นายภากรณ์ ธนประชานนท์ 62010694

1. ให้เปิดไฟล์ http-browse101d.pcapng ค้นหา 3 way handshake แรกในไฟล์แล้ว บันทึกข้อมูลลงในตารางด้านล่าง (ทั้ง Seq# และ Ack# ให้ใช้แบบ raw ในช่อง Flag ให้บอกว่ามี Flag ใดที่ Set บ้าง

SYN

Src Port : 61598	Dest Port : 80
Seq # : 610997682	
Ack # : 0	
Flags : Syn	8192

SYN-ACK

Src Port : 80	Dest Port : 61598
Seq # : 4134094401	
Ack # : 610997683	
Flags : Syn, Ack	14300

ACK

Src Port : 61598	Dest Port : 80
Seq # : 610997683	
Ack # : 4134094402	
Flags : Ack	65780

- ค่าความยาวข้อมูลของ packet ทั้ง 3 เท่ากับเท่าไรบ้าง 66,66 ,54 byte
- ใน packet SYN มีข้อมูลอื่นๆ ส่งมาด้วยหรือไม่ อะไรบ้าง (ดูในคอลัมน์ info) และข้อมูลต่างๆ เหล่านั้นมีความหมายอะไรหรือนำไปใช้อะไร (ให้ค้นหาข้อมูลเพิ่มเติมจากหนังสือ)

ข้อมูล	ความหมาย
Win=8192	The window size from TCP header
Len=0	TCP Segment Length
MSS=1460	Maximum segment size
WS=4.	Window scale

- ใน packet SYN-ACK มีข้อมูลอื่นๆ ส่งมาด้วยหรือไม่ อะไรบ้าง (ดูในคอลัมน์ info) และข้อมูลต่างๆ เหล่านั้นมีความหมายอะไรหรือนำไปใช้อะไร

ข้อมูล	ความหมาย
Win=14300	The window size value from the TCP header
Len=0	TCP Segment Length
WS=64	Window scale
SACK_PERM=1	Selective ACKknowledgment

- ให้ดู packet ที่ส่งข้อมูล packet แรก (หรือ packet อื่นก็ได้) ให้ตอบว่าในข้อมูลที่ไม่เท่ากันของ Client กับ Server ในการเลือกใช้ข้อมูลหนึ่ง (เนื่องจากทั้ง 2 ด้านต้องใช้พารามิเตอร์เดียวกันในการส่งข้อมูล) คิดว่ามีหลักในการเลือกอย่างไร

คิดว่าเลือกโดยการที่ Client ส่ง GET ข้อมูลที่อยากได้ไปทาง Server ให้ส่งข้อมูลที่ต้องการกลับมาโดยทาง Server จะส่ง ACK ของ GET กลับไปพร้อมกับข้อมูลที่ต้องการ หากฝั่ง Client ได้รับข้อมูลที่ต้องการแล้วนั้น ก็จะทำการส่ง ACK กลับไปให้ฝั่ง Server รับรู้ด้วย

2. ให้หา Packet ที่ปิด Connection ของ Connection ในข้อ 1 โดยให้บอกขั้นตอนการหาและป้อนรายละเอียดลงในตาราง (ข้อมูล Seq# และ Ack # ให้ใช้แบบ Relative)

Packet# 1663	
Src Port : 61598	Dest Port : 80
Seq # : 323	
Ack # : 1127	
Flags : FIN, ACK	64652

Packet# 1664	
Src Port : 80	Dest Port : 61598
Seq # : 1127	
Ack # : 324	
Flags : FIN, ACK	15424

Packet# 1665	
Src Port : 61598	Dest Port : 80
Seq # : 324	
Ack # : 1128	
Flags : ACK	64652

วิธีค้นหา

ใช้ Filter = ((ip.dst == 173.194.79.121) && (ip.src == 24.6.173.220)) or ((ip.dst == 24.6.173.220) && (ip.src == 173.194.79.121)) เพื่อกรองการเชื่อมต่ออื่นออกไป และหา Flag FIN,ACK

4. จากไฟล์ http-browse101d.pcapng ให้สร้าง display filter ที่สามารถแสดงเฉพาะ packet ต่อไปนี้ โดยไม่มี packet อื่นๆ มาปน (นักศึกษาพยายามคิดด้วยตนเอง)
   - packet SYN และ SYN/ACK ของ 3 way handshake (packet ที่ 1 และ 2)
   - packet SYN/ACK และ ACK ของ 3 way handshake (packet ที่ 2 และ 3)
   - packet SYN และ ACK 3 way handshake (packet ที่ 1 และ 3)

ใช้ (tcp.flags.syn == 1)

ใช้ (tcp.ack == 1) && !(tcp.flags.push == 1)

ใช้ (tcp.seq == 0 or tcp.seq == 1) && !(tcp.flags.push == 1)

5. เราสามารถใช้ค่า RTT ของ TCP handshaking ตามข้อ 4 มาใช้วัดประสิทธิภาพของ Web Server ได้เช่นกัน โดย Server ที่มีค่า RTT น้อย แสดงถึงการตอบสนองที่รวดเร็ว ดังนั้นให้ capture ข้อมูลจากเว็บและใช้ display filter ตามข้อ 4 (ให้นักศึกษาเลือกใช้ตัวที่เหมาะสม) เพื่อหาค่า RTT ของเว็บต่างๆ จำนวน 3 เว็บ แล้วนำค่ามาใส่ตาราง

URL	เวลา
imperva.com	0.005298
rarbg.to	0.004735
coursera.org	0.005583

- ให้ตอบว่าระหว่าง RTT ที่วัดในครั้งนี้ กับ HTTP RTT ที่วัดในครั้งก่อนหน้านี้ บอกถึงอะไร และแตกต่างกันอย่างไร

RTT ที่วัดในครั้งนี้คือการวัดประสิทธิภาพแค่ช่วงการเชื่อมต่อ TCP handshake แต่ HTTP RTT ที่วัดคราวที่แล้วคือวัดประสิทธิภาพเมื่อ Browser ส่ง request ไปแล้วจนได้รับ response จาก server