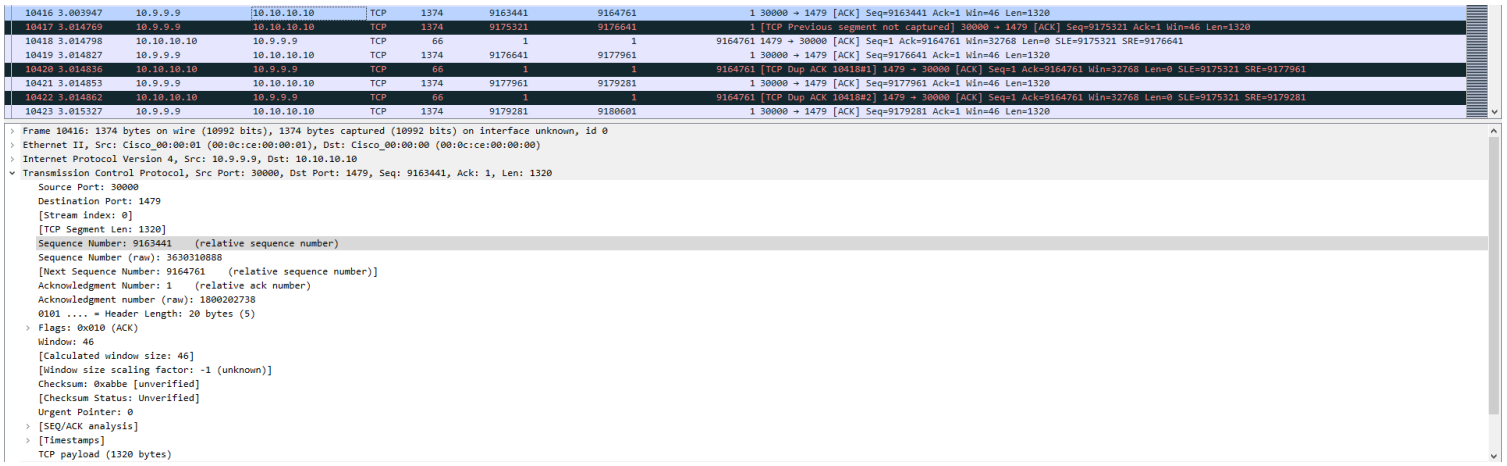
นายภากรณ์ ธนประชานนท์ 62010694

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

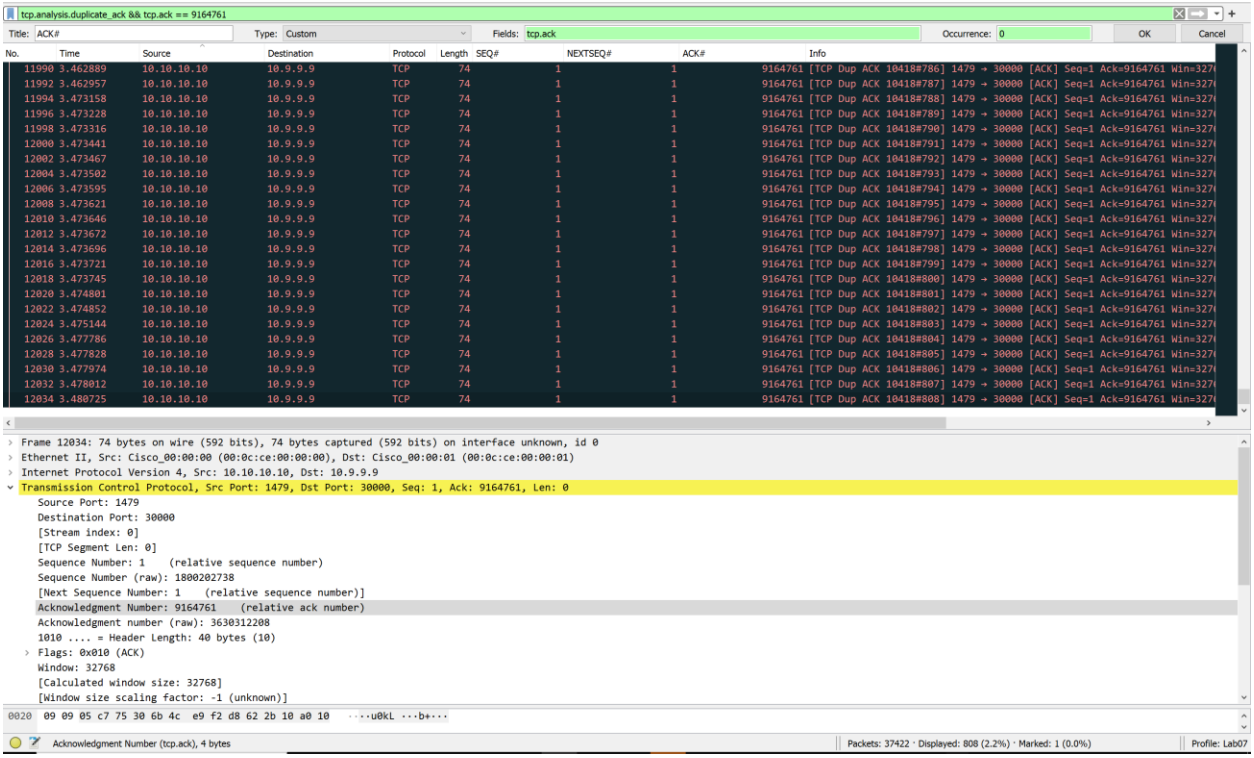


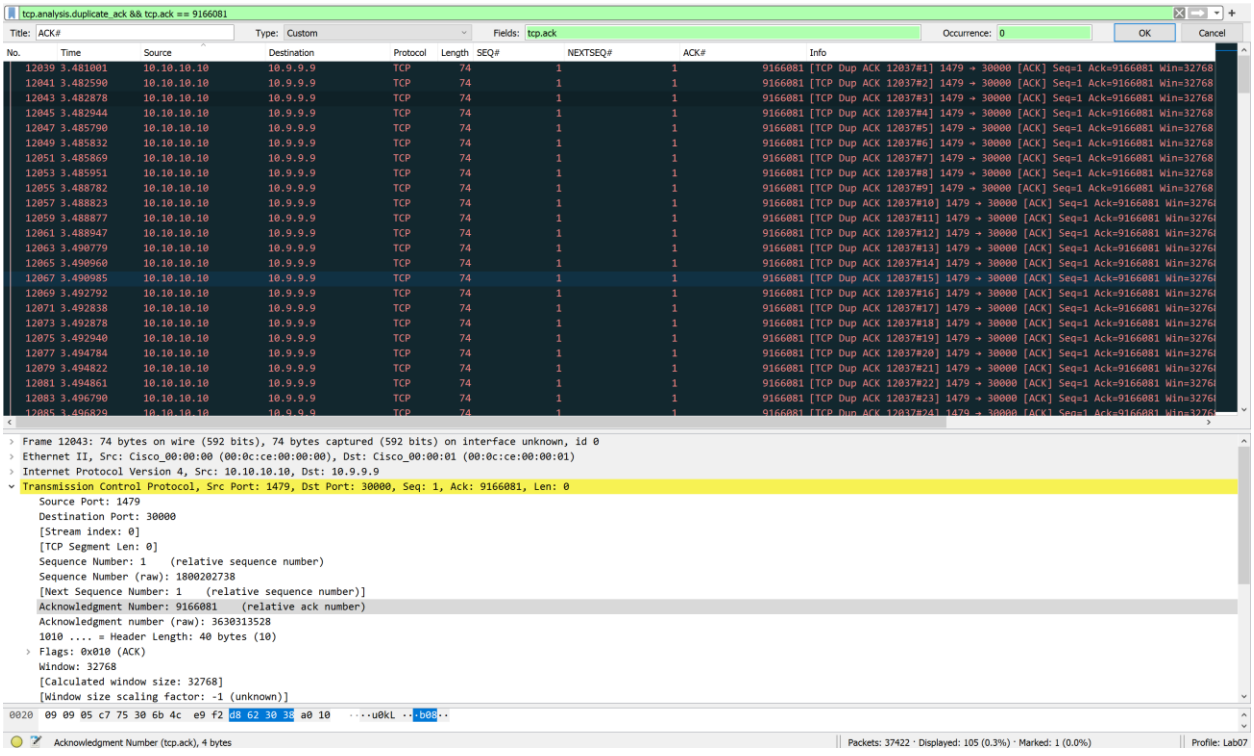
10416 3.003947	10.9.9.9	10.10.10.10	TCP	1374	9163441	9164761	1 30000 → 1479 [ACK] Seq=9163441 Ack=1 Win=46 Len=1320
10417 3.014769	10.9.9.9	10.10.10.10	TCP	1374	9175321	9176641	1 [TCP Previous segment not captured] 30000 → 1479 [ACK] Seq=9175321 Ack=1 Win=46 Len=1320
10418 3.014798	10.10.10.10	10.9.9.9	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
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=9175321 SRE=9179281
10423 3.015327	10.9.9.9	10.10.10.10	TCP	1374	9179281	9180601	1 30000 → 1479 [ACK] Seq=9179281 Ack=1 Win=46 Len=1320

```
> Frame 10416: 1374 bytes on wire (10992 bits), 1374 bytes captured (10992 bits) on interface unknown, id 0
> Ethernet II, Src: Cisco_00:00:01 (00:0c:ce:00:00:01), Dst: Cisco_00:00:00 (00:0c:ce:00:00:00)
> Internet Protocol Version 4, Src: 10.9.9.9, Dst: 10.10.10.10
v Transmission Control Protocol, Src Port: 30000, Dst Port: 1479, Seq: 9163441, Ack: 1, Len: 1320
    Source Port: 30000
    Destination Port: 1479
    [Stream index: 0]
    [TCP Segment Len: 1320]
    Sequence Number: 9163441    (relative sequence number)
    Sequence Number (raw): 3630310888
    [Next Sequence Number: 9164761    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1800202738
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 46
    [Calculated window size: 46]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xabbe [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (1320 bytes)
```

ดูใน TCP Protocol พบว่า TCP payload มีขนาด 1320 bytes ; Packet 10416 Next Sequence คือ 9164761 แต่ Packet 10417 ที่ได้มากลับมี Sequence เป็น 9175321 ; หายไป 9175321 – 9164761 = 10560 bytes ; หายไป 10,560/1320 = 8 Packet

4. จาก segment lost ใน packet 10416 หลังจากนั้นจะพบว่ามี Duplicate Ack เกิดขึ้นเป็นจำนวนมาก ให้อธิบายสาเหตุของการเกิด Duplicate Ack และเกิด Duplicate Ack กี่ครั้งในกรณี packet 10416





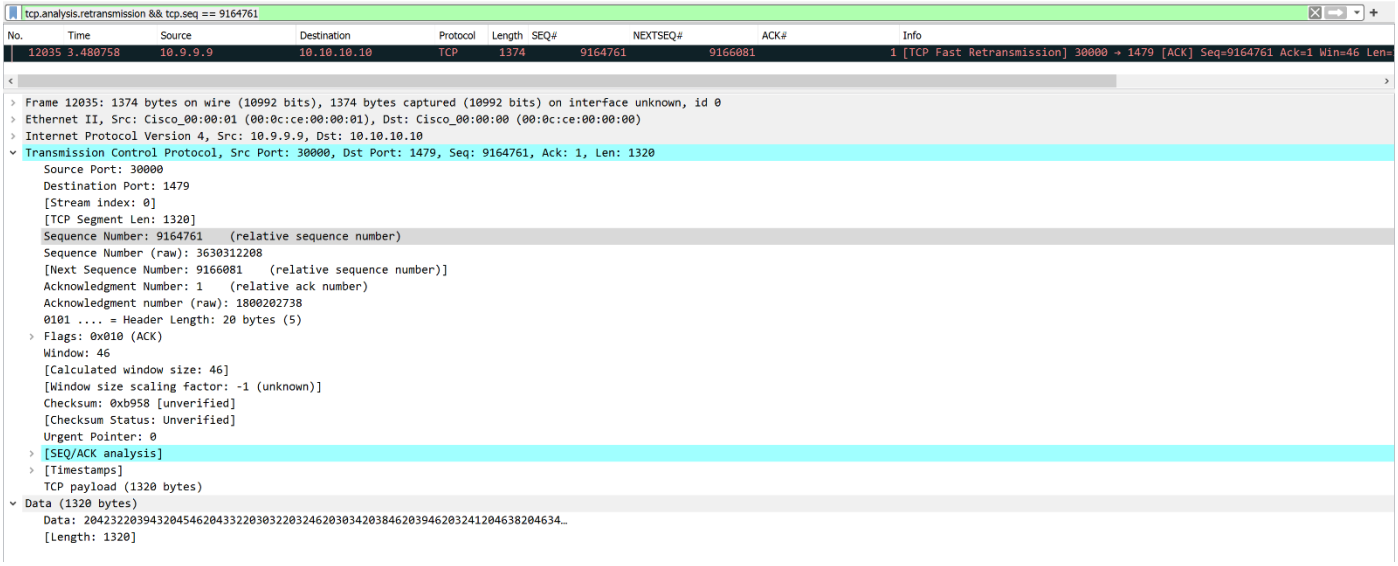
เกิดจากการส่ง Ack ไปแล้วยังไม่มีการตอบกลับมา จึงทำการส่ง Ack ซ้ำไปอีกครั้งทำให้เกิดการ Duplicate

ใช้ filter “tcp.analysis.duplicate_ack && tcp.ack == 9164761” จะพบว่ามี 808 Packets

ใช้ filter “tcp.analysis.duplicate_ack && tcp.ack == 9166081” จะพบว่ามี 105 Packets

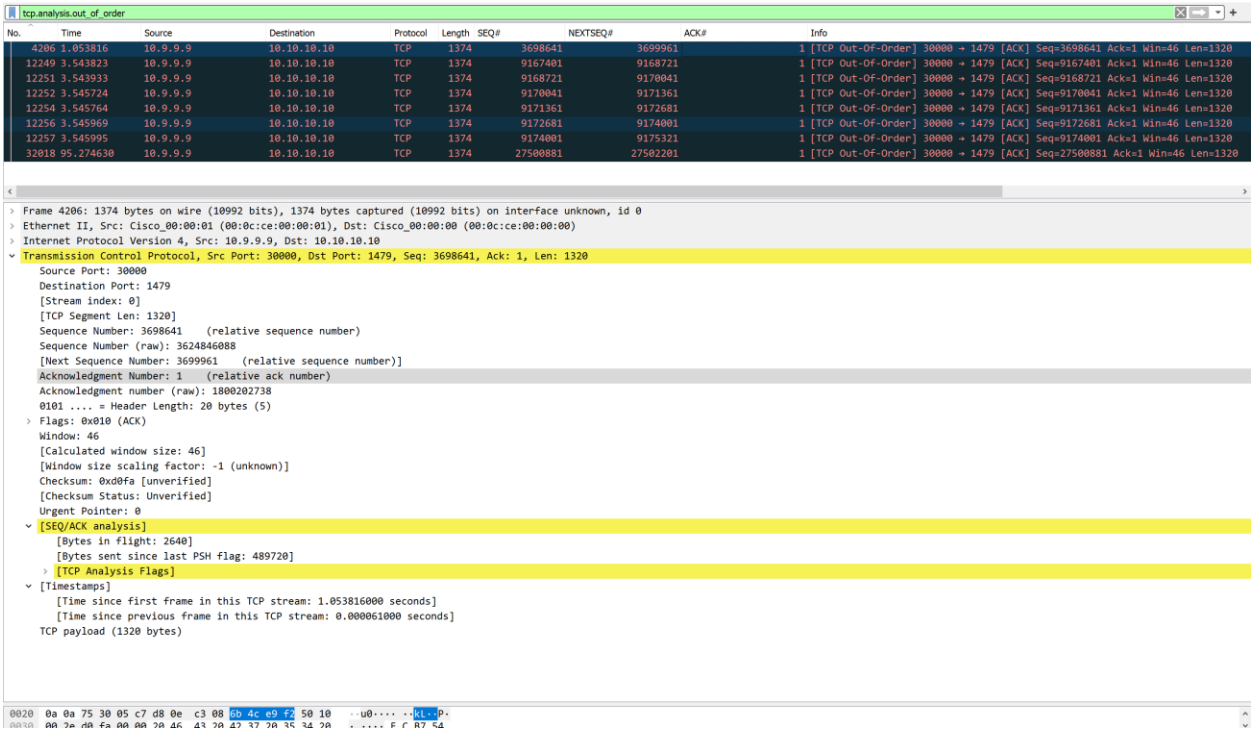
808 + 105 = 913 Packets

5. จากข้อ 3 ข้อมูลที่หายไป ผู้ส่งทราบเมื่อใด ได้มีการส่งใหม่หรือไม่ และส่งใหม่ใน packet ใด ใช้เวลาเท่าใดในการส่งใหม่



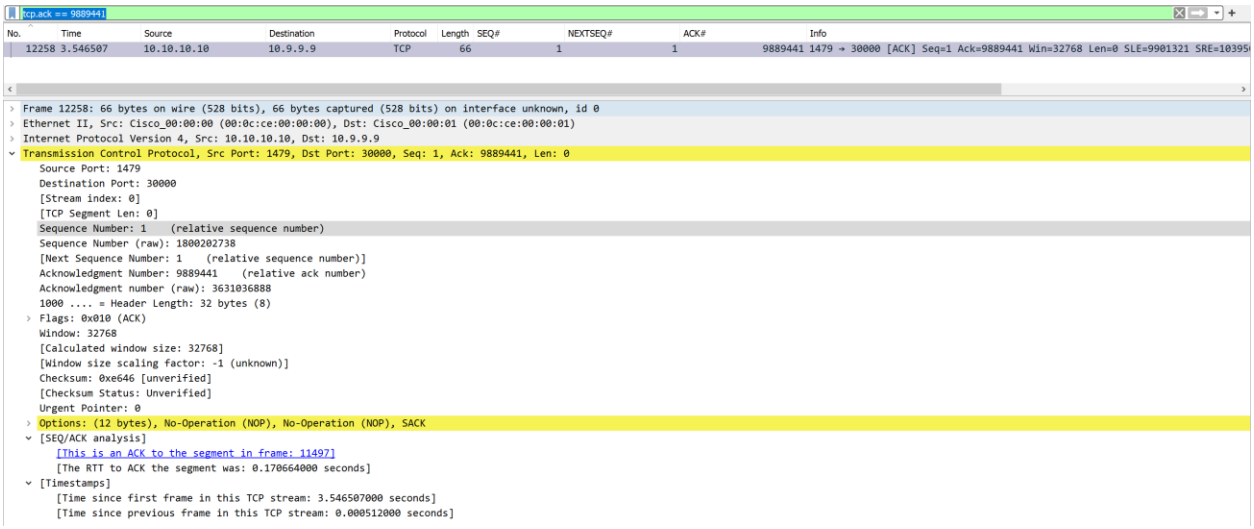
ใช้ filter “tcp.analysis.retransmission && tcp.seq == 9164761” พบว่าส่งที่ Packet 12035 ; SET REF ที่ 10416 สรุปได้ว่าส่งใหม่เมื่อเวลาผ่านไป 0.531226 วินาทีจน Packet 12257 ที่ขาดไปตัวสุดท้ายเดินทางมาถึง

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



Out of order ของ Segment 12246 โดยได้ที่รับ Sequence Number ไม่ต่อกับ Packet ก่อนหน้า

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



ใช้ filter “tcp.ack == 9889441” ซึ่งเป็นเลข Ack ของ 12259 จะพบว่า มี Packet เดียว จึงเป็น retransmission จาก RTO Timer เพราะมีการไม่มีส่ง Duplicate Ack ไป และ Packet ไม่ได้เป็น Fast retransmission