กิจกรรมที่ 1 : การติดตั้ง Wireshark และการใช้งานเบื้องต้น

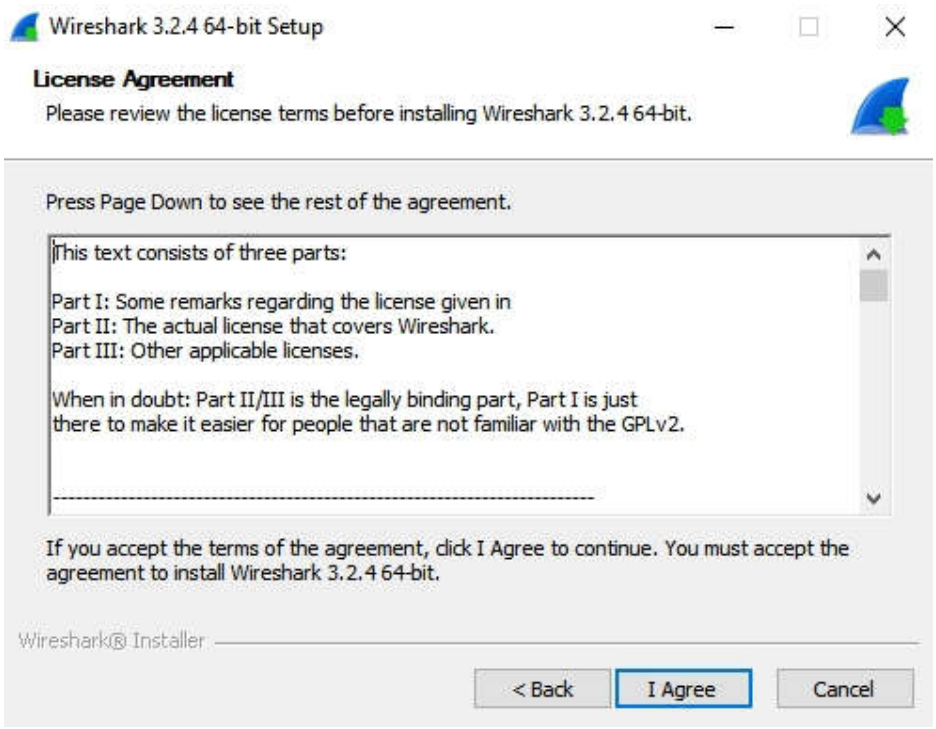
Wireshark เป็นโปรแกรมสำหรับวิเคราะห์ packet ในระบบเครือข่าย สามารถติดตั้งได้หลาย platform ทั้ง Linux, Unix หรือ Window โดยอาศัย pcap ในการจับ packet บน interface ของเครื่อง และมี TShark เป็น commnad line ด้วย

คุณสมบัติของ Wireshark

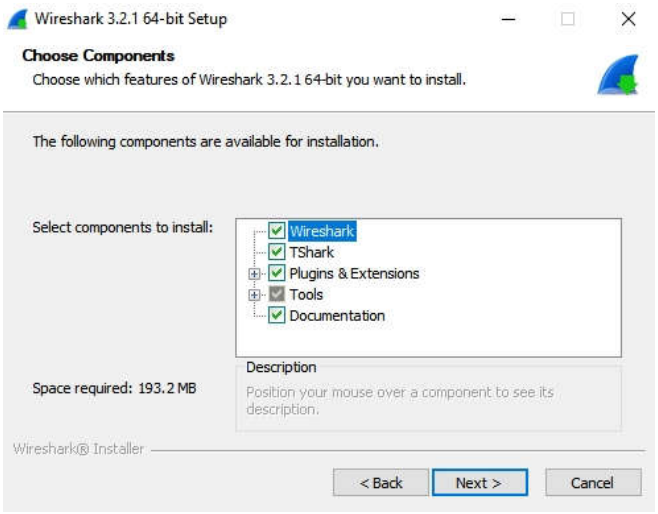
1. สามารถจับข้อมูลในระบบเครือข่าย network ได้ รวมถึงอ่านข้อมูล packet จากไฟล์มาวิเคราะห์ได้
2. สามารถดักจับข้อมูลได้หลายแบบทั้ง Ethernet, IEEE 802.11, PPP และ loopback
3. ใช้งานได้ทั้งบน GUI และ command line (TShark)
4. สามารถ filter ข้อมูลได้
5. มีเครื่องมือวิเคราะห์เครือข่ายให้ใช้งานค่อนข้างมาก
6. จับข้อมูล USB แบบ raw data ได้
7. ดักจับข้อมูลได้ทั้งแบบ มีสาย (lan) และไร้สาย (wireless)

การติดตั้ง

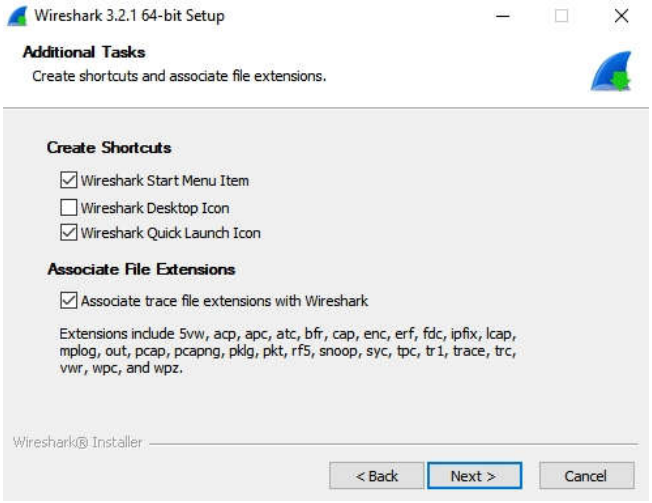
1. เข้าหน้าเว็บ https://www.wireshark.org/download.html
2. เลือก Windows Installer (64-bit) โหลดและติดตั้ง



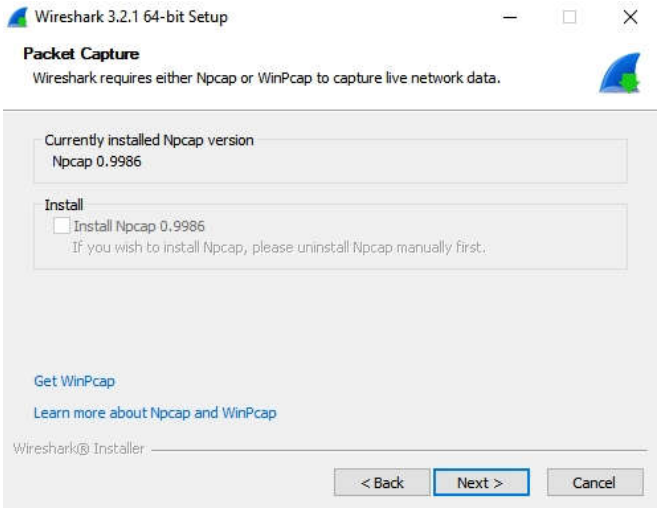
3. กด Next



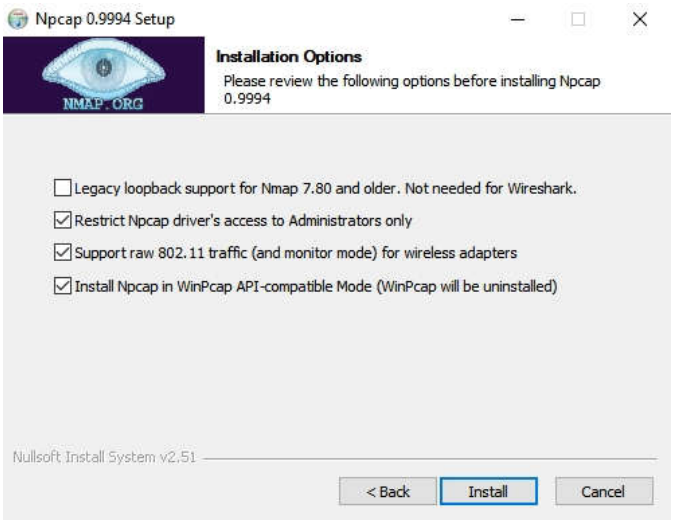
4. เลือกตามต้องการว่าจะเอา Desktop Icon หรือ Quick Launch หรือไม่



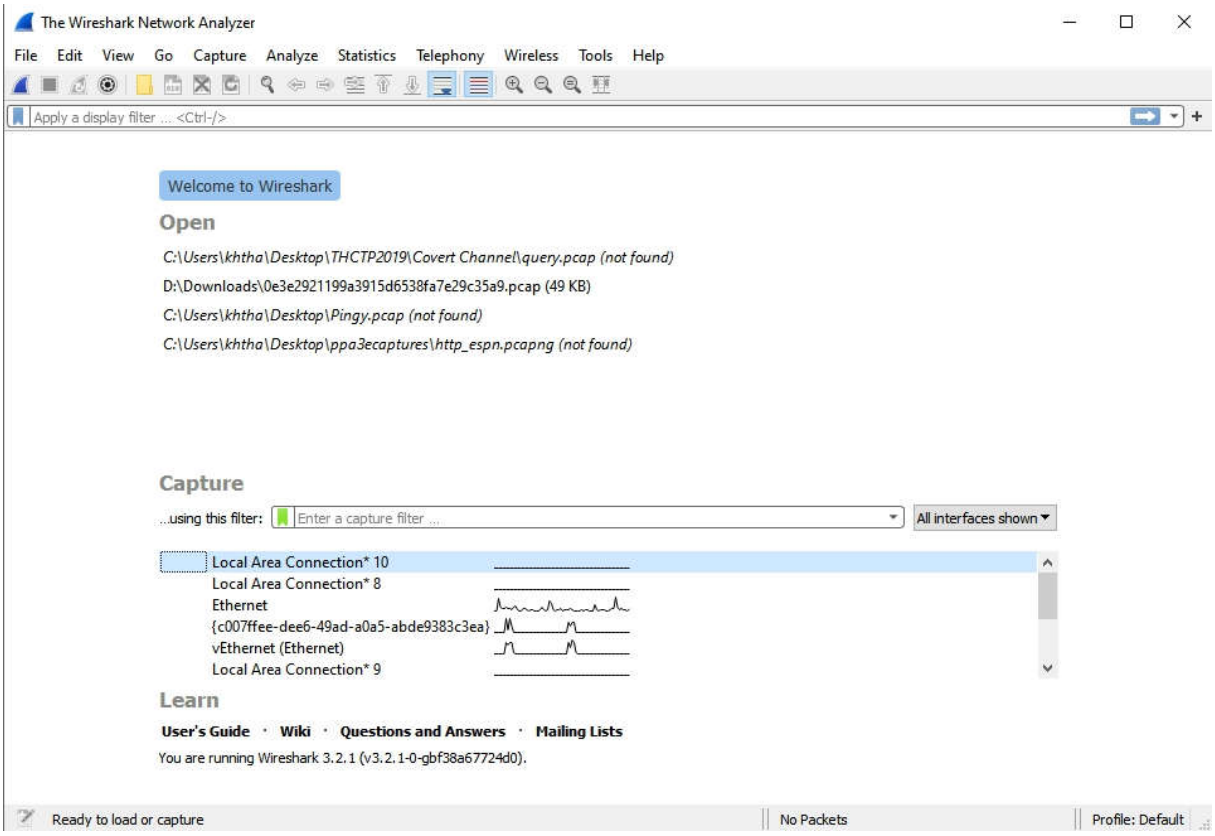
5. Next ไปเรื่อยๆ เลือกติดตั้ง Npcap ถ้ายังไม่ติดตั้ง



6. ในหน้าติดตั้ง Npcap ให้เลือกหมด ยกเว้นตัวแรก



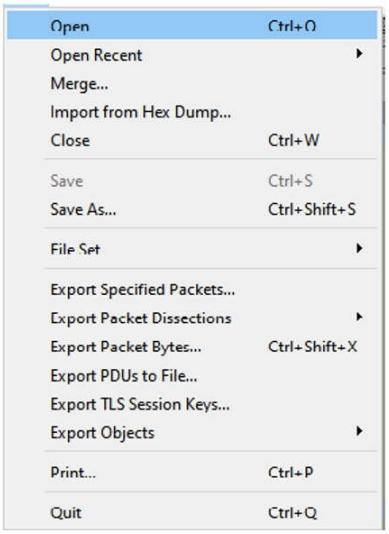
7. จากนั้นกด Next ไปเรื่อย จนเสร็จ เมื่อเปิดโปรแกรมจะได้หน้าจอดังนี้ (การเปิดโปรแกรมให้คลิกขวา More -> Run as Administrator ไม่งั้นโปรแกรมจะถาม Admin Mode หลายครั้ง)



การใช้งานเบื้องต้น

1. เมนูประกอบด้วย File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help แต่สำหรับการใช้งานเบื้องต้นในครั้งนี้ จะใช้แค่ File, Edit และ View

- เมนู File

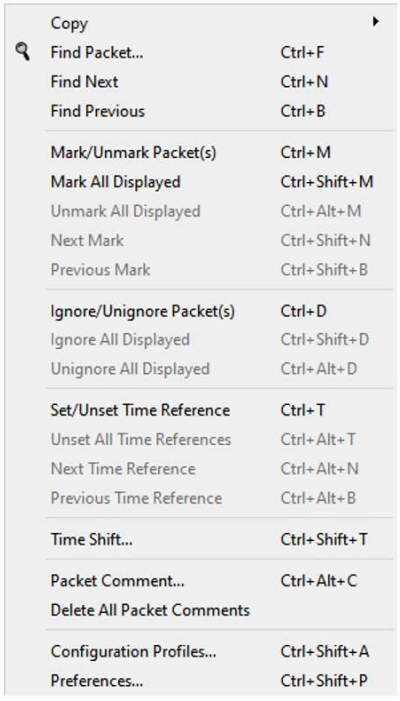


Merge สามารถรวมไฟล์ปัจจุบัน กับ ไฟล์อื่นได้

File Set เรียกดูไฟล์แบบเป็นชุด

Export ใช้ในการ Save บาง Packet หรือบางส่วนไปเป็นไฟล์

- เมนู Edit



Copy ใช้ copy packet ออกเป็นรูปแบบต่างๆ

Find Packet ค้นหา Packet ตามเงื่อนไข

Find Next ค้นหา Packet ถัดไปตามเงื่อนไข

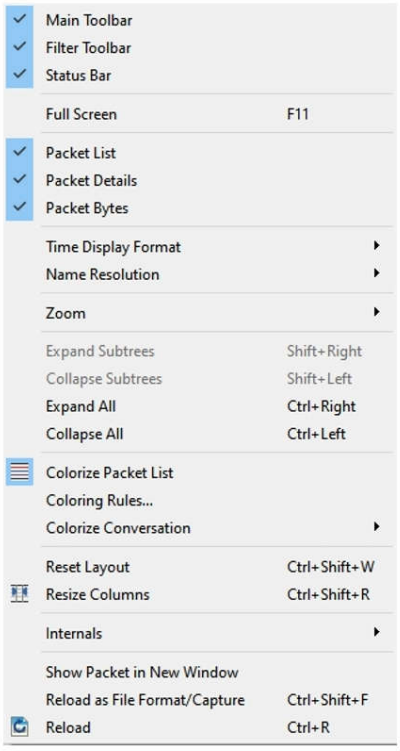
Find Previous ค้นหา Packet ก่อนหน้าตามเงื่อนไข

Mark/Unmark ทำเครื่องหมาย (คลิกขวาได้)

Ignore ไม่สนใจ Packet ในการวิเคราะห์

Time Shift เลื่อนเวลาของ Packet

- เมนู View



Main Toolbar/Filter Toolbar/Status Bar
เลือกแสดง / ไม่แสดง
Packet List/Packet Details/Packet Bytes
แสดง/ไม่แสดง ส่วนของ Packet
Time Display Format รูปแบบการแสดงเวลา
Name Resolution รูปแบบการแสดงชื่อ
Zoom ย่อ/ขยาย Font
Colorize Packet List ระบายสี
Coloring Rules... กำหนดสีที่จะระบาย
Colorize Conversation กำหนดสีโต้ตอบ

2. ส่วนของ Toolbar

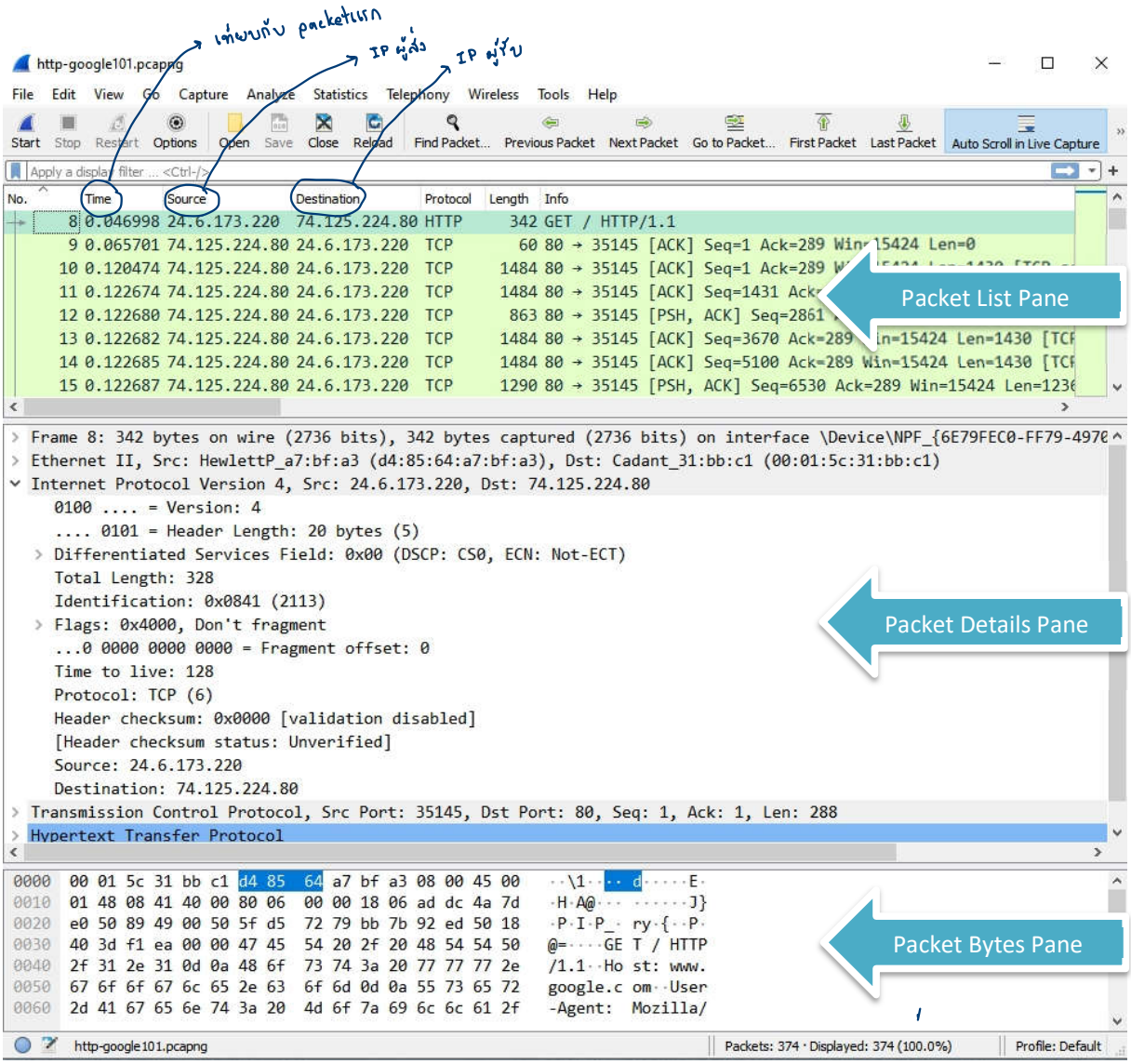
Start Capture	Open Capture File	Find Packet	Coloring	Zoom In
Stop Capture	Save Capture File	Go Back	Auto	Zoom Out
Restart Capture	Close Capture	Forward	Scroll	Zoom 100%
Capture Option	File	Go to Number		Resize Column
	Reload Capture	Go First		
	File	Go Last		

3. เปิดไฟล์ http-google101.pcapng จะพบว่าหน้าจอแบ่งเป็น 3 ส่วน ดังนี้

Packet List Pane เป็นส่วนที่แสดงลำดับของ Packet ที่อยู่ในไฟล์ ดังนั้นสามารถจะดูจำนวน Packet และภาพรวมของข้อมูลที่อยู่ในไฟล์ได้ ถือเป็นส่วนที่มีความสำคัญที่จะใช้ในการวิเคราะห์

Packet Details Pane เป็นส่วนที่แสดงรายละเอียดของข้อมูลในเฟรม โดยจะมีข้อมูลบางส่วนที่ Wireshark ได้เพิ่มเข้าไป เพื่อความสะดวกต่อการใช้งานด้วย จะใช้ข้อมูลส่วนนี้ในการดูรายละเอียดของข้อมูลที่อยู่ภายใน Packet

Packet Bytes Pane เป็นส่วนที่เป็นข้อมูลจริง (Raw Data) ซึ่งหากข้อมูลที่ส่งเป็น Text และไม่มีการเข้ารหัสจะเห็นข้อมูลที่สามารถอ่านได้



ในส่วน Packet List Pane จะมีข้อมูลที่แบ่งออกเป็นคอลัมน์ โดยมีคอลัมน์เบื้องต้นดังนี้

- No. เป็น Packet ที่เท่าไรในไฟล์
- Time ปกติจะแสดงเวลาที่นับจาก Packet แรก แต่สามารถกำหนดให้แสดงเป็นแบบอื่นได้จาก View -> Time Display Format
- Source และ Destination แสดง IP Address ต้นทางและปลายทางของ Packet
- Protocol แสดงว่าใน Packet นี้เป็น Protocol อะไร
- Length แสดงความยาวของ Packet
- Info แสดงข้อมูลแบบย่อของ Packet ที่สร้างขึ้นโดย Wireshark ซึ่งช่วยให้เห็นภาพรวมได้สะดวก

4. ให้ทดลองดังนี้
   - กดที่ชื่อคอลัมน์ เกิดอะไรขึ้น การเรียง Packet เปลี่ยน จาก น้อยไปมาก → มากไปน้อย
   - กดค้างที่ชื่อคอลัมน์แล้วเลื่อน เกิดอะไรขึ้น สามารถเคลื่อนย้ายสลับลำดับ คอลัมน์ ได้
     _____

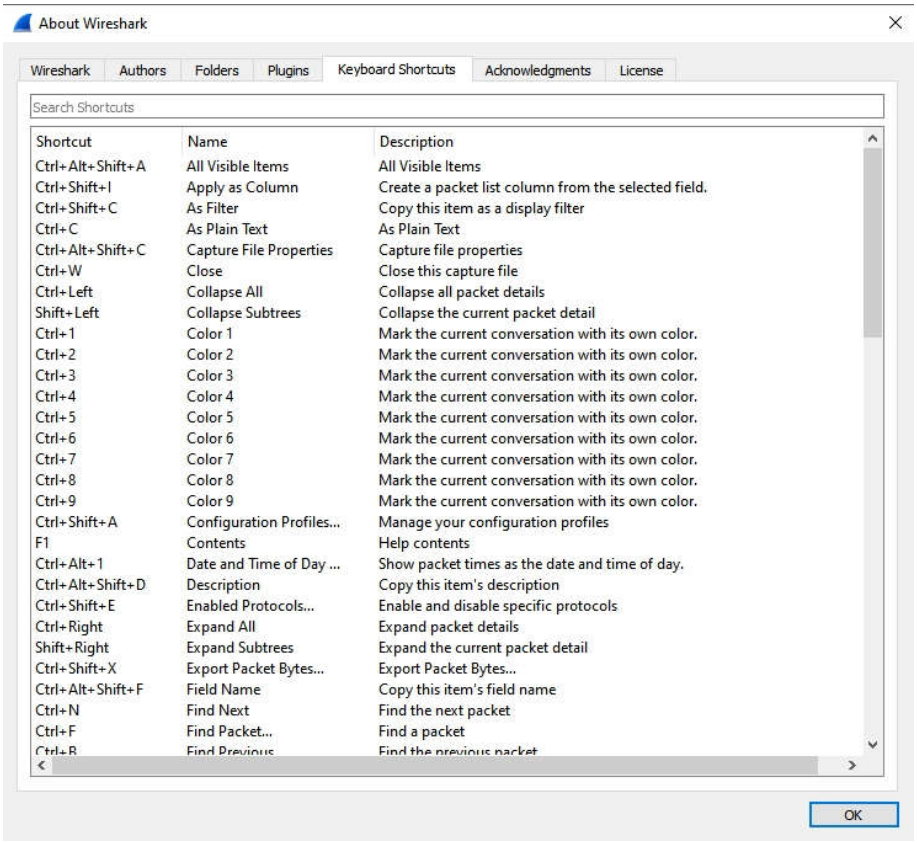
- คลิกขวาที่ชื่อคอลัมน์ เราสามารถทำอะไรได้บ้าง

• เลื่อนการจัดวางข้อมูลใน คอลัมน์ ว่าจะวางตรงกลางหรือชิดข้างไหนของเซลล์ • เลือก คอลัมน์ที่จะแสดง/ซ่อนได้

• สามารถ Edit คอลัมน์ ได้ ex. แก้ไขชื่อ, ประเภท • Remove คอลัมน์

• สามารถ Resize to Contents
Resize column to width

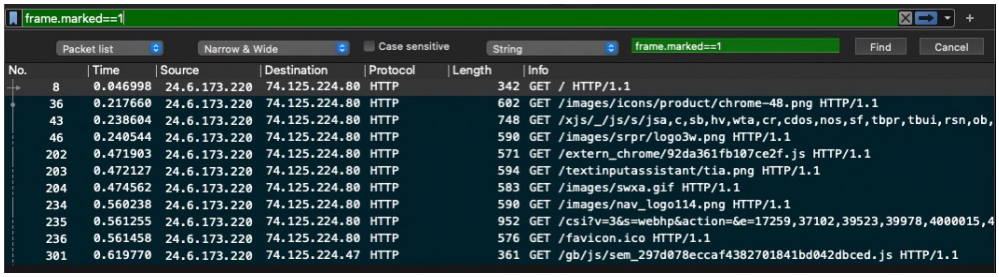
5. การใช้ Shortcut ใน Wireshark สามารถใช้ได้โดยดูได้จาก About -> Keyboard Shortcuts ตามรูป



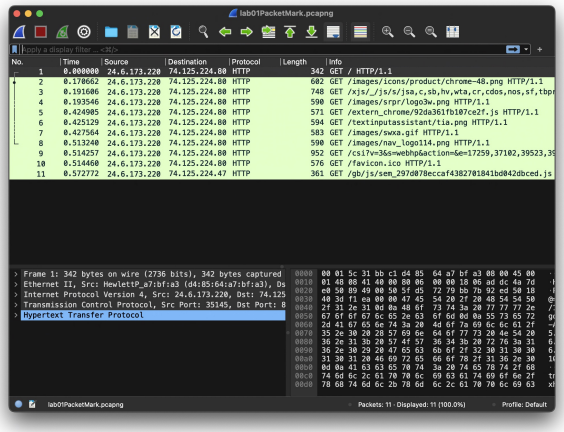
6. ให้ค้นหา Packet ที่มีคำว่า GET และ Mark Packet (Ctrl-M หรือ คลิกขวา -> Mark) ทำไปเรื่อย ให้ครบทั้งไฟล์ ให้ตอบคำถามว่ามีกี่ Packet ที่ Mark ไว้ (ดูได้จาก Status Bar ด้านล่าง) 11 Packet

7. ให้ป้อน frame.marked==1 ลงในช่อง filter ด้านบน เกิดอะไรขึ้นให้อธิบายและ Capture ภาพไว้

เป็นการ filter เอาแต่ packet ที่ถูก mark ไว้



8. ให้ File -> Export Specified Packet.. แล้วเลือก Packet ที่ Mark เอาไว้ Save เป็นไฟล์ แล้วเปิดไฟล์ที่ Save และ Capture ภาพไว้



การเพิ่มคอลัมน์

1. ให้ไปที่ Packet ที่ 8 เลื่อนไปที่ HTTP แล้วขยาย ไปที่บรรทัด Host คลิกขวาแล้วเลือก Apply as Column แล้วบอกว่าในไฟล์มีการใช้ HTTP ไปที่ Host ใดบ้าง

www.google.com

ssl.gstatic.com

2. ให้หาวิธีการที่สามารถทราบรายชื่อ Host ตามข้อ 1 ให้เร็วที่สุด และให้บอกด้วยว่ามีการไป Request ที่ Host เหล่านั้นกี่ครั้ง

statistic ที่เมนูบาร์ เลือก HTTP แล้วดู Request ว่าเจอ host

ดูจำนวนการ Request ใน statistic ที่เมนูบาร์ เลือก HTTP แล้วดู packet counter (มี 11 ครั้ง)

3. ให้นักศึกษาหาวิธีการเพิ่มคอลัมน์ที่ไม่ใช้วิธีการคลิกขวา

- ที่เมนูบาร์ Analyze เลือก Apply as Colum
- short cut คือ shift + command + I หรือ shift + CTRL + I

4. ให้ลบคอลัมน์ที่สร้าง

งานครั้งที่ 1

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา ตามด้วย _lab01 เช่น 64019999_lab01.pdf
- กำหนดส่ง ภายในวันที่ 24 มกราคม 2566 โดยให้ส่งใน Microsoft Teams ของรายวิชา