

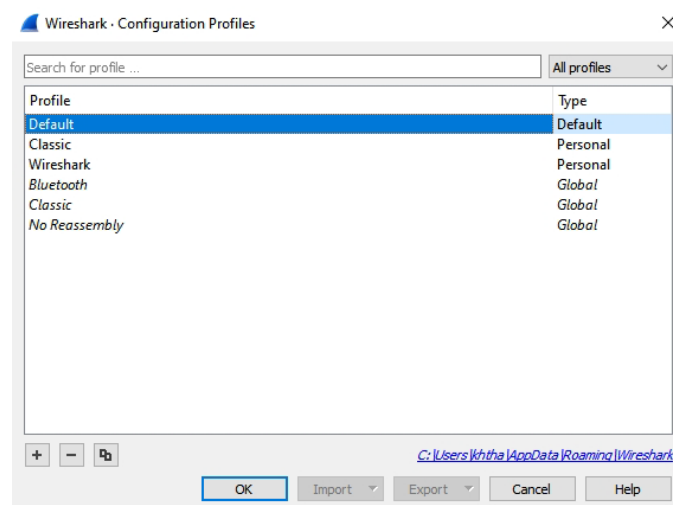
กิจกรรมที่ 2 : การ Capture ข้อมูลจากระบบเครือข่าย

ในกิจกรรมที่ผ่านมา นักศึกษาได้เรียนรู้การติดตั้งโปรแกรม และ การจัดการกับคอลัมน์ ในกิจกรรมนี้ จะทำความเข้าใจกับ Configuration Profiles, การ Capture ข้อมูล และ TCP Delta

Configuration Profile

Configuration Profile คือ รูปแบบการกำหนดค่าการใช้งาน เนื่องจากโปรแกรม Wireshark สามารถนำไปใช้งานได้หลายรูปแบบ ดังนั้นการนำไปใช้งานในแต่ละเรื่องก็อาจจะมีการตั้งค่าไม่เหมือนกัน เช่น การเพิ่มคอลัมน์จากครั้งที่ผ่านๆมา ถือเป็นการเปลี่ยนแปลงโปรแกรม (Configuration) อย่างหนึ่ง การเพิ่มคอลัมน์ Host เข้าไป ทำให้รูปแบบของโปรแกรมเปลี่ยนแปลง หากเปิดไฟล์อื่นที่ไม่จำเป็นจะต้องดูคอลัมน์ Host ก็ต้องลบคอลัมน์นี้ออกไป ทำให้ผู้ใช้งานต้องลำบากในการคอยปรับรูปแบบการแสดงผล (และการกำหนดอื่นๆ)

โปรแกรม Wireshark จึงได้สร้าง Configuration Profile มาให้ โดยหากต้องการเปลี่ยนแปลงรูปแบบการใช้งานก็เพียงแค่เปลี่ยน Profile ใหม่เท่านั้น รูปแบบการใช้งานก็จะเปลี่ยนไปตามที่ต้องการทันที



ในหน้าโปรแกรม Wireshark ให้เลือก Edit -> Configuration Profiles... จะปรากฏหน้าต่างดังรูปด้านบน ซึ่งจะ มี 2 Profiles ที่เป็นของ Wireshark แต่เดิม คือ Classic กับ Default โดย Default จะเป็น Config. ดั้งเดิม ดังนั้นเราไม่ควรใช้ Default Profiles เพราะหากเราปรับเปลี่ยนโปรแกรม เราจะจำไม่ได้ว่า Profile แรกเริ่มเป็นแบบไหนกันแน่ ดังนั้นควรใช้การสร้าง Profile ใหม่ ซึ่งทำได้ 2 วิธี คือ กด + จากรูปด้านบน หรือ คลิกขวาตรงมุมขวาล่างของหน้าต่าง ตรงคำว่า Profile แล้วเลือก New...

วิธีปฏิบัติที่เหมาะสม คือ ใช้ 1 Profile ต่องาน 1 แบบ เพื่อที่เมื่อเจองานลักษณะเดิม จะได้นำ Profile ที่เคยสร้างไว้มาใช้ได้ทันที ไม่ต้องมาปรับแต่ง Wireshark ใหม่

โดยสิ่งที่จะเก็บใน Profile ประกอบด้วย

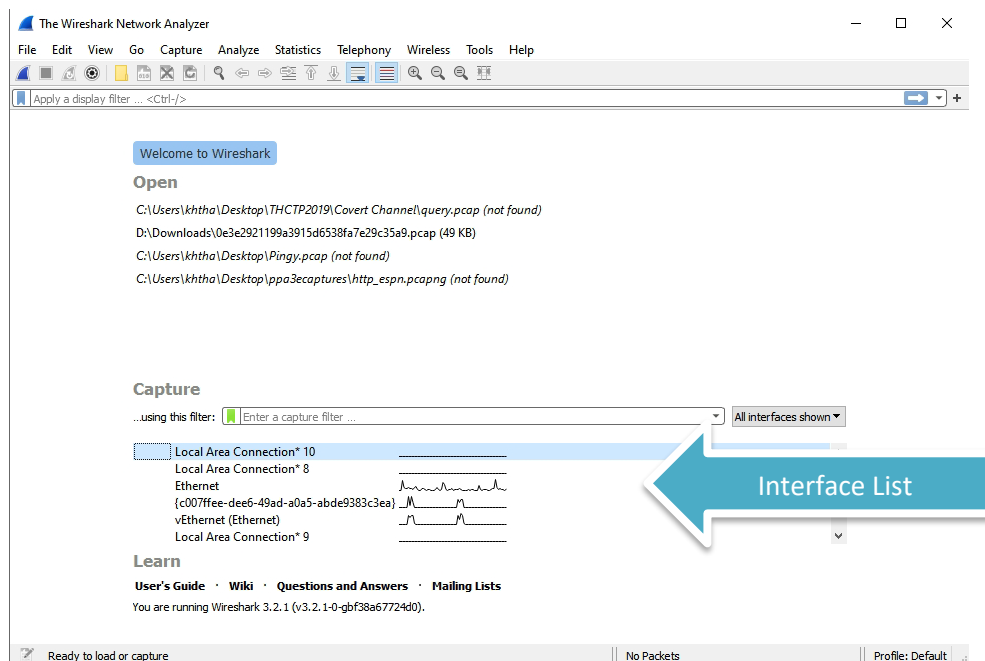
- Preference
- Capture Filters
- Display Filters
- Coloring Rules
- Disable Protocols
- ข้อมูลการแสดงผล เช่น คอลัมน์ หรือ ความกว้างของคอลัมน์

การสร้าง Profile ใหม่ จะเป็นการ copy มาจาก Default Profile ให้ทดลองดังนี้

1. Edit -> Configuration Profiles...
2. กด New (+) แล้วตั้งชื่อว่า Test_Wireshark
3. ทดลองเปิดไฟล์ http-google101.pcapng เพิ่มคอลัมน์ Host เหมือนครั้งที่ผ่านมา
4. เปลี่ยน Profile เป็น Default คอลัมน์แสดงอย่างไร โปรดจดจำว่าไม่ได้เพิ่มคอลัมน์นี้จกจอ(ง)
5. ให้เปลี่ยน Profile เป็น Test_Wireshark แล้วปิดไฟล์

การดักจับข้อมูล

ในการดักจับข้อมูล สามารถดักจับได้หลาย Interface ตาม Interface ที่มีในแต่ละเครื่อง โดย Interface ที่มีข้อมูลจะแสดงเป็นรูปกราฟท้าย Interface นั้น



ให้ทดลองดังนี้

6. เอาเมาส์ไปคลิกที่ Interface ที่มีข้อมูล และ คลิกปุ่ม Start Capture ที่อยู่ใน Toolbar
7. ให้เปิด Browser ใดๆ ก็ได้ แล้วป้อน URL www.ce.kmitl.ac.th (ถ้าเข้าไม่ได้ให้ใช้ Link อื่นได้)
8. เมื่อแสดงผลครบหน้าแล้วสั่งให้หยุด Capture
9. ได้ข้อมูลกี่ Packet 2069 packets

ในการ Capture ในลักษณะข้างต้น จะเห็นว่าจะได้ข้อมูลจำนวนมาก โดยมีข้อมูลที่เราไม่สนใจติดเข้ามาด้วยจำนวนมาก (เรียกว่า Background Data) หากเราต้องการจะสั่งให้ Wireshark ดักจับข้อมูลเฉพาะที่เราสนใจ เราจะต้องใช้เครื่องมือที่เรียกว่า Capture Filter โดย Capture Filter คือ ตัวกรองที่จะใช้ในขณะที่ทำการ Capture โดยสามารถกรองได้ดังนี้

กรองด้วยชื่อ (Host name) กรอบด้วย Network Address (โดยทั่วไปคือ IP Address) และ Port Number ให้ทดลองดังนี้

10. ทำตามขั้นตอนในข้อ 6-8 อีกครั้ง แต่ในช่อง ...using this filter: ให้ป้อน host
www.ce.kmitl.ac.th
11. ทำตามขั้นตอนในข้อ 6-8 อีกครั้ง แต่ในช่อง ...using this filter: ให้ป้อน host 161.246.4.119
12. ขั้นตอนในข้อ 5 และ 6 ให้ผลต่างกันอย่างไร

จำนวน packets ไม่เท่ากัน

13. ใน Packet Details Pane หัวข้อ Internet Protocol Version 4 ให้หาส่วนที่เขียนว่า Source และ Destination ให้นักศึกษาลองเดาความหมายว่าหมายถึงอะไร

Source : ผู้ส่งของ IP คู่นี้

Destination: ปลายทาง IP ของเว็บ

14. ทำตามขั้นตอนในข้อ 6-8 อีกครั้ง แต่ในช่อง ...using this filter: ให้ป้อน src host 161.246.4.119
15. ทำตามขั้นตอนในข้อ 6-8 อีกครั้ง แต่ในช่อง ...using this filter: ให้ป้อน dst host 161.246.4.119
16. จากข้อ 14 และข้อ 15 การทำงานแตกต่างกันอย่างไร เพราะอะไร

ข้อ 14 ให้ 161.246.4.119 เป็น source หมายความว่า host นี้เป็น destination ของ host ปลายทาง host ที่แสดงคือ เว็บที่เก็ตรหัสไป

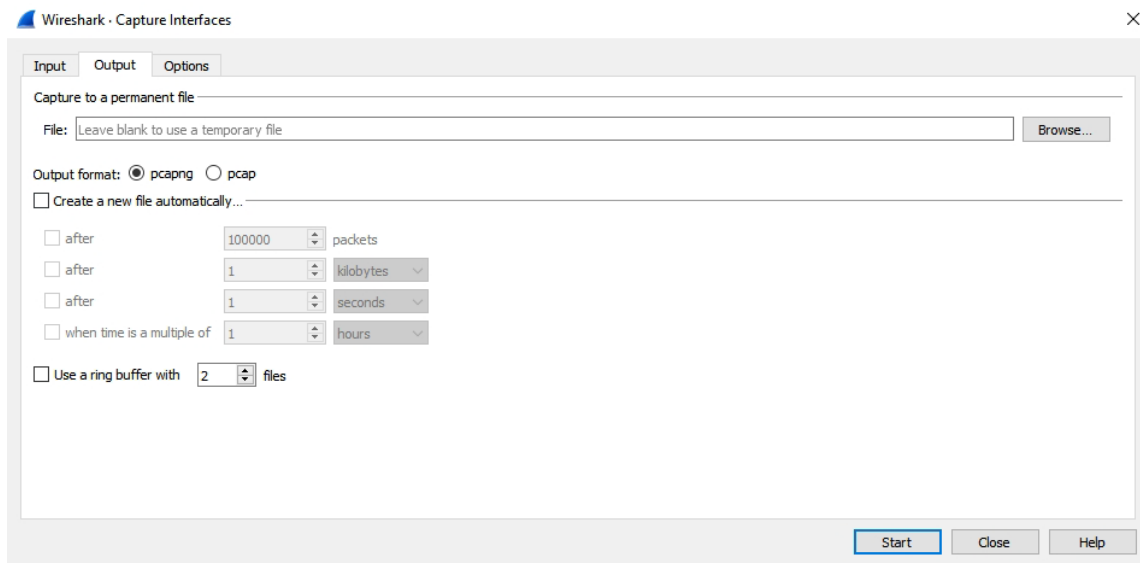
17. ถ้าป้อน not host 161.246.4.119 คิดว่าจะหมายถึงอะไร

ไม่แสดง packets ที่มี IP 161.246.4.119

18. ให้นักศึกษาสรุปการใช้งานการใช้ Capture Filter เบื้องต้น

ทำแบบที่กรอง packets ที่ต้องการหรือไม่ต้องการ capture ได้

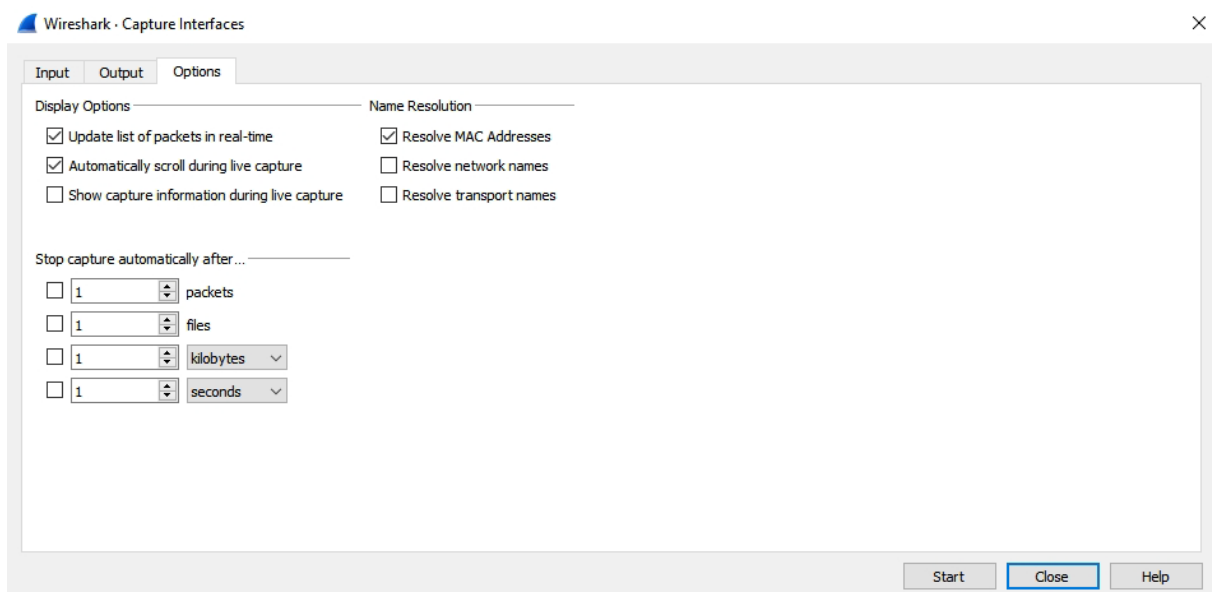
ใน Wireshark สามารถกำหนดเงื่อนไขของการดักจับข้อมูลได้ หากเลือก Capture Option จาก Toolbar



ใน Tab Output เราสามารถกำหนดให้ save ข้อมูลที่ capture เป็นไฟล์ได้ โดยอัตโนมัติ โดยไม่ต้องคอย save เอง นอกจากนั้นยังสามารถกำหนดเงื่อนไขได้

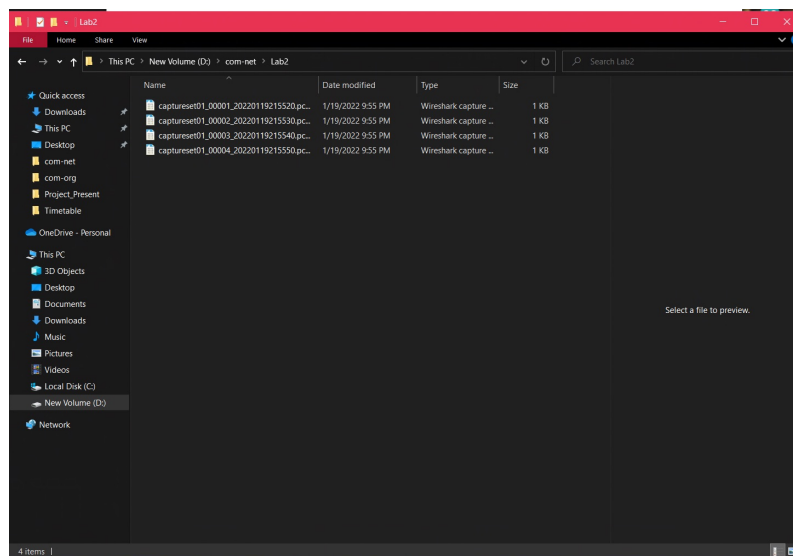
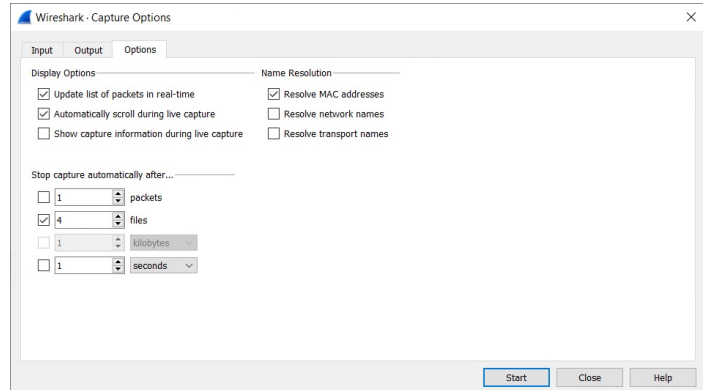
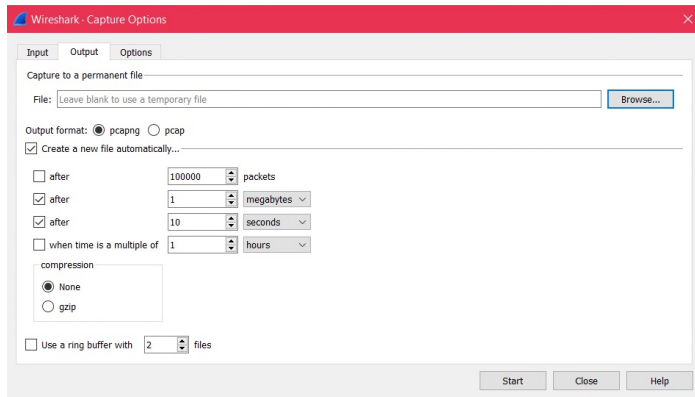
- สร้างไฟล์ใหม่ทุก จำนวน packet ที่กำหนด
- สร้างไฟล์ใหม่ เมื่อไฟล์มีขนาดถึงขนาดที่กำหนด ซึ่งจะทำให้ 1 ไฟล์ไม่ใหญ่มากเกินไป
- สร้างไฟล์ใหม่ ทุกช่วงเวลาที่จะระบุ

สามารถกำหนดให้ทำงานแบบ Ring Buffer คือ ย้อนกลับไปใช้ไฟล์เดิม เพื่อป้องกันไม่ให้ใช้พื้นที่ในฮาร์ดดิสก์มากเกินไปได้อีกด้วย



ใน Tab Options ยังสามารถกำหนดการหยุด Capture ได้ด้วย โดยสามารถกำหนดได้ว่าให้หยุดเมื่อ Capture ครบกี่ Packet หรือ ครบกี่ไฟล์ หรือ ครบขนาดที่ต้องการ หรือ ครบเวลาที่ต้องการ

19. ให้สร้างไฟล์ชื่อ captureset01.pcapng โดยกำหนดเงื่อนไขให้ขึ้นไฟล์ใหม่ทุก 1 MB และทุก 10 วินาที และหยุดหลังจาก 4 ไฟล์ หลังจากกด start ให้ไปที่ไซต์ <http://www.openoffice.org> และกดดูไปเรื่อยๆ ไม่น้อยกว่า 40 วินาที ให้ Capture ภาพหน้าของการตั้งค่า และภาพไฟล์ Output ลงในที่ว่างด้านล่างนี้



20. ให้ไปที่ File -> File Set -> List Files มีอะไรเกิดขึ้น อธิบาย

มี 4 File ที่ทำไปจนหมดแล้วไฟล์จับคูป

ข้อมูลเวลา

ปัญหาเกี่ยวกับเวลาเป็นปัญหาสำคัญในระบบเครือข่าย เช่น ความล่าช้าในการทำงาน โดยความล่าช้าหรือเวลาที่เสียไปในการทำงานในการทำงานของระบบเครือข่ายจะเรียกว่า Latency ซึ่งโดยทั่วไปจะวัดตั้งแต่เวลาที่ Host ส่ง Request ออกไป จนถึงเวลาที่ Reply กลับมา โดยทั่วไป

การพิจารณาเกี่ยวกับเวลาใน Wireshark จะดูที่คอลัมน์ Time เป็นหลัก ปกติคอลัมน์ Time จะแสดงข้อมูล Seconds Since Beginning of Capture โดยเริ่มจาก 0.000000000 ซึ่งจะใช้พิจารณา แต่เพื่อให้เห็นค่าระหว่าง Packet (เรียกว่า delta time) ให้เปลี่ยนการแสดงผลในช่อง Time เป็น **View | Time Display Format | Seconds Since**

Previous Displayed Packet

21. ให้สร้างและใช้ Profile ใหม่ เพื่อไม่กระทบกับ Default Profile
22. ให้ capture ข้อมูลระหว่างเครื่องนักศึกษา กับ www.ce.kmitl.ac.th เท่านั้น
23. ตั้งการแสดงผล Time เป็น Seconds Since Previous Displayed Packet
24. ให้หาค่าเวลาที่มากที่สุดในช่อง Time เป็น packet ที่เท่าไร 17 และให้ถามเพื่อนอีก 2 คน พบที่เดียวกันหรือไม่ ของเพื่อน packet ที่เท่าไร 46 ของเพื่อน packet 22 และ 29

-
25. ใน Packet Details Pane หัวข้อ Transmission Control Protocol (จะเรียนในบทที่ 3) คลิกขวาที่ Time since previous frame in this TCP stream แล้วเลือก Apply as Column ให้ตั้งชื่อคอลัมน์ว่า TCP Delta และเลื่อนมาใกล้ๆ Time

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{D6DB428C-ACA3-4424-A94A-D43F6A65603F}, id 0
> Ethernet II, Src: Dell_02:eb:60 (18:66:da:02:eb:60), Dst: HuaweiTe_fb:24:d5 (c4:b8:b4:fb:24:d5)
> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 161.246.4.119
v Transmission Control Protocol, Src Port: 1847, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 1847
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Sequence number (raw): 1546021792
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
> Flags: 0x002 (SYN)
  Window size value: 64240
  [Calculated window size: 64240]
  Checksum: 0x6840 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
> Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
v [Timestamps]
  [Time since first frame in this TCP stream: 0.000000000 seconds]
  [Time since previous frame in this TCP stream: 0.000000000 seconds]
```

26. ค่า TCP Delta นี้เป็นระยะเวลาของ Latency ที่คิดเฉพาะใน TCP Stream เดียวกัน เนื่องจากในการขอข้อมูล 1 หน้าเว็บ อาจมีการขอข้อมูลหลายครั้ง สำหรับแต่ละส่วนของเว็บ ซึ่งอาจขอไปพร้อมๆ กันก็ได้ (หลาย Stream) ดังนั้นค่าเวลาในช่อง Time ที่เป็น Seconds Since Previous Displayed Packet จึงอาจไม่สะท้อน ความล่าช้าที่เกิดขึ้นจริง ค่า TCP Delta นี้ จึงสามารถตรวจสอบความล่าช้าได้ชัดเจนกว่า

27. ให้หาค่าเวลาที่มากที่สุดในช่อง TCP Delta เป็น packet ที่เท่าไร 17 และให้ถามเพื่อนอีก 2 คน พบที่เดียวกันหรือไม่ ของเพื่อน packet ที่เท่าไร ห่ม ขวเมือง packets ๑๒ และ ๒๑ เป็นการทำงานอะไร protocol TCP

Capture ภาพของ packet list pane ลงในที่ว่างด้านล่าง

No.	Time	Source	Destination	Protocol	Length	Time since previous frame in this TCP stream	Info
17	3.636273	161.246.4.119	192.168.1.107	TCP	66	3.875332000	[TCP Retransmission] 80 → 49389 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 SACK_PERM=1 WS=32
13	0.057086	192.168.1.107	161.246.4.119	HTTP	835	0.057086000	GET /slideshow2.css HTTP/1.1
16	0.054833	192.168.1.107	161.246.4.119	TCP	54	0.054833000	49387 → 80 [ACK] Seq=1674 Ack=4927 Win=516 Len=0
8	0.042748	161.246.4.119	192.168.1.107	TCP	1506	0.042748000	80 → 49387 [ACK] Seq=1 Ack=893 Win=239 Len=1452 [TCP segment of a reassembled PDU]
12	0.042532	192.168.1.107	161.246.4.119	TCP	54	0.042532000	49387 → 80 [ACK] Seq=893 Ack=4356 Win=510 Len=0
7	0.022776	161.246.4.119	192.168.1.107	TCP	60	0.030289000	80 → 49387 [ACK] Seq=1 Ack=893 Win=239 Len=0
14	0.009659	161.246.4.119	192.168.1.107	TCP	60	0.009659000	80 → 49387 [ACK] Seq=4356 Ack=1674 Win=294 Len=0
11	0.007855	161.246.4.119	192.168.1.107	HTTP	1505	0.007855000	HTTP/1.1 200 OK (text/html)
4	0.006646	161.246.4.119	192.168.1.107	TCP	60	0.007508000	80 → 49386 [ACK] Seq=1 Ack=2 Win=405 Len=0
5	0.000131	161.246.4.119	192.168.1.107	TCP	66	0.006777000	80 → 49389 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 SACK_PERM=1 WS=32
9	0.001496	161.246.4.119	192.168.1.107	TCP	1506	0.001496000	80 → 49387 [ACK] Seq=1453 Ack=893 Win=239 Len=1452 [TCP segment of a reassembled PDU]
10	0.000074	192.168.1.107	161.246.4.119	TCP	54	0.000074000	49387 → 80 [ACK] Seq=893 Ack=2905 Win=516 Len=0
6	0.000042	192.168.1.107	161.246.4.119	TCP	54	0.000042000	49389 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
18	0.000025	192.168.1.107	161.246.4.119	TCP	66	0.000025000	[TCP Dup ACK 6#1] 49389 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0 SLE=0 SRE=1
15	0.000000	161.246.4.119	192.168.1.107	HTTP	625	0.000000000	HTTP/1.1 404 Not Found (text/html)
3	0.000694	192.168.1.107	161.246.4.119	TCP	66	0.000000000	49389 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000168	192.168.1.107	161.246.4.119	HTTP	946	0.000000000	GET / HTTP/1.1
1	0.000000	192.168.1.107	161.246.4.119	TCP	54	0.000000000	49386 → 80 [FIN, ACK] Seq=1 Ack=1 Win=516 Len=0

28. ให้นักศึกษาตอบคำถามต่อไปนี้

นักศึกษาคิดว่า Packet ที่เป็นการเรียกหน้า Homepage (/) ของหน้าเว็บอยู่ที่ Packet ไດ 2

และ Response Code ของ Packet ข้างต้นอยู่ที่ Packet ไດ 11

งานครั้งที่ 2

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งโดยเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา และ _Lab2 เช่น 63010789_Lab2.pdf
- กำหนดส่ง ภายในวันที่ 26 มกราคม 2564