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 และ เกิด window update ที่ packet 4036

- หลังจากมีการทำ keep alive กี่ครั้ง มีช่วงระยะเวลาเท่าไรบ้าง นับจาก zero window ครั้งก่อน

มี keep alive 6 ครั้ง

ครั้งที่ 1 ห่างกัน 0.477622 วินาที

ครั้งที่ 2 ห่างกัน 0.995377 วินาที

ครั้งที่ 3 ห่างกัน 1.878101 วินาที

ครั้งที่ 4 ห่างกัน 3.704824 วินาที

ครั้งที่ 5 ห่างกัน 7.398856 วินาที

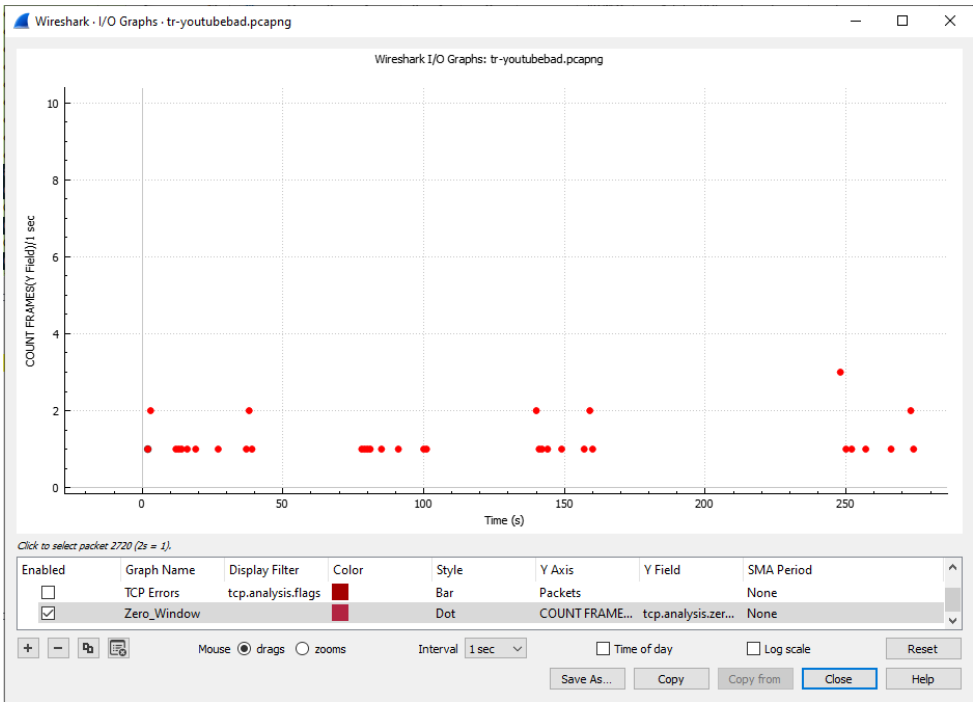
ครั้งที่ 6 ห่างกัน 10.020053 วินาที

โดยช่วงระยะเวลาของ keep alive ในครั้งถัดไป จะเป็น 2 เท่าของครั้งก่อนหน้า

- ระยะเวลาตั้งแต่เกิด zero window ครั้งแรกจนถึง window update ใช้เวลาเท่าไร

ใช้เวลา 25.430224 วินาที

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

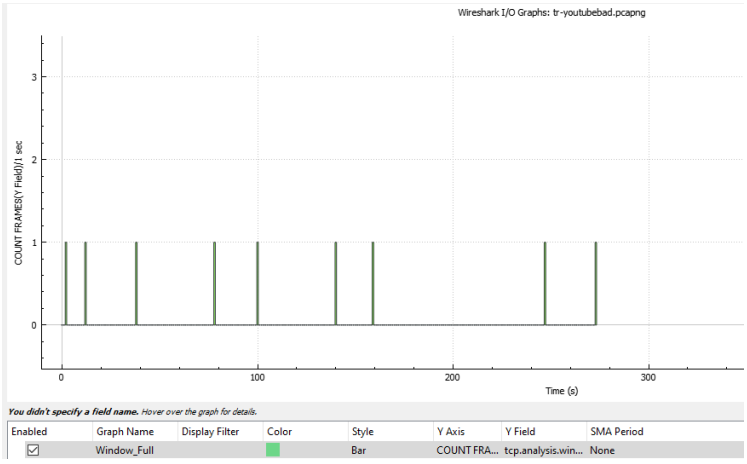


- กราฟบอกข้อมูลอะไร

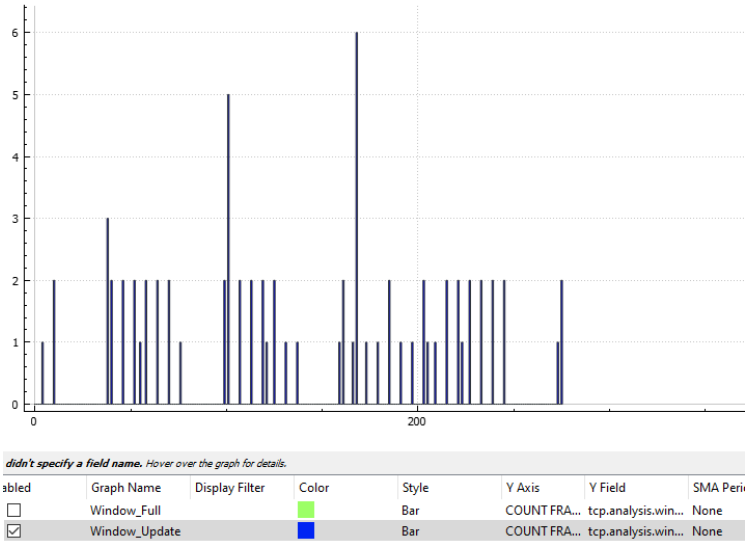
กราฟจะบอกข้อมูลว่าใน 1 วินาที เกิด zero window กี่ครั้ง โดยเมื่อคลิกไปที่จุดสีแดง ในหน้าหลักมันก็จะวิ่งไปที่ packet นั้น ทำเราสามารถหาเหตุการณ์ที่ผิดปกติได้ง่าย

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

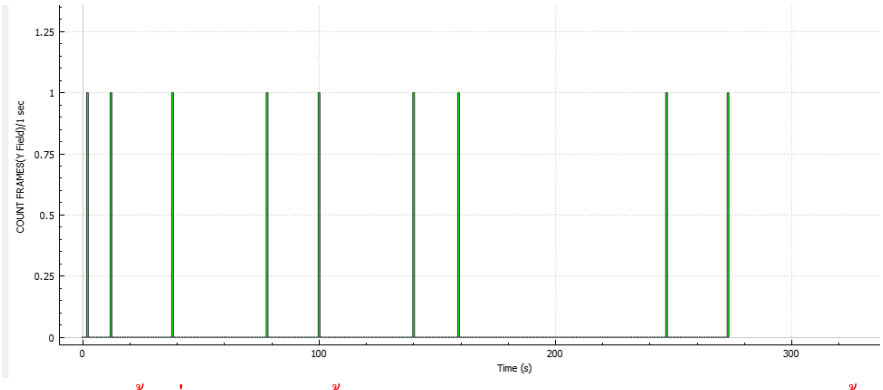


- กราฟแสดงอะไร

กราฟ Window_Full จะแสดง ว่าใน 1 วินาทีเกิด window full กี่ครั้ง

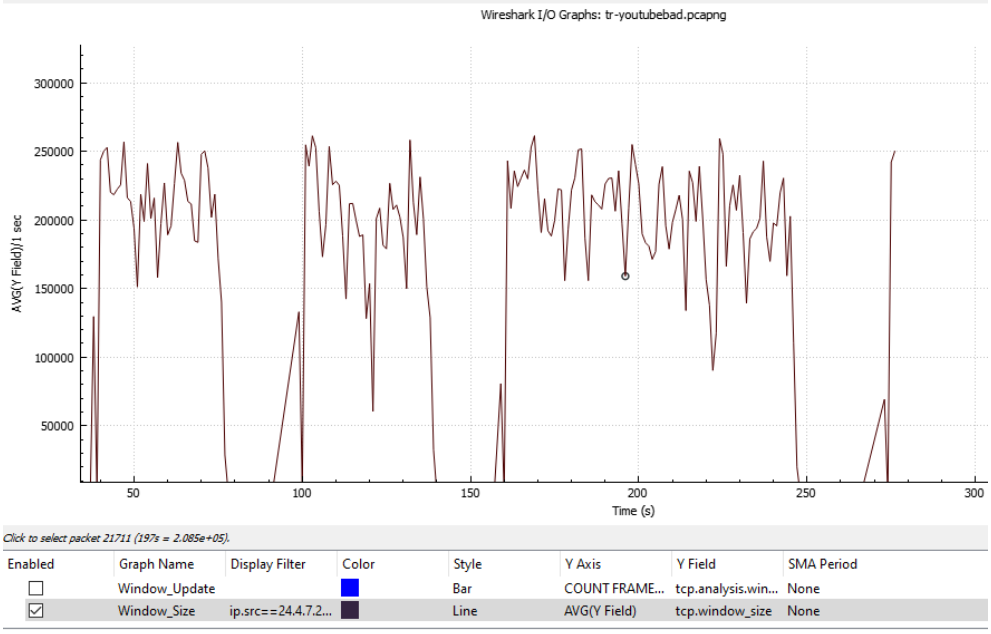
กราฟ Window _Update จะแสดง ว่าใน 1 วินาทีเกิด window update กี่ครั้ง

- จากกราฟสามารถบอกได้หรือไม่ว่ามี window full กี่ครั้ง ให้ Capture รูปประกอบด้วย



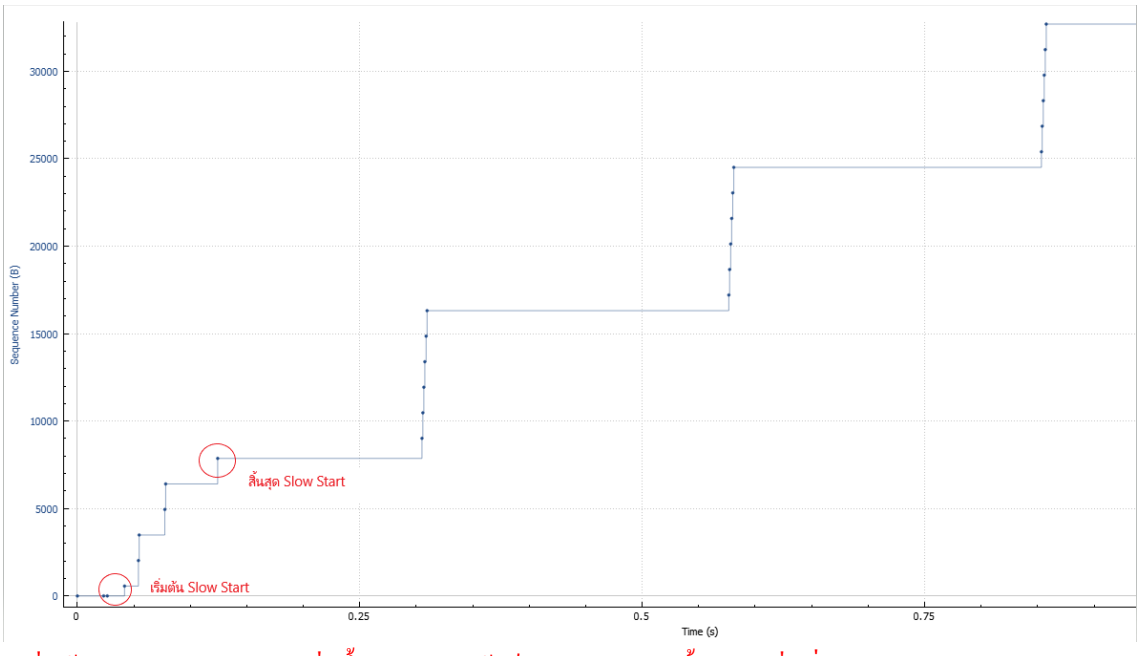
จากกราฟมี window full 9 ครั้ง เนื่องจากกราฟมีทั้งหมด 9 แท่ง และในแต่ละแท่งเกิด window full 1 ครั้ง

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



จากกราฟ เราจะรู้ข้อมูล window size ของ ip:24.4.7.127 ในแต่ละช่วงเวลาว่ามี window size เท่าใด และเมื่อรับข้อมูลจน window เต็มก็จะเกิด window full คือ window size = 0

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



โดยเริ่มต้น Slow Star Segment เพิ่มขึ้นจากก่อนหน้าเป็น 2 เท่า และจุดสิ้นสุดจะเริ่มที่ 1 ใหม่

ไม่มี Congestion Avoidance เกิดขึ้นเนื่องจากหลังจากสิ้นสุด Slow Start Segment ที่ส่งมาจะคงที่ตลอด