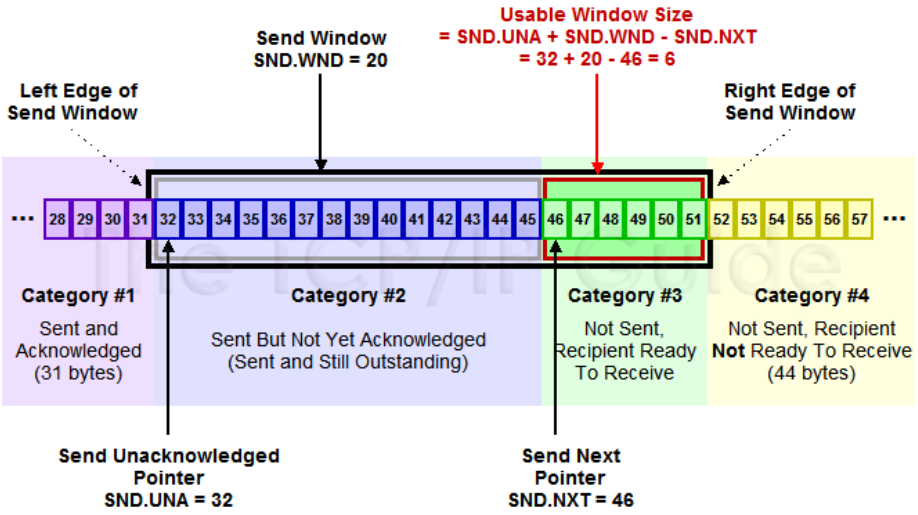
กิจกรรมที่ 8 : TCP Window

กิจกรรมครั้งนี้จะเป็นการทำความเข้าใจกับโปรโตคอล TCP (Transmission Control Protocol) ให้มากยิ่งขึ้น โดยเน้นเรื่องของ TCP Window โดย TCP Window จะแบ่งออกเป็น send Window และ receive Window

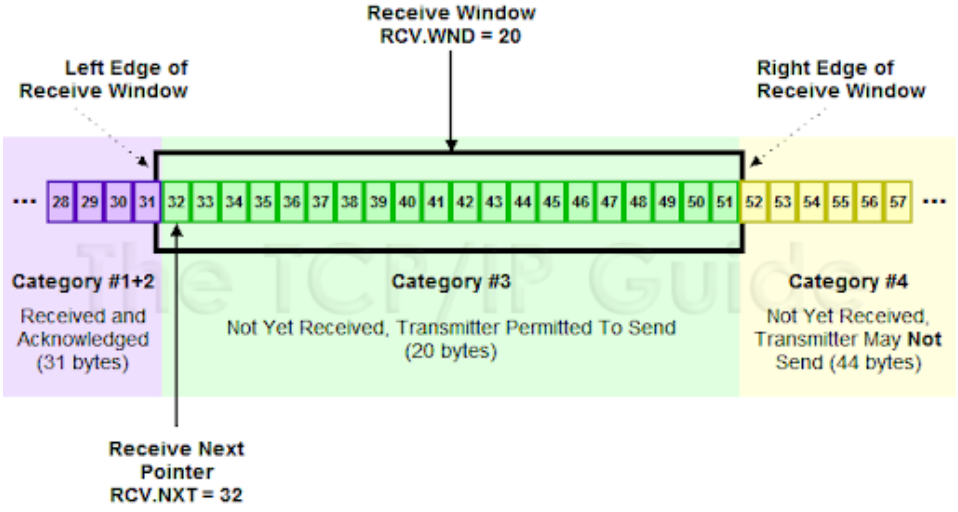
ใน send window จะแบ่งออกเป็น 4 ส่วน คือ

- ข้อมูลที่ส่งแล้วและได้รับ Acknowledge ไปแล้ว
- ข้อมูลที่ส่งไปแล้วแต่ยังไม่ได้รับ Acknowledge (ใน Wireshark จะเรียกว่า byte in flight)
- ข้อมูลที่ยังไม่ได้ส่ง และ ฝั่งรับสามารถรับได้ (ตามขนาดของ receive window)
- ข้อมูลที่ยังไม่ได้ส่ง และ ฝั่งรับไม่พร้อมจะรับเนื่องจากขนาดของ receive window

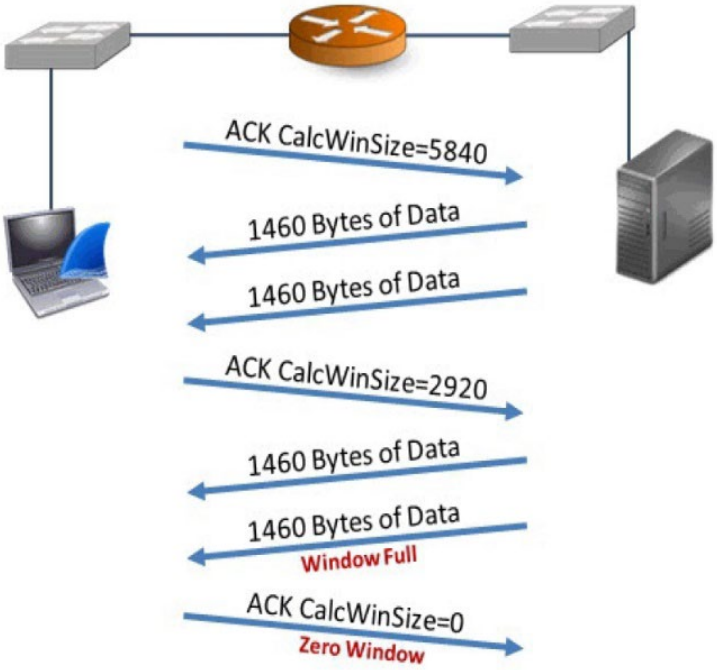


ใน receive window จะแบ่งเป็น 2 ส่วน

- ข้อมูลที่รับแล้วและ Acknowledge ไปแล้ว
- ข้อมูลพร้อมจะรับ



ในระหว่างการสื่อสารทั้ง 2 ด้านจะมีการแจ้งขนาดของ window size ที่เหลือที่ยังรับข้อมูลได้มาใน header ของ TCP โดยมีขนาด 2 ไบต์ โดยมีค่าสูงสุด คือ 65,535 ไบต์ โดยมี Scaling Factor เป็นตัวคูณ ซึ่งหากฝั่งรับไม่สามารถนำข้อมูลออกจาก receive window ได้เร็วพอจะทำให้ Buffer เต็มและเกิด zero window ตามรูป (หมายเหตุข้อมูล window full และ zero window นี้เป็นข้อมูลที่ wireshark สร้างขึ้น เพื่อให้สะดวกต่อการใช้งาน)



1. ให้เปิดไฟล์ tr-youtubebad.pcapng จากนั้นให้ค้นหาเหตุการณ์ zero window โดยใช้ display filter tcp.analysis.zero_window จะเห็นว่ามี zero window เกิดขึ้นจำนวนมาก ให้เลือกบรรทัดแรก แล้วยกเลิก filter โปรแกรม wireshark จะแสดงบริเวณ packet ที่เกิด zero window ครั้งแรก ให้ขยาย TCP หาฟิลด์ calculated window size แล้วสร้างเป็นคอลัมน์ โดยกำหนดให้ Align Center และตั้งชื่อเป็น **WinSize**
   - ให้สังเกตที่ packet 2718 ซึ่งเป็น packet ที่ host 24.4.7.217 ส่ง ACK กลับมา โดยมี window size เหลือเพียง 1,460 ไบต์
   - ต่อมาใน packet 2719 host 208.117.232.102 มีการส่งข้อมูลไปอีก 1,460 ไบต์ ซึ่งจะทำให้เต็ม receive window พอดี และทำให้ wireshark สร้างข้อมูลแจ้งเตือนว่า window full
   - เมื่อถึง Packet 2720 host 24.4.7.217 ก็ส่ง Packet ACK กลับมา โดยมีค่า window size เป็น 0 ทำให้ wireshark สร้างข้อมูลแจ้งเตือนว่า zero window
   - ให้สังเกตช่วงเวลาระหว่าง packet 2720 และ 2721 จะเห็นว่ามีระยะห่างมากกว่าปกติ หมายความว่าฝั่งผู้ส่งเมื่อพบ zero window ก็จะรอฝั่งผู้รับให้เคลียร์ receive window เสียก่อน
   - ใน packet 2721 จะมีการส่ง packet keep alive (คือ packet ACK ที่ไม่มีข้อมูล จากฝั่งผู้ส่ง ซึ่งจะเกิดขึ้นเมื่อ keepalive timer expire)
   - จากนั้นใน packet 2722 ผู้รับจะส่ง ACK กลับมา โดยมี window size เป็น 0 เช่นเดิม และเกิดซ้ำอีกครั้งใน packet 2723 และ 2724

- จนกระทั่ง packet 2725 ฝั่งผู้รับจึงส่ง packet ACK ซึ่งมีขนาดของ window size = 243820 ซึ่งไม่เท่ากับ 0 ซึ่งหมายความว่า receive window ของฝั่งผู้รับว่างแล้ว พร้อมรับข้อมูลใหม่ ณ จุดนี้ ถือว่าเหตุการณ์ zero window สิ้นสุดลง โดย wireshark จะสร้างข้อมูลแจ้งเตือน window update

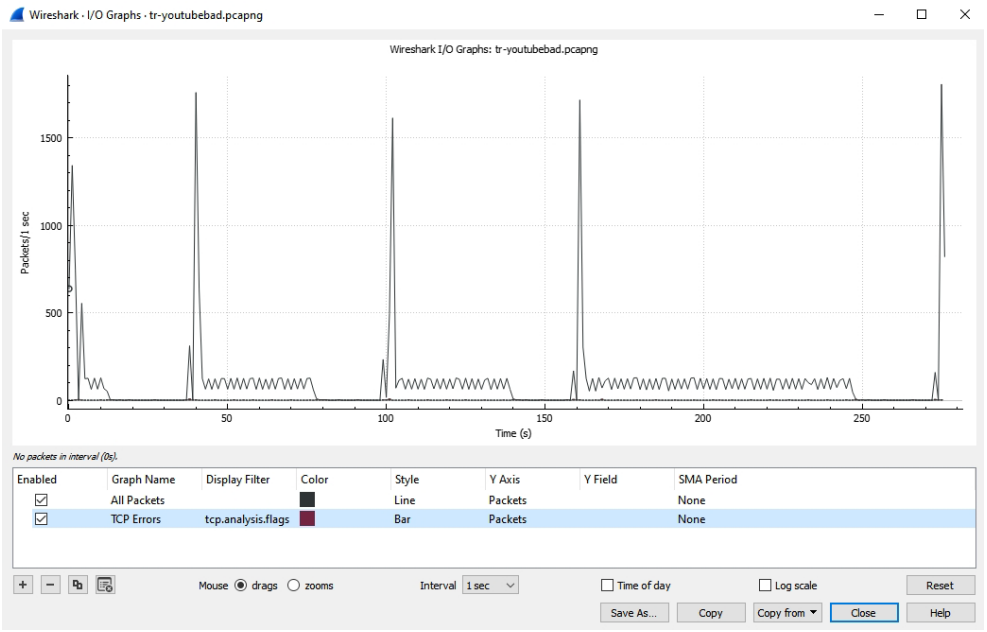
2. ให้นักศึกษาตรวจสอบ zero window ระยะที่ 2 แล้วตอบคำถาม ต่อไปนี้
   - เกิด window full, zero window (เฉพาะครั้งแรก) และ window update ที่ packet ใด
     - window full 4022
     - zero window 4023
     - window update 4036
   - หลังจากมีการทำ keep alive กี่ครั้ง มีช่วงระยะเวลาเท่าไรบ้าง นับจาก zero window ครั้งก่อน
     - ทั้งหมด 7 ครั้งตามภาพ โดยมีเวลา 0.47, 0.99, 1.87, 3.70, 7.39, 10.0 ซึ่งมากขึ้นตามลำดับ

	Time	Source	Destination	Protocol	Info
4020	12.116305	208.117.232.102	24.4.7.217	TCP	80 → 56770 [ACK] Seq
4021	12.316990	24.4.7.217	208.117.232.102	TCP	56770 → 80 [ACK] Seq
4022	12.679273	208.117.232.102	24.4.7.217	TCP	[TCP Window Full] 80
4023	*REF*	24.4.7.217	208.117.232.102	TCP	[TCP ZeroWindow] 567
4024	0.477622	208.117.232.102	24.4.7.217	TCP	[TCP Keep-Alive] 80
4025	*REF*	24.4.7.217	208.117.232.102	TCP	[TCP ZeroWindow] 567
4026	0.995377	208.117.232.102	24.4.7.217	TCP	[TCP Keep-Alive] 80
4027	*REF*	24.4.7.217	208.117.232.102	TCP	[TCP ZeroWindow] 567
4028	1.878101	208.117.232.102	24.4.7.217	TCP	[TCP Keep-Alive] 80
4029	*REF*	24.4.7.217	208.117.232.102	TCP	[TCP ZeroWindow] 567
4030	3.704824	208.117.232.102	24.4.7.217	TCP	[TCP Keep-Alive] 80
4031	*REF*	24.4.7.217	208.117.232.102	TCP	[TCP ZeroWindow] 567
4032	7.398856	208.117.232.102	24.4.7.217	TCP	[TCP Keep-Alive] 80
4033	*REF*	24.4.7.217	208.117.232.102	TCP	[TCP ZeroWindow] 567
4034	10.020053	208.117.232.102	24.4.7.217	TCP	[TCP Keep-Alive] 80
4035	*REF*	24.4.7.217	208.117.232.102	TCP	[TCP ZeroWindow] 567
4036	0.954932	24.4.7.217	208.117.232.102	TCP	[TCP Window Update]

   - ระยะเวลาตั้งแต่เกิด zero window ครั้งแรกจนถึง window update ใช้เวลาเท่าไร

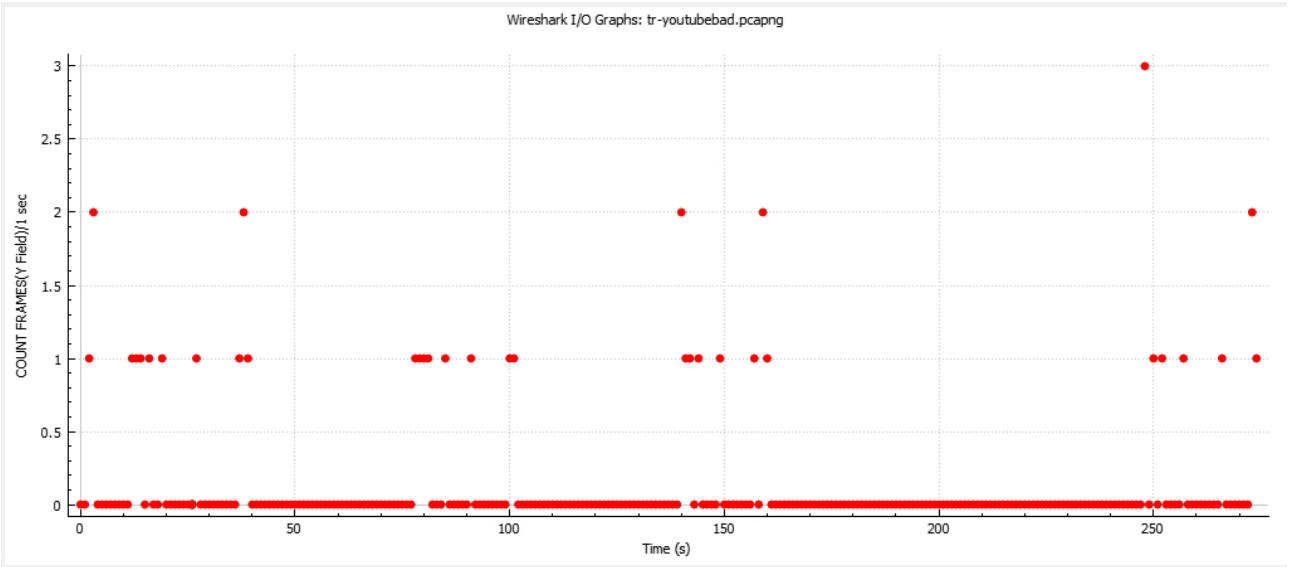
     25.43 วินาที

3. การวิเคราะห์ข้อมูลนอกจากจะทำในหน้าต่าง Packet List และ Packet Detail แล้ว ใน wireshark ยังให้เครื่องมือประเภทกราฟมาด้วย จากไฟล์เดิม ให้นักศึกษาเรียกเมนู Statistics | I/O Graph จะปรากฏหน้าจอดังนี้



- ข้อมูลแกน Y คือ packet/sec แกน x คือเวลา ซึ่งจะเห็นว่าข้อมูลมีการส่งได้ดี (กราฟพุ่งสูง จำนวน 5 ครั้ง) จากนั้นก็ลดลงอย่างมาก
- ในช่องด้านล่าง เราสามารถสร้างกราฟขึ้นมาใหม่ได้ ให้กด + แล้วกำหนดข้อมูลดังนี้
  - Graph Name : Zero_Window
  - Display filter : ว่าง
  - Color : แดง
  - Style : Dot
  - Y Axis : COUNT FRAMES(Y Field)
  - Y Field : tcp.analysis.zero_window
- ให้ Disable กราฟเดิมทั้ง 2 กราฟ
- กราฟบอกข้อมูลอะไร

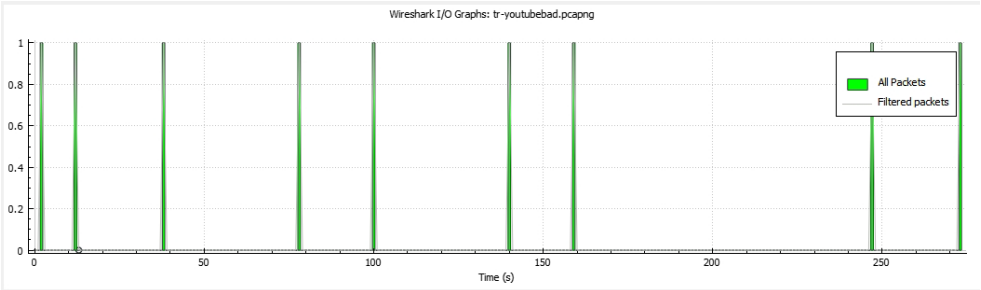
  บอกจำนวนครั้งของการเกิด zero window ต่อวินาที



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
   - กราฟแสดงอะไร

     แสดงการเกิด zero window, window full และ window update ซึ่งจะเห็นได้ว่าเมื่อเกิด window full ก็จะตามด้วยการเกิด zero window และเหตุการณ์จะจบลงเมื่อมี window update

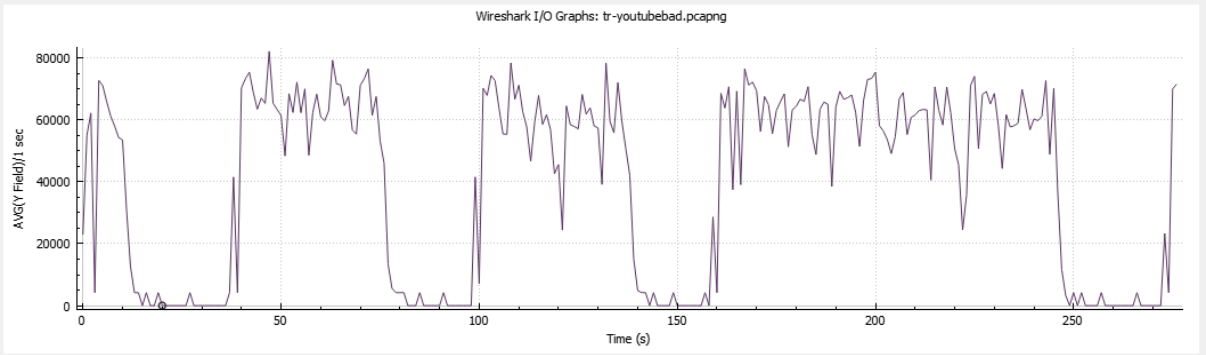
   - จากกราฟสามารถบอกได้หรือไม่ว่ามี window full กี่ครั้ง ให้ Capture รูปประกอบด้วย



     ดูจากกราฟแท่งสีเขียวพบว่ามี 9 ครั้ง

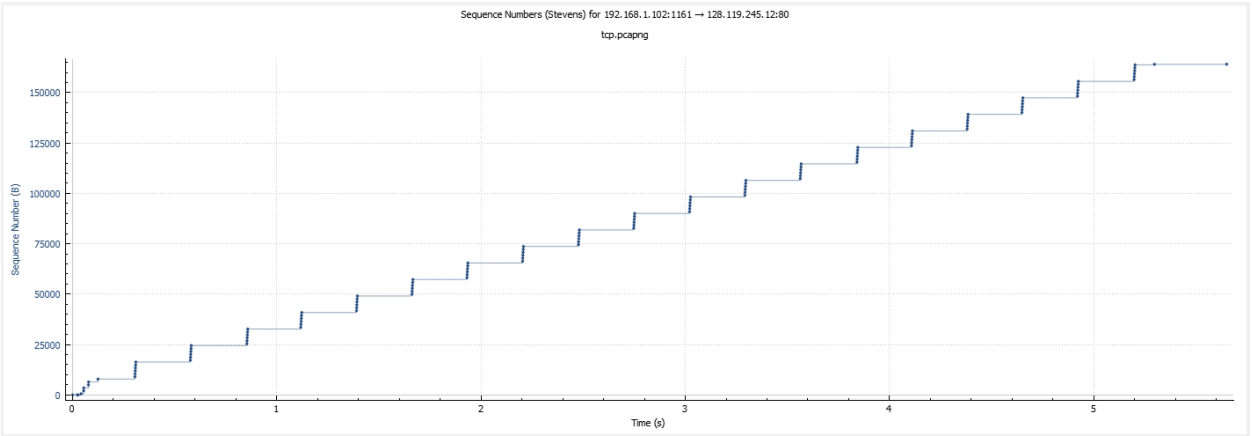
5. ให้สร้าง I/O Graph ใหม่ โดยในช่อง Display Filter ให้ใส่ ip.src==24.4.7.217 ใน Y(AXIS) ใช้ AVG(*) และช่อง Y Field ใช้ tcp.window_size กำหนดประเภทเป็น Line ให้ capture รูป และ อธิบายว่าเราสามารถวิเคราะห์ข้อมูลอะไรจากกราฟนี้

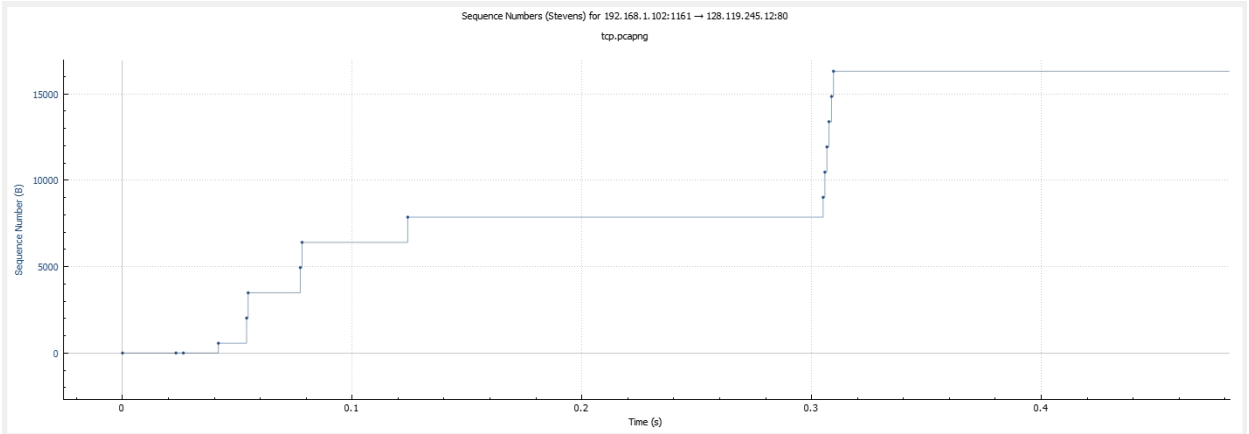
จะเห็นว่ามีปัญหาเกิดขึ้นเกี่ยวกับ window size เป็น 0 โดยพิจารณาคร่าวๆ เกิดปัญหา 4 ครั้ง



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 เริ่มต้นและสิ้นสุดที่ใด และมี Congestion Avoidance เกิดขึ้นหรือไม่

จากภาพรวมจะเห็นว่าช่วงแรกๆ จะมีการทำ slow start และเมื่อขยายเป็นภาพล่าง จะเห็นว่าช่วง slow start เริ่มต้นที่ 0 และสิ้นสุดที่ ประมาณ 0.3 – 0.4 วินาที





สำหรับประเด็นที่ว่า มี Congestion Avoidance หรือไม่นั้น จะเห็นได้ว่าหลังจากที่ส่งครั้งละ 6 Segment แล้ว ผู้ส่งก็รักษาระดับการส่งไว้ที่ 6 Segment ไปตลอด ไม่ได้มีการเพิ่มขึ้นอีก จึงถือว่ามีการใช้ Congestion Avoidance แล้ว