3. ให้ใช้ข้อมูลจาก Packet Bytes Pane เพื่อหาความยาวของข้อมูล และตอบคำถามต่อไปนี้

- ความยาวเฟรมทั้งหมด 534 bytes

- ความยาวของ Header Ethernet II 14 bytes

- ความยาวของ TCP Header 20 bytes

- เหตุผลที่ Header ของข้อมูลต้องซ้อนเป็นชั้นๆ คือ เพื่อความเป็นระเบียบและง่ายต่อการหา

4. จากรูปแบบของ HTTP Message ตามรูป และ HTTP Request และ Response ที่ดักจับได้ ให้ตอบคำถามต่อไปนี้ (สามารถใช้วิธี Capture แล้ว Highlight ข้อมูลเพื่อตอบคำถามได้)

```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36 E
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
HTTP/1.1 200 OK\r\n
Date: Sat, 06 Feb 2021 11:08:04 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sat, 06 Feb 2021 06:59:02 GMT\r\n
ETag: "80-5baa578c45089"\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 1/1]
[Time since request: 0.293792000 seconds]
[Request in frame: 8]
```

- Browser และ Server ใช้ HTTP version ใด HTTP/1.1

- Browser เป็นโปรแกรมอะไร Microsoft edge

- Server เป็นโปรแกรมอะไร Apache/2.4.6

-ภาษาที่ Browserระบุว่าสามารถรับจากServerได้ en-US

- Status Code ที่ส่งกลับมาจากServer มายัง Browser 200

-ค่าของ Last-Modified ของไฟล์ที่ Sat, 06 Feb 2021 06:59:02 GMT

- มีข้อมูลกี่ไบต์ที่ส่งมายัง Browser 128 bytes

- ให้สรุปว่า header field name ตาม HTTP message format ของข้อมูลที่ส่งกลับมีอะไรบ้าง

Date, Sever ,Last-Modified, Etag, Accept-Ranges, Content-Length, Keep-Alive, Connection, Content-Type

7. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP (ถ้าทำถูกจะมีแค่ 4 บรรทัด บรรทัด แต่อาจมี favicon ติดมาไม่ต้องไปสนใจ) 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

Server จะตอบ 304 Not Modified ถ้าทรัพยากรไม่มีการเปลี่ยนแปลงตั้งแต่เวลาที่ระบุ

- ในการตอบกลับของ Server ครั้งที่ 2 มีการส่งไฟล์มาด้วยหรือไม่ จะอธิบายอย่างไร

```
HTTP/1.1 304 Not Modified\r\n
Date: Sat, 06 Feb 2021 11:51:18 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=99\r\n
ETag: "173-5baa578c444d1"\r\n
```

ไม่ เพราะ header field name ไม่มี Content-Length

10. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol 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

No.	Time	Source	Destination	Protocol	Length	Info
5	0.297617	192.168.0.21	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
9	0.604994	128.119.245.12	192.168.0.21	HTTP	1454	HTTP/1.1 200 OK (text/html)
10	0.604994	128.119.245.12	192.168.0.21	HTTP	1454	Continuation
12	0.605068	128.119.245.12	192.168.0.21	HTTP	1454	Continuation
13	0.605068	128.119.245.12	192.168.0.21	HTTP	715	Continuation

มี GET 1 ครั้ง

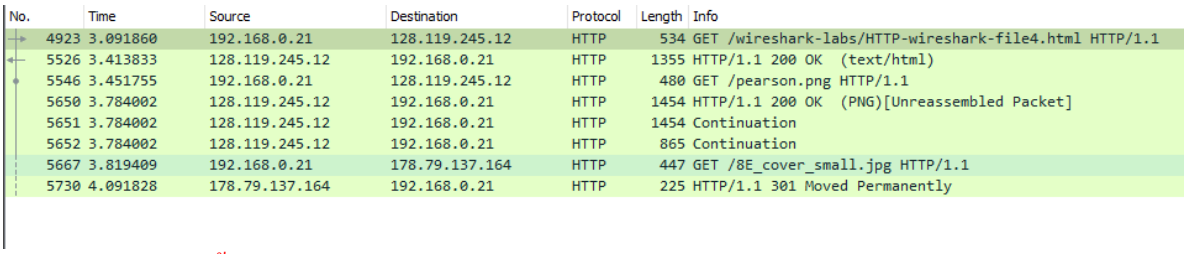
```
    9 0.604994    128.119.245.12    192.168.0.21    HTTP    1454 HTTP/1.1 200 OK  (text/html)
```

```
HTTP/1.1 200 OK\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
```

มี 1 packet ตามรูปด้านบนที่มี status code และมี status code : 200

12. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP และให้ตอบคำถามต่อไปนี้

- มี HTTP GET กี่ครั้ง จาก url ใดบ้าง



No.	Time	Source	Destination	Protocol	Length	Info
4923	3.091860	192.168.0.21	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
5526	3.413833	128.119.245.12	192.168.0.21	HTTP	1355	HTTP/1.1 200 OK (text/html)
5546	3.451755	192.168.0.21	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
5650	3.784002	128.119.245.12	192.168.0.21	HTTP	1454	HTTP/1.1 200 OK (PNG)[Unreassembled Packet]
5651	3.784002	128.119.245.12	192.168.0.21	HTTP	1454	Continuation
5652	3.784002	128.119.245.12	192.168.0.21	HTTP	865	Continuation
5667	3.819409	192.168.0.21	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
5730	4.091828	178.79.137.164	192.168.0.21	HTTP	225	HTTP/1.1 301 Moved Permanently

มี HTTP GET 2 ครั้ง

จาก url : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

http://gaia.cs.umass.edu/pearson.png

http://kurose.cslash.net/8E_cover_small.jpg

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

มีการ download ทีละไฟล์ เนื่องจากตอนเปิดเว็บจะ download ภาพ pearson.png ก่อนแล้วโหลดภาพ cover_small.jpg ทีหลัง หรือดูได้จากคอลัมน์ Time ใน wireshark

13. ให้คลิ๊กขวาที่ Transmission Control Protocol | Protocol Preferences แล้วติ๊กที่ Allow subdissector to reassemble TCP streams เกิดอะไรขึ้น

ก่อน

No.	Time	Source	Destination	Protocol	Length	Info
4923	3.091860	192.168.0.21	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
5526	3.413833	128.119.245.12	192.168.0.21	HTTP	1355	HTTP/1.1 200 OK (text/html)
5546	3.451755	192.168.0.21	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
5650	3.784002	128.119.245.12	192.168.0.21	HTTP	1454	HTTP/1.1 200 OK (PNG)[Unreassembled Packet]
5651	3.784002	128.119.245.12	192.168.0.21	HTTP	1454	Continuation
5652	3.784002	128.119.245.12	192.168.0.21	HTTP	865	Continuation
5667	3.819409	192.168.0.21	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
5730	4.091828	178.79.137.164	192.168.0.21	HTTP	225	HTTP/1.1 301 Moved Permanently

หลัง

No.	Time	Source	Destination	Protocol	Length	Info
4923	3.091860	192.168.0.21	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
5526	3.413833	128.119.245.12	192.168.0.21	HTTP	1355	HTTP/1.1 200 OK (text/html)
5546	3.451755	192.168.0.21	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
5652	3.784002	128.119.245.12	192.168.0.21	HTTP	865	HTTP/1.1 200 OK (PNG)
5667	3.819409	192.168.0.21	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
5730	4.091828	178.79.137.164	192.168.0.21	HTTP	225	HTTP/1.1 301 Moved Permanently

ไม่มี packet continuation

14. ให้ไปที่ บรรทัดที่เป็น 200 OK แล้วไปที่ Hypertext Transfer Protocol แล้ว Expand Subtrees ออกมาทั้งหมด แล้วไปที่บรรทัด **Time since request** แล้วเลือก **Apply as Column** ให้ตั้งชื่อว่า HTTP Delta จากนั้นให้ Sort จะพบ packet ที่ใช้เวลามากที่สุด

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Info
5650	3.784002	128.119.245.12	192.168.0.21	HTTP	1454	0.332247000	HTTP/1.1 200 OK (PNG)[Unreassembled Pack
5526	3.413833	128.119.245.12	192.168.0.21	HTTP	1355	0.321973000	HTTP/1.1 200 OK (text/html)
5730	4.091828	178.79.137.164	192.168.0.21	HTTP	225	0.272419000	HTTP/1.1 301 Moved Permanently
5667	3.819409	192.168.0.21	178.79.137.164	HTTP	447		GET /8E_cover_small.jpg HTTP/1.1
5652	3.784002	128.119.245.12	192.168.0.21	HTTP	865		Continuation
5651	3.784002	128.119.245.12	192.168.0.21	HTTP	1454		Continuation
5546	3.451755	192.168.0.21	128.119.245.12	HTTP	480		GET /pearson.png HTTP/1.1
4923	3.091860	192.168.0.21	128.119.245.12	HTTP	534		GET /wireshark-labs/HTTP-wireshark-file4.

15. ให้นักศึกษาตรวจสอบ RTT ของเว็บ www.ce.kmitl.ac.th, www.reg.kmitl.ac.th, www.kmitl.ac.th และเว็บอื่นอีก 1 เว็บ (นักศึกษาเลือกเอง) ให้บอกว่าค่า RTT ของแต่ละเว็บมีค่าใด ให้เรียงลำดับน้อยไปมาก ให้นักศึกษาแสดงขั้นตอนการทำงาน (เขียนอธิบายย่อๆ และ Capture รูปประกอบ) และเปรียบเทียบค่ากับเพื่อนอีก 1 คน

www.ce.kmitl.ac.th

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Request URI	Info
6	0.203468	161.246.4.119	192.168.0.21	HTTP	1454	0.134396000	http://www.ce.kmitl.ac.th/	HTTP/1.1 200 OK (text/html)
309	0.777761	161.246.4.119	192.168.0.21	HTTP	1454	0.102773000	http://www.ce.kmitl.ac.th/images/announcement_head.jpg	HTTP/1.1 200 OK (JPEG JFIF image)
57	0.405220	161.246.4.119	192.168.0.21	HTTP	1454	0.095134000	http://www.ce.kmitl.ac.th/banner/1502351141_MicrosoftImagine.jpg	HTTP/1.1 200 OK (application/javascript)
421	1.835714	161.246.4.119	192.168.0.21	HTTP	626	0.093402000	http://www.ce.kmitl.ac.th/glossy/glossy.js	HTTP/1.1 404 Not Found (text/html)
333	0.779123	161.246.4.119	192.168.0.21	HTTP	1454	0.087298000	http://www.ce.kmitl.ac.th/	HTTP/1.1 200 OK (JPEG JFIF image)

www.reg.kmitl.ac.th

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Request URI	Info
11	0.223655	161.246.34.224	192.168.0.21	HTTP	448	0.073979000	http://www.reg.kmitl.ac.th/index/	HTTP/1.1 301 Moved Permanently (text/html)
9	0.147277	161.246.34.224	192.168.0.21	HTTP	435	0.073681000	http://www.reg.kmitl.ac.th/	HTTP/1.1 302 Found
10	0.149676	192.168.0.21	161.246.34.224	HTTP	548			GET /index/ HTTP/1.1
5	0.073596	192.168.0.21	161.246.34.224	HTTP	496			GET / HTTP/1.1

www.kmitl.ac.th

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Request URI	Info
9	0.152945	161.246.34.11	192.168.0.21	HTTP	599	0.083917000	http://www.kmitl.ac.th/	HTTP/1.1 301 Moved Permanently (text/html)
5	0.069028	192.168.0.21	161.246.34.11	HTTP	492			GET / HTTP/1.1

www.pt.ac.th

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Request URI	Info
247	1.583117	122.154.59.5	192.168.0.21	HTTP	500	0.078970000	http://www.pt.ac.th/	HTTP/1.1 200 OK (text/html)
216	1.504147	192.168.0.21	122.154.59.5	HTTP	489			GET / HTTP/1.1

ขั้นตอนการทำงาน

1.กด capture แล้วเข้าเว็บตามด้านบน

2.ใช้ display filter : http

3.กด sort คอลัมน์ HTTP Delta

เรียงลำดับจากน้อยไปมาก

1. www.reg.kmitl.ac.th (0.73979000)

2. www.pt.ac.th (0.78970000)

3. www.kmitl.ac.th (0.83917000)

4. www.ce.kmitl.ac.th (0.134396000)

เปรียบเทียบกับเพื่อน

1. www.reg.kmitl.ac.th (0.019618000)

2. www.kmitl.ac.th (0.030770000)

3. www.ce.kmitl.ac.th (0.05982000)

4. www.bangkok.go.th (0.150547000)