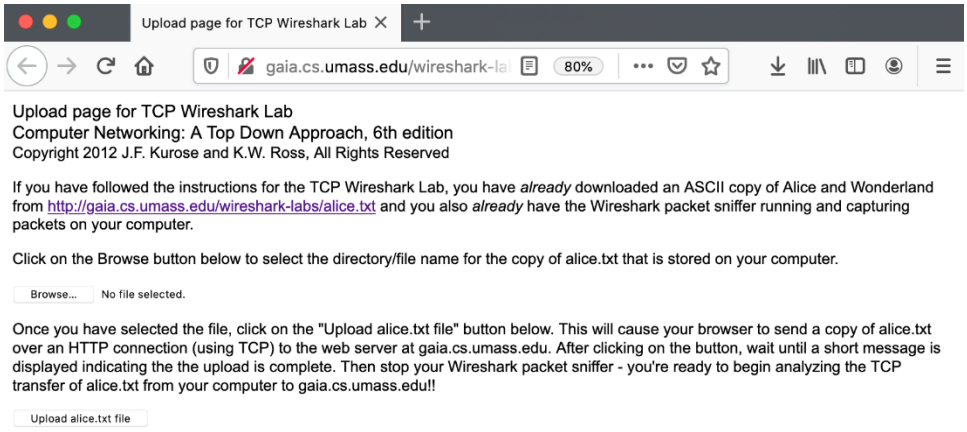
# Lab 06: TCP Reliable Communication

ในปฏิบัติการส่วนนี้เราจะสำรวจพฤติกรรมการทำงานของ TCP มากขึ้นในรายละเอียด ซึ่งเราจะศึกษาโดยการวิเคราะห์จากบันทึกร่องรอยการรับส่ง TCP segments ในการส่งไฟล์ขนาด 150 KB (ซึ่งเป็นไฟล์ที่เก็บนวนิยายเรื่อง Alice's Adventures in Wonderland ซึ่งเขียนโดย Lewi Carrol) จากเครื่องคอมพิวเตอร์ของผู้เรียนไปยังเครื่อง server เราจะศึกษาการที่ TCP ใช้ sequence number กับ acknowledgement number เพื่อให้รองรับการการถ่ายโอนข้อมูลแบบที่เชื่อถือได้ (reliable data transfer) เราจะได้เห็นอัลกอริทึมการควบคุมความคับคั่ง (congestion control algorithm) ของ TCP ทั้งช่วงที่งานแบบ slow start และช่วงที่ทำงานแบบ congestion avoidance และเราจะได้เห็นกลไกควบคุมการไหล (flow control) ของ TCP นอกจากนี้เรายังได้ดูการสร้างการเชื่อมต่อของ TCP (TCP connection) และศึกษาประสิทธิภาพ (throughput และ round-trip time) ของ TCP connection ระหว่าง เครื่องคอมพิวเตอร์ของผู้เรียนและเครื่อง server

## A. A bulk TCP transfer from your computer to a remote server

ก่อนจะเริ่มสำรวจพฤติกรรมของ TCP เราจะใช้ Wireshark เพื่อเก็บร่องรอยของ packet ของการส่งข้อมูลของ TCP จากเครื่องคอมพิวเตอร์ของผู้เรียนไปยัง server เพื่อการดังกล่าว ผู้เรียนจะเข้าไปยัง web page ที่อนุญาตให้ระบุชื่อไฟล์ซึ่งเก็บอยู่บนเครื่องของผู้เรียน (ซึ่งเป็นไฟล์ที่เก็บข้อมูล ASCII ของนวนิยายเรื่อง Alice in Wonderland) และส่งไฟล์ดังกล่าวไปยัง web server โดยการใช้ HTTP POST method ในกรณีนี้เราจะใช้ POST method แทนที่จะใช้ GET method เนื่องด้วยเราต้องการจะส่งไฟล์ที่มีข้อมูลขนาดใหญ่จากเครื่องคอมพิวเตอร์ของเราไปยังคอมพิวเตอร์ปลายทาง ซึ่งแน่นอนว่าเราจะใช้ Wireshark เก็บร่องรอยการรับส่ง TCP segments จากคอมพิวเตอร์ผู้เรียน โดยให้ทำตามขั้นตอนต่อไปนี้

1. เปิด web browser และเข้าไปที่ URL ต่อไปนี้ http://gaia.cs.umass.edu/wireshark-labs/alice.txt และดาวน์โหลดไฟล์ Alice in Wonderland โดยให้บันทึกไฟล์ด้วยชื่อ alice.txt นี้ไว้บนเครื่องของผู้เรียน
2. เข้าไปที่ http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html โดย browser จะปรากฏหน้าจอคล้ายภาพต่อไปนี้

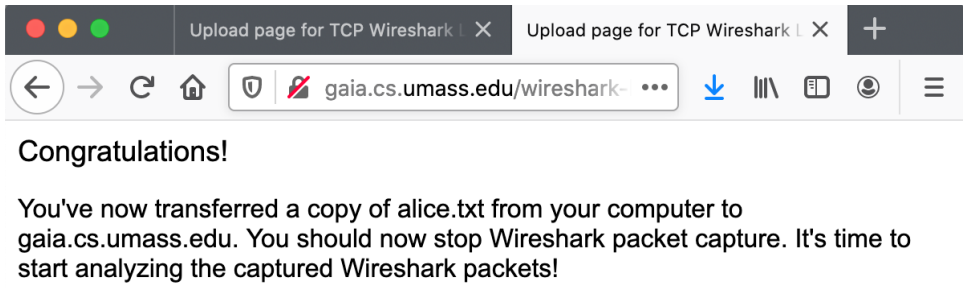



รูป 1 หน้าเว็บสำหรับอัพโหลดไฟล์จากเครื่องคอมพิวเตอร์ของผู้เรียนไปยัง gaia.cs.umass.edu

3. กดปุ่ม browse และเลือกไฟล์ Alice in Wonderland ที่ผู้เรียนได้ดาวน์โหลดมาเก็บไว้ก่อนหน้านี้ แต่อย่าพึ่งกดปุ่ม “Upload alice.txt file”
4. เปิด Wireshark และเริ่มทำการ capture packet โดยใช้ Capture filter ต่อไปนี้

```
host gaia.cs.umass.edu
```

5. สลับกลับไปที่หน้า browser และกดปุ่ม “Upload alice.txt file” เพื่อที่จะอัพโหลดไฟล์ไปยังเครื่อง gaia.cs.umass.edu หลังจากที่อัพโหลดไฟล์เรียบร้อยแล้วจะพบข้อความ Congratulations! บนหน้าจอคล้ายภาพต่อไปนี้




รูป 2 หน้าเว็บแสดงข้อความการอัพโหลดไฟล์สำเร็จ

6. สลับไปหน้า Wireshark และสั่งให้หยุด capture

7. ให้ save ไฟล์ไว้ด้วยชื่อ Lab06-A.pcapng

ก่อนที่จะทำการวิเคราะห์พฤติกรรมของ TCP connection ในรายละเอียด ลองมาดูภาพรวมจากการดูไฟล์ trace โดยเริ่มจากการดู HTTP POST message ที่ใช้ upload ไฟล์ alice.txt ไปยัง gaia.cs.umass.edu ให้ค้นหา message ดังกล่าวใน Packet List Pane และดูรายละเอียดของ HTTP message ดังกล่าวใน Packet Details Pane เพื่อที่เราจะเห็นข้อมูลของ HTTP POST message โดยละเอียดได้ โดยมีบางสิ่งที่ควรรู้ก่อน

ใน body ของ HTTP POST message มีเนื้อหาของไฟล์ alice.txt ซึ่งมีขนาดใหญ่เกินกว่า 152 bytes ถึงแม้นว่าไฟล์ดังกล่าวอาจจะไม่ได้ถือว่าใหญ่มาก แต่ HTTP POST message นี้ก็ใหญ่เกินกว่าที่จะใส่ลงไปใน TCP segment เดียวได้ ซึ่งในความเป็นจริงแล้ว หากดูใน Wireshark เราจะอาจะพบว่า HTTP POST message ดังกล่าวถูกแบ่งกระจายออกไปมากกว่า 100 TCP segments ได้เลยทีเดียว

คราวนี้เราลองมาพิจารณา TCP segments บางส่วน เริ่มต้นให้พิมพ์ “tcp” ในช่อง Display filter เพื่อกรองให้ Packet List Pane แสดงเฉพาะ packets ที่มีการใช้งาน TCP ซึ่งเราจะสังเกตใน Packet List Pane ที่คอลัมน์ Info ได้ว่ามี TCP segment ที่มีการเซต SYN bit ไว้ (เป็น packet ลำดับแรกในการทำ three-way handshake) ซึ่งส่งไปเพื่อขอสร้าง TCP connection กับ gaia.cs.umass.edu นอกจากนี้เราจะสังเกตเห็น TCP segment ที่มีเซต SYN-ACK (เป็น packet ลำดับที่สองในการทำ three-way handshake) รวมถึงเราจะสังเกตเห็น TCP segment ที่บรรจุ HTTP POST message ด้วย

## Questions (A)

หลังจากที่ค้นเจอ HTTP POST message ให้คลิกขวาที่ packet ดังกล่าว และเลือก Follow -> TCP Stream จะพบว่ามีหน้าต่าง Follow TCP Stream ซึ่งแสดงข้อมูลที่รับส่งใน TCP connection นั้นๆ ปรากฏขึ้นมา และย่อหน้าต่างดังกล่าวไปและตอบคำถามต่อไปนี้

1) หมายเลข IP address และหมายเลข TCP port อะไร (source IP and source Port) ที่คอมพิวเตอร์ของผู้เรียนใช้ในการส่งไฟล์ alice.txt ยังยัง gaia.cs.umass.edu?
   192.168.1.6:37926 ดูที่ Source and tcp.srcport
2) หมายเลข IP address และหมายเลข TCP port ใดที่ gaia.cs.umass.edu ใช้ในการส่งและรับ TCP segment ใน connection
   128.119.245.12:80 ดูที่ Destination and tcp.dstport

3) ผู้รับ segments ใน TCP connection นี้ สามารถใช้ Selective Acknowledgements ได้หรือไม่ (อนุญาตให้ TCP สามารถทำงานเหมือนกับผู้รับเฉกเช่นใน “selective repeat”)? สามารถสังเกตได้จากอะไร? (คำใบ้: สามารถค้นหาคำตอบได้จากตอนเริ่มสร้าง TCP connection ซึ่งจะมีการตกลงกันระหว่าง client และ server)

   ใช้ได้ดูจาก tcp.options.sack_perm ใน tcp segment ตัวแรก

4) SYN segment ถูกส่งจากเครื่องของผู้เรียน เพื่อใช้ในการเริ่มต้นสร้าง TCP connection ระหว่างเครื่องของผู้เรียนและและ gaia.cs.umass.edu หมายเลข sequence number ของ SYN segment ดังกล่าวมีค่าเท่าใด? (กรุณาดูค่า raw sequence number ที่อยู่ใน TCP header ไม่ใช่ค่า packet No. และก็ไม่ใช่ค่า relative sequence number ซึ่งเป็นค่าที่จะปรับให้เสมือนว่าเริ่มนับจาก 0 ตอนเริ่มต้น TCP connection นั้นๆ) ค่าของ field ใดใน TCP header ที่ใช้บ่งบอกว่า TCP segment ดังกล่าวเป็น SYN segment?

   3412583966 ดูจาก tcp.seq_raw

   SYN segment ดูจาก field flag บิตที่ 1 (…. …. …. ..1.)

5) SYN-ACK segment ถูกส่งจาก gaia.cs.umass.edu มายังเครื่องคอมพิวเตอร์ของผู้เรียนเพื่อตอบ SYN segment หมายเลข sequence number ของ SYN-ACK segment ดังกล่าวมีค่าเท่าใด? ค่าของ field ใดใน TCP header ที่ใช้บ่งบอกว่า TCP segment ดังกล่าวเป็น SYN-ACK segment? ค่า Acknowledgement ใน SYN-ACK segment มีค่าเป็นเท่าใด?

   2328165267 ดูจาก tcp.seq_raw

   3412583967 ดูจาก tcp.ack_raw

6) ขนาดของ field ที่ชื่อ Header Length ใน TCP header มีขนาดความยาวกี่บิท? มีค่าสูงสุดและต่ำสุดเป็นเท่าไร?

   4bit ค่าต่ำสุดที่เจอคือ 20 bytes สูงสุดคือ 32 bytes

   เป็นการนำตัวเลขbitคูณกับ4 bytes

7) ตรวจสอบค่า Header Length ของ SYN segment โดยหากดูค่าใน Packet Bytes Pane พบว่ามีค่าเท่าใด? ขนาดของ TCP header ของ SYN segment มีขนาดเท่าใด? ขนาดของ TCP header มีความสัมพันธ์กับค่า Header Length อย่างไร?

   Header Length: 0x80
   TCP header: 32 bytes
   เป็นการนำค่าด้านหน้า(8)มาคูณ 4 bytes
   https://stackoverflow.com/questions/53502007/calculating-tcp-header-length

8) ตรวจสอบค่า Header Length ของ SYN-ACK segment โดยหากดูค่าใน Packet Bytes Pane พบว่ามีค่าเท่าใด? ขนาดของ TCP header ของ SYN-ACK segment มีขนาดเท่าใด? ขนาดของ TCP header มีความสัมพันธ์กับค่า Header Length อย่างไร?

Header Length: 0x80
TCP header: 32 bytes
เป็นการนำค่าด้านหน้า(8)มาคูณ 4 bytes
https://stackoverflow.com/questions/53502007/calculating-tcp-header-length

9) TCP segment ที่บรรจุ HTTP header ของ HTTP POST มี หมายเลข sequence number เป็นค่าเท่าใด? TCP segment นี้มี payload (data) ขนาดกี่ bytes? เนื้อหาทั้งหมดของไฟล์ alice.txt สามารถบรรจุเข้ามาใน segment นี้ segment เดียวได้หรือไม่?

1. 3412583967
2. 728 bytes
3. ไม่ได้

10) หากพิจารณา TCP segment ที่บรรจุ HTTP POST message เป็น segment แรกในส่วนการส่ง data ของ TCP connection

a. ที่เวลาเท่าใด segment แรกในการส่ง data (segment ที่บรรจุ HTTP POST) ถูกส่งออกไป?

0.262554 s

b. ที่เวลาเท่าใด ที่ได้รับ ACK ของ segment ในการส่ง data segment แรก?

0.530483 s

c. ค่า RTT ที่คำนวณจากการส่ง data segment แรก และ ACK มีค่าเท่าใด?

0.267929 s

d. ค่า RTT ที่คำนวณจากการส่ง data segment ที่สอง และ ACK มีค่าเท่าใด?

0.267941 s

หมายเหตุ: ผู้เรียนสามารถดูค่า RTT ที่ Wireshark คำนวณให้ได้ โดยเข้าไปที่ Statistics -> TCP Stream Graph -> Round Trip Time Graph โดยให้ปรับทิศทางการวิเคราะห์หาค่า Round Trip Time เป็นทิศการส่งจากเครื่องผู้เรียนไปยัง gaia.cs.umass.edu

11) จาก TCP segment 4 segments แรกที่บรรจุ data (Length ใน TCP header ไม่ใช่ 0) แต่ละอันมีความยาวกี่ bytes (header รวมกับ payload)

782 12762 1466 2878 ดูจาก length (ผู้เรียนอนุมานว่าheaderในที่นี้หมายถึงheaderของทุกlayer)

12) ให้ผู้เรียนเปิด header ของ TCP และนำ Sequence Number, Next Sequence Number และ Acknowledgement Number (ทั้งสาม field ให้ใช้แบบ relative number) ไปเพิ่มเป็นคอลัมน์ใน Packet List Pane โดยจากการสังเกตข้อมูลที่แสดงใน 3 คอลัมน์ที่เพิ่มเข้ามา แต่ละ TCP segment นำส่ง application payload (data) ขนาดกี่ bytes? ขนาดของ application payload ดังกล่าวมีความสัมพันธ์อย่างไรกับค่า MSS ณ ตอนที่ทำ three-way handshake?

728, 12708, 1412, 2824, 8472, 14120, 8472, 5648, 11296, 2824, 14120, 728, 11296, 20768, 16384, 16384, 4865 มี segment ที่ส่ง payload ขนาดเท่ากับ MSS จาก three-way handshakes

13) จากที่ผู้เรียนสังเกตการส่ง ACK ตอบกลับของ segment ที่นำส่ง data จากเครื่องของผู้เรียนไปยัง gaia.cs.umass.edu จำนวน 10 segments แรก ฝั่งผู้รับจะตอบ ACK ในแต่ละครั้งหลังจากได้รับข้อมูลเป็นปริมาณเท่าใด? ผู้เรียนพบกรณีที่ฝั่งผู้รับตอบ ACK ในทุกๆ segment ที่ได้รับหรือไม่?

เฉลี่ย ACK 1.2 ครั้งต่อ 1 segment

ไม่ได้พบกรณีที่ฝั่งผู้รับตอบ ACK ในทุกๆ segment ที่ได้รับ

14) ฝั่ง client แจ้งไปยังฝั่ง server เพื่อขอปิด TCP connection ที่เวลาเท่าใด? TCP segment ที่ใช้แจ้งปิด connection มีการเซต flags อะไรบ้าง? TCP segment ดังกล่าวมีค่า sequence number กับ acknowledge number เป็นค่าอะไร? ใน TCP segment ที่ฝั่ง server ตอบกลับมามีค่า sequence number กับ acknowledge number เป็นค่าอะไร?

ไม่มีการขอปิดจากฝั่งclient

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 69 | 1.342849 | 128.119.245.12 | 80 | 192.168.1.6 | 37926 | TCP | 60 | 20 | 1 | 1 | 153050 | 0 80 → 37926 [ACK] Seq=1 Ack=153050 Win=262272 Len=0 |
| 70 | 1.343834 | 128.119.245.12 | 80 | 192.168.1.6 | 37926 | HTTP | 831 | 20 | 1 | 778 | 153050 | 777 HTTP/1.1 200 OK (text/html) |
| 71 | 1.386231 | 192.168.1.6 | 37926 | 128.119.245.12 | 80 | TCP | 54 | 20 | 153050 | 153050 | 778 | 0 37926 → 80 [ACK] Seq=153050 Ack=778 Win=130304 Len=0 |
| 72 | 6.343593 | 128.119.245.12 | 80 | 192.168.1.6 | 37926 | TCP | 60 | 20 | 778 | 779 | 153050 | 0 80 → 37926 [FIN, ACK] Seq=778 Ack=153050 Win=264320 Len=0 |
| 73 | 6.343629 | 192.168.1.6 | 37926 | 128.119.245.12 | 80 | TCP | 54 | 20 | 153050 | 153050 | 779 | 0 37926 → 80 [ACK] Seq=153050 Ack=779 Win=130304 Len=0 |

15) ฝั่ง server แจ้งไปยังฝั่ง client เพื่อขอปิด TCP connection ที่เวลาเท่าใด? TCP segment ที่ใช้แจ้งปิด connection มีการเซต flags อะไรบ้าง? TCP segment ดังกล่าวมีค่า sequence number กับ acknowledge number เป็นค่าอะไร? ใน TCP segment ที่ฝั่ง client ตอบกลับมามีค่า sequence number กับ acknowledge number เป็นค่าอะไร?

6.343593 s
Flag FIN ACK
seq 778
ack 153050
ตอบกลับ
seq 153050
ack 779

16) จงคำนวณ throughput (ปริมาณ bytes ที่ส่งต่อหน่วยเวลา) ของ TCP connection นี้ พร้อมทั้งอธิบายว่าสามารถคำนวณค่า throughput ในกรณีนี้ได้อย่างไร?

    24 kBps
    ใช้ filter tcp.stream eq 1
    กด Capture File Properties -> Average bytes/s ของ display

## B. TCP Retransmissions

ในส่วนต่อไปนี้จะเป็นการศึกษาการทำงานของกลไกล retransmission ใน TCP เนื่องด้วยการจำลองกรณี packet loss จำเป็นต้องคุ้นเคยกับการใช้เครื่องมือเฉพาะบางประเภท ปฏิบัติการในส่วนนี้จึงจะเป็นการให้ผู้เรียนศึกษาจากไฟล์ packet capture ที่มีกรณี packet loss เกิดขึ้นแทนการทดลองดักจับด้วยตนเอง โดยให้เปิดไฟล์ **tr-twohosts.pcapng** ที่เตรียมไว้ โดยในกรณีที่มีการกล่าวถึง Sequence Number หรือ Acknowledgement Number ในกรณีต่อไปนี้ ให้พิจารณาหมายเลขแบบ relative number

## Questions (B)

17) จากการศึกษาไฟล์ที่กำหนดให้ ฝั่งผู้ส่งข้อมูลใช้หมายเลข IP หมายเลขอะไร? ฝั่งผู้รับข้อมูลใช้หมายเลข IP หมายเลขอะไร? มีการใช้งาน application layer protocol ใดในการส่งไฟล์ข้อมูล?

    Sender IP: 200.236.31.1
    Receiver IP: 192.168.1.72
    Protocol: FTP
    ดูจาก packet detail pane ว่าตัวไหน tcp มี payload

18) ใน Packet List Pane เลื่อนไปสำรวจ packet หมายเลข 29019 ถึง packet หมายเลข 29028 โดยให้พิจารณาค่า relative number ของหมายเลข Sequence Number, Next Sequence Number และ Acknowledgement Number ของ packets เหลานี้ จากนั้นอธิบายว่าเกิดเหตุการณ์ผิดปกติอะไรขึ้นในช่วงการส่ง packet No. 29022 กับ 29023

    จากการส่ง 29022 กับ 29033 มีsequence numberที่ไม่ต่อเนื่องกัน สังเกตได้จากทั้งตัวเลขและจากที่wireshark ระบุไว้ว่า TCP previous segment not captured

19) ใน Packet List Pane ให้คลิกขวาที่ packet หมายเลข 29022 และเลือก Follow -> TCP Stream จากนั้นค้นหาว่ามีการส่ง Sequence Number หมายเลข 12243561 ออกไปที่ packet หมายเลขใด? เมื่อเวลาใด?

    31524 เวลา 56.206393 ใช้ filter tcp.seq == 12243561

20) นับจากช่วงเวลาที่ผู้รับข้อมูลระบุเป็นครั้งแรกว่าต้องการหมายเลข Sequence Number 12243561 เป็นลำดับถัดไป ไปจนถึงช่วงเวลาที่มีการส่ง Sequence Number ดังกล่าวออกไป เป็นช่วงระเวลาเวลาห่างกันเท่าไร?

1.895002 วินาที หาได้จากการตั้งให้เวลาของACK 12243561เป็นrefและไปดูเวลาของsegment31524

21) จากข้อ 19) การส่ง Sequence Number หมายเลข 12243561 เป็นการส่งออกไปแบบปกติหรือเป็นการ retransmission? หากเป็นการ retransmission เป็นการส่งซ้ำด้วยสาเหตุใด ระหว่าง Retransmission Timeout หรือว่า triple duplicate ACKs

retransmission เป็นเพราะtimeout สังเกตดูจากการhandshake RTTอยู่ที่ประมาณ 0.3 s ช่วงเวลาที่เราส่งack ซ้ำครั้งที่3จนถึงการretransmitเป็น 1.870855 s ซึ่งมากกว่าRTTมาก

22) จากข้อ 20) ในช่วงเวลาดังกล่าว มีการส่ง duplicate ACKs มาทั้งหมดกี่ครั้ง? มีการระบุหมายเลข Acknowledgement Number เป็นหมายเลขอะไร?

137 ครั้ง ACK12243561 ดูได้จาก packet list pane ตรง info

# Submission

จงตอบคำถามในส่วนที่ระบุหัวข้อ Question ตั้งแต่ (A) ไปจนถึง (B) ซึ่งมีคำถามร่วมทั้งหมด 22 ข้อ โดยในคำตอบของแต่ละข้อด้วยให้อธิบายด้วยว่าหาคำตอบมาได้อย่างไร ตัวอย่างเช่น อธิบายว่าสามารถค้น packet ตามที่โจทย์ระบุได้ด้วยวิธีการใด หรือค่าที่นำมาตอบ นำมาจาก field ใดของ header ตาม protocol ใด

**ในกรณีที่คัดลอกคำตอบของคนอื่นมา ให้ระบุชื่อของบุคคลที่เป็นต้นฉบับมาด้วย หากตรวจพบว่ามีการลอกมาแต่ไม่มีการระบุชื่อบุคคลที่เป็นต้นฉบับ ผู้สอนจะถือว่าทุจริตและอาจพิจารณาลงโทษให้ตกเกณฑ์รายวิชาในทันที**

การส่งงาน ให้เขียนหรือพิมพ์หมายเลขข้อและคำตอบของข้อนั้นๆ และส่งเป็นไฟล์ PDF เท่านั้น กรุณาตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา ตามด้วย section และ _lab06 ตามตัวอย่างต่อไปนี้ 64019999_sec20_lab06.pdf