กิจกรรมที่ 8 : TCP Window

Q(2) :ให้นักศึกษาตรวจสอบ zero window ระยะที่ 2 แล้วตอบคำถาม ต่อไปนี้

เกิด window full, zero window (เฉพาะครั้งแรก) และ window update ที่ packet ใด

: เกิด window full ที่ packet 4022 เกิด zero window ที่ packet 4023 และเกิด window update ที่ packet 4036

No.	Time	Source	Destination	Protocol	Length	WinSize	Info
4021	12.316990	24.4.7.217	208.117.232.102	TCP	54	328	56770 → 80 [ACK] Seq=1270 Ack=4248122 Win=328 Len=0
4022	12.679273	208.117.232.102	24.4.7.217	TCP	382	8384	[TCP Window Full] 80 → 56770 [PSH, ACK] Seq=4248122
4023	12.889025	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1270 Ack=4248
4024	13.366647	208.117.232.102	24.4.7.217	TCP	60	8384	[TCP Keep-Alive] 80 → 56770 [ACK] Seq=4248449 Ack=1
4025	13.366693	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1270 Ack=4248
4026	14.362070	208.117.232.102	24.4.7.217	TCP	60	8384	[TCP Keep-Alive] 80 → 56770 [ACK] Seq=4248449 Ack=1
4027	14.362127	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1270 Ack=4248
4028	16.240228	208.117.232.102	24.4.7.217	TCP	60	8384	[TCP Keep-Alive] 80 → 56770 [ACK] Seq=4248449 Ack=1
4029	16.240291	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1270 Ack=4248
4030	19.945115	208.117.232.102	24.4.7.217	TCP	60	8384	[TCP Keep-Alive] 80 → 56770 [ACK] Seq=4248449 Ack=1
4031	19.945256	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1270 Ack=4248
4032	27.344112	208.117.232.102	24.4.7.217	TCP	60	8384	[TCP Keep-Alive] 80 → 56770 [ACK] Seq=4248449 Ack=1
4033	27.344212	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1270 Ack=4248
4034	37.364265	208.117.232.102	24.4.7.217	TCP	60	8384	[TCP Keep-Alive] 80 → 56770 [ACK] Seq=4248449 Ack=1
4035	37.364317	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1270 Ack=4248
4036	38.319249	24.4.7.217	208.117.232.102	TCP	54	166440	[TCP Window Update] 56770 → 80 [ACK] Seq=1270 Ack=4

หลังจากมีการทำ keep alive กี่ครั้ง มีช่วงระยะเวลาเท่าไรบ้าง นับจาก zero window ครั้งก่อน

: เกิดการทำ TCP Keep-Alive ทั้งหมด 6 ครั้ง มีระยะเวลาคือ 0.477622 , 0.995377 , 1.878101 , 3.704824 , 7.398856 และ 10.020053 วินาที ตามลำดับ

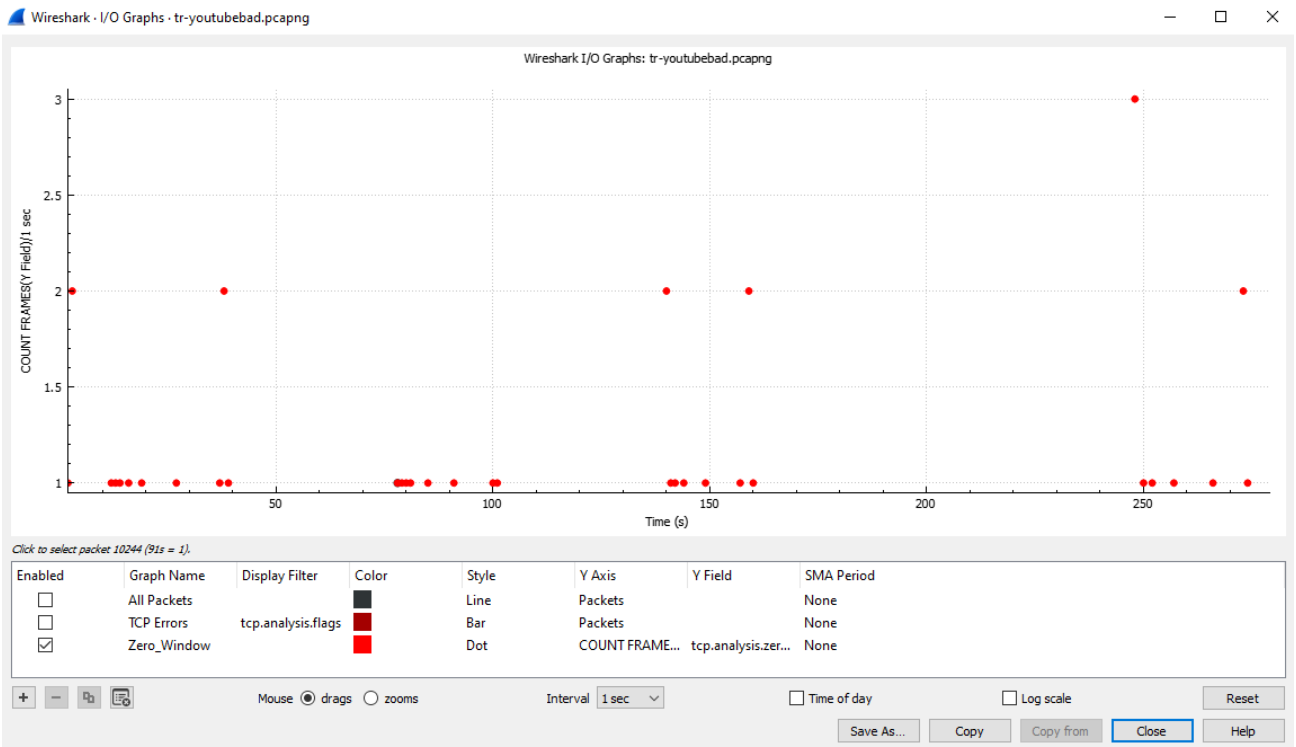
No.	Time	DeltaTime	Source	Destination	Protocol	Length	WinSize	Info
4021	12.316990	0.2006850…	24.4.7.217	208.117.232.102	TCP	54	328	56770 → 80 [ACK] Seq=1270 Ack=4248122 W
4022	12.679273	0.3622830…	208.117.232.102	24.4.7.217	TCP	382	8384	[TCP Window Full] 80 → 56770 [PSH, ACK]
4023	12.889025	0.2097520…	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1
4024	13.366647	0.4776220…	208.117.232.102	24.4.7.217	TCP	60	8384	[TCP Keep-Alive] 80 → 56770 [ACK] Seq=4
4025	13.366693	0.0000460…	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1
4026	14.362070	0.9953770…	208.117.232.102	24.4.7.217	TCP	60	8384	[TCP Keep-Alive] 80 → 56770 [ACK] Seq=4
4027	14.362127	0.0000570…	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1
4028	16.240228	1.8781010…	208.117.232.102	24.4.7.217	TCP	60	8384	[TCP Keep-Alive] 80 → 56770 [ACK] Seq=4
4029	16.240291	0.0000630…	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1
4030	19.945115	3.7048240…	208.117.232.102	24.4.7.217	TCP	60	8384	[TCP Keep-Alive] 80 → 56770 [ACK] Seq=4
4031	19.945256	0.0001410…	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1
4032	27.344112	7.3988560…	208.117.232.102	24.4.7.217	TCP	60	8384	[TCP Keep-Alive] 80 → 56770 [ACK] Seq=4
4033	27.344212	0.0001000…	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1
4034	37.364265	10.020053…	208.117.232.102	24.4.7.217	TCP	60	8384	[TCP Keep-Alive] 80 → 56770 [ACK] Seq=4
4035	37.364317	0.0000520…	24.4.7.217	208.117.232.102	TCP	54	0	[TCP ZeroWindow] 56770 → 80 [ACK] Seq=1
4036	38.319249	0.9549320…	24.4.7.217	208.117.232.102	TCP	54	166440	[TCP Window Update] 56770 → 80 [ACK] Se

ระยะเวลาตั้งแต่เกิด zero window ครั้งแรกจนถึง window update ใช้เวลาเท่าไร

: เกิด Zero Window ครั้งแรกที่ packet 4023 ที่เวลา 12.889025 วินาทีและเกิด Window Update ที่ packet 4036 ที่เวลา 38.319249 วินาที ดังนั้นเราจะได้ระยะเวลาตั้งแต่เกิด Zero Window จนถึง Window Update เท่ากับ 38.319249 – 12.889025 = 25.430224 วินาที

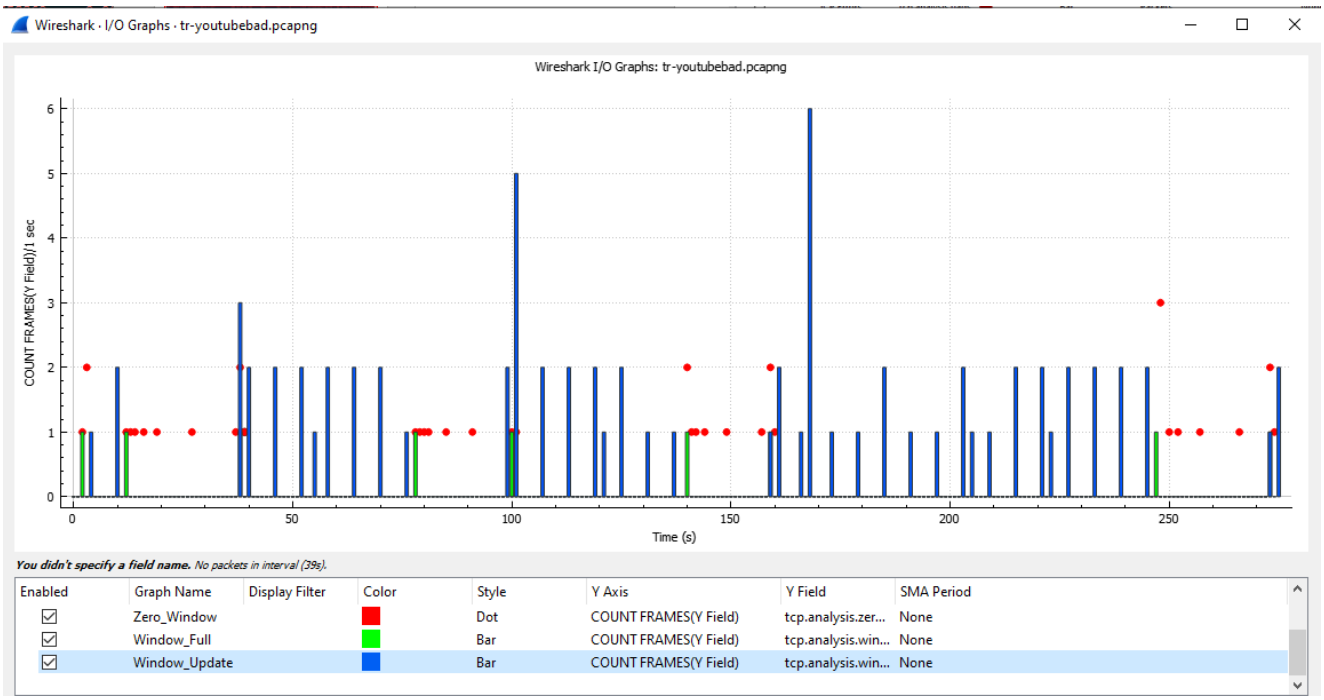
Q(3) : จากการวิเคราะห์ข้อมูลจาก Statistics I/O Graph กราฟบอกข้อมูลอะไร

A(3) : จากกราฟที่ได้เป็นการบอกข้อมูลจำนวนครั้งที่เกิด Zero Window อยู่ในแนวแกน Y และเทียบกับเวลาในแนวแกน X



Q(4) : ให้สร้างกราฟเพิ่มอีก 2 กราฟ ดังนี้

- ชื่อ Window_Full โดยใน Y(AXIS) ใช้ COUNT FRAMES(Y Field) และช่อง Y Field ใช้ tcp.analysis.window_full กำหนดประเภทเป็น Bar สีเขียว
- ชื่อ Window_Update โดยใน Y(AXIS) ใช้ COUNT FRAMES(*) และช่อง Y Field ใช้ tcp.analysis.window_update กำหนดประเภทเป็น Bar สีน้ำเงิน

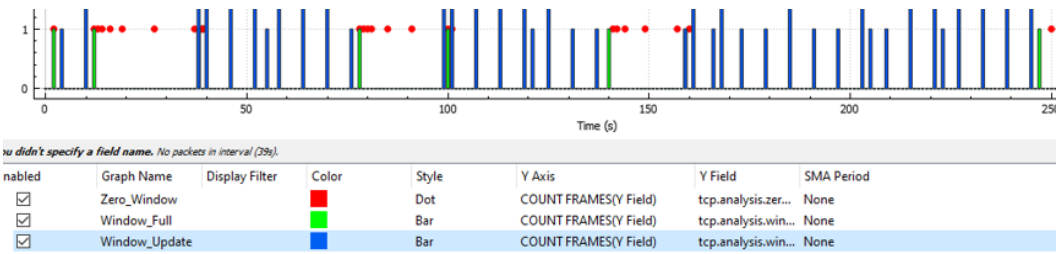


Q(4.1) : กราฟแสดงอะไร

A(4.1) : จากกราฟ bar สีเขียว แสดงจำนวนครั้งที่พบการเกิด window full (แกน Y) โดยเทียบกับเวลา (แกน X) และ จากกราฟ bar สีน้ำเงิน แสดงจำนวนครั้งที่พบการเกิด window update (แกน Y) โดยเทียบกับเวลา (แกน X)

Q(4.2) : จากกราฟสามารถบอกได้หรือไม่ว่ามี window full กี่ครั้ง ให้ Capture รูปประกอบด้วย

A(4.2) : สามารถบอกได้จากกราฟ bar สีเขียว ที่เกิดขึ้นบนกราฟจำนวน 6 ครั้ง แสดงถึงการเกิด window full



u didn't specify a field name. No packets in interval (39s).

nabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	Zero_Window			Dot	COUNT FRAMES(Y Field)	tcp.analysis.zer...	None
☑	Window_Full			Bar	COUNT FRAMES(Y Field)	tcp.analysis.win...	None
☑	Window_Update			Bar	COUNT FRAMES(Y Field)	tcp.analysis.win...	None

Q(5) : ให้สร้าง I/O Graph ใหม่ดังนี้

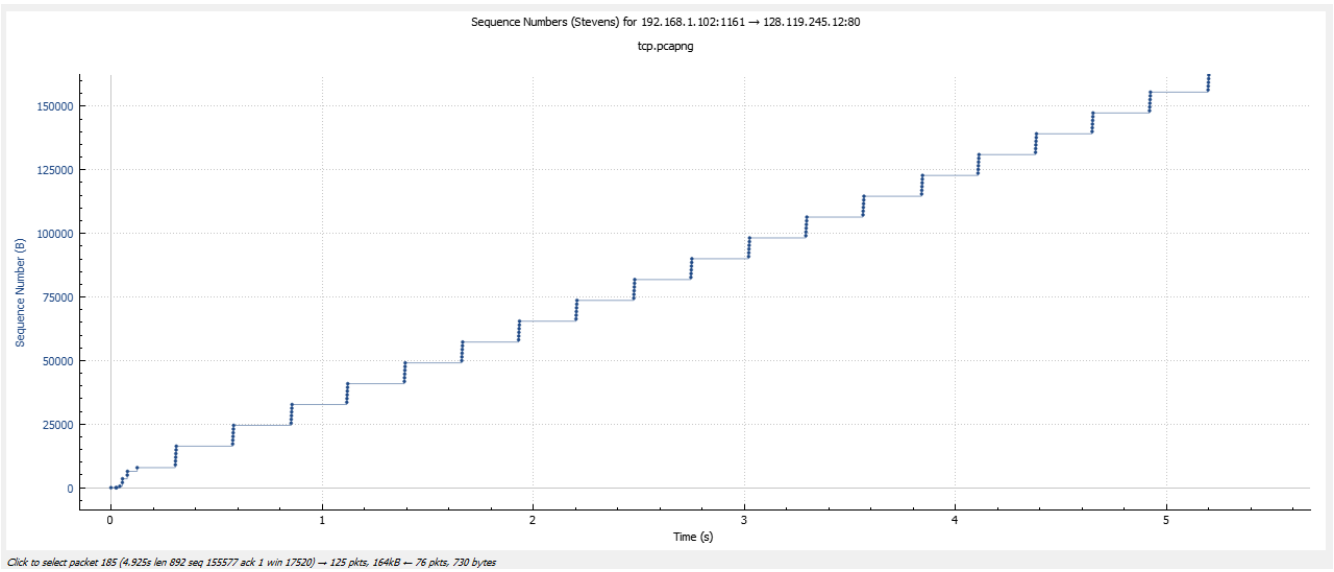
โดยในช่อง Display Filter ให้ใส่ ip.src==24.4.7.217 ใน Y(AXIS) ใช้ AVG(*) และช่อง Y Field ใช้ tcp.window_size กำหนดประเภทเป็น Line ให้ capture รูป และ อธิบายว่าเราสามารถวิเคราะห์ข้อมูลอะไรจากกราฟนี้

You didn't specify a field name. Click to select packet 14391 (121s = 6.047e+04).

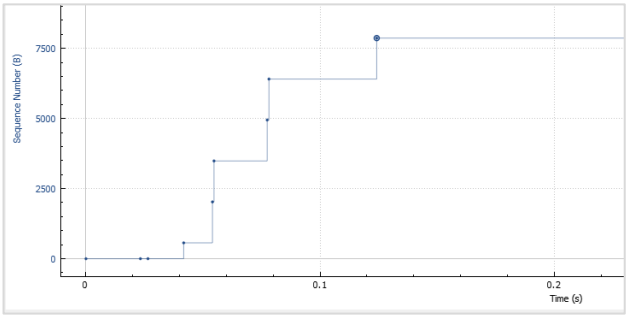
Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	Window_Full			Bar	COUNT FRAMES(Y Field)	tcp.analysis.win...	None
☑	Window_Update			Bar	COUNT FRAMES(Y Field)	tcp.analysis.win...	None
☑	AVG_Window_S...	ip.src == 24.4.7.217		Line	AVG(Y Field)	tcp.window_size	None

A(5) : จากกราฟที่ได้เป็นการบอกข้อมูลจำนวนค่าเฉลี่ยของขนาด window หรือ window size ของ packet ที่เกิดจาก src ip คือ 24.4.7.217 อยู่ในแนวแกน Y และเทียบกับเวลาในแนวแกน X สามารถนำมาใช้วิเคราะห์ความสามารถของการรับ-ส่ง ข้อมูลระหว่าง send window และ receive window ได้

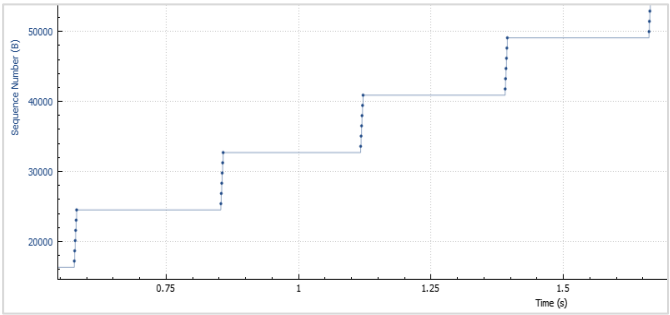
Q(6) :ในการควบคุม congestion control ของ TCP จะมีหลักอยู่ 2 ข้อ คือ Slow Start และ Congestion Avoidance ให้เปิดไฟล์ tcp.pcapng แล้วดูที่ Statistics->TCP Stream Graph-> Time-Sequence-Graph(Stevens) โดยแต่ละจุดแสดงถึงการส่งในแต่ละ segment ร่วมกับ Statistics-> Flow Graph นักศึกษาสามารถบอกได้หรือไม่ว่า Slow Start เริ่มต้นและสิ้นสุดที่ใดและมี Congestion Avoidance เกิดขึ้นหรือไม่



เป็นกราฟที่ทำการ Switch Direction โดยจากกราฟในไฟล์ tcp.pcapng เราสามารถเห็นกระบวนการของ Slow Start และ Congestion Avoidance ได้ ดังนี้

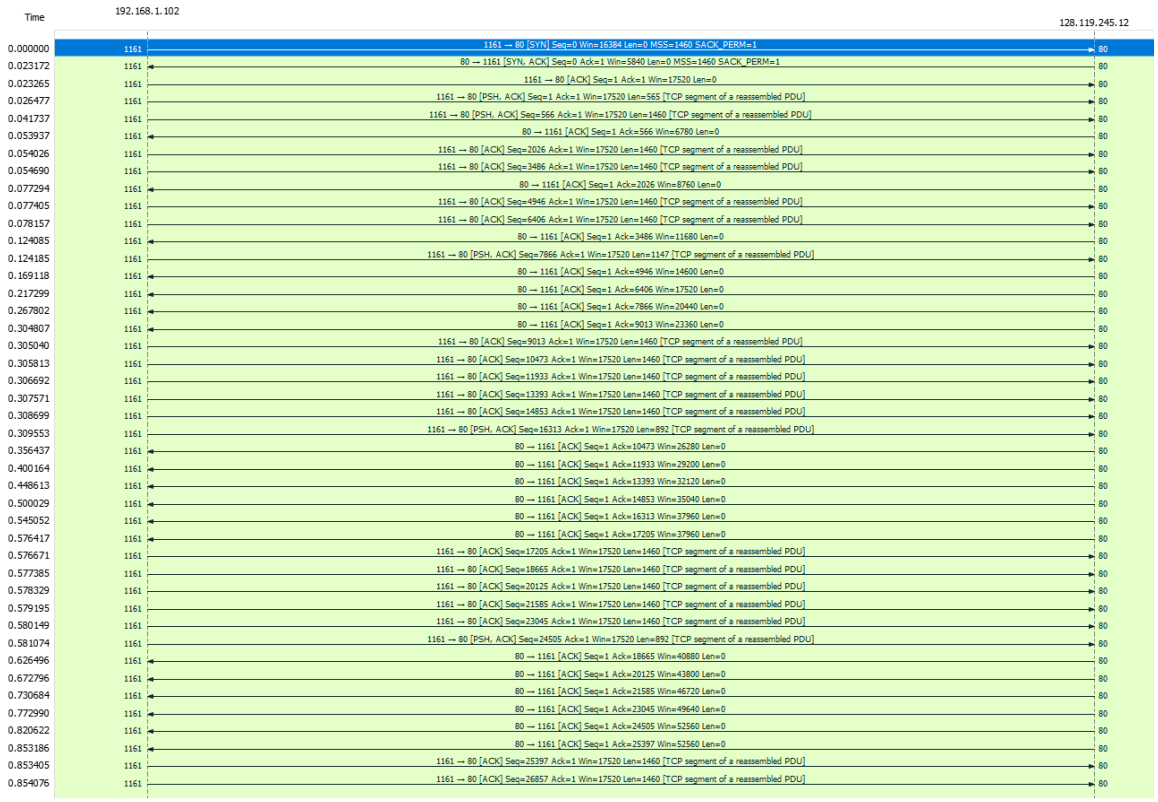


กราฟแสดงการเกิด **Slow Start** จะสังเกตุเห็นได้จากค่าของ sequence Number ที่มีค่าเพิ่มขึ้นแบบ exponential (เช่น 1 , 2 , 4 , 8 , 16 , ...)



กราฟแสดงการเกิด **Congestion Avoidance** จะสังเกตุเห็นได้จากค่าของ sequence Number ที่มีค่าเพิ่มขึ้นแบบอย่างคงที่ หรือแบบ Linear (เช่น +1, +2, +3 , ...)

เป็นกราฟที่ได้จาก Flow Graph ซึ่งหากเรานำมาวิเคราะห์อาจใช้ parameter “Win” ที่มาจาก Window Size มาหาช่วงต่างๆ ได้ เช่น ในช่วงแรก win มีการเพิ่มขึ้นอย่างต่อเนื่อง เช่น 6780 -> 8760 -> 11680 -> ... -> 62780 อาจแสดงถึงช่วง Slow Start ได้



ส่วนต่อมาค่า win มีการเพิ่มขึ้นแบบค่าคงที่ที่ 62780 ก็อาจวิเคราะห์ได้ว่าช่วงนี้เป็น Congestion Avoidance