

Lab 06: TCP Reliable Communication

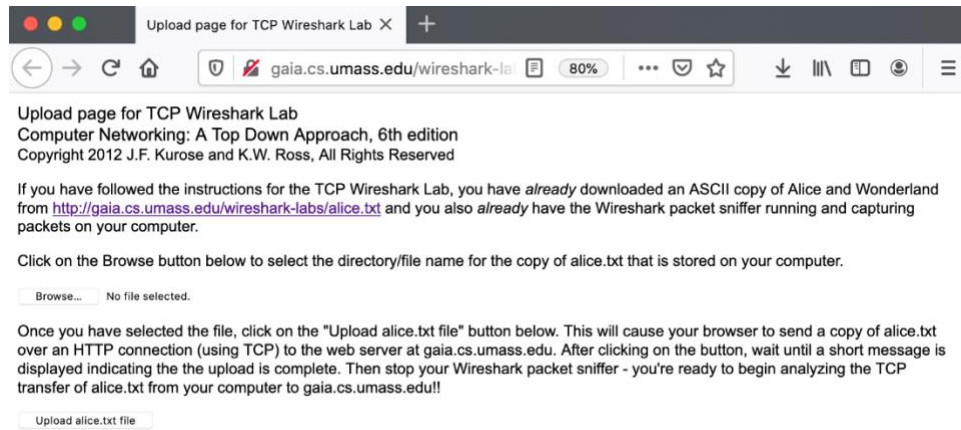
ในปฏิบัติการส่วนนี้เราจะสำรวจพฤติกรรมการทำงานของ TCP มากขึ้นในรายละเอียด ซึ่งเราจะศึกษาโดยการวิเคราะห์จากบันทึกการรับส่ง TCP segments ในการส่งไฟล์ขนาด 150 KB (ซึ่งเป็นไฟล์ที่เก็บนวนิยายเรื่อง Alice's Adventures in Wonderland ซึ่งเขียนโดย Lewis Carroll) จากเครื่องคอมพิวเตอร์ของผู้เรียนไปยังเครื่อง server เราจะศึกษาการใช้ sequence number กับ acknowledgement number เพื่อให้รองรับการถ่ายโอนข้อมูลแบบที่เชื่อถือได้ (reliable data transfer) เราจะได้เห็นอัลกอริทึมการควบคุมความคับคั่ง (congestion control algorithm) ของ TCP ทั้งช่วงที่ทำงานแบบ 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 เพื่อดังกล่าว ผู้เรียนจะเข้าไปยัง web page ที่อนุญาตให้ระบุชื่อไฟล์ซึ่งเก็บอยู่บนเครื่องของผู้เรียน (ซึ่งเป็นไฟล์ที่เก็บข้อมูล ASCII ของนวนิยายเรื่อง Alice in Wonderland) และส่งไฟล์ดังกล่าวไปยัง web server โดยการใช้ HTTP POST method ในกรณีนี้เราจะใช้ POST method แทนที่จะใช้ GET method เนื่องจากเราต้องการจะส่งไฟล์ที่มีข้อมูลขนาดใหญ่จากเครื่องคอมพิวเตอร์ของเราไปยังคอมพิวเตอร์ปลายทาง 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

01076117 Computer Networks in Practice
Computer Engineering, KMITL

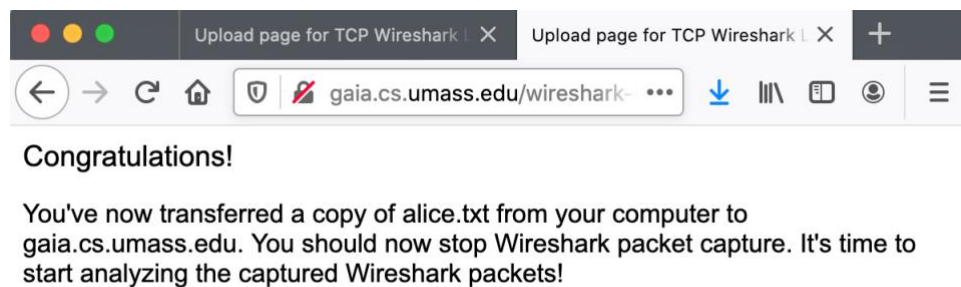


รูป 1 หน้าเว็บสำหรับอัปโหลดไฟล์จากเครื่องคอมพิวเตอร์ของผู้เรียนไปยัง gaia.cs.umass.edu

- กดปุ่ม **browse** และเลือกไฟล์ **Alice in Wonderland** ที่ผู้เรียนได้ดาวน์โหลดมาเก็บไว้ก่อนหน้านี้อย่างใดก็ตาม แต่อย่าเพิ่งกดปุ่ม **“Upload alice.txt file”**
- เปิด **Wireshark** และเริ่มทำการ **capture packet** โดยใช้ **Capture filter** ต่อไปนี้

host gaia.cs.umass.edu

- สลับกลับไปหน้า **browser** และกดปุ่ม **“Upload alice.txt file”** เพื่อที่จะอัปโหลดไฟล์ไปยังเครื่อง **gaia.cs.umass.edu** หลังจากอัปโหลดไฟล์เรียบร้อยแล้วจะพบข้อความ **Congratulations!** บนหน้าจอคล้ายภาพต่อไปนี้



รูป 2 หน้าเว็บแสดงข้อความการอัปโหลดไฟล์สำเร็จ

- 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 ถึงแม้ว่าไฟล์ดังกล่าวอาจจะไม่ได้ถือว่าใหญ่มาก แต่ HTTP POST message นี้ก็ใหญ่เกินกว่าที่จะใส่ลงไปใน TCP segment เดียวได้ ซึ่งในความเป็นจริงแล้ว หากดูใน Wireshark เราอาจจะพบว่า 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 จะพบว่า มีหน้าต่าง Follow TCP Stream ซึ่งแสดงข้อมูลที่รับส่งใน TCP connection นั้นๆ ปรากฏขึ้นมา และย่อหน้าต่างดังกล่าวไป และตอบคำถามต่อไปนี้

- 1) หมายเลข IP address และหมายเลข TCP port อะไร (source IP and source Port) ที่คอมพิวเตอร์ของผู้เรียนใช้ในการส่งไฟล์ alice.txt ไปยัง gaia.cs.umass.edu?
 - a. source IP : 10.66.6.197
 - b. source Port : 56406
- 2) หมายเลข IP address และหมายเลข TCP port ใดที่ gaia.cs.umass.edu ใช้ในการส่งและรับ TCP segment ใน connection

tcp.stream eq 0							
o.	Time	ICMP RTT	Source	Destination	Protocol	Length	Info
1	0.000000		10.66.6.197	128.119.245.12	TCP	78	56406 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2066739688 TSecr=0 SACK_PERM
2	0.290066		128.119.245.12	10.66.6.197	TCP	66	80 → 56406 [SYN, ACK] Seq=1 Win=20200 Len=0 MSS=1380 SACK_PERM WS=128
3	0.291065		10.66.6.197	128.119.245.12	TCP	54	56406 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
4	0.291916		10.66.6.197	128.119.245.12	HTTP	1434	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1

- a.
- b. IP : 128.119.245.12

c. Port : 80

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

a. ได้

```
Transmission Control Protocol, Src Port: 56406, Dst Port: 80, Seq: 0, Len: 0
Source Port: 56406
Destination Port: 80
[Stream index: 0]
> [Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2166107257
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1011 .... = Header Length: 44 bytes (11)
> Flags: 0x002 (SYN)
Window: 65535
[Calculated window size: 65535]
Checksum: 0xb96c [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Ope
> [Timestamps]
```

b.

- 4) SYN segment ถูกส่งจากเครื่องของผู้เรียน เพื่อใช้ในการเริ่มต้นสร้าง TCP connection ระหว่างเครื่องของผู้เรียน และและ 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?

```
Transmission Control Protocol, Src Port: 56406, Dst Port: 80, Seq: 0, Len: 0
Source Port: 56406
Destination Port: 80
[Stream index: 0]
> [Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2166107257
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1011 .... = Header Length: 44 bytes (11)
> Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... = Congestion Window Reduced: Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
.... ....0... = Push: Not set
.... .....0.. = Reset: Not set
> .... ....1. = Syn: Set
.... ....0 = Fin: Not set
[TCP Flags: .....S.]
Window: 65535
[Calculated window size: 65535]
Checksum: 0xb96c [unverified]
```

a.

b. Sequence Number (raw): 2166107257

c. Flags: 0x002 (SYN)

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

```
Transmission Control Protocol, Src Port: 80, Dst Port: 56406, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 56406
[Stream index: 0]
> [Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 4097876504
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2166107258
1000 .... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... = Congestion Window Reduced: Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set
.... .... 0... = Push: Not set
.... ..... 0.. = Reset: Not set
> .... .... .1. = Syn: Set
.... .... ...0 = Fin: Not set
[TCP Flags: .....A..S.]
Window: 29200
[Calculated window size: 29200]
Checksum: 0x561f [unverified]
```

- a. Sequence Number (raw): 4097876504
c. Flags: 0x012 (SYN, ACK)
- 6) ขนาดของ field ที่ชื่อ Header Length ใน TCP header มีขนาดความยาวกี่บิต? มีค่าสูงสุดและต่ำสุดเป็นเท่าไร?
- a. 352 bits
b. 160 bits
- 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?

```
Transmission Control Protocol, Src Port: 56406, Dst Port: 80, Seq: 0, Len: 0
Source Port: 56406
Destination Port: 80
[Stream index: 0]
> [Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2166107257
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1011 .... = Header Length: 44 bytes (11)
Flags: 0x002 (SYN)
Window: 65535
[Calculated window size: 65535]
Checksum: 0xb96c [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Op
> [Timestamps]
```

- a.
b. 44 bytes เท่ากัน

- 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?

```
Transmission Control Protocol, Src Port: 80, Dst Port: 56406, Seq: 0, Ack: 1, Len: 0
  Source Port: 80
  Destination Port: 56406
  [Stream index: 0]
  > [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 4097876504
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2166107258
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
  Window: 29200
  [Calculated window size: 29200]
  Checksum: 0x561f [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP)
  > [Timestamps]
  > [SEQ/ACK analysis]
```

- a. 32
b. เท่ากัน
- 9) TCP segment ที่บรรจุ HTTP header ของ HTTP POST มีหมายเลข sequence number เป็นค่าเท่าใด? TCP segment นี้มี payload (data) ขนาดกี่ bytes? เนื้อหาทั้งหมดของไฟล์ alice.txt สามารถบรรจุเข้ามาใน segment นี้ segment เดียวได้หรือไม่?
- a. Sequence Number (raw): 2166107258
b. TCP payload (1380 bytes)
c. 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?
- i. Arrival Time: Feb 1, 2024 18:16:51.407750000 +07

```
Frame 4: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface en0, id 0
  Section number: 1
  > Interface id: 0 (en0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 1, 2024 18:16:51.407750000 +07
  UTC Arrival Time: Feb 1, 2024 11:16:51.407750000 UTC
  Epoch Arrival Time: 1706786211.407750000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000851000 seconds]
  [Time delta from previous displayed frame: 0.000851000 seconds]
  [Time since reference or first frame: 0.291916000 seconds]
  Frame Number: 4
  Frame Length: 1434 bytes (11472 bits)
  Capture Length: 1434 bytes (11472 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http:mime_multipart]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
  > Ethernet II, Src: Apple_a8:6e:3b (74:a6:cd:a8:6e:3b), Dst: HuaweiTechno_ba:bd:2f (80:69:33:ba:bd:2f)
```

- ii. ที่เวลาเท่าใด ที่ได้รับ ACK ของ segment ในการส่ง data segment แรก?

01076117 Computer Networks in Practice
Computer Engineering, KMITL

- i. Arrival Time: Feb 1, 2024 18:16:51.407753000 +07

```
▼ Frame 5: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface en0, id 0
  Section number: 1
  > Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 1, 2024 18:16:51.407753000 +07
    UTC Arrival Time: Feb 1, 2024 11:16:51.407753000 UTC
    Epoch Arrival Time: 1706786211.407753000
    [Time shift for this packet: 0.00000000 seconds]
    [Time delta from previous captured frame: 0.000003000 seconds]
    [Time delta from previous displayed frame: 0.000003000 seconds]
    [Time since reference or first frame: 0.291919000 seconds]
    Frame Number: 5
    Frame Length: 1434 bytes (11472 bits)
    Capture Length: 1434 bytes (11472 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
  > Ethernet II, Src: Apple_a8:6e:3b (74:a6:cd:a8:6e:3b), Dst: HuaweiTechno_ba:bd:2f (80:69:33:ba:bd:2f)
  > Internet Protocol Version 4, Src: 10.66.6.197, Dst: 128.119.245.12
```

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

```
Source Port: 56406
Destination Port: 80
[Stream index: 0]
> [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 1380]
  Sequence Number: 1381 (relative sequence number)
  Sequence Number (raw): 2166108638
  [Next Sequence Number: 2761 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 4097876505
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
  Window: 4096
  [Calculated window size: 262144]
  [Window size scaling factor: 64]
  Checksum: 0x07f9 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
    [Time since first frame in this TCP stream: 0.291919000 seconds]
    [Time since previous frame in this TCP stream: 0.000003000 seconds]
  > [SEQ/ACK analysis]
    [iRTT: 0.291065000 seconds]
    [Bytes in flight: 2760]
    [Bytes sent since last PSH flag: 2760]
    TCP payload (1380 bytes)
  > Hypertext Transfer Protocol
```

- i.
ii. [iRTT: 0.291065000 seconds]

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

```
Source Port: 56406
Destination Port: 80
[Stream index: 0]
> [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 1380]
  Sequence Number: 2761 (relative sequence number)
  Sequence Number (raw): 2166110018
  [Next Sequence Number: 4141 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 4097876505
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
  Window: 4096
  [Calculated window size: 262144]
  [Window size scaling factor: 64]
  Checksum: 0xcdbd [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
    [Time since first frame in this TCP stream: 0.291923000 seconds]
    [Time since previous frame in this TCP stream: 0.000004000 seconds]
  > [SEQ/ACK analysis]
    [iRTT: 0.291065000 seconds]
    [Bytes in flight: 4140]
    [Bytes sent since last PSH flag: 4140]
    TCP payload (1380 bytes)
  > Hypertext Transfer Protocol
```

- i.
ii. [iRTT: 0.291065000 seconds]

01076117 Computer Networks in Practice
Computer Engineering, KMITL

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)

a. $1434 \times 4 = 5736$ bytes

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 ดังกล่าวนี้อาจมีความสัมพันธ์อย่างไรกับค่า MSS ณ ตอนที่ทำ three-way handshake?

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Sequence Number	Next Sequence Number	Acknowledgment Number	Info
1	0.000000		10.66.6.197	128.119.245.12	TCP	78	0	0	1	0 56486 -> 88 [SYN, Seq=0 Win=65535 Len=0 MSS=1460 TSval=204673608 TSecr=0 SACK_PERM
2	0.290866		128.119.245.12	10.66.6.197	TCP	66	88	88	0	88 -> 56486 [SYN, ACK] Seq=1 Win=29200 Len=0 MSS=1388 SACK_PERM=1
3	0.291865		10.66.6.197	128.119.245.12	TCP	54	56486	56486	0	56486 -> 88 [ACK] Seq=1 Ack=1 Win=29200 Len=0
4	0.291915		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	POST /vulnshark-labs/lab3-1-reply.htm HTTP/1.1
5	0.291919		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
6	0.291923		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
7	0.291928		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
8	0.291931		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
9	0.291934		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
10	0.291937		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
11	0.291940		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
12	0.291944		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
13	0.291948		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation

- a. Sequence Number, Next Sequence Number และ Acknowledgement Number
- c. 0, 1, 0
- d. 0, 1, 1
- e. 1, 1, 1

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

No.	Time	ICMP RTT	Source	Destination	Protocol	Length	Sequence Number	Next Sequence Number	Acknowledgment Number	Info
1	0.000000		10.66.6.197	128.119.245.12	TCP	78	0	0	1	0 56486 -> 88 [SYN, Seq=0 Win=65535 Len=0 MSS=1460 TSval=204673608 TSecr=0 SACK_PERM
2	0.290866		128.119.245.12	10.66.6.197	TCP	66	88	88	0	88 -> 56486 [SYN, ACK] Seq=1 Win=29200 Len=0 MSS=1388 SACK_PERM=1
3	0.291865		10.66.6.197	128.119.245.12	TCP	54	56486	56486	0	56486 -> 88 [ACK] Seq=1 Ack=1 Win=29200 Len=0
4	0.291915		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	POST /vulnshark-labs/lab3-1-reply.htm HTTP/1.1
5	0.291919		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
6	0.291923		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
7	0.291928		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
8	0.291931		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
9	0.291934		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
10	0.291937		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
11	0.291940		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
12	0.291944		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
13	0.291948		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
14	0.500074		128.119.245.12	10.66.6.197	TCP	56	88	88	6900	88 -> 56486 [ACK] Seq=1 Ack=1381 Win=58832 Len=0
15	0.500077		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
16	0.500082		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
17	0.500087		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
18	0.500094		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
19	0.500097		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
20	0.500101		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
21	0.500105		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
22	0.500109		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
23	0.500113		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
24	0.500117		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
25	0.500121		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
26	0.501054		128.119.245.12	10.66.6.197	TCP	56	88	88	6900	88 -> 56486 [ACK] Seq=1 Ack=20701 Win=78856 Len=0
27	0.501058		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
28	0.501061		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
29	0.501065		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
30	0.501068		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
31	0.501072		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
32	0.501076		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
33	0.501080		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
34	0.501084		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
35	0.501088		10.66.6.197	128.119.245.12	HTTP	1434	1434	1434	0	Continuation
36	0.872131		128.119.245.12	10.66.6.197	TCP	56	88	88	6900	88 -> 56486 [ACK] Seq=1 Ack=20701 Win=78856 Len=0
37	0.872135		128.119.245.12	10.66.6.197	TCP	56	88	88	6900	88 -> 56486 [ACK] Seq=1 Ack=27081 Win=84488 Len=0
38	0.872139		128.119.245.12	10.66.6.197	TCP	56	88	88	6900	88 -> 56486 [ACK] Seq=1 Ack=34581 Win=88384 Len=0
39	0.872143		128.119.245.12	10.66.6.197	TCP	56	88	88	6900	88 -> 56486 [ACK] Seq=1 Ack=41481 Win=112880 Len=0

- a. Ack ตอบกลับทุกๆ 6900
- c. ไม่พบ

14) ผู้ client แฉงไปยังผู้ server เพื่อขอปิด TCP connection ที่เวลาเท่าใด? TCP segment ที่ใช้แฉงปิด connection มีการเซต flags อะไรบ้าง? TCP segment ดังกล่าวนี้อาจมีความสัมพันธ์อย่างไรกับค่า sequence number กับ acknowledge

number เป็นค่าอะไร? ใน TCP segment ที่ฝั่ง server ตอบกลับมามีค่า sequence number กับ
acknowledge number เป็นค่าอะไร?

- a. Time of TCP Connection Closure Request:
 - i. The client requests to close the TCP connection at timestamp 1.825718 seconds.
 - ii. Arrival Time: Feb 1, 2024 18:16:52.941552000 +07
- b. TCP Segment Flags for Closure:
 - i. [FIN, ACK]
- c. Sequence and Acknowledgment Numbers for Closure Request:
 - i. Sequence Number: 153032
 - ii. Acknowledgment Number: 742
- d. Sequence and Acknowledgment Numbers in Server's Response:
 - i. Sequence Number: 742
 - ii. Acknowledgment Number: 153033

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

- a. Time of TCP Connection Closure Request:
 - i. The client requests to close the TCP connection at timestamp 1.823967 seconds.
 - ii. Arrival Time: Feb 1, 2024 18:16:52.939801000 +07
- b. TCP Segment Flags for Closure:
 - i. [FIN, ACK]
- c. Sequence and Acknowledgment Numbers for Closure Request:
 - i. Sequence Number: 741
 - ii. Acknowledgment Number: 153032
- d. Sequence and Acknowledgment Numbers in Server's Response:
 - i. Sequence Number: 153032
 - ii. Acknowledgment Number: 742

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

- a. Statistics > Conversations to find the total bytes and duration of the TCP stream.

b.

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
74:a6:cd:a8:6e:3b	80:69:33:ba:bd:2f	206	215 kB	152	211 kB	54	4 kB	0.000000	2.1036	802 kbps	15 kbps

- c. 802 kbps -> 100.25 kBps

B. TCP Retransmissions

ในส่วนต่อไปนี้จะเป็นการศึกษาการทำงานของกลไก 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 ในกรณีต่อไปนี้จะให้พิจารณาหมายเลขแบบ relative number

Questions (B)

17) จากการดูไฟล์ที่กำหนดให้ ผู้ส่งข้อมูลใช้หมายเลข IP หมายเลขอะไร? ผู้รับข้อมูลใช้หมายเลข IP หมายเลขอะไร? มีการใช้งาน application layer protocol ใดในการส่งไฟล์ข้อมูล?

- a. Source IP : 192.168.1.72
- b. Destination IP : 200.236.31.1
- c. FTP

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 เหล่านี้ จากนั้นอธิบายว่าเหตุการณ์ผิดปกติอะไรขึ้นในช่วงการส่ง packet No. 29022 กับ 29023

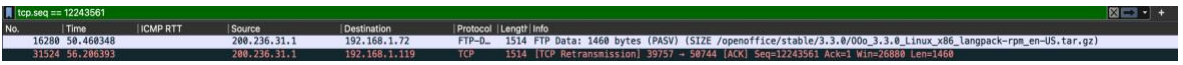
- a. Packet 29022: Has a sequence number of Seq=1 and an acknowledgment number of Ack=1224101.
- b. Packet 29023: Also has a sequence number of Seq=1 and an acknowledgment number of Ack=1224101.
- c. The anomaly between packets 29022 and 29023 is that they both have the same sequence and acknowledgment numbers, which typically should not happen in a normal TCP flow. The sequence number should increment with each new packet that sends data, as it represents the byte number that the sender is transmitting to the receiver. Similarly, acknowledgment numbers should increment to match the next expected byte from the sender.
- d. The sequence number ควรเพิ่มขึ้นตามแต่ละแพ็คเก็ตใหม่ที่ส่งข้อมูล

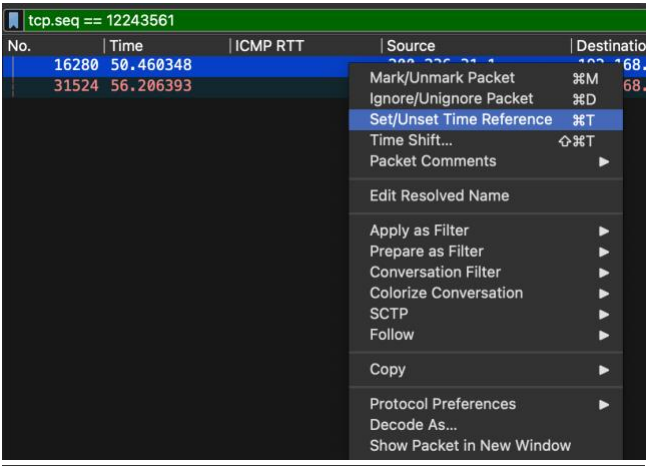
19) ใน Packet List Pane ให้คลิกขวาที่ packet หมายเลข 29022 และเลือก Follow -> TCP Stream จากนั้นค้นหาว่าการส่ง Sequence Number หมายเลข 12243561 ออกไปที่ packet หมายเลขใด? เมื่อเวลาใด?

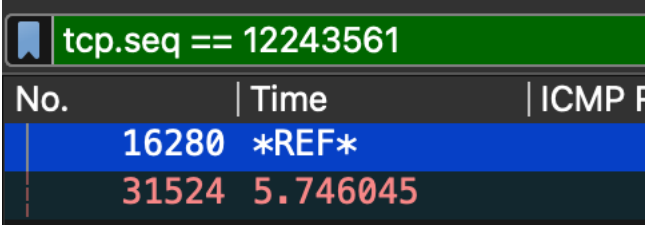
tcp.stream eq 0 && tcp.seq == 12243561					
No.	Time	ICMP RTT	Source	Destination	Protocol Length Info
31524	56.206393		200.236.31.1	192.168.1.119	TCP 54 [TCP Retransmission] 39757 → 50744 [ACK] Seq=12243561 Ack=1 Win=26880 Len=1460

- a.
- b. No. 31524
- c. 56.206393
- d. Arrival Time: Nov 16, 2013 09:03:56.740090000 +07

- 20) นับจากช่วงเวลาที่ได้รับข้อมูลระบุเป็นครั้งแรกว่าต้องการหมายเลข Sequence Number 12243561 เป็นลำดับถัดไป ไปจนถึงช่วงเวลาที่มีการส่ง Sequence Number ดังกล่าวออกไป เป็นช่วงระยะเวลาห่างกันเท่าไร?

a. 

b. 

c. 

d. 5.746045 sc

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

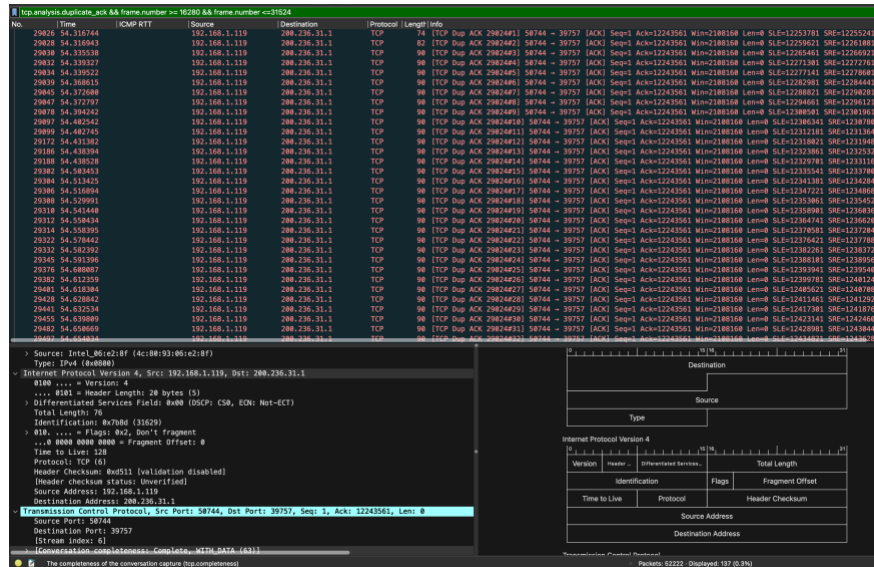
a. Retransmission Timeout

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

a. tcp.analysis.duplicate_ack && frame.number >= 16280 && frame.number <= 31524

b. 137 ครั้ง

01076117 Computer Networks in Practice Computer Engineering, KMITL



c.

d. Acknowledgment Number: 12243561 (relative ack number)

Submission

จงตอบคำถามในส่วนที่ระบุหัวข้อ Question ตั้งแต่ (A) ไปจนถึง (B) ซึ่งมีคำถามรวมทั้งหมด 22 ข้อ โดยในคำตอบของแต่ละข้อด้วยให้อธิบายด้วยว่าหาคำตอบมาได้อย่างไร ตัวอย่างเช่น อธิบายว่าสามารถค้น packet ตามที่โจทย์ระบุได้ด้วยวิธีการใด หรือค่าที่นำมาตอบ นำมาจาก field ไດของ header ตาม protocol ไດ

ในกรณีที่คัดลอกคำตอบของคนอื่นมา ให้ระบุชื่อของบุคคลที่เป็นต้นฉบับมาด้วย หากตรวจพบว่าการลอกมาแต่ไม่มีการระบุชื่อบุคคลที่เป็นต้นฉบับ ผู้สอนจะถือว่าทุจริตและอาจพิจารณาลงโทษให้ตกเกณทรายวิชาในทันที

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