

## นายภากรณ์ ธนประชาชนนท์ 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 หายไปที่ Packet บวก วิธีการหาแบบย่อๆ

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	3.014859	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\_00:00:00:00:00:01 (00:0c:cc:00:00:01), Dst: Cisco\_00:00:00:00:00:00 (00:0c:cc: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]

[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  $10560/1320 = 8$  Packet

4. จาก segment lost ใน packet 10416 หลังจากนั้นจะพบว่ามี Duplicate Ack เกิดขึ้นเป็นจำนวนมาก หืออธิบายสาเหตุของการเกิด Duplicate Ack และเกิด Duplicate Ack ที่ครั้งในกรณี packet 10416

tcp.analysis.duplicate\_ack && tcp.ack == 9164761

Title: ACK# Type: Custom Fields: tcp.ack Occurrence: 0 OK Cancel

No.	Time	Source	Destination	Protocol	Length	SEQ#	NEXTSEQ#	ACK#	Info
11990	3.462889	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188786] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
11992	3.462957	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188787] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
11994	3.473158	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188788] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
11996	3.473228	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188789] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
11998	3.473316	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188790] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12000	3.473441	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188791] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12002	3.473467	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188792] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12004	3.473502	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188793] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12006	3.473595	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188794] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12008	3.473621	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188795] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12010	3.473646	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188796] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12012	3.473672	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188797] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12014	3.473696	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188798] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12016	3.473721	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188799] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12018	3.473745	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188800] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12020	3.474801	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188801] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12022	3.474852	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188802] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12024	3.475144	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188803] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12026	3.477786	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188804] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12028	3.477828	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188805] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12030	3.477974	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188806] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12032	3.478012	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188807] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768
12034	3.480725	10.10.10.10	10.9.9.9	TCP	74	1	1	9164761	[TCP Dup ACK 104188808] 1479 → 30000 [ACK] Seq=1 Ack=9164761 Win=32768

> Frame 12034: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface unknown, id 0  
> Ethernet II, Src: Cisco\_00:00:00 (00:0c:cc:00:00:00), Dst: Cisco\_00:00:01 (00:0c:cc:00:00:01)  
> Internet Protocol Version 4, Src: 10.10.10.10, Dst: 10.9.9.9  
v Transmission Control Protocol, Src Port: 1479, Dst Port: 30000, Seq: 1, Ack: 9164761, Len: 0  
Source Port: 1479  
Destination Port: 30000  
[Stream index: 0]  
[TCP Segment Len: 0]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 1800202738  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 9164761 (relative ack number)  
Acknowledgment number (raw): 3630312208  
1010 .... = Header Length: 40 bytes (10)  
> Flags: 0x010 (ACK)  
Window: 32768  
[Calculated window size: 32768]  
[Window size scaling factor: -1 (unknown)]  
0020 09 09 05 c7 75 30 6b 4c e9 f2 d8 62 2b 10 a0 10 .....u0Kl...b+....  
Acknowledgment Number (tcp.ack), 4 bytes Packets: 37422 · Displayed: 808 (2.2%) · Marked: 1 (0.0%) Profile: Lab07

tcp.analysis.duplicate\_ack && tcp.ack == 9166081

Title: ACK# Type: Custom Fields: tcp.ack Occurrence: 0 OK Cancel

No.	Time	Source	Destination	Protocol	Length	SEQ#	NEXTSEQ#	ACK#	Info
12039	3.481001	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#1] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12041	3.482590	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#2] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12043	3.482878	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#3] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12045	3.482944	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#4] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12047	3.485790	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#5] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12049	3.485832	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#6] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12051	3.485869	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#7] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12053	3.485951	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#8] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12055	3.488782	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#9] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12057	3.488823	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#10] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12059	3.488877	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#11] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12061	3.488947	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#12] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12063	3.490779	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#13] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12065	3.490960	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#14] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12067	3.490985	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#15] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12069	3.492792	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#16] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12071	3.492838	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#17] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12073	3.492878	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#18] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12075	3.492940	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#19] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12077	3.494784	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#20] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12079	3.494822	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#21] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12081	3.494861	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#22] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12083	3.496790	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#23] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768
12085	3.496829	10.10.10.10	10.9.9.9	TCP	74	1	1	9166081	[TCP Dup ACK 12037#24] 1479 → 30000 [ACK] Seq=1 Ack=9166081 Win=32768

> Frame 12043: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface unknown, id 0  
> Ethernet II, Src: Cisco\_00:00:00 (00:0c:cc:00:00:00), Dst: Cisco\_00:00:01 (00:0c:cc:00:00:01)  
> Internet Protocol Version 4, Src: 10.10.10.10, Dst: 10.9.9.9  
v Transmission Control Protocol, Src Port: 1479, Dst Port: 30000, Seq: 1, Ack: 9166081, Len: 0  
Source Port: 1479  
Destination Port: 30000  
[Stream index: 0]  
[TCP Segment Len: 0]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 1800202738  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 9166081 (relative ack number)  
Acknowledgment number (raw): 3630313528  
1010 .... = Header Length: 40 bytes (10)  
> Flags: 0x010 (ACK)  
Window: 32768  
[Calculated window size: 32768]  
[Window size scaling factor: -1 (unknown)]  
0020 09 09 05 c7 75 30 6b 4c e9 f2 d8 62 30 3e a0 10 .....u0Kl...b08..  
Acknowledgment Number (tcp.ack), 4 bytes Packets: 37422 · Displayed: 105 (0.3%) · Marked: 1 (0.0%) Profile: Lab07

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 ไດ ใช้เวลาเท่าใดในการส่งใหม่

tcp.analysis.retransmission && tcp.seq == 9164761									
No.	Time	Source	Destination	Protocol	Length	SEQ#	NEXTSEQ#	ACK#	Info
12035	3.480758	10.9.9.9	10.10.10.10	TCP	1374	9164761	9166081	9166081	1 [TCP Fast Retransmission] 30000 → 1479 [ACK] Seq=9164761 Ack=1 Win=46 Len=
<									
>									
Frame 12035: 1374 bytes on wire (10992 bits), 1374 bytes captured (10992 bits) on interface unknown, id 0									
Ethernet II, Src: Cisco_00:00:00:01 (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									
Transmission Control Protocol, Src Port: 30000, Dst Port: 1479, Seq: 9164761, Ack: 1, Len: 1320									
Source Port: 30000									
Destination Port: 1479									
[Stream index: 0]									
[TCP Segment Len: 1320]									
Sequence Number: 9164761 (relative sequence number)									
Sequence Number (raw): 3630312208									
[Next Sequence Number: 9166081 (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: 0xb958 [unverified]									
[Checksum Status: Unverified]									
Urgent Pointer: 0									
> [SEQ/ACK analysis]									
> [Timestamps]									
TCP payload (1320 bytes)									
Data (1320 bytes)									
Data: 204232203943204546204332203032203246203034203846203946203241204638204634..									
[Length: 1320]									

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

No.	Time	Source	Destination	Protocol	Length	SEQ#	NEXTSEQ#	ACK#	Info
4206	1.053816	10.9.9.9	10.10.10.10	TCP	1374	3698641	3699961		1 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=3698641 Ack=1 Win=46 Len=1320
12249	3.543823	10.9.9.9	10.10.10.10	TCP	1374	9167401	9168721		1 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=9167401 Ack=1 Win=46 Len=1320
12251	3.543933	10.9.9.9	10.10.10.10	TCP	1374	9168721	9170041		1 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=9168721 Ack=1 Win=46 Len=1320
12252	3.545724	10.9.9.9	10.10.10.10	TCP	1374	9170041	9171361		1 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=9170041 Ack=1 Win=46 Len=1320
12254	3.545764	10.9.9.9	10.10.10.10	TCP	1374	9171361	9172681		1 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=9171361 Ack=1 Win=46 Len=1320
12256	3.545969	10.9.9.9	10.10.10.10	TCP	1374	9172681	9174001		1 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=9172681 Ack=1 Win=46 Len=1320
12257	3.545995	10.9.9.9	10.10.10.10	TCP	1374	9174001	9175321		1 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=9174001 Ack=1 Win=46 Len=1320
32018	95.274630	10.9.9.9	10.10.10.10	TCP	1374	27500881	27502201		1 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=27500881 Ack=1 Win=46 Len=1320

< >

> Frame 4206: 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

▼ Transmission Control Protocol, Src Port: 30000, Dst Port: 1479, Seq: 3698641, Ack: 1, Len: 1320

Source Port: 30000

Destination Port: 1479

[Stream index: 0]

[TCP Segment Len: 1320]

Sequence Number: 3698641 (relative sequence number)

Sequence Number (raw): 3624846888

[Next Sequence Number: 3699961 (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: 0xd0fa [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

▼ [SEQ/ACK analysis]

[Bytes in flight: 2640]

[Bytes sent since last PSH flag: 489720]

> [TCP Analysis Flags]

▼ [Timestamps]

[Time since first frame in this TCP stream: 1.053816000 seconds]

[Time since previous frame in this TCP stream: 0.000061000 seconds]

TCP payload (1320 bytes)

0020 0a 0a 75 30 05 c7 d8 0e c3 08 6b 4c e9 f2 50 10 - u0----- l- p-  
0020 0d 7a d8 fa 0d 0d 7a d8 d3 7a d3 7a d3 7a d3 7a - ..... F r R7 d4

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

tcp.ack == 9889441									
No.	Time	Source	Destination	Protocol	Length	SEQ#	NEXTSEQ#	ACK#	Info
12258	3.546507	10.10.10.10	10.9.9.9	TCP	66	1		1	9889441 1479 → 30000 [ACK] Seq=1 Ack=9889441 Win=32768 Len=0 SLE=9901321 SRE=10395
< >									
> Frame 12258: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface unknown, id 0									
> Ethernet II, Src: Cisco_00:00:00 (00:0c:ce:00:00:00), Dst: Cisco_00:00:01 (00:0c:ce:00:00:01)									
> Internet Protocol Version 4, Src: 10.10.10.10, Dst: 10.9.9.9									
▼ Transmission Control Protocol, Src Port: 1479, Dst Port: 30000, Seq: 1, Ack: 9889441, Len: 0									
Source Port: 1479									
Destination Port: 30000									
[Stream index: 0]									
[TCP Segment Len: 0]									
Sequence Number: 1 (relative sequence number)									
Sequence Number (raw): 1800282738									
[Next Sequence Number: 1 (relative sequence number)]									
Acknowledgment Number: 9889441 (relative ack number)									
Acknowledgment number (raw): 3631036888									
1000 ..... = Header Length: 32 bytes (8)									
> Flags: 0x010 (ACK)									
Window: 32768									
[Calculated window size: 32768]									
[Window size scaling factor: -1 (unknown)]									
Checksum: 0xe646 [unverified]									
[Checksum Status: Unverified]									
Urgent Pointer: 0									
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), SACK									
▼ [SEQ/ACK analysis]									
[This is an ACK to the segment in frame: 11497]									
[The RTT to ACK the segment was: 0.170664000 seconds]									
▼ [Timestamps]									
[Time since first frame in this TCP stream: 3.546507000 seconds]									
[Time since previous frame in this TCP stream: 0.000512000 seconds]									

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