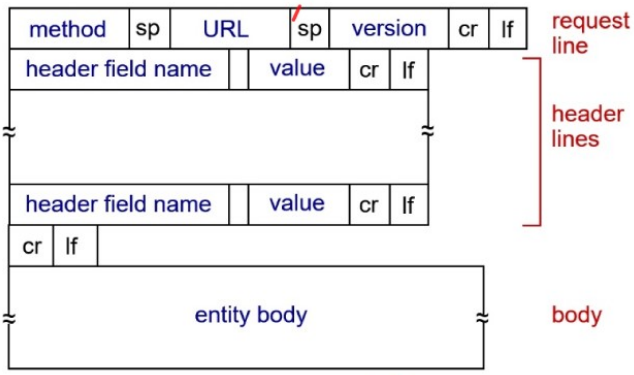
ชยภาภรณ์ รัฐประชานนท์ 62010694

01076010 เครือข่ายคอมพิวเตอร์ : 2/2563
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

กิจกรรมที่ 4 : HTTP

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

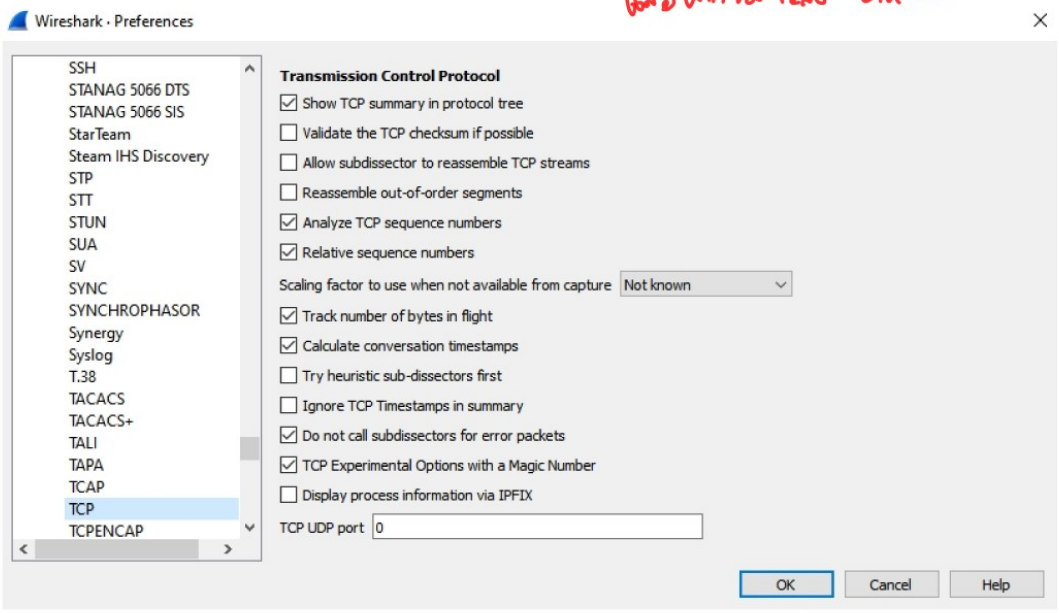
1. ให้ใช้ Wireshark เริ่มทำการ Capture และป้อน url : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html เสร็จแล้วให้หยุด
2. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP (ถ้าทำถูกจะมีแค่ 2 บรรทัด แต่อาจมี favicon ติดมาไม่ต้องไปสนใจ)
   (กรณีบรรทัดที่ 2 (Response) เป็น 304 Not Modified ให้ปิด Browser แล้วทำใหม่)
3. ให้ใช้ข้อมูลจาก Packet Bytes Pane เพื่อหาความยาวของข้อมูล และตอบคำถามต่อไปนี้
   - ความยาวเฟรมทั้งหมด 523 bytes
   - ความยาวของ Header Ethernet II 14 bytes
   - ความยาวของ TCP Header 20 bytes
   - เหตุผลที่ Header ของข้อมูลต้องซ้อนเป็นชั้นๆ คือ
     การเข้ารหัสข้อมูลตาม OSI Module แต่ละ Layer จะมีการใส่ Header ของแต่ละชั้น เพื่อให้ชั้นนั้นสามารถถอดรหัส Header ให้ตรงกับ Layer ที่อยู่ด้วยได้
4. จากรูปแบบของ HTTP Message ตามรูป และ HTTP Request และ Response ที่ดักจับได้ ให้ตอบคำถามต่อไปนี้ (สามารถใช้วิธี Capture แล้ว Highlight ข้อมูลเพื่อตอบคำถามได้)



   - Browser และ Server ใช้ HTTP version ใด 1
   - Browser เป็นโปรแกรมอะไร 2
   - Server เป็นโปรแกรมอะไร 3

- ภาษาที่ Browser ระบุว่าสามารถรับจาก Server ได้
  _____ 4 _____
- Status Code ที่ส่งกลับมาจาก Server มายัง Browser
- ค่าของ Last-Modified ของไฟล์ที่ Server _____ 5 _____
- มีข้อมูลกี่ไบต์ที่ส่งมายัง Browser _____ 6 _____
- ให้สรุปว่า header field name ตาม HTTP message format ของข้อมูลที่ส่งกลับมีอะไรบ้าง Response Version Status Code Response phrase
  Date, Server, Last modified, ETag, Accept-Ranges, Content-Length, Keep-Alive, Content-Type, File Data

5. ให้นักศึกษาหาวิธี clear cache ของ Browser ที่ตนเองใช้อยู่ แล้วจัดการ clear ให้เรียบร้อย
6. เปิด Wireshark ใหม่แล้ว Capture ที่ url http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html จากนั้นให้กด Reflash เพื่อโหลดหน้าอีกครั้ง จากนั้นให้หยุด Capture
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 _____
     เวลาที่ระบุการเปลี่ยนแปลงข้อมูลบนฝั่ง Server
   - ในการตอบกลับของ Server ครั้งที่ 2 มีการส่งไฟล์มาด้วยหรือไม่ จะอธิบายอย่างไร
     ไม่ เพราะ Server ตอบ State Code 304 กลับมา เพราะ If-Modified-Since จะเป็นเงื่อนไขว่าหาก ข้อมูล ถูกแก้ไข หลังจาก เวลาที่ระบุ
8. ให้ไปที่ Edit | Preference... | Protocol | TCP ตามรูป server จะส่ง status 200 กลับมา และหากไม่จะส่ง status 304 กลับมาแทน



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

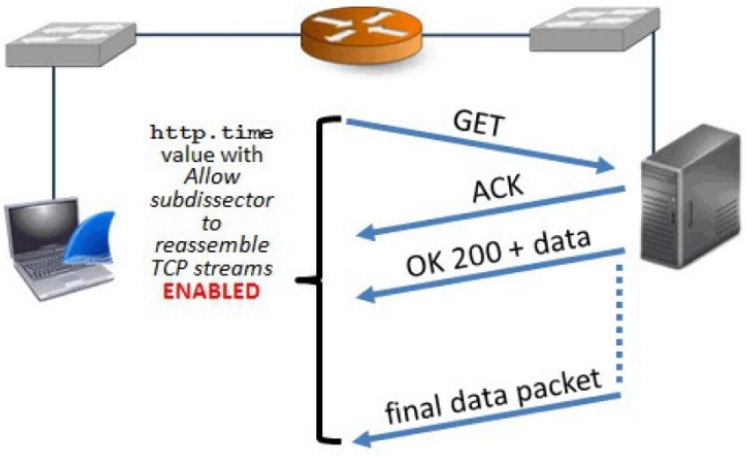
9. ให้ทำตามข้อ 5 อีกครั้ง และเปิด Wireshark ใหม่แล้ว Capture ที่ url http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html จากนั้นให้หยุด Capture
10. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP (ถ้าทำถูกจะมี 5 บรรทัด) ซึ่งจะเห็นว่าหลังจากข้อมูล HTTP/1.1 200 OK แล้ว ยังมีข้อมูลตามมาอีก 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

     1 ครั้ง และ packet ตอบกลับมี Status Code : 200
11. ให้ทำตามข้อ 5 อีกครั้ง และเปิด Wireshark ใหม่แล้ว Capture ที่ url http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html จากนั้นให้หยุด Capture
12. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP และให้ตอบคำถามต่อไปนี้
   - มี HTTP GET กี่ครั้ง จาก url ใดบ้าง

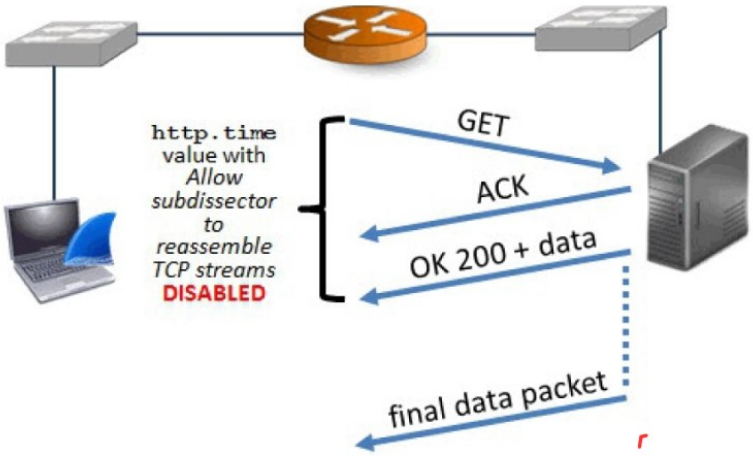
     3 ครั้ง : gaia.cs.umass.edu, gaia.cs.umass.edu, kurose.cslash.net
   - นักศึกษาคิดว่า ภาพทั้ง 2 ภาพในไฟล์ มีการ download ทีละไฟล์ (serial) หรือทำพร้อมๆ กัน (parallel) ให้อธิบาย

     parallel เพราะ time เริ่มต้นในการรอพร้อมกัน
13. ให้คลิ๊กขวาที่ Transmission Control Protocol | Protocol Preferences แล้วติ๊กที่ **Allow subdissector to reassemble TCP streams** เกิดอะไรขึ้น

    ผลลัพธ์ออกมาแบบไม่ dissect packet ทำให้เห็น packet ไม่ครบ



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



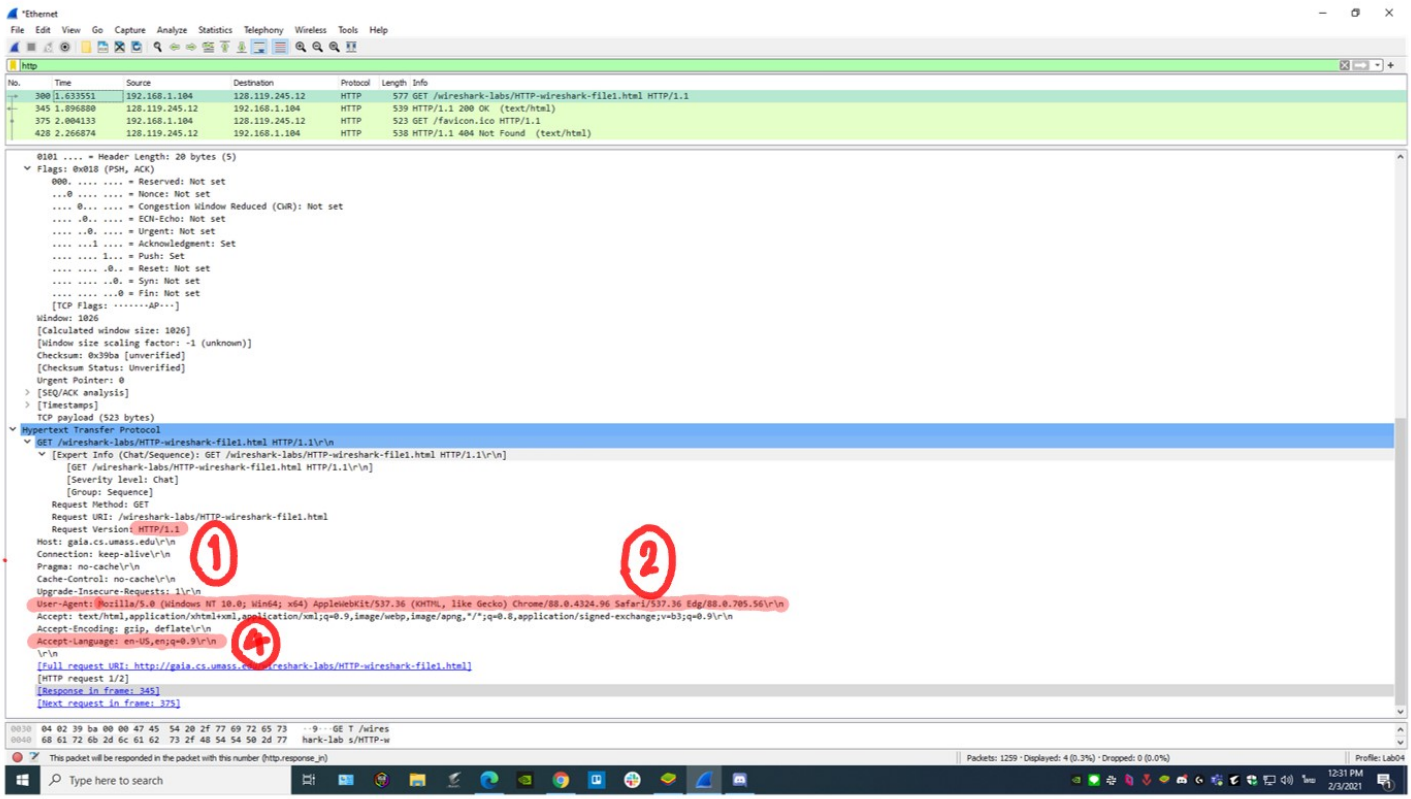
ค่า http.time เมื่อ Disable Allow subdissector to reassemble TCP streams

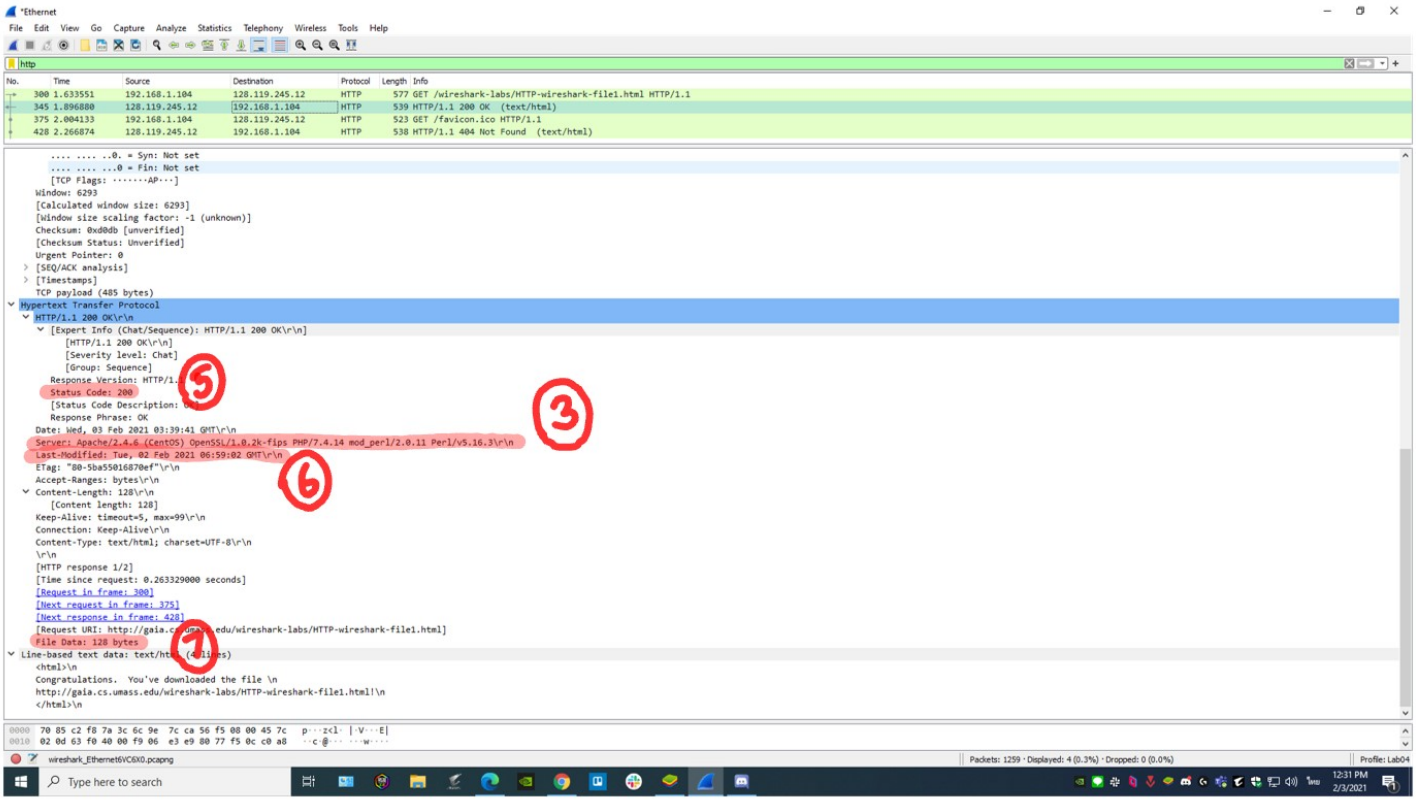
ในการตรวจสอบความล่าช้าในการทำงานของ Web Server เราจะใช้ค่า RTT (Round Trip Time) ซึ่งเป็นค่าเวลาตั้งแต่ GET จนถึงตอบกลับ (OK 200) ซึ่งจะบอกได้ถึงการตอบสนองต่อการเรียกใช้ของ Web Server ตัวนั้น ซึ่งสำหรับ Wireshark จะมีผลกระทบจาก การกำหนดค่า **Allow subdissector to reassemble TCP streams** ตามรูป คือ หาก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

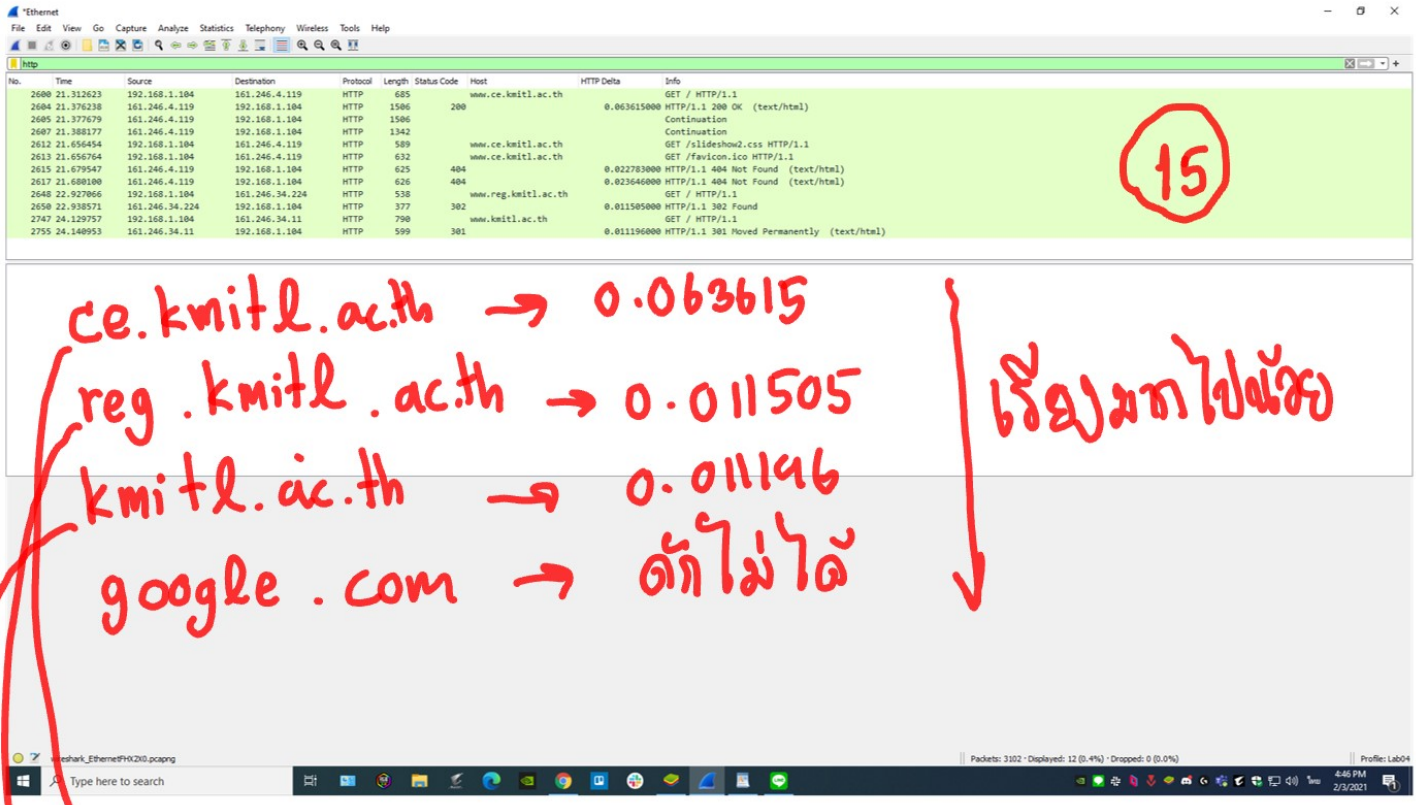
14. ให้ไปที่ บรรทัดที่เป็น 200 OK แล้วไปที่ Hypertext Transfer Protocol แล้ว Expand Subtrees ออกมาทั้งหมด แล้วไปที่บรรทัด **Time since request** แล้วเลือก **Apply as Column** ให้ตั้งชื่อว่า HTTP Delta จากนั้นให้ Sort จะพบ packet ที่ใช้เวลามากที่สุด
15. ให้นักศึกษาตรวจสอบ RTT ของเว็บ www.ce.kmitl.ac.th, 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

งานครั้งที่ 4

- การส่งงาน ให้ส่งเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา
- ส่วนบนของหน้าแรกให้มี รหัสนักศึกษา และ ชื่อนักศึกษา
- ให้ส่งโดยทำเป็นคำตอบแยกออกมา อาจมีรูปประกอบคำตอบเพื่อความชัดเจน
- กำหนดส่ง ภายในวันที่ 7 กุมภาพันธ์ 2564


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
300 1.633551 192.168.1.104 128.119.245.12 HTTP 577 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
345 1.896880 128.119.245.12 192.168.1.104 HTTP 539 HTTP/1.1 200 OK (text/html)
375 2.004133 192.168.1.104 128.119.245.12 HTTP 523 GET /favicon.ico HTTP/1.1
428 2.266874 128.119.245.12 192.168.1.104 HTTP 538 HTTP/1.1 404 Not Found (text/html)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····AP···]
Window: 1026
[Calculated window size: 1026]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x39ba [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (523 bytes)
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
[GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file1.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Pragma: no-cache\r\n
Cache-Control: no-cache\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 Edg/88.0.705.56\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
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 request 1/2]
[Response in frame: 345]
[Next request in frame: 375]
1
2
4
Packets: 1259 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%)
Profile: Lab04
Type here to search
12:31 PM
2/3/2021


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
300 1.633551 192.168.1.104 128.119.245.12 HTTP 577 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
345 1.896880 128.119.245.12 192.168.1.104 HTTP 539 HTTP/1.1 200 OK (text/html)
375 2.004133 192.168.1.104 128.119.245.12 HTTP 523 GET /favicon.ico HTTP/1.1
428 2.266874 128.119.245.12 192.168.1.104 HTTP 538 HTTP/1.1 404 Not Found (text/html)
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····AP···]
Window: 6293
[Calculated window size: 6293]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xd0db [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (485 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.
Status Code: 200
[Status Code Description:
Response Phrase: OK
Date: Wed, 03 Feb 2021 03:39:41 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: Tue, 02 Feb 2021 06:59:02 GMT\r\n
ETag: "80-5ba55016870ef"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
[Content length: 128]
Keep-Alive: timeout=5, max=99\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: 0.263329000 seconds]
[Request in frame: 300]
[Next request in frame: 375]
[Next response in frame: 428]
[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
5
3
6
7
wireshark_Ethernet6VC6X0.pcapng
Packets: 1259 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%)
Profile: Lab04
Type here to search
12:31 PM
2/3/2021



เริ่มโหลด html → css → component อื่นๆ

status 302

status 301