กิจกรรมที่ 2 : การ Capture ข้อมูลจากระบบเครือข่าย

Configuration Profile

การสร้าง Profile ใหม่นี้ 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

   ➔ คอลัมน์จะกลับมาเหมือนเดิม คือ ไม่มีคอลัมน์ Host เพราะคอลัมน์ Host จะอยู่ใน Profile Test_Wireshark เมื่อเปลี่ยน profile เป็น Default จึงไม่แสดงอีก
5. ให้เปลี่ยน Profile เป็น Test_Wireshark แล้วปิดไฟล์

การดักจับข้อมูล

ให้ทดลองดังนี้

1. เอาเมาส์ไปคลิกที่ Interface ที่มีข้อมูล และ คลิกปุ่ม Start Capture ที่อยู่ใน Toolbar
2. ให้เปิด Browser ใดๆ ก็ได้ แล้วป้อน URL www.ce.kmitl.ac.th (ถ้าเข้าไม่ได้ให้ใช้ Link อื่นได้)
3. แล้วสั่งให้หยุด Capture
4. ได้ข้อมูลกี่ Packet _____

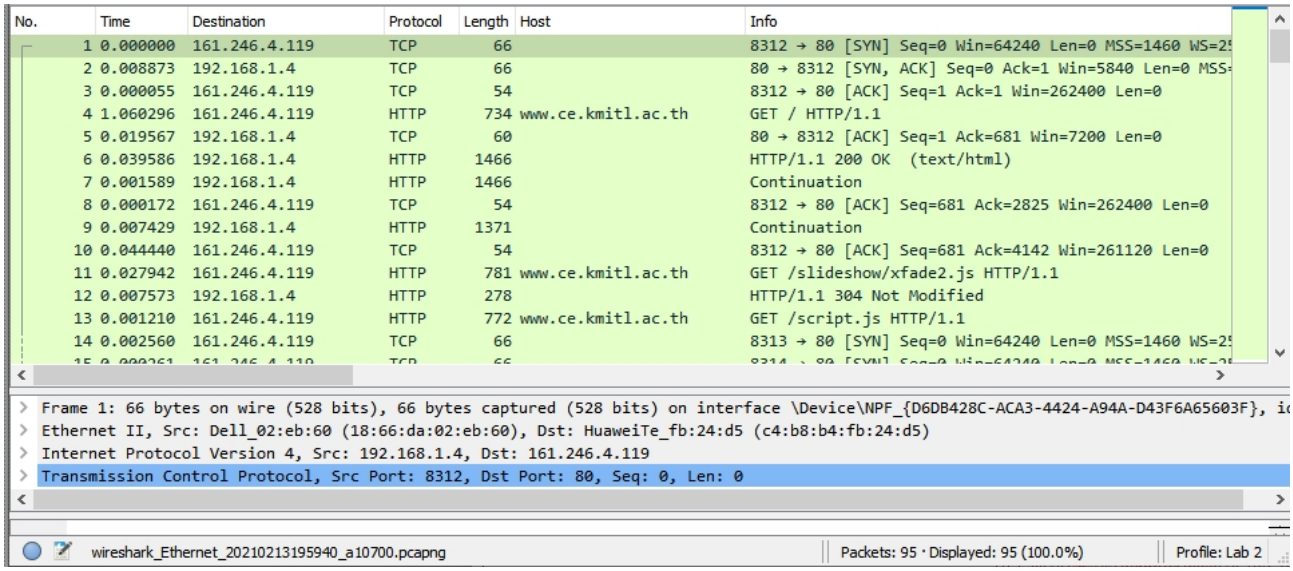
   ➔ ไม่แน่นอน ขึ้นกับการทำงานในเวลานั้น
5. ทำตามขั้นตอนในข้อ 1-3 อีกครั้ง แต่ในช่อง ...using this filter: ให้ป้อน **host www.ce.kmitl.ac.th**

   ➔ ไม่แน่นอน ขึ้นกับการทำงานในเวลานั้น แต่ควรได้น้อยกว่าข้อ 4
   เนื่องจากมีการกรองออก
6. ทำตามขั้นตอนในข้อ 1-3 อีกครั้ง แต่ในช่อง ...using this filter: ให้ป้อน **host 161.246.4.119**

   ➔ ผลลัพธ์ควรเหมือนกับข้อ 5 เนื่องจากเป็นเครื่องเดียวกัน
7. ขั้นตอนในข้อ 5 และ 6 ต่างกันอย่างไร

   ➔ เหมือนกัน
   ผลลัพธ์ควรเหมือนกัน เพราะเป็นการ Capture จากเว็บไซต์เดิม แต่ผลอาจแตกต่างกันได้บ้าง กรณีที่ไม่ได้หยุด Capture ทันทีหลังจากโหลดหน้าเว็บเสร็จ

ใช้ host www.ce.kmitl.ac.th

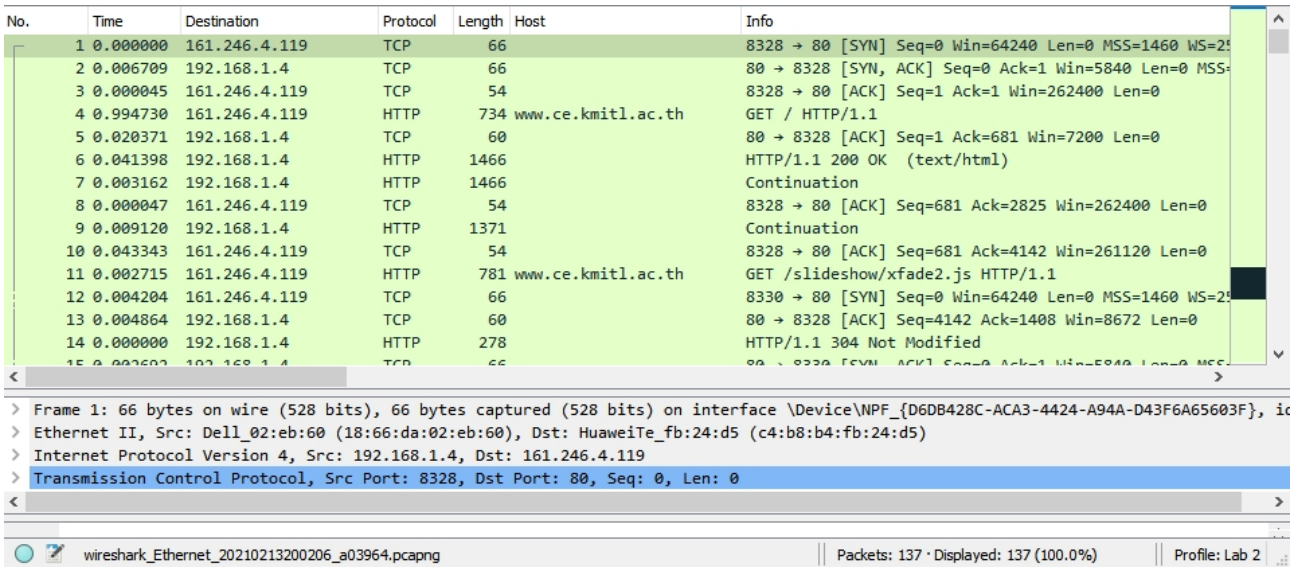


No.	Time	Destination	Protocol	Length	Host	Info
1	0.000000	161.246.4.119	TCP	66		8312 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
2	0.008873	192.168.1.4	TCP	66		80 → 8312 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
3	0.000055	161.246.4.119	TCP	54		8312 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
4	1.060296	161.246.4.119	HTTP	734	www.ce.kmitl.ac.th	GET / HTTP/1.1
5	0.019567	192.168.1.4	TCP	60		80 → 8312 [ACK] Seq=1 Ack=681 Win=7200 Len=0
6	0.039586	192.168.1.4	HTTP	1466		HTTP/1.1 200 OK (text/html)
7	0.001589	192.168.1.4	HTTP	1466		Continuation
8	0.000172	161.246.4.119	TCP	54		8312 → 80 [ACK] Seq=681 Ack=2825 Win=262400 Len=0
9	0.007429	192.168.1.4	HTTP	1371		Continuation
10	0.044440	161.246.4.119	TCP	54		8312 → 80 [ACK] Seq=681 Ack=4142 Win=261120 Len=0
11	0.027942	161.246.4.119	HTTP	781	www.ce.kmitl.ac.th	GET /slideshow/xfade2.js HTTP/1.1
12	0.007573	192.168.1.4	HTTP	278		HTTP/1.1 304 Not Modified
13	0.001210	161.246.4.119	HTTP	772	www.ce.kmitl.ac.th	GET /script.js HTTP/1.1
14	0.002560	161.246.4.119	TCP	66		8313 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25

```
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{D6DB428C-ACA3-4424-A94A-D43F6A65603F}, id
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
Transmission Control Protocol, Src Port: 8312, Dst Port: 80, Seq: 0, Len: 0
```

wireshark_Ethernet_20210213195940_a10700.pcapng | Packets: 95 · Displayed: 95 (100.0%) | Profile: Lab 2

ใช้ host 161.246.4.119



No.	Time	Destination	Protocol	Length	Host	Info
1	0.000000	161.246.4.119	TCP	66		8328 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
2	0.006709	192.168.1.4	TCP	66		80 → 8328 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
3	0.000045	161.246.4.119	TCP	54		8328 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
4	0.994730	161.246.4.119	HTTP	734	www.ce.kmitl.ac.th	GET / HTTP/1.1
5	0.020371	192.168.1.4	TCP	60		80 → 8328 [ACK] Seq=1 Ack=681 Win=7200 Len=0
6	0.041398	192.168.1.4	HTTP	1466		HTTP/1.1 200 OK (text/html)
7	0.003162	192.168.1.4	HTTP	1466		Continuation
8	0.000047	161.246.4.119	TCP	54		8328 → 80 [ACK] Seq=681 Ack=2825 Win=262400 Len=0
9	0.009120	192.168.1.4	HTTP	1371		Continuation
10	0.043343	161.246.4.119	TCP	54		8328 → 80 [ACK] Seq=681 Ack=4142 Win=261120 Len=0
11	0.002715	161.246.4.119	HTTP	781	www.ce.kmitl.ac.th	GET /slideshow/xfade2.js HTTP/1.1
12	0.004204	161.246.4.119	TCP	66		8330 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
13	0.004864	192.168.1.4	TCP	60		80 → 8328 [ACK] Seq=4142 Ack=1408 Win=8672 Len=0
14	0.000000	192.168.1.4	HTTP	278		HTTP/1.1 304 Not Modified

```
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{D6DB428C-ACA3-4424-A94A-D43F6A65603F}, id
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
Transmission Control Protocol, Src Port: 8328, Dst Port: 80, Seq: 0, Len: 0
```

wireshark_Ethernet_20210213200206_a03964.pcapng | Packets: 137 · Displayed: 137 (100.0%) | Profile: Lab 2

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

   ➔ Source หมายถึง Source IP Address, Destination หมายถึง Destination IP Address

   Source IP Address คือ IP Address ของเครื่องที่เป็นต้นทาง

   Destination IP Address คือ IP Address ของเครื่องที่เป็นปลายทาง

9. ทำตามขั้นตอนในข้อ 1-3 Capture Filter แต่ในช่อง ...using this filter: ให้ป้อน src host **161.246.4.119**
10. ทำตามขั้นตอนในข้อ 1-3 Capture Filter แต่ในช่อง ...using this filter: ให้ป้อน dst host **161.246.4.119**

11. จากข้อ 9 และข้อ 10 การทำงานแตกต่างกันอย่างไร เพราะอะไร

    ➔ ข้อ 9 จะได้ 9 Packet เป็น Packet เฉพาะที่มาจาก Web Server

    ➔ ข้อ 10 จะได้ 12 Packet เป็น Packet เฉพาะที่ไปยัง Web Server

12. ถ้าป้อน **not host 161.246.4.119** คิดว่าจะหมายถึงอะไร

    ➔ หมายถึงให้ Capture ทุก Packet ที่ไม่ได้มาจากหรือส่งไปที่ IP Address 161.246.4.119

13. ให้นักศึกษาสรุปการใช้งานการใช้ Capture Filter เบื้องต้น

    ➔ สามารถเลือก Capture เพื่อให้ได้ข้อมูลที่ต้องการได้ เช่น จากเครื่องหรือไปยังเครื่องที่ต้องการ

14. 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 และไฟล์ Output

    ➔ จะมีการสร้างไฟล์ 4 ไฟล์ในชื่อ captureset01.pcapng – captureset04.pcapng

15. ให้ไปที่ File –> File Set –> List Files มีอะไรเกิดขึ้น อธิบาย

    ➔ สามารถเรียกดูไฟล์เป็น Set ได้

ข้อมูลเวลา

1. ให้สร้างและใช้ Profile ใหม่ เพื่อไม่กระทบกับ Default Profile
2. ให้ capture ข้อมูลจากเครื่องนักศึกษาไปที่ **www.ce.kmitl.ac.th**
3. ตั้งการแสดงผล Time เป็น Seconds Since Previous Displayed Packet
4. ให้หาค่าเวลาที่มากที่สุดในช่อง Time เป็น packet ที่เท่าไร _____ และให้ถามเพื่อนอีก 3 คน พบที่เดียวกันหรือไม่ ของเพื่อน packet ที่เท่าไร _____

    ➔ แต่ละคนอาจได้ไม่เท่ากัน

5. 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
6. ค่า TCP Delta นี้เป็นระยะเวลาของ Latency ที่คิดเฉพาะใน TCP Stream เดียวกัน เนื่องจากในการขอข้อมูล 1 หน้าเว็บ อาจมีการขอข้อมูลหลายครั้ง สำหรับแต่ละส่วนของเว็บ ซึ่งอาจขอไปพร้อมๆ กันก็ได้ ดังนั้นค่าเวลาในช่อง Time ที่เป็น Seconds Since Previous Displayed Packet จึงอาจไม่สะท้อน ความล่าช้าที่เกิดขึ้นจริง ค่า TCP Delta นี้ จึงสามารถตรวจสอบความล่าช้าได้ชัดเจนกว่า
7. ให้หาค่าเวลาที่มากที่สุดในช่อง TCP Delta เป็น packet ที่เท่าไร _____ และให้ถามเพื่อนอีก 3 คน พบที่เดียวกันหรือไม่ ของเพื่อน packet ที่เท่าไร _____

    เป็นการทำงานอะไร _____

➔ โดยทั่วไปจะเป็นตำแหน่งที่มีการ GET เพราะเป็นการดึงไฟล์ดังนั้นจึงใช้เวลานาน แต่หากทิ้งการ Capture ไว้นาน อาจมีการทำงานอย่างอื่นนานกว่าก็ได้

8. ให้นักศึกษาตอบคำถามต่อไปนี้

นักศึกษาคิดว่า Packet ที่เป็นการเรียกหน้า Homepage (/) ของหน้าเว็บอยู่ที่ Packet ใด _____

และ Response Code ของ Packet ข้างต้นอยู่ที่ Packet ใด _____

➔ หากเริ่มการ Capture ถูกต้อง โดยมีการใช้ capture filter เป็น www.ce.kmitl.ac.th packet ที่ get / จะอยู่ที่ packet ที่ 4 อาจจะขยับบ้างแต่ไม่มาก

➔ สำหรับ response กรณีนี้จะอยู่ที่ packet 6

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.4	161.246.4.119	TCP	8531 → 80 [SYN] Se
2	0.009144	161.246.4.119	192.168.1.4	TCP	80 → 8531 [SYN, AC
3	0.000057	192.168.1.4	161.246.4.119	TCP	8531 → 80 [ACK] Se
4	1.312833	192.168.1.4	161.246.4.119	HTTP	GET / HTTP/1.1
5	0.019338	161.246.4.119	192.168.1.4	TCP	80 → 8531 [ACK] Se
6	0.052006	161.246.4.119	192.168.1.4	HTTP	HTTP/1.1 200 OK
7	0.001780	161.246.4.119	192.168.1.4	HTTP	Continuation
8	0.000050	192.168.1.4	161.246.4.119	TCP	8531 → 80 [ACK] Se
9	0.006947	161.246.4.119	192.168.1.4	HTTP	Continuation
10	0.050667	192.168.1.4	161.246.4.119	TCP	8531 → 80 [ACK] Se
11	0.022356	192.168.1.4	161.246.4.119	HTTP	GET /slideshow/xfa
12	0.008685	192.168.1.4	161.246.4.119	TCP	8533 → 80 [SYN] Se
13	0.000321	192.168.1.4	161.246.4.119	TCP	8534 → 80 [SYN] Se
14	0.001364	161.246.4.119	192.168.1.4	TCP	80 → 8531 [ACK] Se
15	0.004152	161.246.4.119	192.168.1.4	TCP	80 → 8533 [SYN, AC