นายภากรณ์ ธนประชานนท์ 62010694

2. ให้นักศึกษาตรวจสอบ zero window ระยะที่ 2 แล้วตอบคำถาม ต่อไปนี้

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

4022,4023,4036

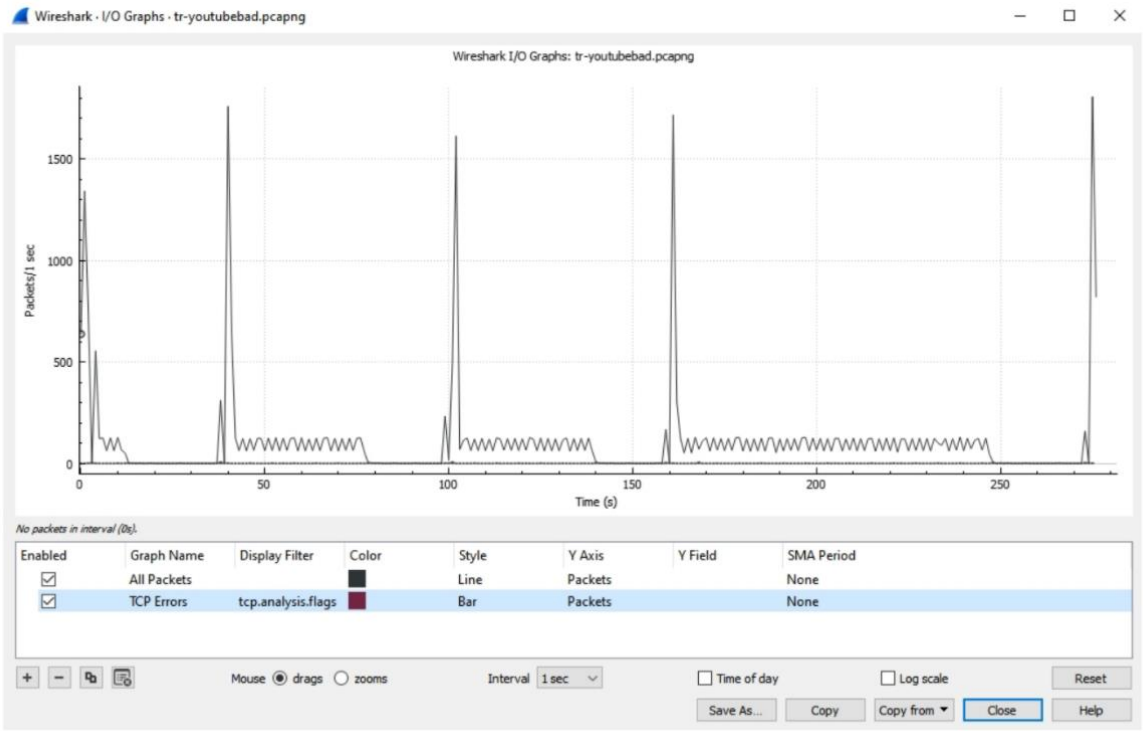
   - หลังจากมีการทำ keep alive กี่ครั้ง มีช่วงระยะเวลาเท่าไรบ้าง นับจาก zero window ครั้งก่อน

Keep Alive 6 ครั้ง 0.477622,0.995377,1.878101,3.704824,7.398856,10.020053 sec

   - ระยะเวลาตั้งแต่เกิด zero window ครั้งแรกจนถึง window update ใช้เวลาเท่าไร

25.430224 sec

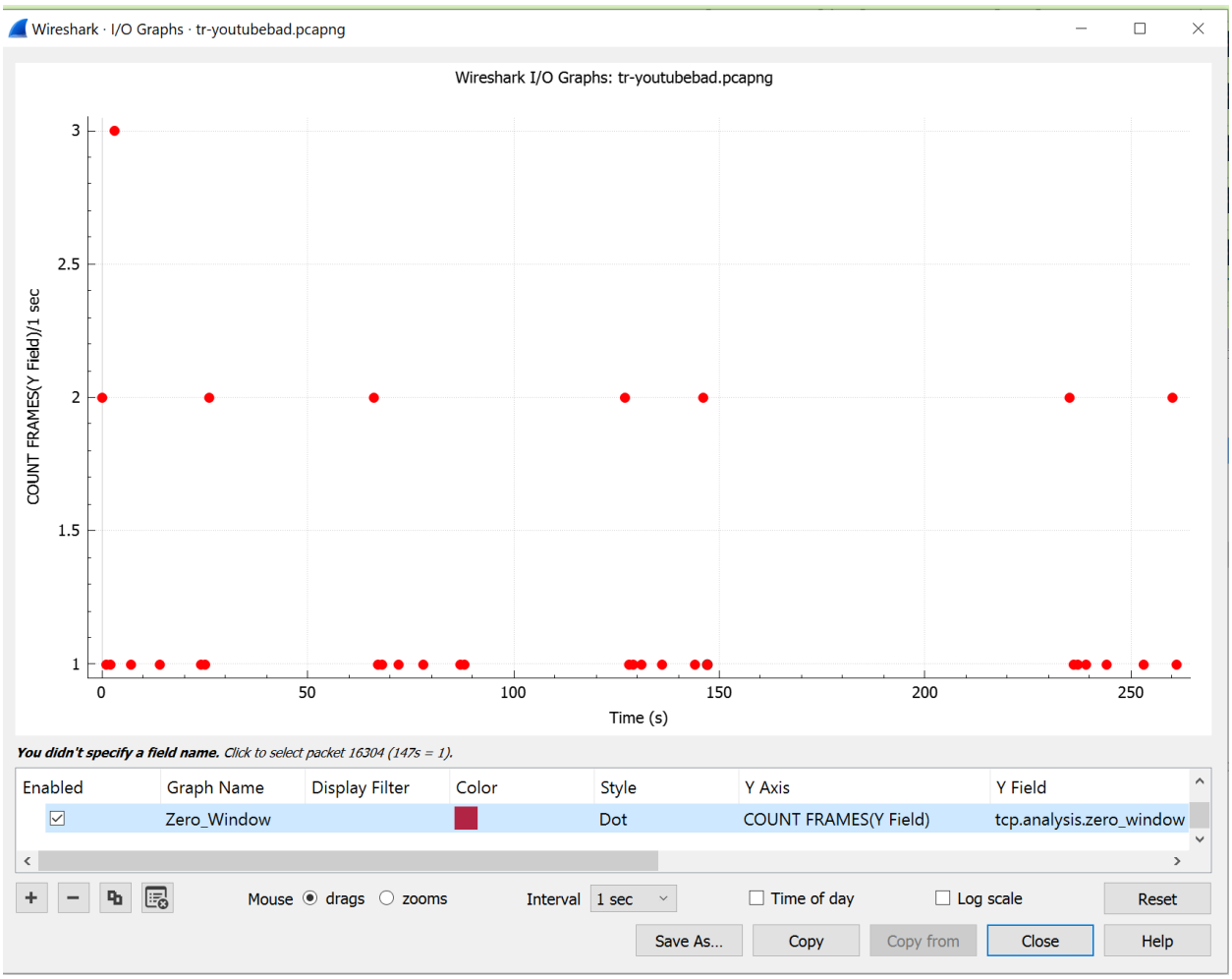
3. การวิเคราะห์ข้อมูลนอกจากจะทำในหน้าต่าง Packet List และ Packet Detail แล้ว ใน wireshark ยังให้เครื่องมือประเภทกราฟมาด้วย จากไฟล์เดิม ให้นักศึกษาเรียกเมนู Statistics I I/O Graph จะปรากฏหน้าจอดังนี้



- ข้อมูลแกน Y คือ packet/sec แกน x คือเวลา ซึ่งจะเห็นว่าข้อมูลมีการส่งได้ดี (กราฟพุ่งสูง จำนวน 5 ครั้ง) จากนั้นก็ลดลงอย่างมาก
- ในช่องด้านล่าง เราสามารถสร้างกราฟขึ้นมาใหม่ได้ ให้กด + แล้วกำหนดข้อมูลดังนี้

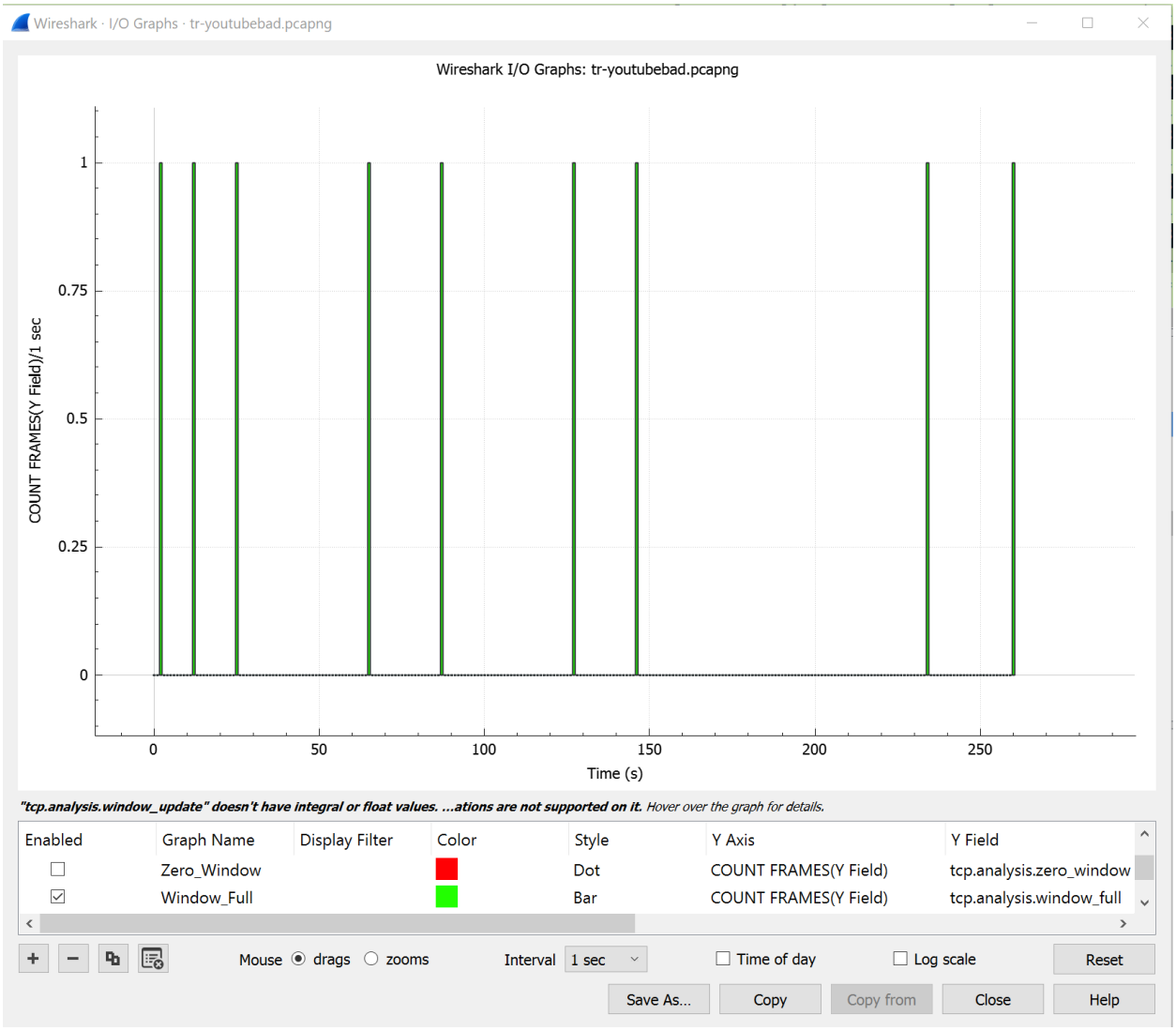
- Graph Name : Zero_Window
- Display filter : ว่าง
- Color : แดง
- Style : Dot
- Y Axis : COUNT FRAMES(Y Field)
- Y Field : tcp.analysis.zero_window

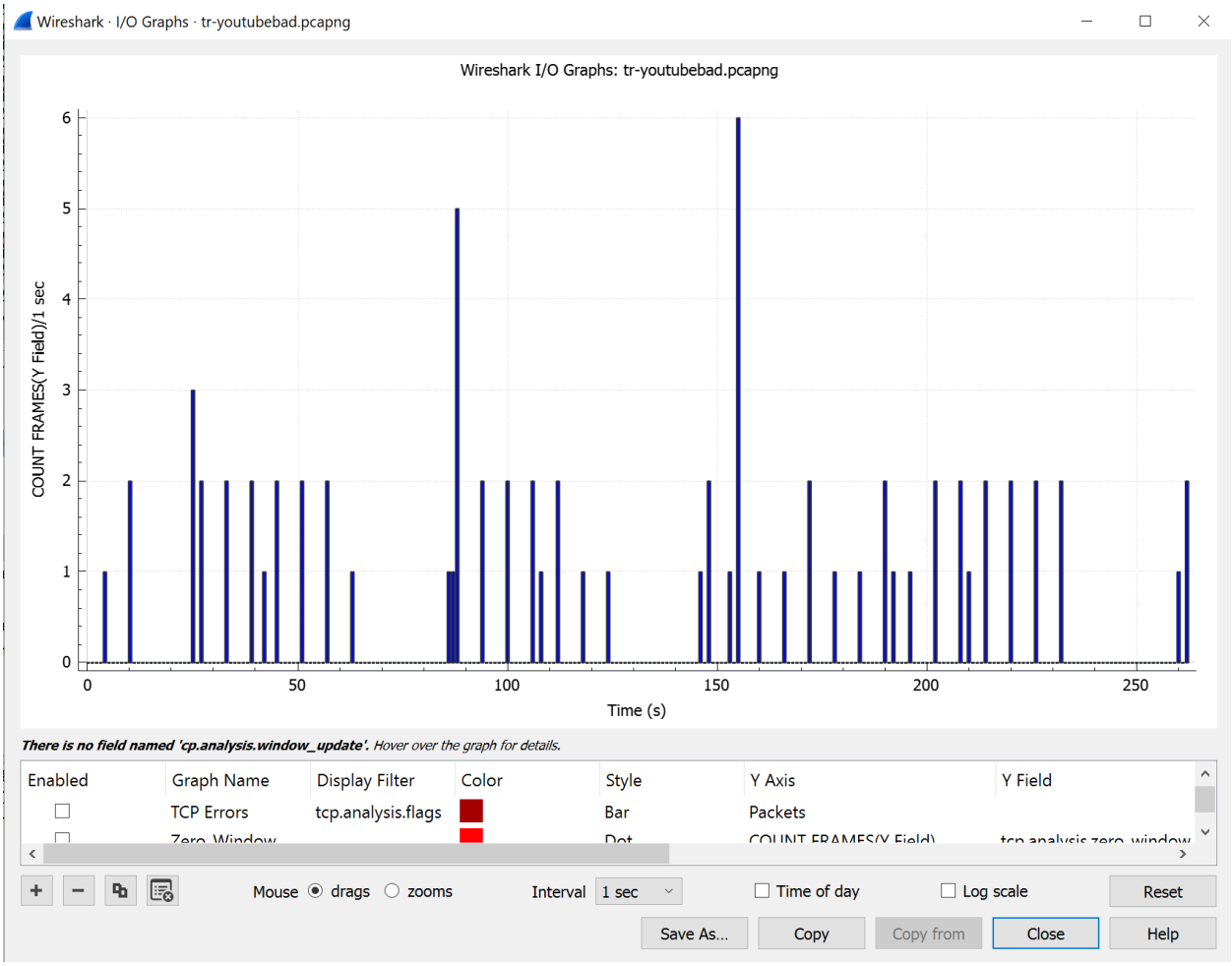
- ให้ Disable กราฟเดิมทั้ง 2 กราฟ
- กราฟบอกข้อมูลอะไร



บ่งบอกจำนวนการเกิด Zero Window ในแต่ละวินาทีตามรูปแบบ Dot

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


Wireshark · I/O Graphs · tr-youtubebad.pcapng
Wireshark I/O Graphs: tr-youtubebad.pcapng
COUNT FRAMES(Y Field)/1 sec
1
0.75
0.5
0.25
0
0
50
100
150
200
250
Time (s)
"tcp.analysis.window_update" doesn't have integral or float values. ...ations are not supported on it. Hover over the graph for details.
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
Zero_Window
Dot
COUNT FRAMES(Y Field)
tcp.analysis.zero_window
Window_Full
Bar
COUNT FRAMES(Y Field)
tcp.analysis.window_full
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Copy from
Close
Help

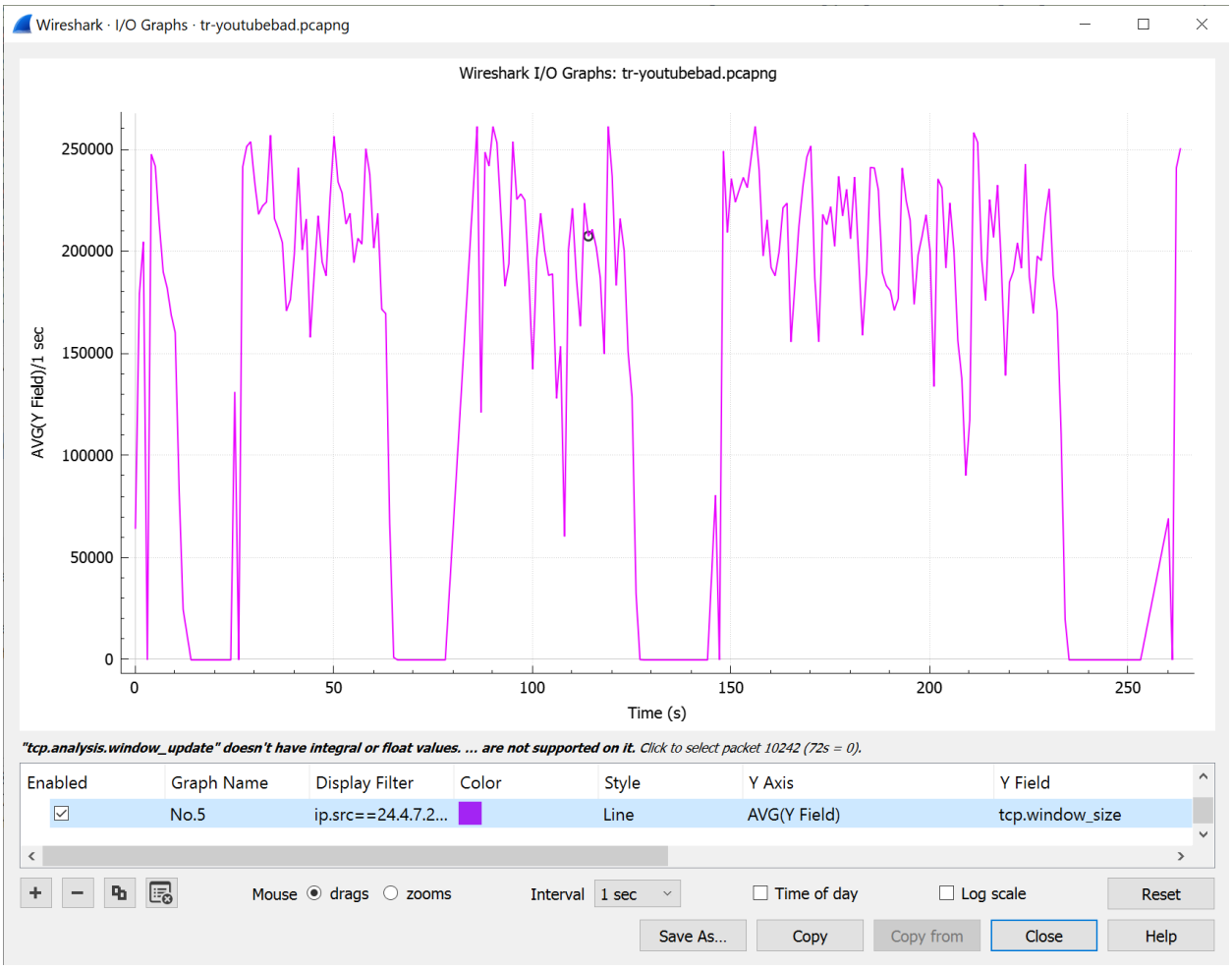


บ่งบอกจำนวนการเกิด Window_Full และ Window_Update ในแต่ละวินาทีตามรูปแบบ Bar

- จากกราฟสามารถบอกได้หรือไม่ว่ามี window full กี่ครั้ง ให้ Capture รูปประกอบด้วย

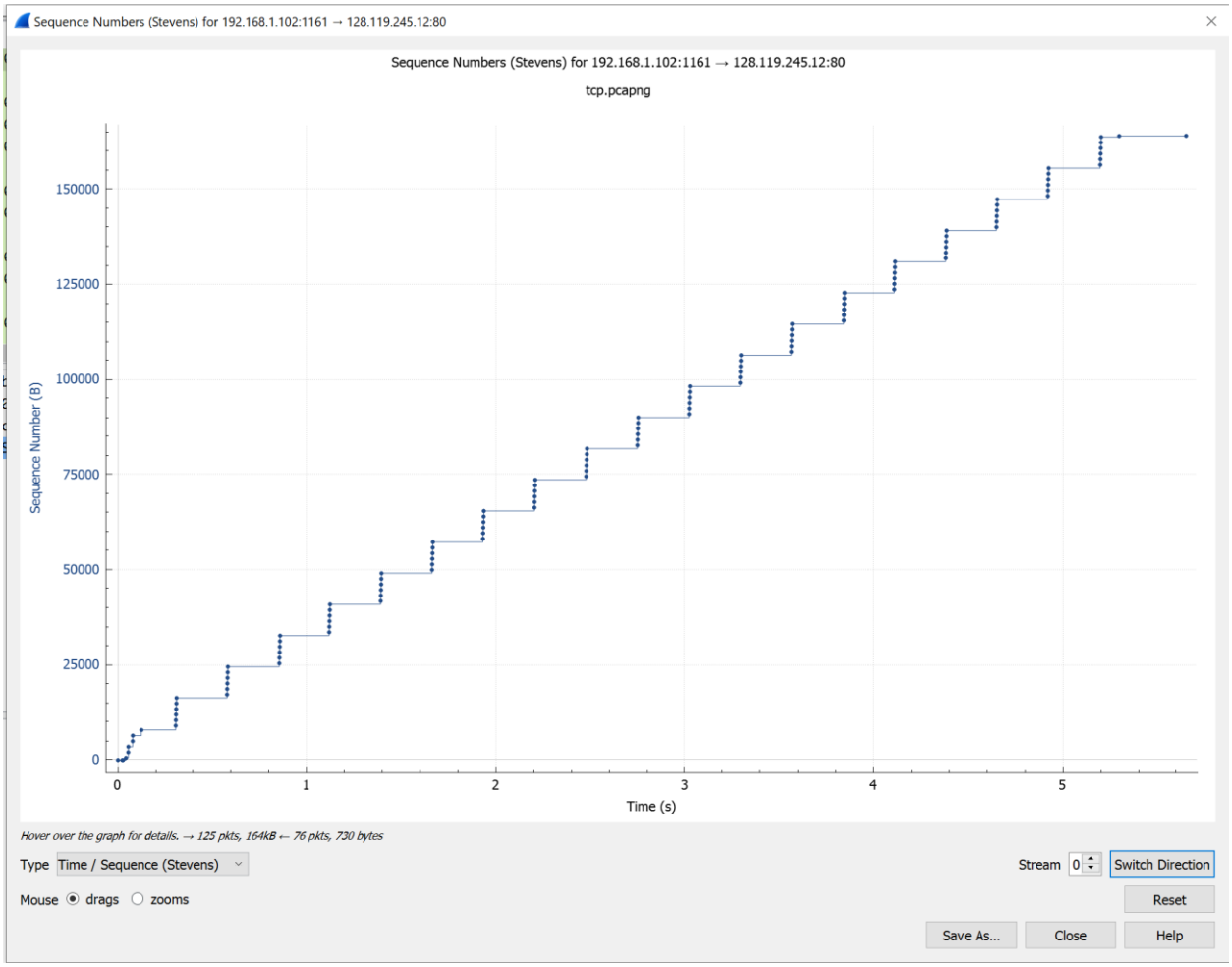
บอกได้ 9 ครั้ง (รูปกราฟสีเขียวด้านบน)

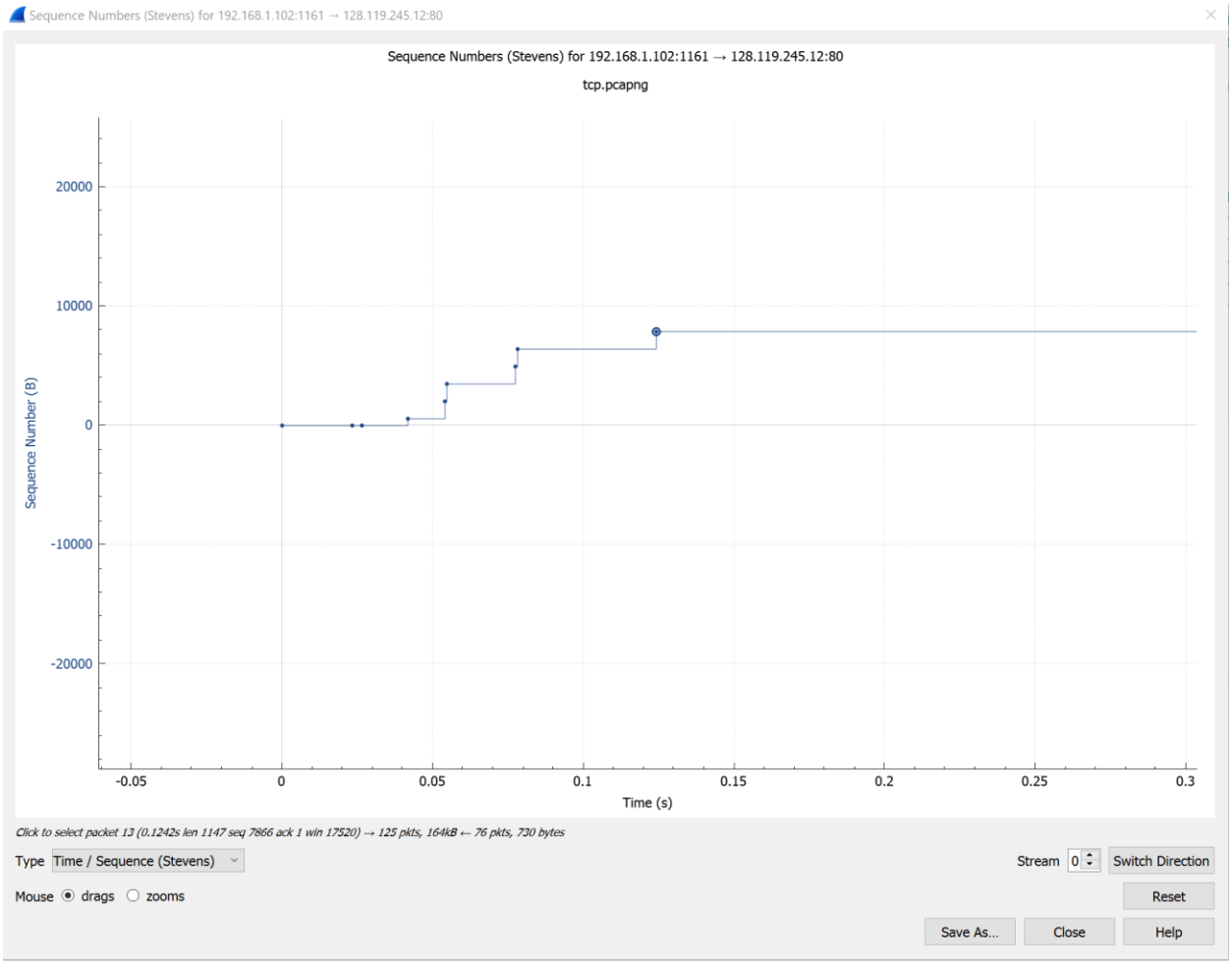
5. ให้สร้าง I/O Graph ใหม่ โดยในช่อง Display Filter ให้ใส่ ip.src==24.4.7.217 ใน Y(AXIS) ใช้ AVG(*) และช่อง Y Field ใช้ tcp.window_size กำหนดประเภทเป็น Line ให้ capture รูป และ อธิบายว่าเราสามารถวิเคราะห์ข้อมูลอะไรจากกราฟนี้



สามารถบอกจำนวน Window Size ที่สามารถทำการรับข้อมูลได้ในหน่วยวินาทีนั้นๆ โดยช่วงที่ Window Size สูง หมายถึงฝั่งรับพร้อมจะทำการรับข้อมูล จน Window Size ลงลดจนเหลือ 0 บ่งบอกว่าเกิด Zero Window ฝั่งรับเต็มแล้ว ต้องทำการรอจน Window Size กลับมาว่างอีกครั้งเป็นวัฏจักรไปเรื่อยๆ

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


Sequence Numbers (Stevens) for 192.168.1.102:1161 → 128.119.245.12:80
Sequence Numbers (Stevens) for 192.168.1.102:1161 → 128.119.245.12:80
tcp.pcapng
Sequence Number (B)
150000
125000
100000
75000
50000
25000
0
0
1
2
3
4
5
Time (s)
Hover over the graph for details. → 125 pkts, 164kB ← 76 pkts, 730 bytes
Type
Time / Sequence (Stevens)
Stream
0
Switch Direction
Mouse
drags
zooms
Reset
Save As...
Close
Help



Slow Start ที่ Packet 3 จบที่ Packet 13 หลังจากนั้นจะเข้าสู่ Congestion Avoidance