01076010 เครือข่ายคอมพิวเตอร์ : 2/2563 ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

## <u>กิจกรรมที่ 4 : HTT</u>P

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

- 1. ให้ใช้ Wireshark เริ่มทำการ Capture และป้อน url : <a href="http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html">http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html</a> 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 \_\_\_\_\_
  - ความยาวของ Header Ethernet II \_\_\_\_\_
  - ความยาวของ TCP Header \_\_\_\_\_
  - เหตุผลที่ Header ของข้อมูลต<sup>้</sup>องซ้อนเป็นชั้นๆ คือ

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

	method	sp	UF	RL		sp		version			cr	lf	request line
	header fie	eld n	ame		va	alue		cr	lf				
Ž	;								â				header lines
ĺ	header fie	header field name				value cr If							
	cr If												
Ĩ	entity body												body

- Browser และ Server ใช้ HTTP version ใด \_\_\_\_\_
- Browser เป็นโปรแกรมอะไร \_\_\_\_\_\_
- Server เป็นโปรแกรมอะไร \_\_\_\_\_\_

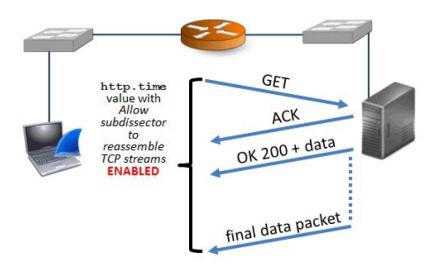
	_	ภาษาที่ Browser	ะบุว <sup>่</sup> าสามารถรับจาก Server ได้									
	- Status Code ที่ส่งกลับมาจาก Server มายัง Browser											
	_	- ค่าของ Last-Modified ของไฟล์ที่ Server										
	-		มายัง Browser									
	-	ให้สรุปว่า headei	field name ตาม HTTP message format ของข้อมูลที่ส่งกลับมีอะไรบ้าง									
5.	จ. ให <sub>้</sub>	นักศึกษาหาวิธี clec	ar cache ของ Browser ที่ตนเองใช้อยู่ แล้วจัดการ clear ให้เรียบร <sup>้</sup> อย									
6.	เปิด	ด Wireshark ใหม่แ	ล้ว Capture ที่ url http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-									
			ด Reflash เพื่อโหลดหน้าอีกครั้ง จากนั้นให้หยุด Capture									
			1									
7.	ให้	ใช้ display filter : h	ttp เพื่อให้แสดงเฉพาะ Protocol HTTP (ถ้าทำถูกจะมีแค่ 4 บรรทัด บรรทัด แต <sup>่</sup> อาจมี									
	fav	vicon ติดมาไม <sup>่</sup> ต้องไ	์ปสนใจ) และตอบคำถามต่อไปนี้									
	_	ใน HTTP GFT ครั้	งที่ 1 มีคำว่า IF-MODIFIED-SINCE หรือไม่									
			งที่ 2 มีคำว่า IF-MODIFIED-SINCE หรือไม่									
	-		<del> </del>									
	-	- ( <b>ถ้ามี) ข้อมูลที่ต่อจาก</b> IF-MODIFIED-SINCE มีความหมายอย่างไร										
	-	- ในการตอบกลับของ Server ครั้งที่ 2 มีการส่งไฟล์มาด้วยหรือไม่ จะอธิบายอย่างไร										
0	9 °	Id Edit   Droforon	To Drotocol   TCD mosics									
8.	۴N	un cait i Prejereni	ce। Protocol I TCP ตามรูป									
	✓ W	Vireshark · Preferences	×									
		SSH	^ Transmission Control Protocol									
		STANAG 5066 DTS STANAG 5066 SIS	✓ Show TCP summary in protocol tree									
		StarTeam	☐ Validate the TCP checksum if possible									
		Steam IHS Discovery STP	Allow subdissector to reassemble TCP streams									
		STT	Reassemble out-of-order segments									
		STUN SUA	✓ Analyze TCP sequence numbers									
		SV	✓ Relative sequence numbers									
		SYNC SYNCHROPHASOR	Scaling factor to use when not available from capture   Not known   V									
		Synergy	✓ Track number of bytes in flight  ✓ Calculate conversation timestamps									
		Syslog T.38	☐ Try heuristic sub-dissectors first									
		TACACS	☐ Ignore TCP Timestamps in summary									
		TACACS+ TALI	☑ Do not call subdissectors for error packets									
		TAPA	☑ TCP Experimental Options with a Magic Number									
		TCAP TCP	☐ Display process information via IPFIX									
		TCPENCAP	∨ TCP UDP port 0									
	<	<b>&gt;</b>	OK Cancel Help									

## ให้แน่ใจว่า <u>ไม่</u>ตึ๊กที่ Allow subdissector to reassemble TCP streams

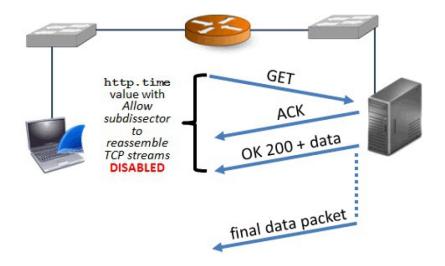
- 9. ให้ทำตามข้อ 5 อีกครั้ง และเปิด Wireshark ใหม่แล้ว Capture ที่ url <a href="http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html">http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html</a> จากนั้นให้หยุด Capture
- 10. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP (ถ้าทำถูกจะมี 5 บรรทัด) ซึ่งจะเห็นว่าหลังจาก ข้อมูล HTTP/1.1 200 OK แล้ว ยังมีข้อมูลตามมาอีก เนื่องจากไฟล์ html มีความยาวมาก (มากกว่า 4000 ไบต์) ทำให้ไม่สามารถส่งมาใน 1 packet ได้ จึงมีการแบ่งเป็นหลายๆ ส่วน (โดย TCP) ดังนั้นใน Wireshark จึง แสดงคำว่า Continuation ให้นักศึกษาตอบคำถามต่อไปนี้
  - มี HTTP GET กี่ครั้ง และมี packet ใดบ้างที่มี Status Code และเป็น Status Code ใด
- 11. ให้ทำตามข้อ 5 อีกครั้ง และเปิด Wireshark ใหม่แล้ว Capture ที่ url <a href="http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html">http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html</a> จากนั้นให้หยุด Capture
- 12. ให้ใช้ display filter : http เพื่อให้แสดงเฉพาะ Protocol HTTP และให้ตอบคำถามต่อไปนี้
   มี HTTP GET กี่ครั้ง จาก แป ใดบ้าง

  - นักศึกษาคิดว่า ภาพทั้ง 2 ภาพในไฟล์ มีการ download ทีละไฟล์ (serial) หรือทำพร<sup>้</sup>อมๆ กัน (parallel) ให้อธิบาย
- 13. ให้คลิ๊กขวาที่ Transmission Control Protocol | Protocol Preferences แล้วติ๊กที่ Allow subdissector to reassemble TCP streams เกิดอะไรขึ้น

\_\_\_\_\_



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



า คา http.time เมื่อ Disable Allow subdissector to reassemble TCP streams

ในการตรวจสอบความล่าช้าในการทำงานของ Web Server เราจะใช้ค่า RTT (Round Trip Time) ซึ่งเป็นค่า เวลาตั้งแต่ GET จนถึงตอบกลับ (OK 200) ซึ่งจะบอกได้ถึงการตอบสนองต่อการเรียกใช้ของ Web Server ตัวนั้น ซึ่ง สำหรับ Wireshark จะมีผลกระทบจาก การกำหนดค่า Allow subdissector to reassemble TCP streams ตาม รูป คือ หาก Disable จะคิดเฉพาะ packet HTTP OK 200 แต่ถ้า Enable ก็จะเป็นเวลาที่นับรวมถึงการโหลดข้อมูล ทั้งหมด 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. ให<sup>้</sup>นักศึกษาตรวจสอบ RTT ของเว็บ <u>www.ce.kmitl.ac.th</u>, <u>www.reg.kmitl.ac.th</u>, <u>www.kmitl.ac.th</u> และเว็บ อื่นอีก 1 เว็บ (นักศึกษาเลือกเอง) ให<sup>้</sup>บอกว<sup>่</sup>าค<sup>่</sup>า RTT ของแต<sup>่</sup>ละเว็บมีค<sup>่</sup>าใด ให<sup>้</sup>เรียงลำดับน<sup>้</sup>อยไปมาก ให<sup>้</sup> นักศึกษาแสดงขั้นตอนการทำงาน (เขียนอธิบายย<sup>่</sup>อๆ และ Capture รูปประกอบ) และเปรียบเทียบค<sup>่</sup>ากับ เพื่อนอีก 1 คน

## งานครั้งที่ 4

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