

กิจกรรมที่ 1 : การติดตั้ง Wireshark และการใช้งานเบื้องต้น

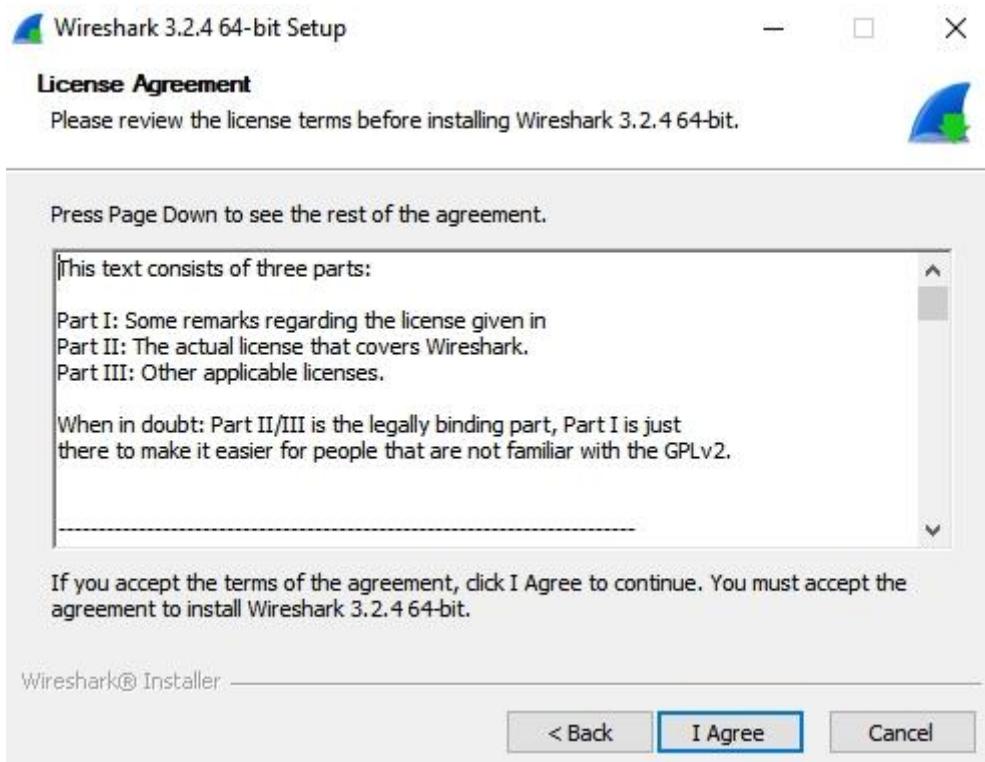
Wireshark เป็นโปรแกรมสำหรับวิเคราะห์ packet ในระบบเครือข่าย สามารถติดตั้งได้หลาย platform ทั้ง Linux, Unix หรือ Windows โดยอาศัย pcap ในการจับ packet บน interface ของเครื่อง และมี TShark เป็น command line ด้วย

គុណសមប័តិខែង Wireshark

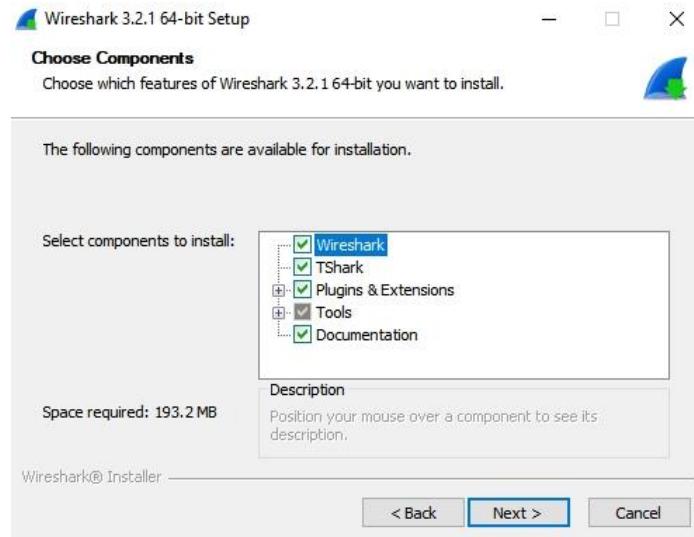
- สามารถจับข้อมูลในระบบเครือข่าย network โดย รวมถึงอ่านข้อมูล packet จากไฟล์มาวิเคราะห์ได้
 - สามารถตัดกัจฉับข้อมูลได้หลายแบบทั้ง Ethernet, IEEE 802.11, PPP และ loopback
 - ใช้งานได้ทั้งบน GUI และ command line (TShark)
 - สามารถ filter ข้อมูลได้
 - มีเครื่องมือวิเคราะห์เครือข่ายให้ใช้งานค่อนข้างมาก
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

ກາງຕິດຕັ້ງ

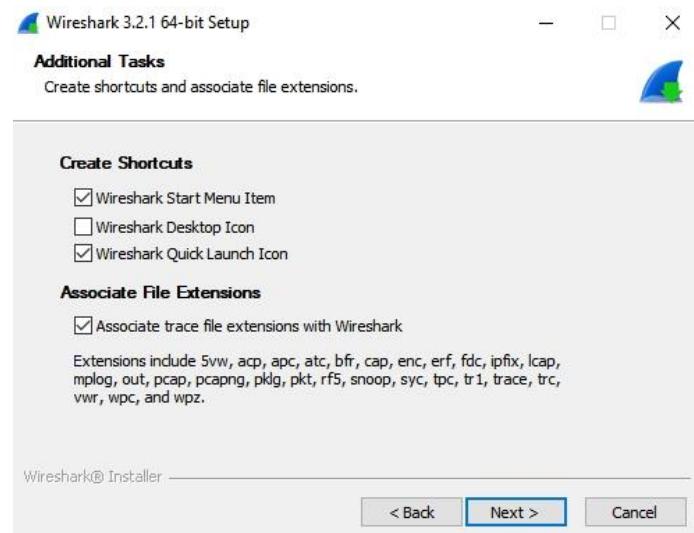
1. เข้าหน้าเว็บ <https://www.wireshark.org/download.html>
 2. เลือก Windows Installer (64-bit) โหลดและติดตั้ง



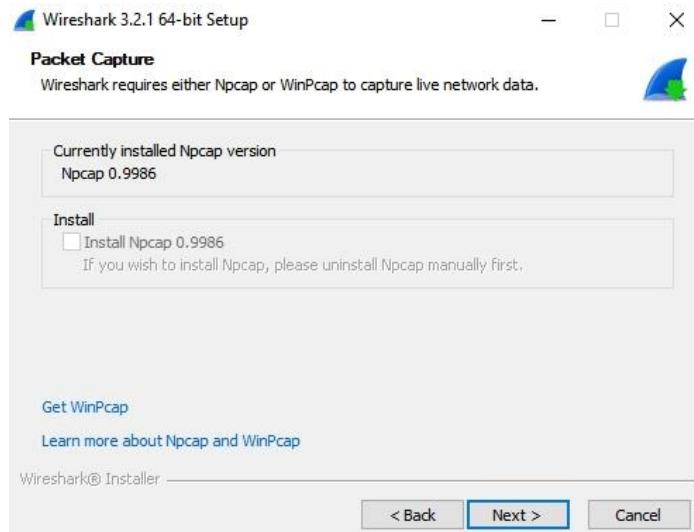
3. กด Next



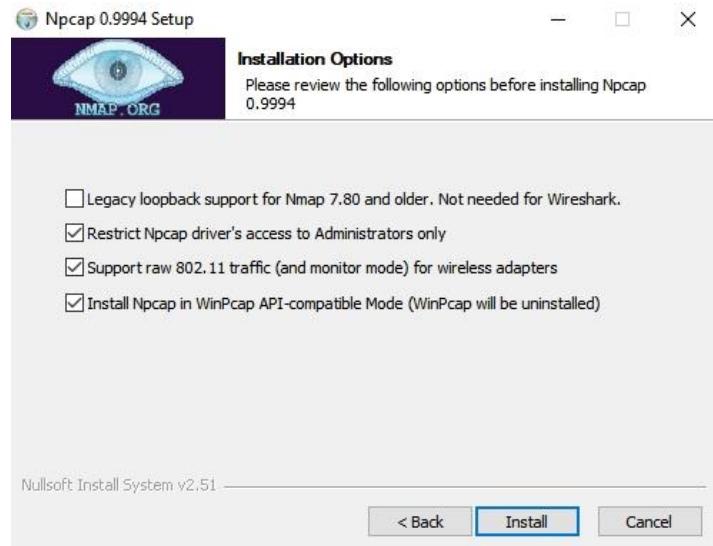
4. เลือกตามต้องการว่าจะเอา Desktop Icon หรือ Quick Launch หรือไม่



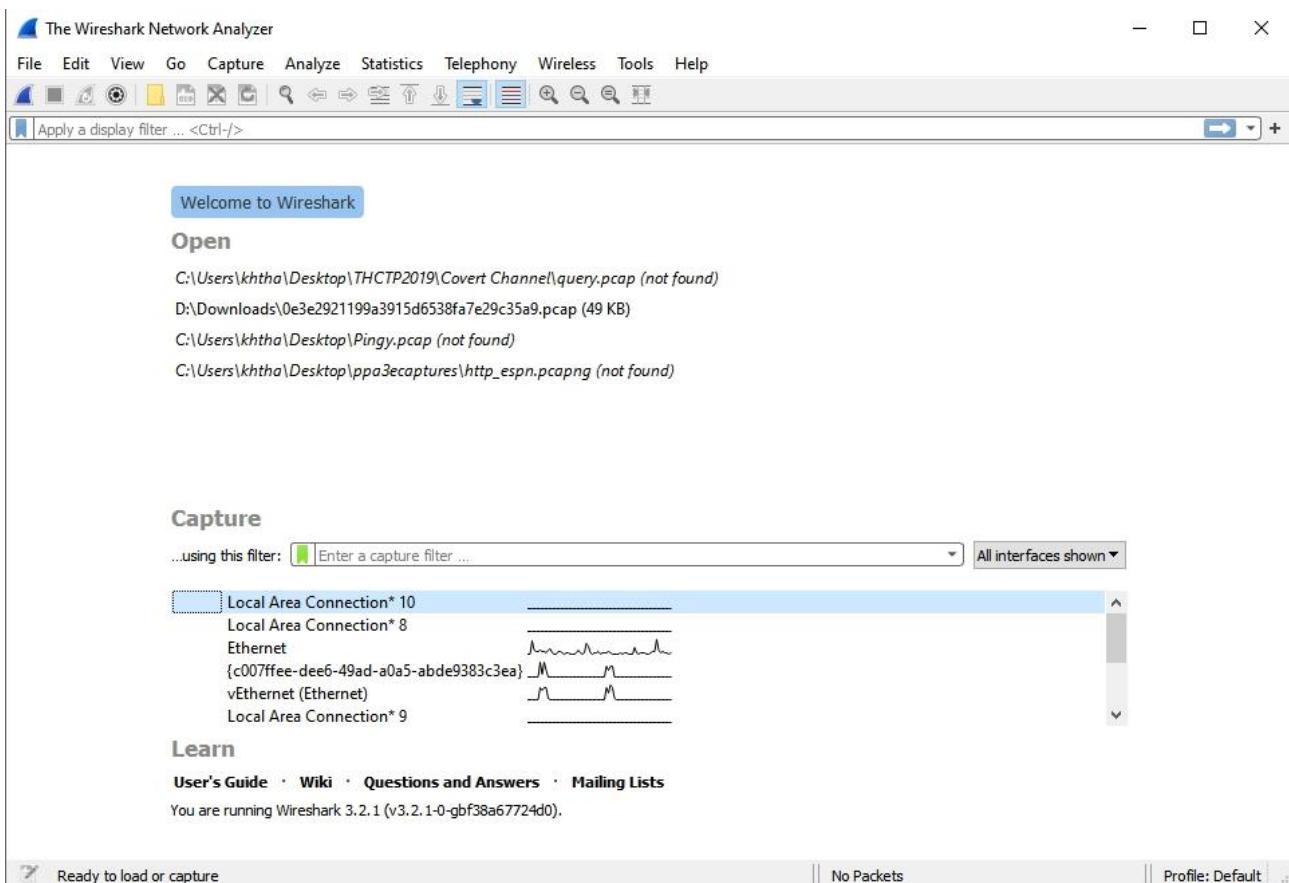
5. Next ไปเรื่อยๆ เลือกติดตั้ง Npcap ถ้ายังไม่ติดตั้ง



6. ในหน้าติดตั้ง Npcap ให้เลือกหมวด ยกเว้นตัวแรก



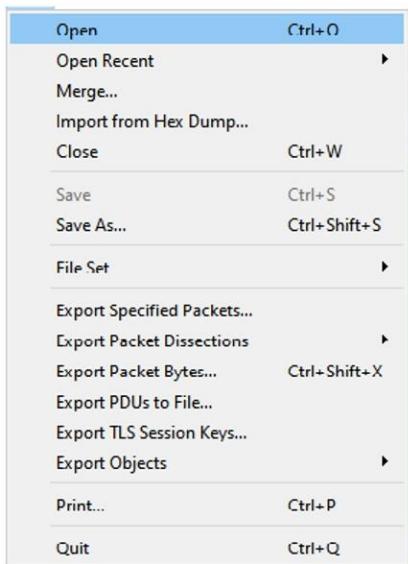
7. จากนั้นกด Next ไปเรื่อยๆ จนเสร็จ เมื่อเปิดโปรแกรมจะได้หน้าจอดังนี้ (การเปิดโปรแกรมให้คลิกขวา More -> Run as Administrator ไม้งั้นโปรแกรมจะถูก Admin Mode หลายครั้ง)



การใช้งานเบื้องต้น

- เม뉴ประกอบด้วย File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help และสำหรับการใช้งานเบื้องต้นในครั้งนี้ จะใช้แค่ File, Edit และ View

• เมนู File

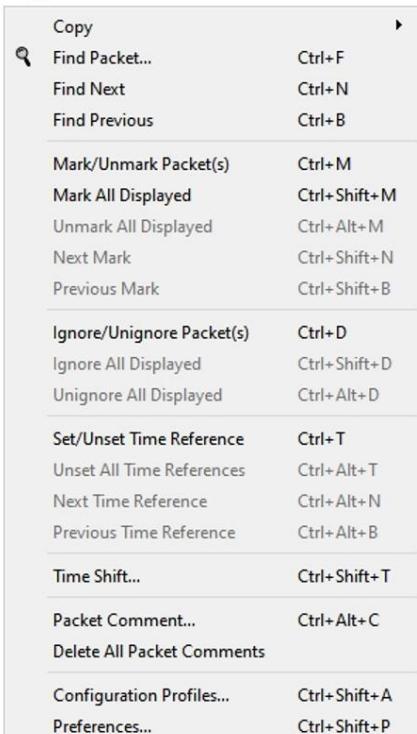


Merge สามารถรวมไฟล์ปัจจุบัน กับ ไฟล์อื่นได้

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

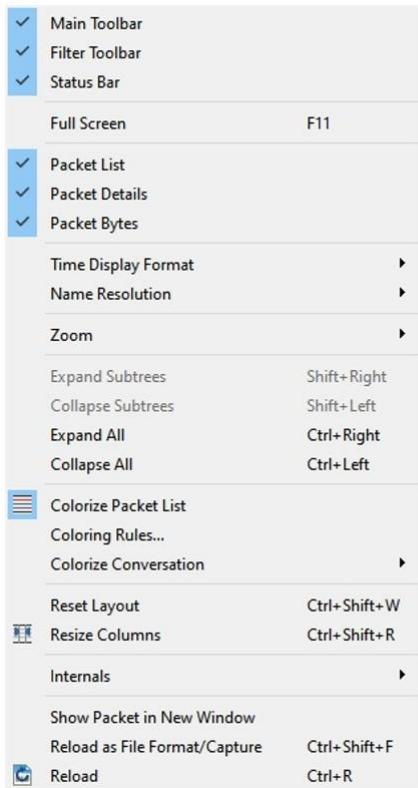
Find Previous ค้นหา Packet ก่อนหน้าตามเงื่อนไข

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 ระบายสี

Coloring Rules... กำหนดสีที่จะระบาย

Colorize Conversation กำหนดสีトイ้ตอับ

2. ส่วนของ Toolbar



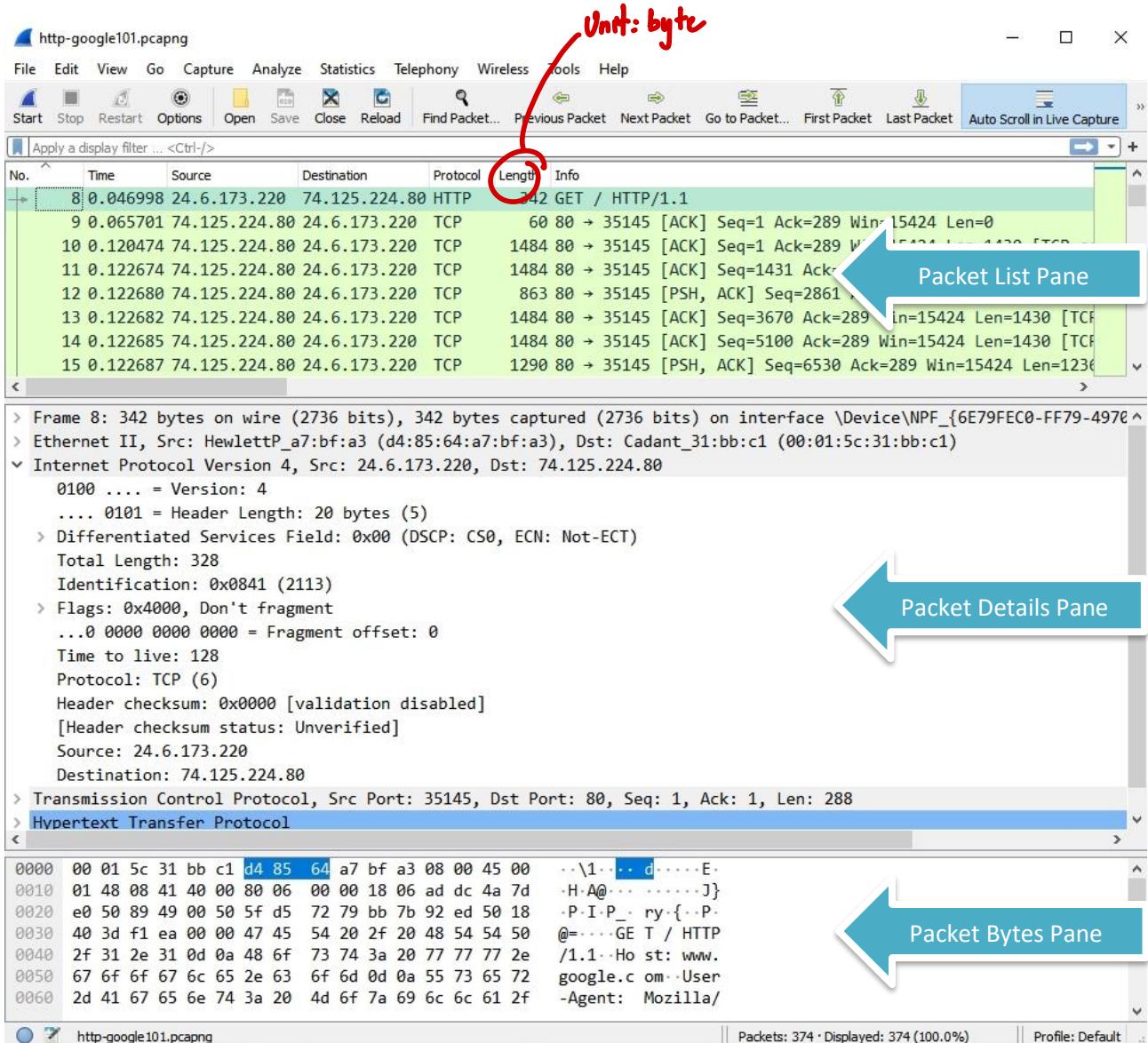
Start Capture	Open Capture File	Find Packet	Coloring	Zoom In
Stop Capture	Save Capture File	Go Back	Auto	Zoom Out
Restart Capture	Close Capture File	Forward	Scroll	Zoom 100%
Capture Option	Reload Capture	Go to Number		Resize Column
	File	Go First		
		Go Last		

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

Packet List Pane เป็นส่วนที่แสดงลำดับของ Packet ที่อยู่ในไฟล์ ตั้งนั้นสามารถจัดการงาน 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 โดยมีคอลัมน์เป็นต้นดังนี้

- 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 แสดงข้อมูลของ Packet แบบย่อๆ ที่สร้างขึ้นโดย Wireshark ซึ่งช่วยให้เห็นภาพรวมของไฟล์ได้อย่างดี

4. ให้ทดลองดังนี้

- กดที่ชื่อคอลัมน์ เกิดอะไรขึ้น แล้ว info var ในรูป packet.
- กดค้างที่ชื่อคอลัมน์แล้วเลือน เกิดอะไรขึ้น แล้ว info var padaหัวใจในรูป varinfo.

- คลิกขวาที่ชื่อคอลัมน์ เราสามารถทำอะไรได้บ้าง
 - Mark / Unmark packet. - Ignore / Unignore packet - Set / Unset time.
 - Time shift - Packet comment - copy.

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

Shortcut	Name	Description
Ctrl+Alt+Shift+A	All Visible Items	All Visible Items
Ctrl+Shift+I	Apply as Column	Create a packet list column from the selected field.
Ctrl+Shift+C	As Filter	Copy this item as a display filter
Ctrl+C	As Plain Text	As Plain Text
Ctrl+Alt+Shift+C	Capture File Properties	Capture file properties
Ctrl+W	Close	Close this capture file
Ctrl+Left	Collapse All	Collapse all packet details
Shift+Left	Collapse Subtrees	Collapse the current packet detail
Ctrl+1	Color 1	Mark the current conversation with its own color.
Ctrl+2	Color 2	Mark the current conversation with its own color.
Ctrl+3	Color 3	Mark the current conversation with its own color.
Ctrl+4	Color 4	Mark the current conversation with its own color.
Ctrl+5	Color 5	Mark the current conversation with its own color.
Ctrl+6	Color 6	Mark the current conversation with its own color.
Ctrl+7	Color 7	Mark the current conversation with its own color.
Ctrl+8	Color 8	Mark the current conversation with its own color.
Ctrl+9	Color 9	Mark the current conversation with its own color.
Ctrl+Shift+A	Configuration Profiles...	Manage your configuration profiles
F1	Contents	Help contents
Ctrl+Alt+1	Date and Time of Day ...	Show packet times as the date and time of day.
Ctrl+Alt+Shift+D	Description	Copy this item's description
Ctrl+Shift+E	Enabled Protocols...	Enable and disable specific protocols
Ctrl+Right	Expand All	Expand packet details
Shift+Right	Expand Subtrees	Expand the current packet detail
Ctrl+Shift+X	Export Packet Bytes...	Export Packet Bytes...
Ctrl+Alt+Shift+F	Field Name	Copy this item's field name
Ctrl+N	Find Next	Find the next packet
Ctrl+F	Find Packet...	Find a packet
Ctrl+R	Find Previous	Find the previous packet

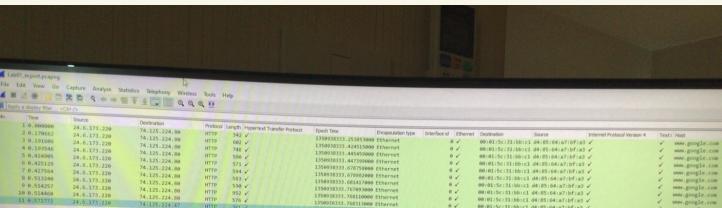
- ให้คนหา Packet ที่มีคำว่า GET และ Mark Packet (Ctrl-M หรือ คลิกขวา -> Mark) ทำไปเรื่อยๆ ให้ครบทั้งไฟล์ ให้ตอบคำถามว่ามีกี่ Packet ที่ Mark ไว้ (ดูได้จาก Status Bar ด้านล่าง) 11 packet.
- ให้ป้อน frame.marked==1 ลงในช่อง filter ด้านบน เกิดอะไรขึ้นให้อธิบายและ Capture ภาพไว้
- ให้ File -> Export Specified Packet.. และเลือก Packet ที่ Mark เอาไว้ Save เป็นไฟล์ และเปิดไฟล์ที่ Save และ Capture ภาพไว้

การเพิ่มคอลัมน์

- ให้ไปที่ Packet ที่ 8 เลื่อนไปที่ HTTP แล้วขยาย ไปที่บรรทัด Host คลิกขวาแล้วเลือก Apply as Column และบอกว่าในไฟล์มีการใช้ HTTP ไปที่ Host ใดบ้าง
 - ssl.gstatic.com
 - www.google.com



```
> Frame #1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on Interface 'Virtual Machine Interface' at 00:0c:29:ff:ff:00, id 0x0000000000000001
  EtherType: IEEE 802.3 (0x0800)
  Internet Protocol Version 4, Src: Hypervisor [192.168.128.1], Dst: Cedant-31:b0:c1 [80:01:5c:31:b0:c1]
  Transmission Control Protocol, Src Port: 36145, Dst Port: 80, Seq: 1, Ack: 1, Len: 208
  Hypertext Transfer Protocol
```



2. ให้หาวิธีการที่สามารถทราบรายชื่อ Host ตามข้อ 1 ให้เร็วที่สุด และให้บอกด้วยว่ามีการไป Request ที่ Host เหล่านั้นกี่ครั้ง
- กดลงมาแล้ว edit column. , Request ที่เก็บบันทึกมา 1 กรณี chHtp.request)
google.com 10 กรณี sql.gstatic.com 1 กรณี.
3. ให้นักศึกษาหาวิธีการเพิ่มคอลัมน์ที่ไม่ใช้วิธีการคลิกขวา
Ctrl + shift + P
-
4. ให้ลับคอลัมน์ที่สร้าง

งานครั้งที่ 1

ให้ส่งข้อความที่ได้เหตุоб (เขียนเรื่องและข้อด้วย) พร้อมภาพที่ได้ Capture

- การส่งงาน ให้ส่งเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา
- ส่วนบนของหน้าแรกให้มี รหัสนักศึกษา และ ชื่อนักศึกษา
- งานที่ส่งทำได้ 2 รูปแบบ คือ 1) เขียนเพิ่มเติมลงใน Sheet นี้ หรือ 2) ทำเป็นคำตอบแยกออกมา โดยให้มีหัวข้อเรื่อง และ ข้อด้วย เพื่อให้ทราบว่าเป็นคำตอบของส่วนไหน
- กำหนดส่ง ภายในวันที่ 17 มกราคม 2563