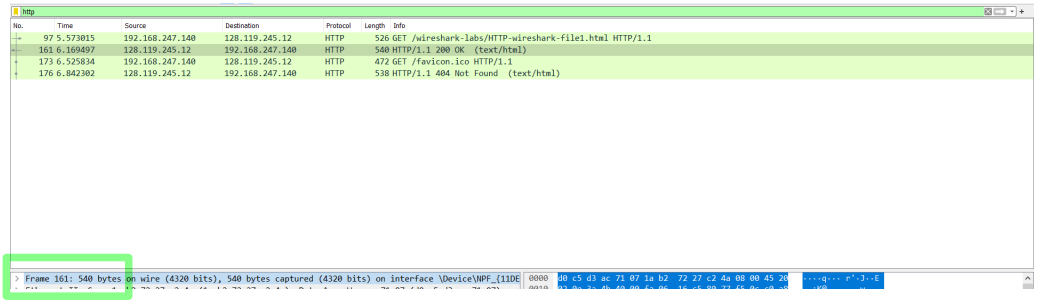
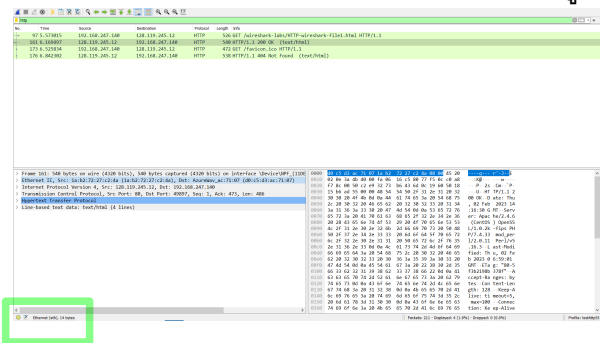
กิจกรรมที่ 4 : HTTP

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

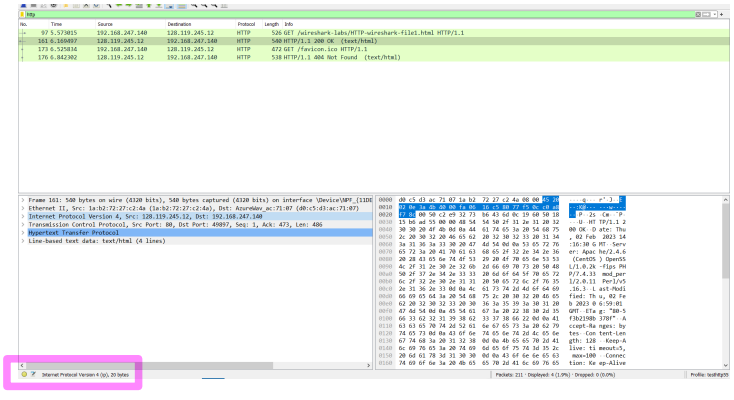
1. ให้ใช้ Wireshark เริ่มทำการ Capture และป้อน url : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html เสร็จแล้วให้หยุด
2. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ HTTP (ที่ถูกต้องควรจะมีแค่ 2 แพ็กเกต ในกรณีที่มีเกิน 2 แพ็คเกต อาจมาจากกรณี favicon ติดมาด้วย แต่ไม่ต้องไปสนใจแพ็คเกตที่เกินมา)
   (กรณีบรรทัดที่ 2 (Response) เป็น 304 Not Modified ให้เคลียร์ cache ของ browser แล้วทำใหม่)
3. ใน Packet List Pane ให้เลือก packet ที่เป็น HTTP Response และหาว่ามีความยาวของทั้ง frame เป็นเท่าไร **540 bytes** ให้บันทึก screenshot หน้าจอส่วนที่แสดงความยาวมาแสดง



4. ใน packet ตามข้อ 3 ความยาวเฉพาะส่วน header ของ Ethernet II เป็นเท่าไร **14 bytes** ให้บันทึก screenshot หน้าจอส่วนที่แสดงความยาวมาแสดง (Hint: หาข้อมูลจาก Packet Byte Pane)



5. ใน packet ตามข้อ 3 ความยาวเฉพาะส่วน header ของ Transmission Control Protocol เป็นเท่าไร **20 bytes** ให้บันทึก screenshot หน้าจอส่วนที่แสดงความยาวมาแสดง



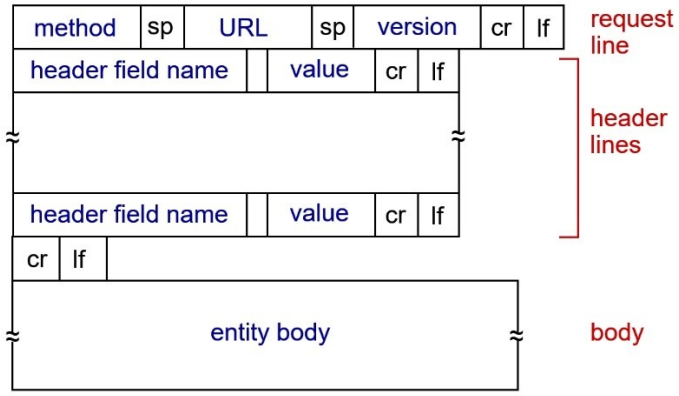
6. เพราะเหตุใด header ของ packet ต้องซ้อนเป็นชั้นๆ จงอธิบายเหตุผล

เพราะในแต่ละชั้นจะมี **header** ของแต่ละส่วน ไว้เช็คความถูกต้องในการเดินทางแต่ละ**layer**

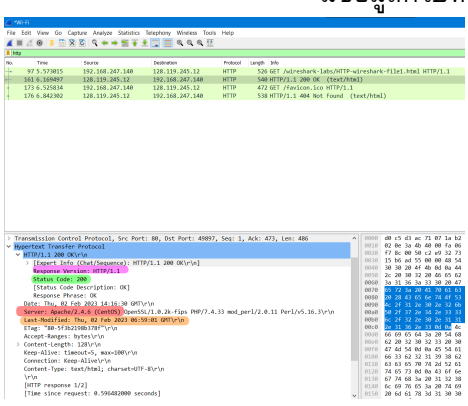
app -> frons port -> network ->link ->physical

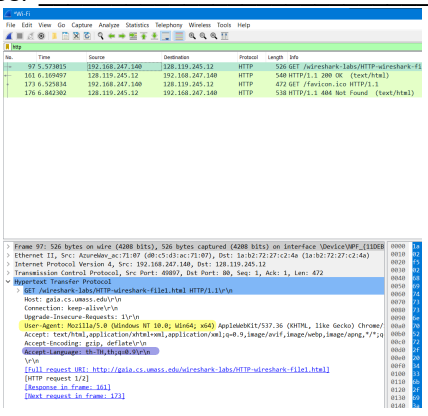
(Ht) (Hn) (Hl)

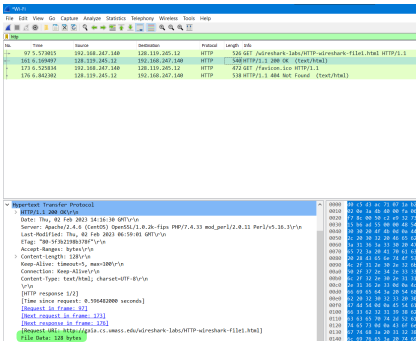
7. จากรูปแบบของ HTTP Message ตามรูป และ HTTP Request และ Response ที่ดักจับได้ ให้ตอบคำถามต่อไปนี้ (สามารถใช้วิธี capture แล้ว highlight ข้อมูลเพื่อตอบคำถามได้)



- browser และ server ใช้ HTTP version ใด HTTP/1.1
- browser เป็นโปรแกรมอะไร Mozilla/5.0 (Windoes NT 10.0;Win64; x64)
- server เป็นโปรแกรมอะไร Apache/2.4.6 (centos)
- ภาษาที่ browser ระบุว่าสามารถรับจาก server ได้ th-TH
- status code ที่ส่งกลับมาจาก server มายัง browser 200
- ค่าของ Last-Modified ของไฟล์ที่ server THU, 02 Feb 2023
- มีข้อมูลกี่ไบต์ที่ส่งมายัง browser 128 bytes







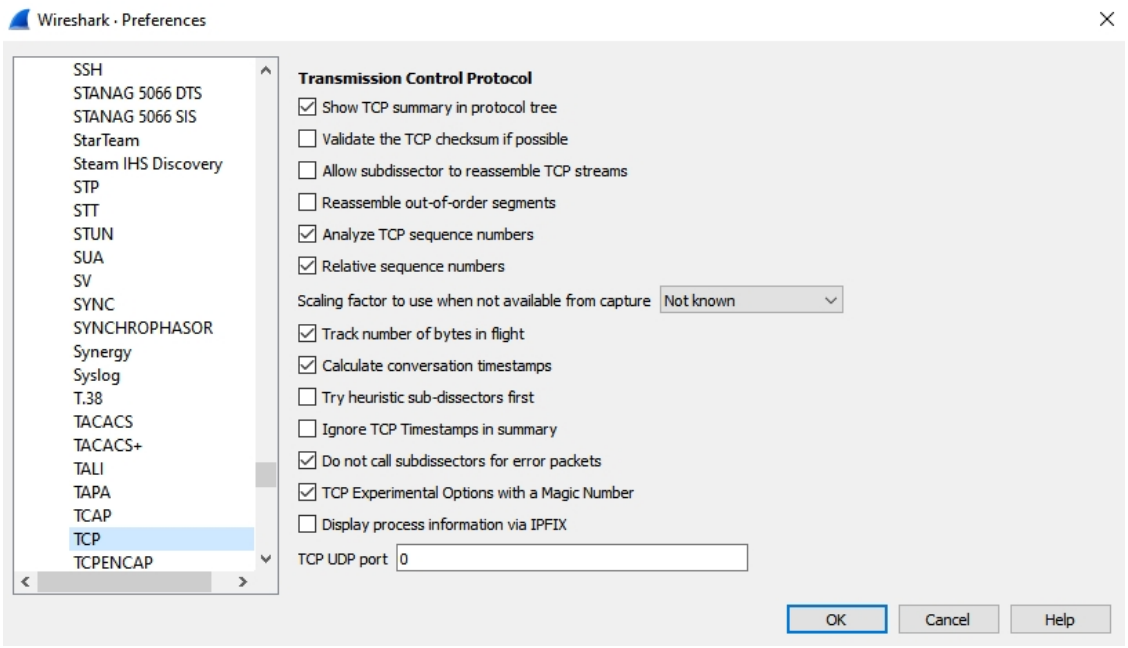
- ให้สรุปว่า header field name ตาม HTTP message format ของข้อมูลที่ส่งกลับมีอะไรบ้าง

Date, Server, Last-Modified, E-Tag, Accept-Rarger.

Content-Length, Keep-Aline, Conrection, Content-Type

8. ให้นักศึกษาหาวิธี clear cache ของ browser ที่ตนเองใช้อยู่ แล้วจัดการ clear ให้เรียบร้อย

9. เปิด Wireshark ใหม่แล้ว capture การเรียกหน้าเว็บเพจไปยัง url http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html จากนั้นให้กด refresh เพื่อโหลดหน้าอีกครั้ง จากนั้นให้หยุด capture
10. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ HTTP (ที่ถูกต้องควรจะมีแค่ 4 แพ็กเกต ในกรณีที่มีเกิน 4 แพ็คเกต อาจมาจากกรณี favicon ติดมาด้วย แต่ไม่ต้องไปสนใจแพ็คเกตที่เกินมา) และตอบคำถามต่อไปนี้
    - ใน HTTP GET ครั้งที่ 1 มีคำว่า IF-MODIFIED-SINCE หรือไม่ ไม่มี
    - ใน HTTP GET ครั้งที่ 2 มีคำว่า IF-MODIFIED-SINCE หรือไม่ มี
    - **(ถ้ามี) ข้อมูลที่ต่อจาก** IF-MODIFIED-SINCE มีความหมายอย่างไร
      การตรวจสอบล่าสุดวันที่เท่าไหร่ เวลาใด
      เช่น Fri, 30 Jan 2023 06:55:03 GMT
    - ในการตอบกลับของ server ครั้งที่ 2 มีการส่งไฟล์มาด้วยหรือไม่ สามารถอธิบายได้ว่าอย่างไร
      ไม่มีการส่งไฟล์กลับมา
11. ให้ไปที่ Edit | Preference… | Protocol | TCP ตามรูป

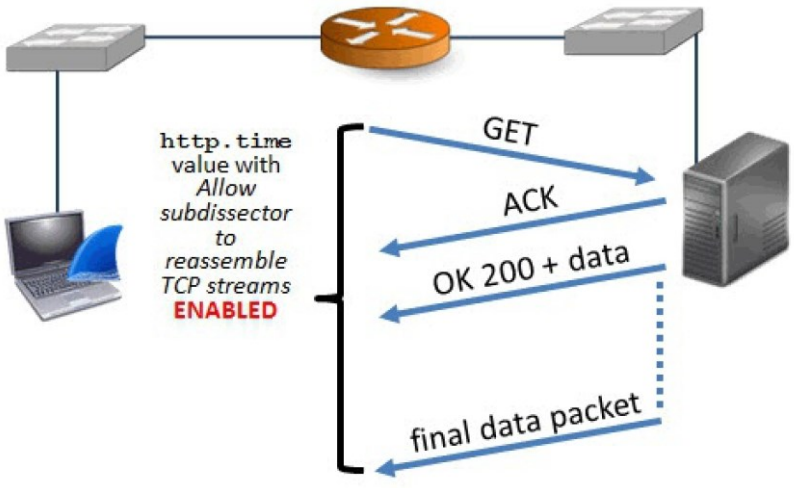


ให้แน่ใจว่า ไม่ติ๊กที่ **Allow subdissector to reassemble TCP streams**

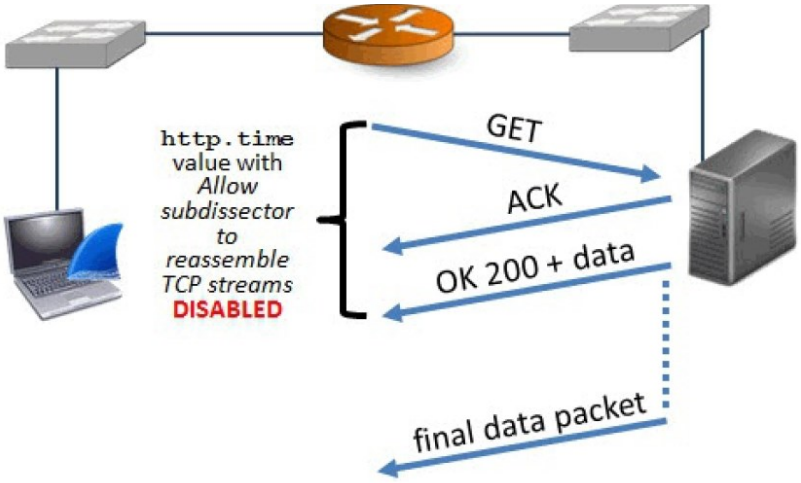
12. ให้ทำตามข้อ 8 อีกครั้ง และเปิด Wireshark ใหม่แล้ว capture การเรียกหน้าเว็บเพจไปยัง url http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html จากนั้นให้หยุด capture
13. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ HTTP (ถ้าทำถูกจะมี 5 บรรทัด) ซึ่งจะเห็นว่าหลังจากข้อมูล HTTP/1.1 200 OK แล้ว ยังมีข้อมูลตามมาอีก เนื่องจากไฟล์ html มีความยาวมาก (มากกว่า 4000 ไบต์) ทำให้ไม่สามารถส่งมาใน 1 packet ได้ จึงมีการแบ่งเป็นหลายๆ ส่วน (โดย TCP) ดังนั้นใน Wireshark จึงแสดงคำว่า Continuation ให้นักศึกษาตอบคำถามต่อไปนี้

- มี HTTP GET กี่ครั้ง และมี packet ใดบ้างที่มี Status Code และเป็น Status Code ใด
  มี HTTP 1 มี GET 1 Status code : 200

14. ให้ทำตามข้อ 8 อีกครั้ง และเปิด Wireshark ใหม่แล้ว capture การเรียกหน้าเว็บเพจไปยัง url http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html จากนั้นให้หยุด capture
- ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ HTTP และให้ตอบคำถามต่อไปนี้
- มี HTTP GET กี่ครั้ง และไปยัง url ใดบ้าง
  มี HTTP และ GET อย่างละ 3 อัน
  wireshark-labs/HTTP-wiresharlk-file4.html
  pearson.png
  8E_cover_small.jpg
- ผู้เรียนคิดว่า ภาพทั้ง 2 ภาพในไฟล์ ถูกทำการ download ทีละไฟล์ (serialize) หรือถูก download ไปพร้อมๆ กัน (parallelize) ให้อธิบาย
  ภาพ 2 ภาพ จะถูก dowload ทีละไฟล์ เพราะมี GET .png หรือ .jpg แยกกัน
  แสดงถึงการ dowload ทีละไฟล์
- ให้คลิ๊กขวาที่ Transmission Control Protocol | Protocol Preferences แล้วติ๊กที่ **Allow subdissector to reassemble TCP streams** เกิดอะไรขึ้น
  Packet continua จะหายไป เพราะว่า เป็นการรวบ TCP พวกข้อความยาวๆ
ที่ปกติส่งครั้งเดียวไม่พอ คืออันที่ขึ้น continue จะถูกรวมไปแล้ว ทำให้ไม่มีขึ้น packet continua



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) ซึ่งจะบอกได้ถึงการตอบสนองต่อการเรียกใช้ของ Web Server ตัวนั้น ซึ่งสำหรับ Wireshark จะมีผลกระทบจาก การกำหนดค่า **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 แล้วไปที่ Hypertext Transfer Protocol แล้วขยาย subtrees ออกมาทั้งหมด แล้วไปที่บรรทัด **Time since request** แล้วเลือก **Apply as Column** ให้ตั้งชื่อว่า HTTP Delta จากนั้นให้ sort เพื่อหา packet ที่มีเวลา HTTP Delta มากที่สุด
16. ให้นักศึกษาตรวจสอบ RTT ของ 3 เว็บดังนี้ 1) http://example.com/ 2) http://www.http2demo.io/ 3) http://www.vulnweb.com/ และเว็บอื่นอีก 1 เว็บ (ผู้เรียนเลือกเอง) ให้บอกว่าค่า RTT ของแต่ละเว็บมีค่าใด ให้เรียงลำดับน้อยไปมาก ให้นักศึกษาแสดงขั้นตอนการทำงาน (เขียนอธิบายย่อๆ และบันทึก screenshot ประกอบ) และเปรียบเทียบค่ากับเพื่อนอีก 1 คน ว่าลำดับเหมือนกันหรือไม่ อย่างไร

RTT : http://example.com/ < http://www.vulnweb.com/ < http://gaia.cs.umass.edu/kurose_ross/interactive/ < http://www.http2demo.io/

1. เลือก Web ที่ต้องการ Capture
2. Capture website และกดหยุด ป้อนในช่อง display filter : HTTP เพื่อดูผลลัพธ์
3. ดูช่อง RTT (HTTP Delta) ดูเวลาที่ใช้ในแต่ละ website และนำมาเปรียบเทียบกับ web ที่ยังไม่ได้เปรียบเทียบ

http://example.com/

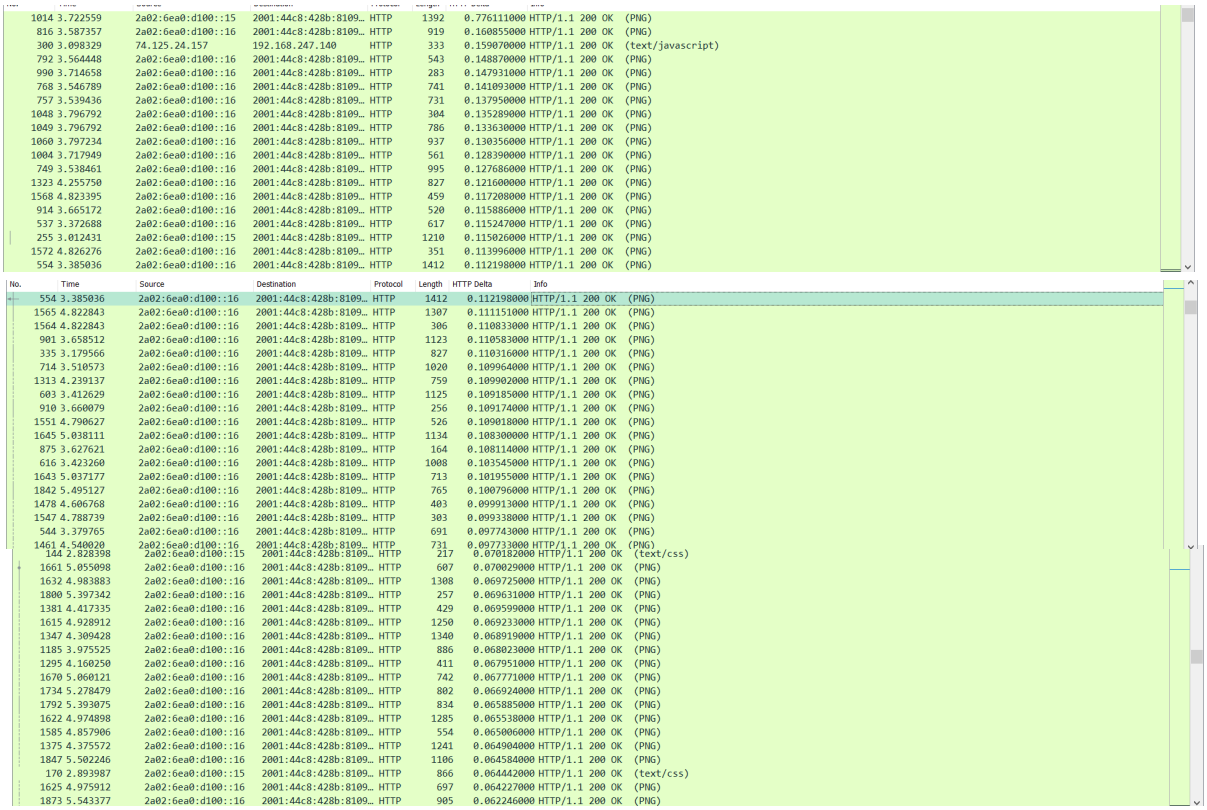
No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Info
527	3.215025	2606:2800:220:1:248…	2001:44c8:428b:8109…	HTTP	1096	0.296197000	HTTP/1.1 200 OK (text/html)
522	2.918828	2001:44c8:428b:8109…	2606:2800:220:1:248…	HTTP	509		GET / HTTP/1.1

http://gaia.cs.umass.edu/kurose_ross/interactive/ เว็บที่เลือกเพิ่ม 1 เว็บ

http

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Info
195	3.730421	128.119.245.12	192.168.247.140	HTTP	134	0.789565000	HTTP/1.1 200 OK (text/html)
426	4.336222	128.119.245.12	192.168.247.140	HTTP	437	0.741052000	HTTP/1.1 200 OK (JPEG JFIF image)
287	4.150117	128.119.245.12	192.168.247.140	HTTP	1272	0.555131000	HTTP/1.1 200 OK (application/javascript)
373	4.280844	128.119.245.12	192.168.247.140	HTTP	70	0.549074000	HTTP/1.1 200 OK (PNG)
263	4.089393	128.119.245.12	192.168.247.140	HTTP	758	0.530364000	HTTP/1.1 200 OK (text/css)
197	3.731770	192.168.247.140	128.119.245.12	HTTP	513		GET /kurose_ross/interactive/devmode-icon.png HTTP/1.1
130	3.595170	192.168.247.140	128.119.245.12	HTTP	494		GET /kurose_ross/header_graphic_book_8E_3.jpg HTTP/1.1
129	3.594986	192.168.247.140	128.119.245.12	HTTP	448		GET /kurose_ross/interactive/questions.js HTTP/1.1
112	3.559029	192.168.247.140	128.119.245.12	HTTP	461		GET /kurose_ross/interactive/custom.css HTTP/1.1
65	2.940856	192.168.247.140	128.119.245.12	HTTP	519		GET /kurose_ross/interactive/ HTTP/1.1

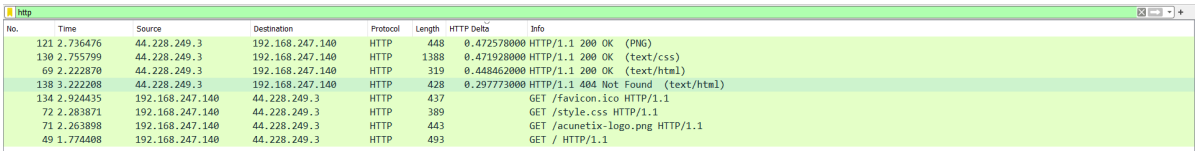
http://www.http2demo.io/



No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Info
1014	3.722559	2a02:6ea0:d100::15	2001:44c8:428b:8109…	HTTP	1392	0.776111000	HTTP/1.1 200 OK (PNG)
816	3.587357	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	919	0.160855000	HTTP/1.1 200 OK (PNG)
300	3.098329	74.125.24.157	192.168.247.140	HTTP	333	0.159070000	HTTP/1.1 200 OK (text/javascript)
792	3.564448	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	543	0.148870000	HTTP/1.1 200 OK (PNG)
990	3.714658	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	283	0.147931000	HTTP/1.1 200 OK (PNG)
768	3.546789	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	741	0.141093000	HTTP/1.1 200 OK (PNG)
757	3.539436	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	731	0.137950000	HTTP/1.1 200 OK (PNG)
1048	3.796792	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	304	0.135289000	HTTP/1.1 200 OK (PNG)
1049	3.796792	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	786	0.133630000	HTTP/1.1 200 OK (PNG)
1060	3.797234	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	937	0.130356000	HTTP/1.1 200 OK (PNG)
1004	3.717949	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	561	0.128390000	HTTP/1.1 200 OK (PNG)
749	3.538461	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	995	0.127686000	HTTP/1.1 200 OK (PNG)
1323	4.255750	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	827	0.121600000	HTTP/1.1 200 OK (PNG)
1568	4.823395	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	459	0.117208000	HTTP/1.1 200 OK (PNG)
914	3.665172	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	520	0.115886000	HTTP/1.1 200 OK (PNG)
537	3.372688	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	617	0.115247000	HTTP/1.1 200 OK (PNG)
255	3.012431	2a02:6ea0:d100::15	2001:44c8:428b:8109…	HTTP	1210	0.115026000	HTTP/1.1 200 OK (PNG)
1572	4.826276	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	351	0.113996000	HTTP/1.1 200 OK (PNG)
554	3.385036	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1412	0.112198000	HTTP/1.1 200 OK (PNG)

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Info
554	3.385036	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1412	0.112198000	HTTP/1.1 200 OK (PNG)
1565	4.822843	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1307	0.111151000	HTTP/1.1 200 OK (PNG)
1564	4.822843	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	306	0.110833000	HTTP/1.1 200 OK (PNG)
901	3.658512	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1123	0.110583000	HTTP/1.1 200 OK (PNG)
335	3.179566	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	827	0.110316000	HTTP/1.1 200 OK (PNG)
714	3.510573	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1020	0.109964000	HTTP/1.1 200 OK (PNG)
1313	4.239137	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	759	0.109902000	HTTP/1.1 200 OK (PNG)
603	3.412629	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1125	0.109185000	HTTP/1.1 200 OK (PNG)
910	3.660079	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	256	0.109174000	HTTP/1.1 200 OK (PNG)
1551	4.790627	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	526	0.109018000	HTTP/1.1 200 OK (PNG)
1645	5.038111	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1134	0.108300000	HTTP/1.1 200 OK (PNG)
875	3.627621	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	164	0.108114000	HTTP/1.1 200 OK (PNG)
616	3.423260	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1008	0.103545000	HTTP/1.1 200 OK (PNG)
1643	5.037177	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	713	0.101955000	HTTP/1.1 200 OK (PNG)
1842	5.495127	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	765	0.100796000	HTTP/1.1 200 OK (PNG)
1478	4.606768	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	403	0.099913000	HTTP/1.1 200 OK (PNG)
1547	4.788739	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	303	0.099338000	HTTP/1.1 200 OK (PNG)
544	3.379765	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	691	0.097743000	HTTP/1.1 200 OK (PNG)
1461	4.540020	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	731	0.097713000	HTTP/1.1 200 OK (PNG)
144	2.828398	2a02:6ea0:d100::15	2001:44c8:428b:8109…	HTTP	217	0.070182000	HTTP/1.1 200 OK (text/css)
1661	5.055098	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	607	0.070029000	HTTP/1.1 200 OK (PNG)
1632	4.983883	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1308	0.069725000	HTTP/1.1 200 OK (PNG)
1800	5.397342	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	257	0.069631000	HTTP/1.1 200 OK (PNG)
1381	4.417335	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	429	0.069599000	HTTP/1.1 200 OK (PNG)
1615	4.928912	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1250	0.069233000	HTTP/1.1 200 OK (PNG)
1347	4.309428	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1340	0.068919000	HTTP/1.1 200 OK (PNG)
1185	3.975525	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	886	0.068023000	HTTP/1.1 200 OK (PNG)
1295	4.160250	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	411	0.067951000	HTTP/1.1 200 OK (PNG)
1670	5.060121	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	742	0.067771000	HTTP/1.1 200 OK (PNG)
1734	5.278479	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	802	0.066924000	HTTP/1.1 200 OK (PNG)
1792	5.393075	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	834	0.065885000	HTTP/1.1 200 OK (PNG)
1622	4.974898	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1285	0.065538000	HTTP/1.1 200 OK (PNG)
1585	4.857906	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	554	0.065006000	HTTP/1.1 200 OK (PNG)
1375	4.375572	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1241	0.064904000	HTTP/1.1 200 OK (PNG)
1847	5.502246	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	1106	0.064584000	HTTP/1.1 200 OK (PNG)
170	2.893987	2a02:6ea0:d100::15	2001:44c8:428b:8109…	HTTP	866	0.064442000	HTTP/1.1 200 OK (text/css)
1625	4.975912	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	697	0.064227000	HTTP/1.1 200 OK (PNG)
1873	5.543377	2a02:6ea0:d100::16	2001:44c8:428b:8109…	HTTP	905	0.062246000	HTTP/1.1 200 OK (PNG)

http://www.vulnweb.com/



No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Info
121	2.736476	44.228.249.3	192.168.247.140	HTTP	448	0.472578000	HTTP/1.1 200 OK (PNG)
130	2.755799	44.228.249.3	192.168.247.140	HTTP	1388	0.471928000	HTTP/1.1 200 OK (text/css)
69	2.222870	44.228.249.3	192.168.247.140	HTTP	319	0.448462000	HTTP/1.1 200 OK (text/html)
138	3.222208	44.228.249.3	192.168.247.140	HTTP	428	0.297773000	HTTP/1.1 404 Not Found (text/html)
134	2.924435	192.168.247.140	44.228.249.3	HTTP	437		GET /favicon.ico HTTP/1.1
72	2.283871	192.168.247.140	44.228.249.3	HTTP	389		GET /style.css HTTP/1.1
71	2.263898	192.168.247.140	44.228.249.3	HTTP	443		GET /acunetix-logo.png HTTP/1.1
49	1.774408	192.168.247.140	44.228.249.3	HTTP	493		GET / HTTP/1.1

เทียบกับของเพื่อน

ค่าของ RTT ของแต่ละ ถึงเป็น ดังนี้ ตามลำดับห้วยไปขวา www.columbia.edu/~fdc/sample.html (0.289233000) www.example.com (0.423403000) www.vulnweb.com (0.674765000) และ www.http2demo.io (1.949719000)

งานครั้งที่ 4

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา ตามด้วย section และ _lab04 ตามตัวอย่างต่อไปนี้ 64019999_sec20_lab04.pdf
- กำหนดส่ง ภายในวันที่ 10 กุมภาพันธ์ 2566 โดยให้ส่งใน Microsoft Teams ของรายวิชา