

64010443 ນິສ້າຮລ ອູຍໍຕີ  
ງ

01076117 ปฏิบัติการเครือข่ายคอมพิวเตอร์ 2/2565

ภาควิชาบริหารธุรกิจและการบัญชี

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

### กิจกรรมที่ 1 : การติดตั้ง Wireshark และการใช้งานเบื้องต้น

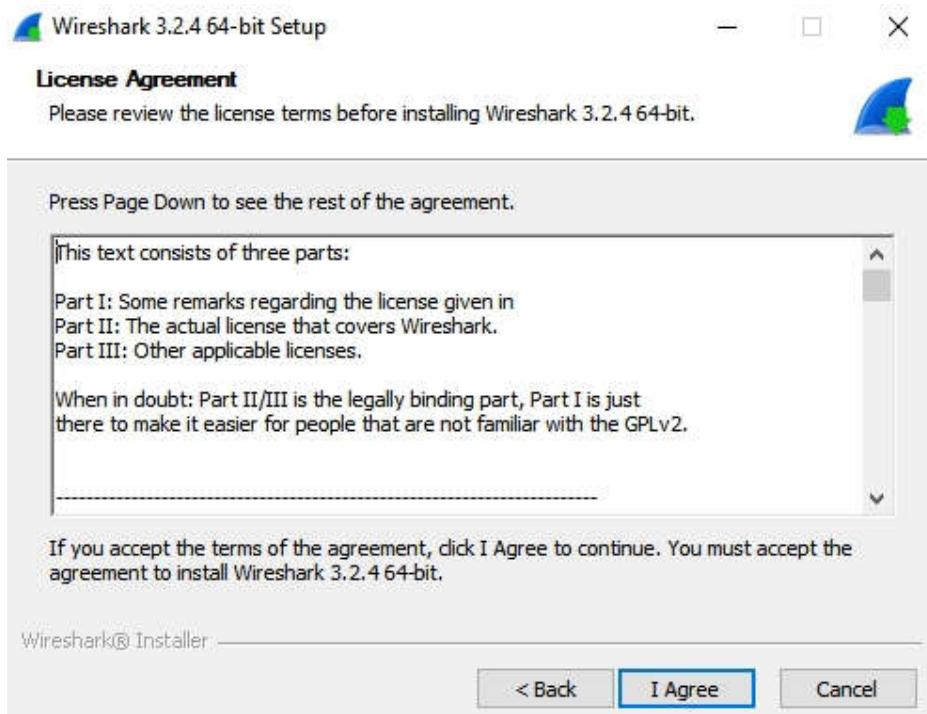
Wireshark เป็นโปรแกรมสำหรับวิเคราะห์ packet ในระบบเครือข่าย สามารถติดตั้งได้หลาย platform ทั้ง Linux, Unix หรือ Window โดยอาศัย pcap ในการจับ packet บน interface ของเครื่อง และมี TShark เป็น command line ด้วย

## คุณสมบัติของ Wireshark

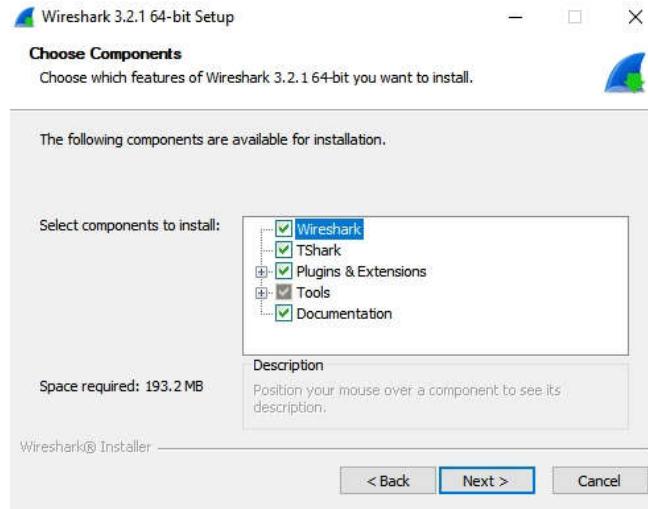
- สามารถจับข้อมูลในระบบเครือข่าย network ได้ รวมถึงอ่านข้อมูล packet จากไฟล์มาร์คeraที่ได้
  - สามารถดักจับข้อมูลได้หลายแบบทั้ง Ethernet, IEEE 802.11, PPP และ loopback
  - ใช้งานได้ทั้งบน GUI และ command line (TShark)
  - สามารถ filter ข้อมูลได้
  - มีเครื่องมือวิเคราะห์เครือข่ายให้ใช้งานค่อนข้างมาก
  - จับข้อมูล USB แบบ raw data ได้
  - ดักจับข้อมูลได้ทั้งแบบ มีสาย (lan) และไร้สาย (wireless)

การติดตั้ง

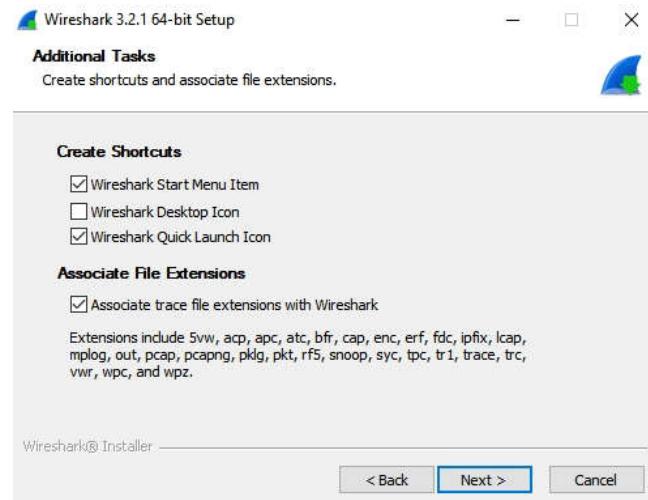
1. เข้าหน้าเว็บ <https://www.wireshark.org/download.html>
  2. เลือก Windows Installer (64-bit) โหลดและติดตั้ง



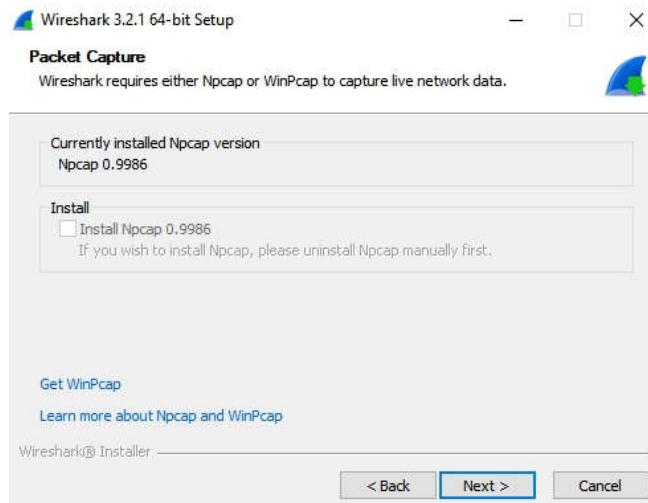
3. ۱۹ Next



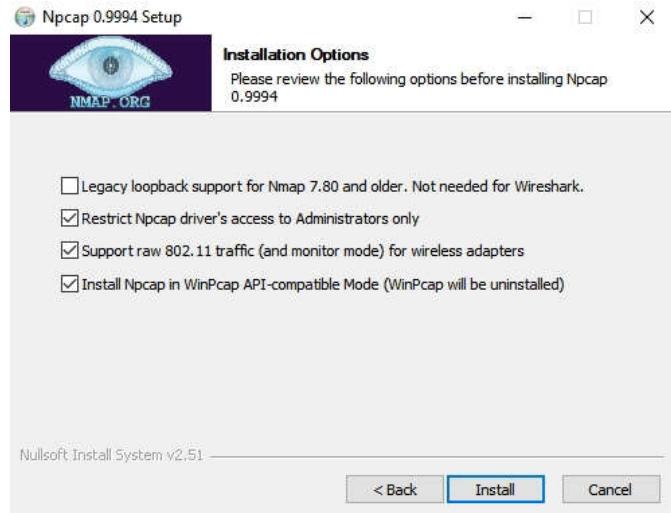
4. เลือกตามต้องการว่าจะเอา Desktop Icon หรือ Quick Launch หรือไม่



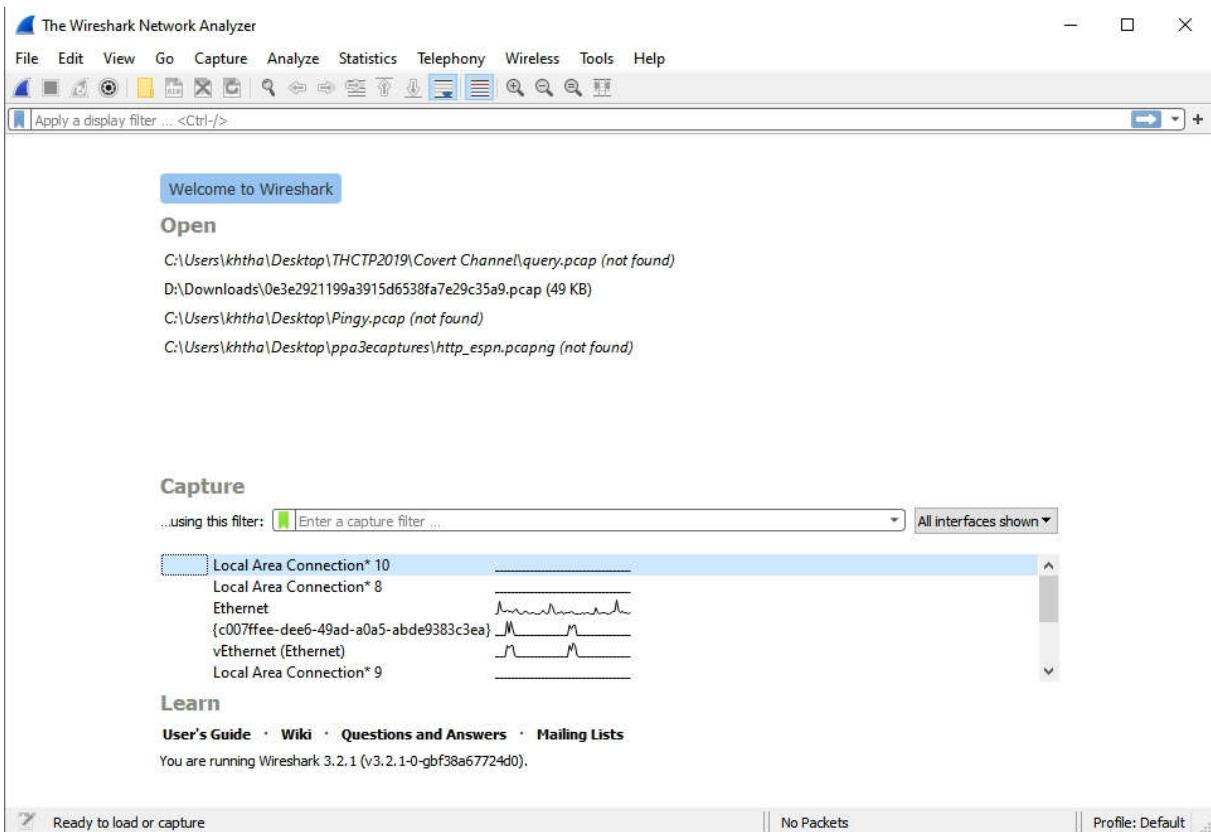
5. Next ไปเรื่อยๆ เลือกติดตั้ง Npcap ถ้ายังไม่ติดตั้ง



6. ในหน้าติดตั้ง Npcap ให้เลือกหมวด ยกเว้นตัวแรก



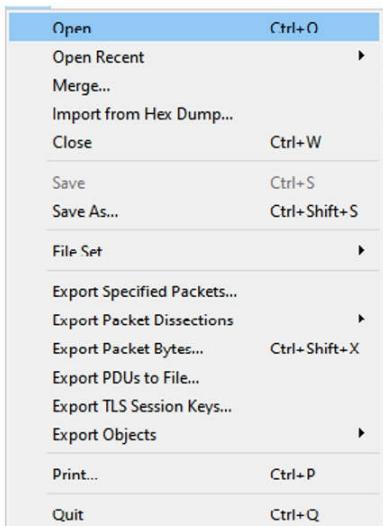
7. จากนั้นกด Next ไปเรื่อย จนเสร็จ เมื่อเปิดโปรแกรมจะได้หน้าดังนี้ (การเปิดโปรแกรมให้คลิกขวา More -> Run as Administrator ไม่งั้นโปรแกรมจะถูก Admin Mode หลายครั้ง)



## การใช้งานเบื้องต้น

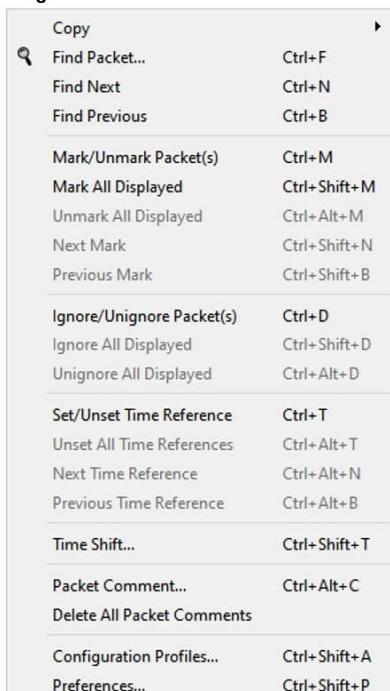
- เมนูประกอบด้วย File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help แต่สำหรับการใช้งานเบื้องต้นในครั้งนี้ จะใช้แค่ File, Edit และ View

### • เมนู File



**Merge** สามารถรวมไฟล์ปัจจุบัน กับ ไฟล์อื่นได้  
**File Set** เรียกดูไฟล์แบบเป็นชุด  
**Export** ใช้ในการ Save บาง Packet หรือบางส่วน  
ไปเป็นไฟล์

### • เมนู Edit



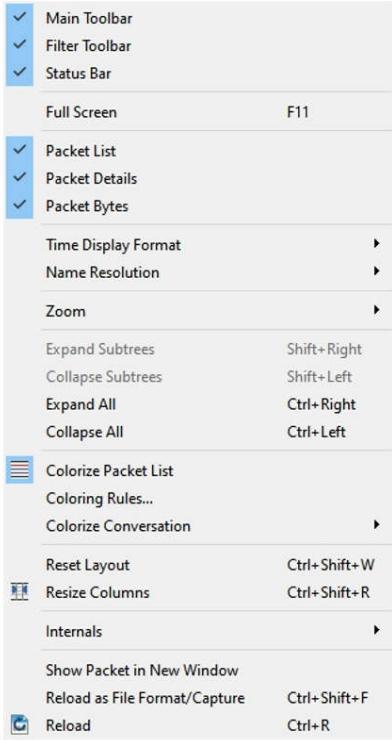
**Copy** ใช้ copy packet ออกเป็นรูปแบบต่างๆ  
**Find Packet** ค้นหา Packet ตามเงื่อนไข  
**Find Next** ค้นหา Packet ถัดไปตามเงื่อนไข  
**Find Previous** ค้นหา Packet ก่อนหน้าตามเงื่อนไข

**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 ระบายน้ำ

Coloring Rules... กำหนดสีที่จะระบายน้ำ

Colorize Conversation กำหนดสีให้ตอบ

2. ส่วนของ Toolbar

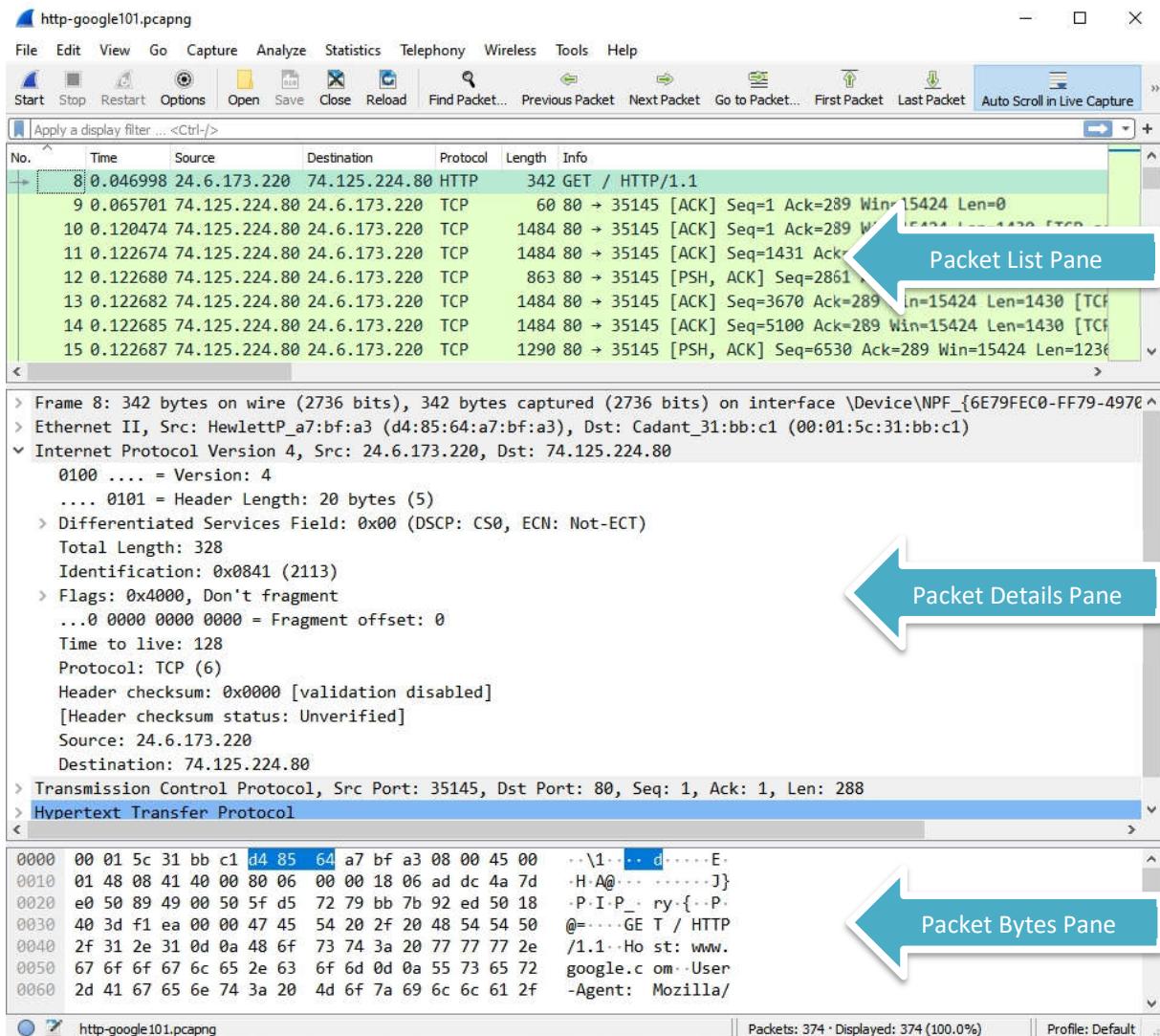


3. เปิดไฟล์ http-google101.pcapng จะพบว่าหน้าจอแบ่งเป็น 3 ส่วน ดังนี้

**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 และไม่มีการเข้ารหัส จะเห็นข้อมูลที่สามารถอ่านได้



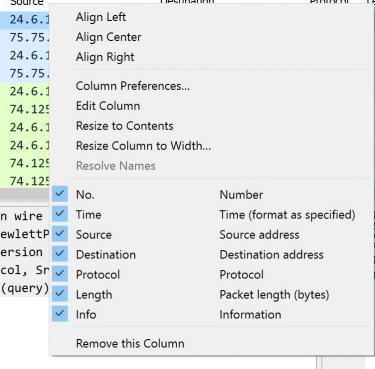
ในส่วน Packet List Pane จะมีข้อมูลที่แบ่งออกเป็นคอลัมน์ โดยมีคอลัมน์เบื้องต้นดังนี้

- 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

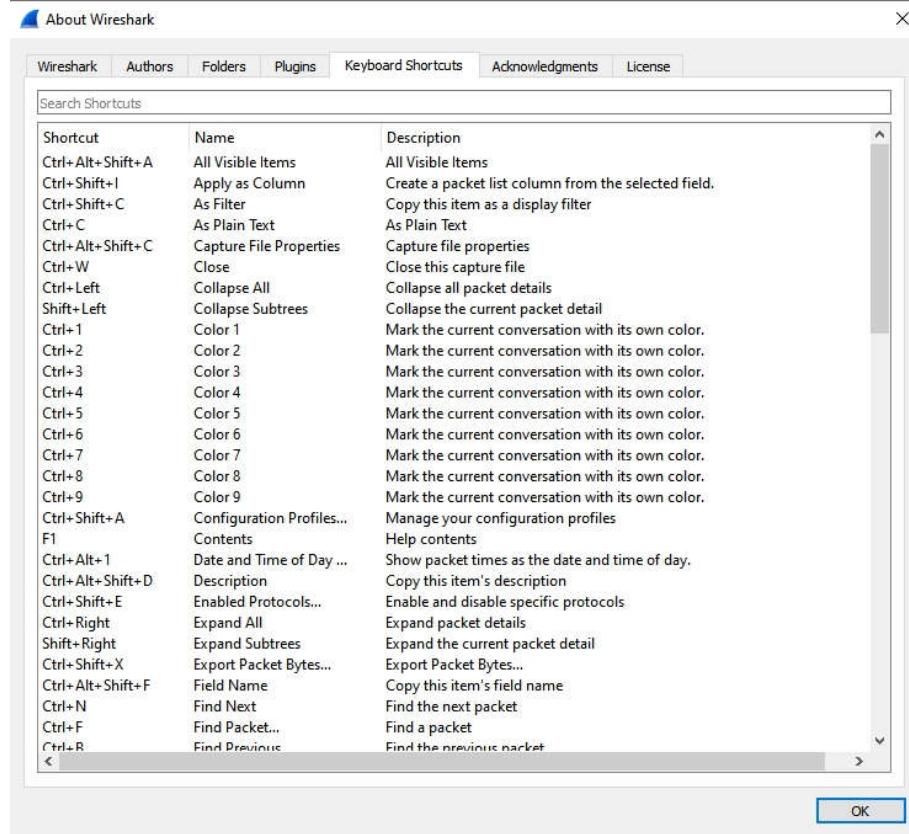
#### 4. ให้ทดลองดังนี้

- กดที่ชื่อคอลัมน์ เกิดอะไรขึ้น เปลี่ยนการเรียงลำดับ package
- กดค้างที่ชื่อคอลัมน์แล้วเลื่อน เกิดอะไรขึ้น ทำให้สามารถลากหัว column ได้ตามที่เราต้องการ

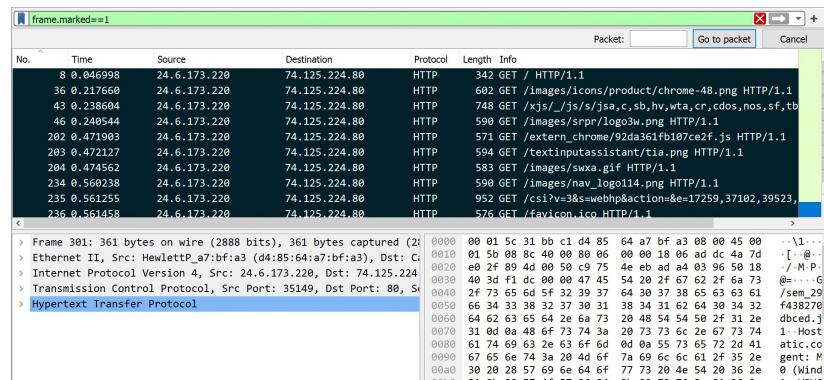
- คลิกขวาที่ชื่อคอลัมน์ เราสามารถทำอะไรได้บ้าง
  - จัดตำแหน่งให้รัดข้าม, ขยายและย่อกล้อง
  - Edit ข้อมูลในช่องกำหนดค่าต่างๆ ในช่องนี้จะมี Column
  - กด鼠标 visualize ได้ , Remove column ได้



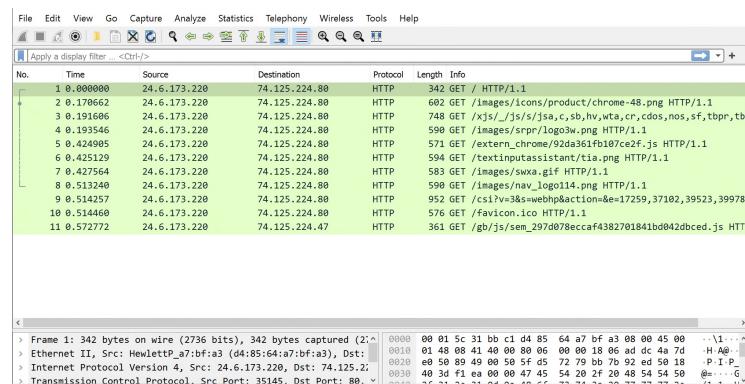
## 5. การใช้ Shortcut ใน Wireshark สามารถใช้ได้โดยตู้ๆ จาก About -> Keyboard Shortcuts ตามรูป



- ให้ค้นหา Packet ที่มีคำว่า GET และ Mark Packet (Ctrl-M หรือ คลิกขวา -> Mark) ทำไปเรื่อยๆ ให้ครบทั้งไฟล์ ให้ตอบคำถามว่ามีกี่ Packet ที่ Mark ไว้ (ดูจาก Status Bar ด้านล่าง) 11 packet
- ให้ป้อน frame.marked==1 ลงในช่อง filter ด้านบน เกิดอะไรขึ้นให้อธิบายและ Capture ภาพไว้ ที่ให้ข้อมูลน้ำใจขององค์ประกอบ packet ที่เรา mark ไว้



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



### การเพิ่มคอลัมน์

1. ให้ไปที่ Packet ที่ 8 เลื่อนไปที่ HTTP และขยายไปที่เบรหัด Host คลิกขวาแล้วเลือก Apply as Column และบอกว่าในไฟล์มีการใช้ HTTP ไปที่ Host ได้บ้าง

www.google.com

ssl.gstatic.com

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

หลังจากเลือก Apply as column แล้วให้ทำการกด sort ที่ column ที่จะ變成 column Host ให้แล้ว

นักการ Request ไปที่ www.google.com 10 ครั้ง ssl.gstatic.com 1 ครั้ง

Protocol	Length	Host
HTTP	270	www.google.com
HTTP	950	www.google.com
HTTP	590	www.google.com
HTTP	583	www.google.com
HTTP	594	www.google.com
HTTP	571	www.google.com
HTTP	590	www.google.com
HTTP	748	www.google.com
HTTP	361	www.google.com

3. ให้นักศึกษาหารวิธีการเพิ่มคอลัมน์ที่ไม่ใช่วิธีการคลิกขวา

ไปที่เบรหัด Host กดเลือก Host แล้ว กด Ctrl + Shift + 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

## ข้อ 4 ให้ลบ column ที่สร้าง

### - เลือกง่ายทำการลบ column Host

Screenshot of Wireshark showing a list of network packets. A red arrow points to the 'Host' column header in the table.

No.	Time	Source	Destination	Protocol	Length	Host	Info
367	8.200964	74.125.224.80	24.6.173.220	TCP	60		80 → 35146 [FIN, ACK] Seq=8251 Ack=35146 → 80 [ACK] Seq=1976 Ack=825
368	8.201103	24.6.173.220	74.125.224.80	TCP	54		35146 → 80 [ACK] Seq=1976 Ack=825
369	8.201880	74.125.224.47	24.6.173.220	TCP	60		80 → 35149 [FIN, ACK] Seq=18200 Ack=80
370	8.201883	74.125.224.80	24.6.173.220	TCP	60		80 → 35145 [FIN, ACK] Seq=244186 Ack=244186
371	8.201885	74.125.224.80	24.6.173.220	TCP	60		80 → 35147 [FIN, ACK] Seq=11299 Ack=11299
372	8.202022	24.6.173.220	74.125.224.47	TCP	54		35149 → 80 [ACK] Seq=309 Ack=1820
373	8.202060	24.6.173.220	74.125.224.80	TCP	54		35145 → 80 [ACK] Seq=2585 Ack=244
374	8.202085	24.6.173.220	74.125.224.80	TCP	54		35147 → 80 [ACK] Seq=1053 Ack=113
8	0.046998	24.6.173.220	74.125.224.80	HTTP	342	www.google.com	GET / HTTP/1.1
36	0.217660	24.6.173.220	74.125.224.80	HTTP	602	www.google.com	GET /images/icons/product/chrome-48.png HTTP/1.1
43	0.238604	24.6.173.220	74.125.224.80	HTTP	748	www.google.com	GET /xjs/_/js/s/jsa,c,sb,hv,wta,c
46	0.240544	24.6.173.220	74.125.224.80	HTTP	590	www.google.com	GET /images/srpr/logo3w.png HTTP/1.1
202	0.471903	24.6.173.220	74.125.224.80	HTTP	571	www.google.com	GET /extern_chrome/92da361fb107ce
203	0.472127	24.6.173.220	74.125.224.80	HTTP	594	www.google.com	GET /textinputassistant/tia.png HTTP/1.1
204	0.474562	24.6.173.220	74.125.224.80	HTTP	583	www.google.com	GET /images/swxa.gif HTTP/1.1
234	0.560238	24.6.173.220	74.125.224.80	HTTP	590	www.google.com	GET /images/nav_logo114.png HTTP/1.1
235	0.561255	24.6.173.220	74.125.224.80	HTTP	952	www.google.com	GET /csiv?=&s=webhp&action=&e=17
236	0.561458	24.6.173.220	74.125.224.80	HTTP	576	www.google.com	GET /favicon.ico HTTP/1.1
301	0.619770	24.6.173.220	74.125.224.47	HTTP	361	ssl.gstatic.com	GET /gb/js/sem_297d078eccaf438270

คลิกขวาที่ column Host

Screenshot of Wireshark showing the context menu for the 'Host' column. A red arrow points to the 'Remove this Column' option at the bottom of the menu.

Host	Align Left
	Align Center
	Align Right
	Column Preferences...
	Edit Column
	Resize to Contents
	Resize Column to Width...
	Resolve Names
No.	<input checked="" type="checkbox"/> Number
Time	<input checked="" type="checkbox"/> Time (format as specified)
Source	<input checked="" type="checkbox"/> Source address
Destination	<input checked="" type="checkbox"/> Destination address
Protocol	<input checked="" type="checkbox"/> Protocol
Length	<input checked="" type="checkbox"/> Packet length (bytes)
Host	<input checked="" type="checkbox"/> http.host
Info	<input checked="" type="checkbox"/> Information
Remove this Column	

กด Remove

Host ก็จะหาย หลังจาก Remove

Screenshot of Wireshark showing the packet list after the 'Host' column has been removed. A red arrow points to the 'Time (format as specified)' column header.

No.	Time	Source	Destination	Protocol	Length	Info
359	0.823331	24.6.173.220	74.125.224.80	TCP	54	35146 → 80 [ACK] Seq=1975 Ack=8251 Win=64856 Len=0
360	0.048224	24.6.173.220	74.125.224.47	TCP	54	35148 → 80 [FIN, ACK] Seq=1 Ack=1 Win=65780 Len=0
361	0.084551	74.125.224.47	24.6.173.220	TCP	60	80 → 35148 [FIN, ACK] Seq=1 Ack=2 Win=14336 Len=0
362	0.084678	24.6.173.220	74.125.224.47	TCP	54	35148 → 80 [ACK] Seq=2 Ack=2 Win=65780 Len=0
363	0.182944	24.6.173.220	74.125.224.47	TCP	54	35149 → 80 [FIN, ACK] Seq=308 Ack=18200 Win=65780 Len=0
364	0.183080	24.6.173.220	74.125.224.80	TCP	54	35147 → 80 [FIN, ACK] Seq=1052 Ack=11299 Win=64444 Len=0
365	0.183121	24.6.173.220	74.125.224.80	TCP	54	35146 → 80 [FIN, ACK] Seq=1975 Ack=8251 Win=64856 Len=0
366	0.183157	24.6.173.220	74.125.224.80	TCP	54	35145 → 80 [FIN, ACK] Seq=2584 Ack=244186 Win=246060 Len=0
367	0.200964	74.125.224.80	24.6.173.220	TCP	60	80 → 35146 [FIN, ACK] Seq=8251 Ack=1976 Win=18304 Len=0
368	0.201103	24.6.173.220	74.125.224.80	TCP	54	35146 → 80 [ACK] Seq=1976 Ack=8252 Win=64856 Len=0
369	0.201880	74.125.224.47	24.6.173.220	TCP	60	80 → 35149 [FIN, ACK] Seq=18200 Ack=309 Win=15424 Len=0
370	0.201883	74.125.224.80	24.6.173.220	TCP	60	80 → 35145 [FIN, ACK] Seq=244186 Ack=2585 Win=20672 Len=0
371	0.201885	74.125.224.80	24.6.173.220	TCP	60	80 → 35147 [FIN, ACK] Seq=11299 Ack=1053 Win=16448 Len=0
372	0.202022	24.6.173.220	74.125.224.47	TCP	54	35149 → 80 [ACK] Seq=309 Ack=18201 Win=65780 Len=0
373	0.202060	24.6.173.220	74.125.224.80	TCP	54	35145 → 80 [ACK] Seq=2585 Ack=244187 Win=246060 Len=0
374	0.202085	24.6.173.220	74.125.224.80	TCP	54	35147 → 80 [ACK] Seq=1053 Ack=11300 Win=64444 Len=0
301	0.619770	24.6.173.220	74.125.224.47	HTTP	361	GET /gb/js/sem_297d078eccaf4382701841bd042dbced.js HTTP/1.1
8	0.046998	24.6.173.220	74.125.224.80	HTTP	342	GET / HTTP/1.1
36	0.217660	24.6.173.220	74.125.224.80	HTTP	602	GET /images/icons/product/chrome-48.png HTTP/1.1