sequence number ไม่ตรงกับ packet ก่อนหน้า

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

เป็น retransmission จาก RTO Timer เพราะหาเราห้พบกรอง filter
โดยใส่ "tcp.analysis.duplicate_ack" แล้วไม่พบ packet 12259

งานครั้งที่ 7

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