

กิจกรรมที่ 4 : HTTP

ในกิจกรรมที่ผ่านมา จะเป็นการแนะนำการใช้งาน Wireshark เป็นส่วนใหญ่ในกิจกรรมครั้งนี้ จะเริ่มทำความรู้จักกับ Protocol ใน Application Layer โดย Protocol แรก คือ HTTP (Hypertext Transport Protocol)

1. ให้ใช้ Wireshark เริ่มทำการ Capture และป้อน url : <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html> เลร์ร์แล้วให้หยุด
2. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP (ถ้าทำถูกจะมีแค่ 2 บรรทัด แต่อาจมี favicon และ Not Found ติดมาไม่ต้องไปสนใจ)
(กรณีบรรทัดที่ 2 (Response) เป็น 304 Not Modified ให้เคลียร์แคชของ Browser และทำใหม่)
3. ใน Packet HTTP Response มีความยาวเฟรมทั้งหมดเท่าไร 128 bytes ให้ Capture หน้าจอส่วนที่แสดงความยาวประกอบ

```
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
Line-based text data: text/html (4 lines)
<html>\n
Congratulations. You've downloaded the file \n
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
</html>\n
```

4. ใน Packet ข้อ 3 ความยาวของ Header Ethernet II เป็นเท่าไร 14 bytes ให้ Capture หน้าจอส่วนที่แสดงความยาวประกอบ (Hint : ใช้ Packet Byte Pane)

Index	Hex	Dec	ASCII
0000	4c 1d 96 52 90 72 c0 b1	108 29 150 84 144 114 192 177 171	L..R.r...k@..Eh
0010	02 0e 44 8c 40 00 f9 06	2 14 68 140 64 0 249 6	..D@...`w....
0020	01 69 00 50 fe 91 39 ad	1 105 0 80 128 254 145 57 173	.i P..9.P.
0030	5c a1 bd af 00 00 48 54	92 161 189 175 0 0 72 84	\.....HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 44	48 48 48 79 67 13 10 68	00 OK..D ate: Wed
0050	2c 20 30 32 20 46 65 62	44 32 48 48 32 32 69 98	, 02 Feb 2022 09
0060	3a 32 36 3a 33 39 20 47	58 50 56 58 53 59 48 71	:26:39 G MT..Serv
0070	65 72 3a 20 41 70 61 63	101 115 54 49 53 97 49 99	er: Apac he/2.4.6
0080	20 28 43 65 6e 74 4f 53	32 44 67 51 102 118 79 83	(CentOS) OpenSS
0090	4c 2f 31 2e 30 2e 32 6b	76 47 51 33 48 48 50 98	L/1.0.2k -fips PH
00a0	50 2f 37 2e 34 2e 32 37	80 47 55 51 48 50 52 98	P/7.4.27 mod_per
00b0	6c 2f 32 2e 30 2e 31 31	96 47 54 51 48 50 52 98	1/2.0.11 Perl/v5
00c0	2e 31 36 2e 33 0d 0a 4c	14 53 56 58 65 59 49 76	.16.3..L ast-Modi
00d0	66 69 65 64 3a 20 57 65	102 105 101 101 54 87 49 95	fied: We d, 02 Fe
00e0	62 20 32 30 32 32 20 30	98 32 48 48 50 52 54 98	b 2022 0 6:59:01
00f0	47 4d 54 0d 0a 45 54 61	71 69 85 65 62 64 66 73	GMT ..ETa g: "80-5
0100	64 37 30 33 38 64 36 66	100 55 58 65 53 62 64 74	d7038d6f 9e53"..A
0110	63 63 65 70 74 2d 52 61	99 99 101 111 74 82 85 73	ccept-Ra nges: by
0120	74 65 73 0d 0a 43 6f 6e	102 101 115 100 108 102 105 111	tes ..Con tent-Len
0130	67 74 68 3a 20 31 32 38	107 116 108 54 48 50 52 98	gth: 128 ..Keep-A

Ethernet (eth), 14 bytes

Packets: 1830 · Displayed: 4 (0.2%) · Dropped: 0 (0.0%) || Profile: Lab3_1

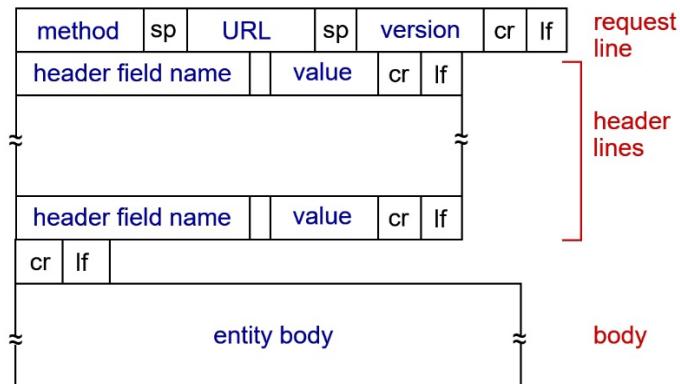
5. ใน Packet ข้อ 3 ความยาวของ TCP Header เป็นเท่าไร 20 bytes ให้ Capture หน้าจอส่วนที่แสดงความยาวประกอบ

```
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 65169, Seq: 1, Ack: 482, Len: 486
  Source Port: 80
  Destination Port: 65169
  [Stream index: 9]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 486]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 967676362
  [Next Sequence Number: 487 (relative sequence number)]
  Acknowledgment Number: 482 (relative ack number)
  Acknowledgment number (raw): 2245443803
  0101 .... = Header Length: 20 bytes (5)
```

6. เหตุผลที่ Header ของข้อมูลต้องซ้อนเป็นชั้นๆ คือ

ข้อมูลจะมีระดับเดียวกัน叫做 layer ไม่ใช่ layer จะมี header ของกันเอง
ตามนี้ application → trasport → network → link → physical

7. จากรูปแบบของ HTTP Message ตามรูป และ HTTP Request และ Response ที่ได้ก้าจับได้ ให้ตอบคำถาม
ตอบใน (สามารถใช้วิธี Capture และ Highlight ข้อมูลเพื่อตอบคำถามได้)



- Browser และ Server ใช้ HTTP version ได้ HTTP / 1.1
- Browser เป็นโปรแกรมอะไร Wireshark
- Server เป็นโปรแกรมอะไร Apache/2.4.6
- ภาษาที่ Browser ระบุว่าสามารถรับจาก Server ได้ text/html ; charset = UFT-8
- Status Code ที่ส่งกลับมาจาก Server หมายง Browser 200 OK
- ค่าของ Last-Modified ของไฟล์ที่ Server Wed, 02 Feb 2022 06:59:01 GMT
- มีข้อมูลกี่比特ที่ส่งมายัง Browser 128 bytes.

```

▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Date: Wed, 02 Feb 2022 09:26:39 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 02 Feb 2022 06:59:01 GMT\r\n
    ETag: "80-5d7038d6f9e53"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.540379000 seconds]
  [Request in frame: 1325]
  [Next request in frame: 1410]
  [Next response in frame: 1413]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
  File Data: 128 bytes

```

- ให้สรุปว่า header field name ตาม HTTP message format ของข้อมูลที่ส่งกลับมีอะไรบ้าง

- Data	- ETag	- Keep - Alive
- Server	- Accept - Ranges	- Connection
- Last - Modified	- Content - Length	- Content - Type

```

▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    Date: Wed, 02 Feb 2022 09:26:39 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 02 Feb 2022 06:59:01 GMT\r\n
    ETag: "80-5d7038d6f9e53"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.540379000 seconds]
  [Request in frame: 1325]
  [Next request in frame: 1410]
  [Next response in frame: 1413]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
  File Data: 128 bytes

```

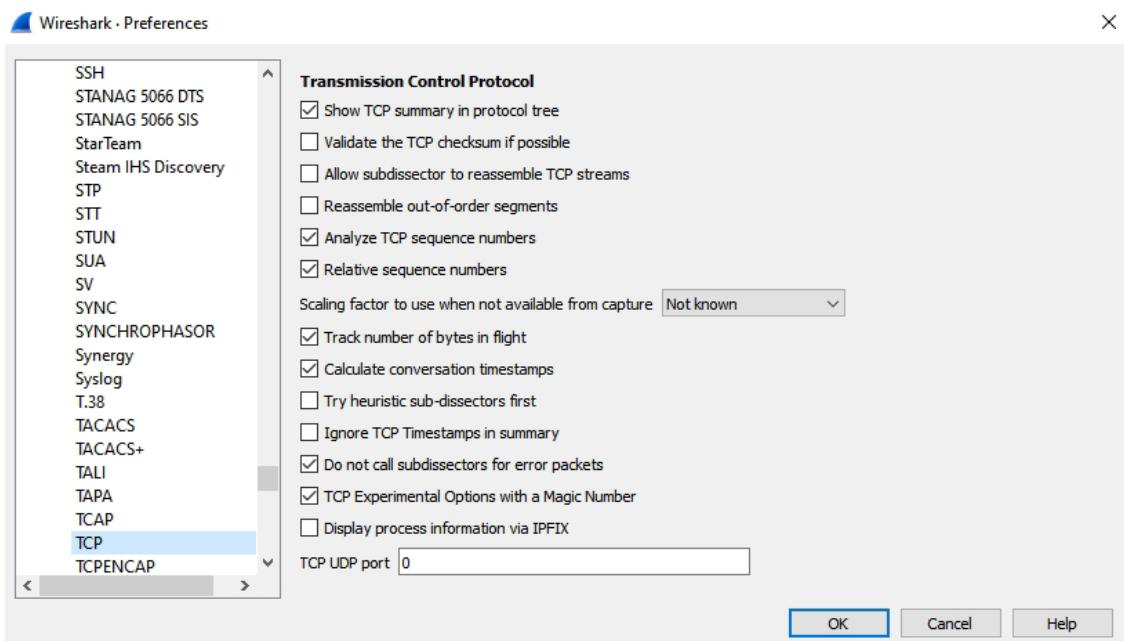
8. ให้นักศึกษาหาวิธี clear cache ของ Browser ที่ตนเองใช้อยู่ และจัดการ clear ให้เรียบร้อย
9. เปิด Wireshark ใหม่แล้ว Capture ที่ url : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html จากนั้นให้กด Reflash เพื่อโหลดหน้าอีกครั้ง จากนั้นให้หยุด Capture

10. ໃຫ້ໃຊ້ display filter : http เพื่อໃຫ້ແສດງເຂົາພາະ Protocol HTTP (ຄໍາທໍາຜູກຈະມີແຕ່ 4 ບຣ້ທັດ ປຣ້ທັດ ແຕ່ອາຈນີ favicon ຕິດມາໄມ້ຕັ້ງປິບສິນໃຈ) ແລະຕອບຄຳຄາມຕອບໂປ່ນີ້

- ໃນ HTTP GET ຄວັງທີ 1 ມີຄໍາວ່າ IF-MODIFIED-SINCE ທີ່ຮູ້ໃນ ໄປໜີ
- ໃນ HTTP GET ຄວັງທີ 2 ມີຄໍາວ່າ IF-MODIFIED-SINCE ທີ່ຮູ້ໃນ ສະໜັບ
- (ຄໍານີ້) ຂໍ້ມູນລື້ຖ້ວາຈາກ IF-MODIFIED-SINCE ມີຄວາມໝາຍອ່າງໄວ

(Wed, 02 Feb 2022 06:59:01 GMT)
*ຂໍ້ມູນລື້ຖ້ວາ Server ຕະຫົບ 304 ລໍາໄຟນາໂປ່ນແກ້ວຕົວທີ່ຕັ້ງປິບສິນໃຈ
ໃນນັ້ນກະໄຟນ໌ເພື່ອ = Server ມີກະຕົບ 304 not modified
ແກ້ວຕາມກ່າວຂໍ້ມູນໃນນັ້ນ, ເປັນຕົວແປ່ນລົງໄວລາທີ່ກ່າວນັດ

11. ໃຫ້ປີ້ Edit | Preference... | Protocol | TCP ຕາມຮູບ



ໃຫ້ແນ່ໃຈວ່າ ໂມື່ຕີກທີ່ Allow subdissector to reassemble TCP streams

12. ໃຫ້ທໍາມານີ້ 8 ອີກຄັ້ງ ແລະເປີດ Wireshark ໃໝ່ແລ້ວ Capture ທີ່ url <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html> ຈາກນີ້ໃຫ້ຍຸດ Capture
13. ໃຫ້ໃຊ້ display filter : http เพื่อໃຫ້ແສດງເຂົາພາະ Protocol HTTP (ຄໍາທໍາຜູກຈະມີ 5 ບຣ້ທັດ) ຜຶ່ງຈະເຫັນວ່າແລ້ວຈາກຂໍ້ມູນ HTTP/1.1 200 OK ແລ້ວ ຍັງມີຂໍ້ມູນຕາມມາດີກ ເນື່ອງຈາກໄຟ້ html ມີຄວາມໝາຍມາກ (ມາກກວ່າ 4000 ໄປຕໍ່) ທຳໃຫ້ມີສາມາດສ່າມາໃນ 1 packet ໄດ້ ຈຶ່ງມີການແບ່ງເປັນໜ່າຍໆ ສ່ວນ (ໂດຍ TCP) ດັ່ງນັ້ນໃນ Wireshark ຈຶ່ງແສດງຄໍາວ່າ Continuation ໃຫ້ນັກຕີກຢາຕອບຄຳຄາມຕອບໂປ່ນີ້

- มี HTTP GET กี่ครั้ง และมี packet ใดบ้างที่มี Status Code และเป็น Status Code ได

มี HTTP GET 1 ครั้ง

packet ที่มี status code ดัง response (packet กี่ 45)

status code : 200

14. ให้ทำการข้อ 5 อีกครั้ง และเปิด Wireshark ใหม่แล้ว Capture ที่ url <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html> จากนั้นให้หยุด Capture

- ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP และให้ตอบคำถามต่อไปนี้
- มี HTTP GET กี่ครั้ง จาก url ใดบ้าง

มี HTTP GET 3 ครั้ง

จาก gaia.cs.umass.edu 2 ครั้ง

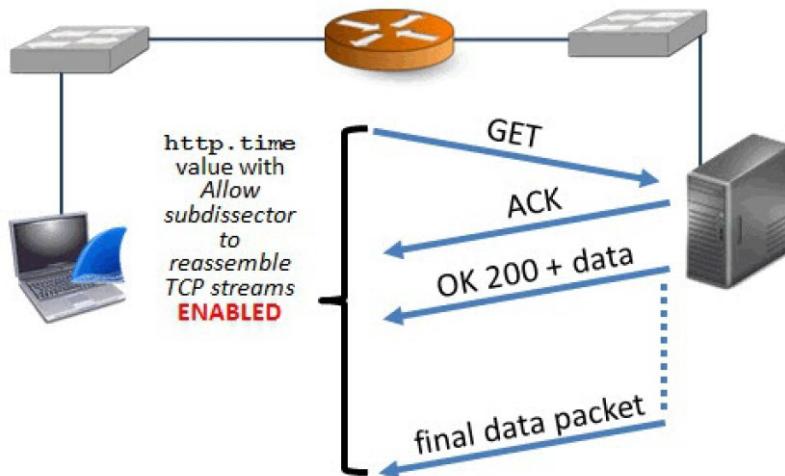
kurose.csplash.net 1 ครั้ง

- นักศึกษาต้องดูว่า ภาพทั้ง 2 ภาพในไฟล์ มีการ download ทีละไฟล์ (serial) หรือทำพร้อมๆ กัน (parallel) ให้อธิบาย

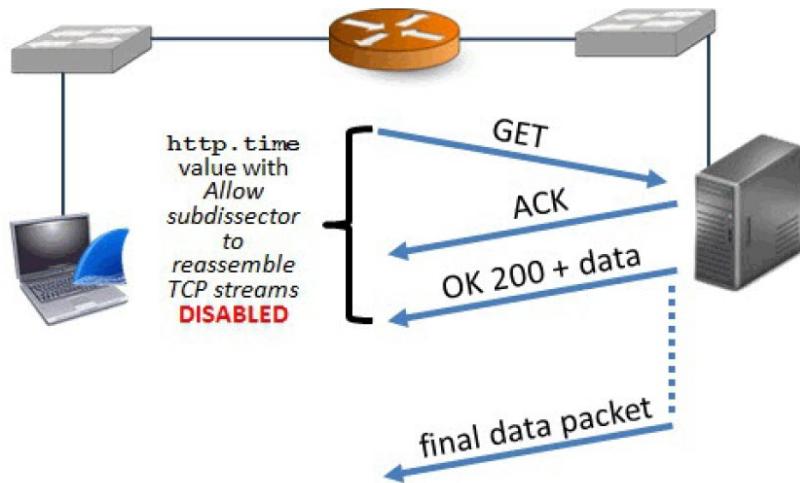
parallel http time (120s) เร็วมากก

ให้คลิกขวาที่ Transmission Control Protocol | Protocol Preferences และติ๊กที่ Allow subdissector to reassemble TCP streams เกิดอะไรขึ้น

packet หลังรับรอง ประกอบด้วย GET/HTTP



ค่า http.time เมื่อ Enable Allow subdissector to reassemble TCP streams



ค่า http.time เมื่อ Disable Allow subdissector to reassemble TCP streams

ในการตรวจสอบความล่าช้าในการทำงานของ Web Server เราจะใช้ค่า RTT (Round Trip Time) ซึ่งเป็นค่าเวลาตั้งแต่ GET จนถึงตอบกลับ (OK 200) ซึ่งจะบอกได้ถึงการตอบสนองของการเรียกใช้ของ Web Server ตัวนั้น ซึ่งสำหรับ Wireshark จะมีผลกระทบจากการกำหนดค่า Allow subdissector to reassemble TCP streams ตามรูป คือ หาก Disable จะคิดเฉพาะ packet HTTP OK 200 แต่ถ้า Enable ก็จะเป็นเวลาที่นับรวมถึงการโหลดข้อมูลทั้งหมด ดังนั้นให้ disable Allow subdissector to reassemble TCP streams ก่อน

15. ให้ไปที่ บรรทัดที่เป็น 200 OK และไปที่ Hypertext Transfer Protocol และ Expand Subtrees ออกมากทั้งหมด และไปที่บรรทัด Time since request และเลือก Apply as Column ให้ตั้งชื่อว่า HTTP Delta จากนั้นให้ Sort จัดพับ packet ที่ใช้เวลามากที่สุด
16. ให้นักศึกษาตรวจสอบ RTT ของเว็บ www.ce.kmitl.ac.th, www.reg.kmitl.ac.th, www.kmitl.ac.th และเว็บอื่นๆ 1 เว็บ (นักศึกษาเลือกเอง) ให้บอกว่าค่า RTT ของแต่ละเว็บมีค่าใด ให้เรียงลำดับน้อยไปมาก ให้นักศึกษาแสดงขั้นตอนการทำงาน (เขียนขอชิปายย่อๆ และ Capture รูปประกอบ) และเปรียบเทียบค่ากับเพื่อนอีก 1 คน ว่าลำดับเหมือนกันหรือไม่ อย่างไร

ขั้นตอน

1. เลือก website `datastruc.ce.kmitl.ac.th`
2. ดาวน์โหลด capture , นำ filter มองว่าในไฟล์มีเน็ตเว็บ HTTP
(ทำแบบนี้ก็จะ website บนcapture 4 website)
3. กด column HTTP Delta เมื่อเรียบร้อย มากไปยังขวา เพื่อป้องบล็อกม packet บนทางขวาของ website

ประเมินกันว่ามัน แนวโน้มจะดีมากน้อย

ประเมินกันว่ามันต่อไป `www.kmitl.ac.th` < `www.reg.kmitl.ac.th` < `datastruc.ce.kmitl.ac.th`

`www.ce.kmitl.ac.th`

16

www.ce.kmitl.ac.th

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Info
527	4.799264	161.246.4.119	192.168.1.105	HTTP	770	0.079237000	HTTP/1.1 200 OK (JPEG/JFIF image)
279	4.508117	161.246.4.119	192.168.1.105	HTTP	1506	0.074772000	HTTP/1.1 200 OK (text/html)
497	4.775791	161.246.4.119	192.168.1.105	HTTP	520	0.064794000	HTTP/1.1 200 OK (PNG)
566	4.845307	161.246.4.119	192.168.1.105	HTTP	1506	0.059499000	HTTP/1.1 200 OK (JPEG/JFIF image)
541	4.833374	161.246.4.119	192.168.1.105	HTTP	1506	0.055948000	HTTP/1.1 200 OK (JPEG/JFIF image)
577	4.845307	161.246.4.119	192.168.1.105	HTTP	1506	0.045051000	HTTP/1.1 200 OK (JPEG/JFIF image)
437	4.698620	161.246.4.119	192.168.1.105	HTTP	849	0.038293000	HTTP/1.1 200 OK (JPEG/JFIF image)
378	4.637212	161.246.4.119	192.168.1.105	HTTP	1188	0.036577000	HTTP/1.1 200 OK (JPEG/JFIF image)
828	5.555716	161.246.4.119	192.168.1.105	HTTP	625	0.031753000	HTTP/1.1 404 Not Found (text/html)
829	5.555787	161.246.4.119	192.168.1.105	HTTP	587	0.030063000	HTTP/1.1 404 Not Found (text/html)
614	4.876075	161.246.4.119	192.168.1.105	HTTP	1506	0.029456000	HTTP/1.1 200 OK (JPEG/JFIF image)
451	4.709387	161.246.4.119	192.168.1.105	HTTP	1506	0.029295000	HTTP/1.1 200 OK (JPEG/JFIF image)
316	4.567685	161.246.4.119	192.168.1.105	HTTP	697	0.029124000	HTTP/1.1 200 OK (text/css)
453	4.709387	161.246.4.119	192.168.1.105	HTTP	1506	0.029080000	HTTP/1.1 200 OK (JPEG/JFIF image)
319	4.567685	161.246.4.119	192.168.1.105	HTTP	1506	0.028718000	HTTP/1.1 200 OK (application/java)
308	4.555706	161.246.4.119	192.168.1.105	HTTP	1506	0.027024000	HTTP/1.1 200 OK (text/css)
425	4.677682	161.246.4.119	192.168.1.105	HTTP	519	0.026936000	HTTP/1.1 200 OK (PNG)
423	4.677682	161.246.4.119	192.168.1.105	HTTP	1304	0.026710000	HTTP/1.1 200 OK (JPEG/JFIF image)
424	4.677682	161.246.4.119	192.168.1.105	HTTP	701	0.026616000	HTTP/1.1 200 OK (JPEG/JFIF image)
646	4.891048	161.246.4.119	192.168.1.105	HTTP	1506	0.026366000	HTTP/1.1 200 OK (JPEG/JFIF image)
643	4.891048	161.246.4.119	192.168.1.105	HTTP	1506	0.026161000	HTTP/1.1 200 OK (PNG)[BoundErrorU]
383	4.649439	161.246.4.119	192.168.1.105	HTTP	1506	0.026139000	HTTP/1.1 200 OK (JPEG/JFIF image)
391	4.649439	161.246.4.119	192.168.1.105	HTTP	1506	0.025911000	HTTP/1.1 200 OK (JPEG/JFIF image)
623	4.876075	161.246.4.119	192.168.1.105	HTTP	1506	0.025456000	HTTP/1.1 200 OK (JPEG/JFIF image)
331	4.574576	161.246.4.119	192.168.1.105	HTTP	1506	0.024483000	HTTP/1.1 200 OK (JPEG/JFIF image)
348	4.594231	161.246.4.119	192.168.1.105	HTTP	1506	0.024240000	HTTP/1.1 200 OK (application/java)
350	4.599571	161.246.4.119	192.168.1.105	HTTP	1506	0.024128000	HTTP/1.1 200 OK (application/java)
352	4.599571	161.246.4.119	192.168.1.105	HTTP	776	0.023821000	HTTP/1.1 200 OK (JPEG/JFIF image)
317	4.567685	161.246.4.119	192.168.1.105	HTTP	1506	0.023740000	HTTP/1.1 200 OK (JPEG/JFIF image)
444	4.703412	161.246.4.119	192.168.1.105	HTTP	1506	0.023599000	HTTP/1.1 200 OK (JPEG/JFIF image)
326	4.573013	161.246.4.119	192.168.1.105	HTTP	783	0.022996000	HTTP/1.1 200 OK (JPEG/JFIF image)
411	4.659428	161.246.4.119	192.168.1.105	HTTP	1506	0.020480000	HTTP/1.1 200 OK (JPEG/JFIF image)
341	4.590731	161.246.4.119	192.168.1.105	HTTP	1506	0.020364000	HTTP/1.1 200 OK (application/java)
476	4.718848	161.246.4.119	192.168.1.105	HTTP	443	0.018264000	HTTP/1.1 200 OK (GIF89a)

www.reg.kmitl.ac.th

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Info
49	3.602128	161.246.34.224	192.168.1.105	HTTP	448	0.041377000	HTTP/1.1 301 Moved Permanently (text/html)
47	3.559197	161.246.34.224	192.168.1.105	HTTP	435	0.022155000	HTTP/1.1 302 Found
48	3.560751	192.168.1.105	161.246.34.224	HTTP	549		GET /index/ HTTP/1.1
45	3.537042	192.168.1.105	161.246.34.224	HTTP	497		GET / HTTP/1.1

www.kmitl.ac.th

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Info
21	2.200420	161.246.127.182	192.168.1.105	HTTP	531	0.018339000	HTTP/1.1 301 Moved Permanently (text/html)
19	2.182081	192.168.1.105	161.246.127.182	HTTP	493		GET / HTTP/1.1

datastruc.ce.kmitl.ac.th

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Info
16	1.884652	161.246.127.86	192.168.1.105	HTTP	1506	0.052109000	HTTP/1.1 200 OK (text/html)
203	2.236303	161.246.127.86	192.168.1.105	HTTP	1506	0.032871000	HTTP/1.1 200 OK
242	2.321154	161.246.127.86	192.168.1.105	HTTP	1506	0.026924000	HTTP/1.1 200 OK
141	2.038477	161.246.127.86	192.168.1.105	HTTP	1506	0.024100000	HTTP/1.1 200 OK (PNG)[BoundErrorU
32	1.937856	161.246.127.86	192.168.1.105	HTTP	1506	0.022900000	HTTP/1.1 200 OK (text/css)
44	1.953085	161.246.127.86	192.168.1.105	HTTP	467	0.019239000	HTTP/1.1 200 OK (text/css)

รูปด้านล่างแสดง RTT ที่ต้องการ

www.kmitl.ac.th < www.reg.kmitl.ac.th < datastruc.ce.kmitl.ac.th

< www.ce.kmitl.ac.th

งานครั้งที่ 4

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งโดยเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา และ _Lab4 เช่น 63010789_Lab4.pdf
- กำหนดส่ง ภายในวันที่ 9 กุมภาพันธ์ 2565