

กิจกรรมที่ 1 : การติดตั้ง Wireshark และการใช้งานเบื้องต้น

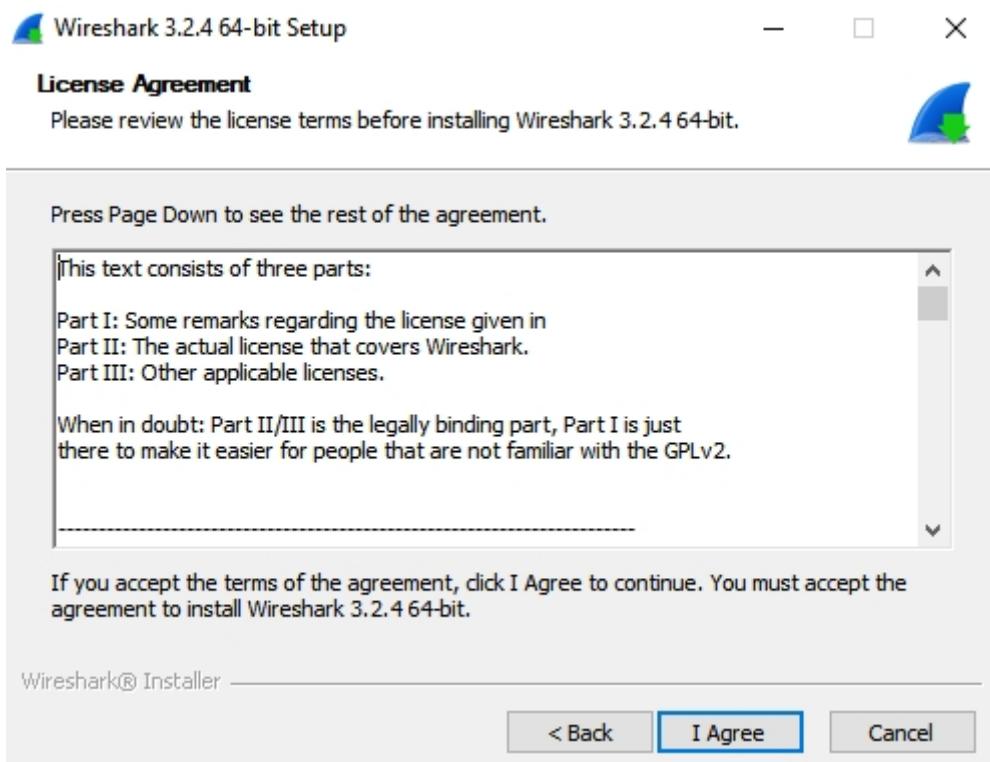
Wireshark เป็นโปรแกรมสำหรับวิเคราะห์ packet ในระบบเครือข่าย สามารถติดตั้งได้หลาย platform ทั้ง Linux, Unix หรือ Windows โดยอาศัย pcap ในการจับ packet บน interface ของเครื่อง และมี TShark เป็น command line ด้วย

คุณสมบัติของ Wireshark

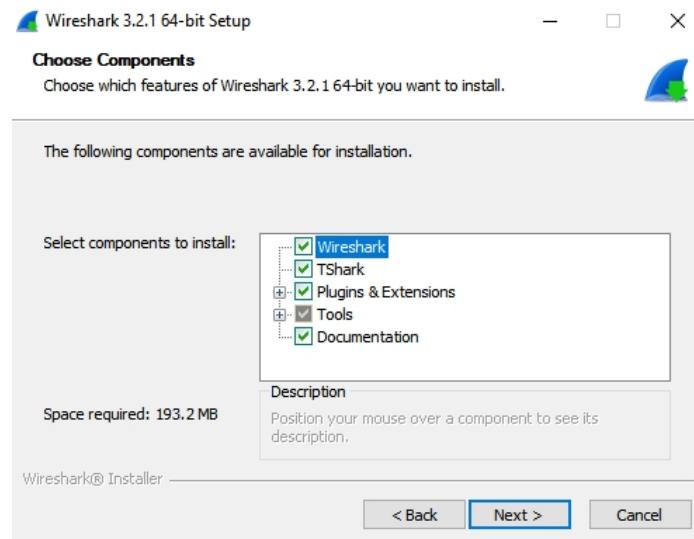
1. สามารถจับข้อมูลในระบบเครือข่าย network ได้ รวมถึงอ่านข้อมูล packet จากไฟล์มาวิเคราะห์ได้
2. สามารถตัดจับข้อมูลได้หลายแบบทั้ง Ethernet, IEEE 802.11, PPP และ loopback
3. ใช้งานได้ทั้งบน GUI และ command line (TShark)
4. สามารถ filter ข้อมูลได้
5. มีเครื่องมือวิเคราะห์เครือข่ายให้ใช้งานค่อนข้างมาก
6.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

การติดตั้ง

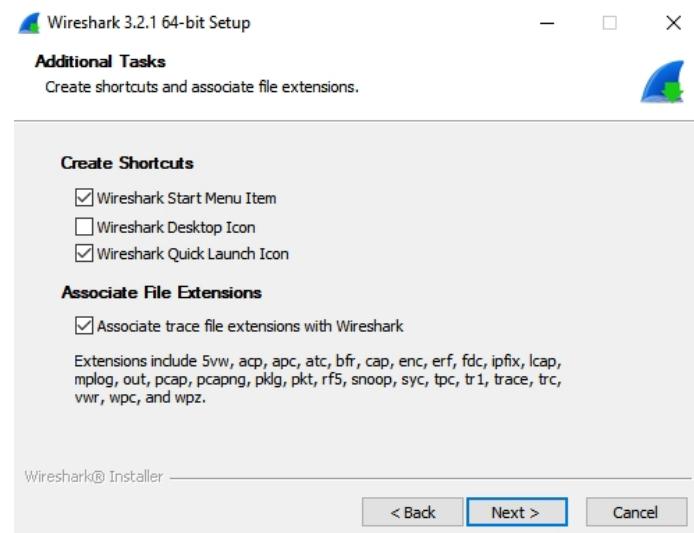
1. เข้าหน้าเว็บ <https://www.wireshark.org/download.html>
2. เลือก Windows Installer (64-bit) โหลดและติดตั้ง



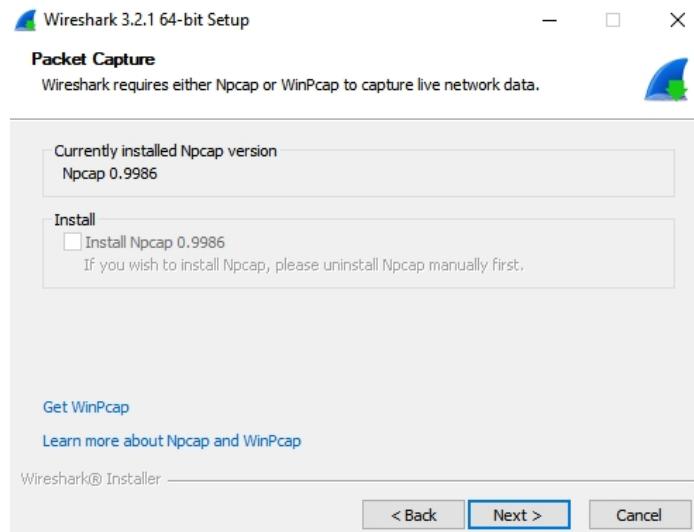
3. กด Next



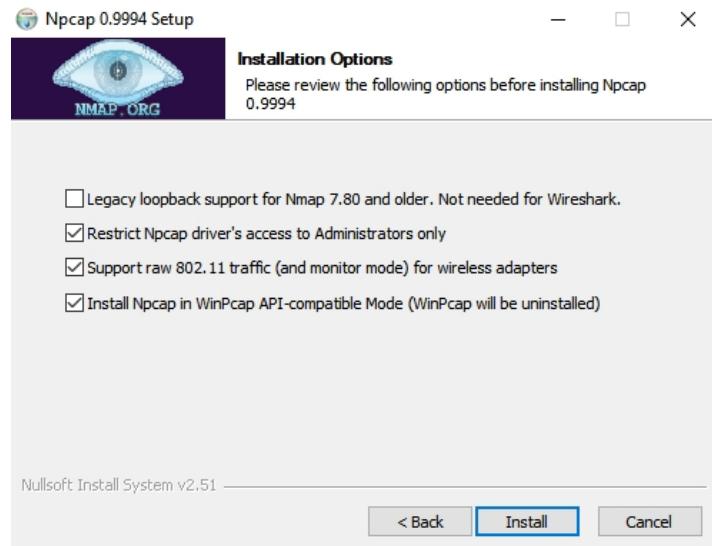
4. เลือกตามต้องการว่าจะเอา Desktop Icon หรือ Quick Launch หรือไม่



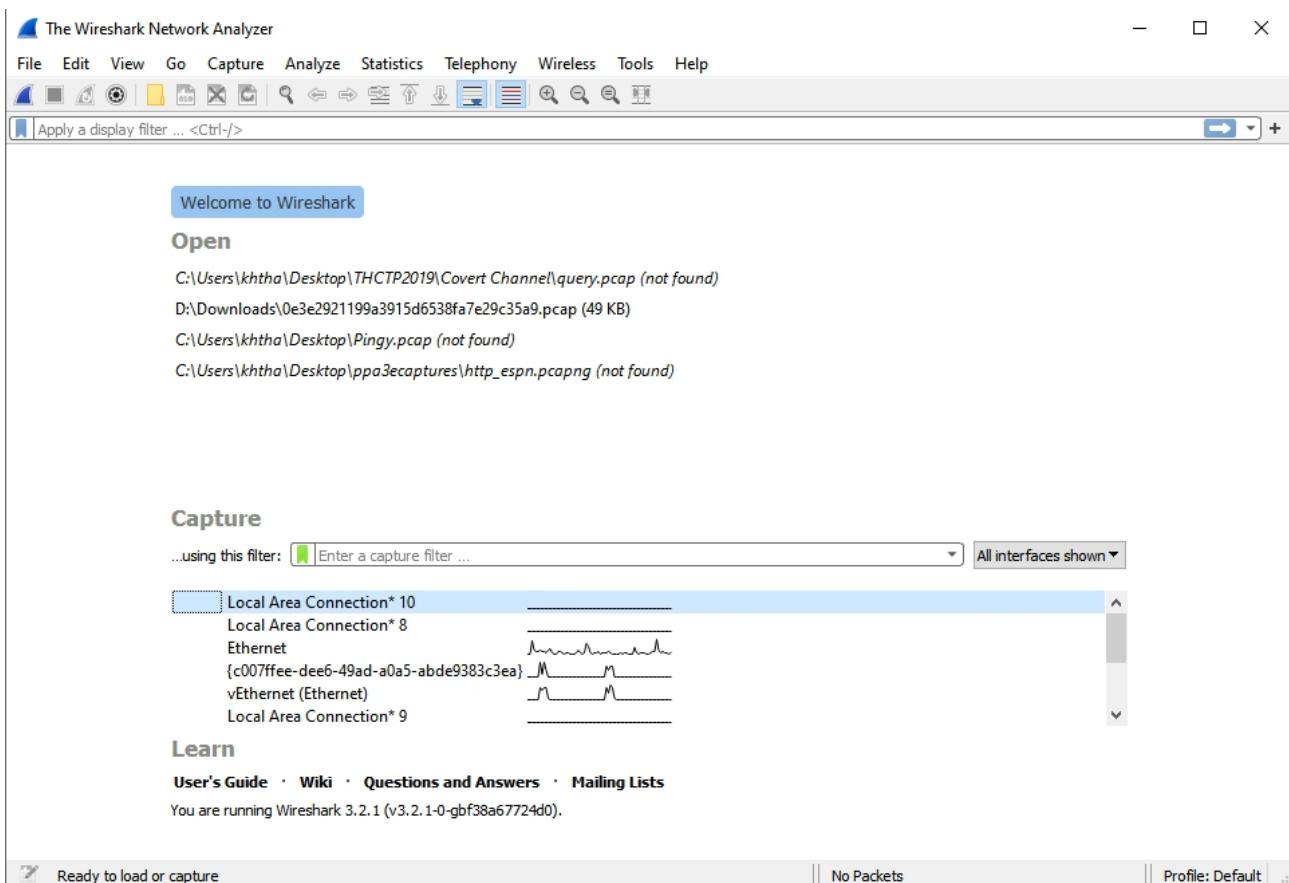
5. Next ไปเรื่อยๆ เลือกติดตั้ง Npcap ถ้ายังไม่ติดตั้ง



6. ในหน้าติดตั้ง Npcap ให้เลือกหยอด ยกเว้นตัวแรก



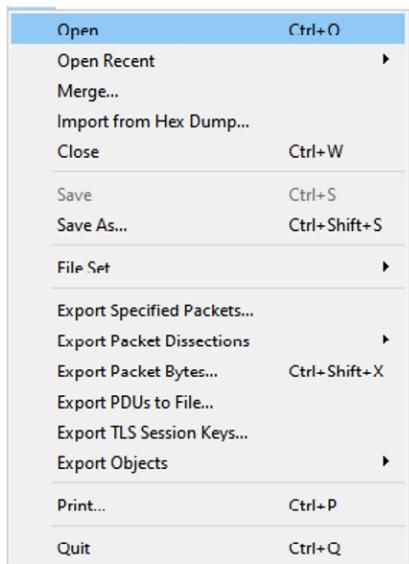
7. จากนั้นกด Next ไปเรื่อยๆ จนเสร็จ เมื่อเปิดโปรแกรมจะได้หน้าจอดังนี้ (การเปิดโปรแกรมให้คลิกขวา More -> Run as Administrator ไม้งั้นโปรแกรมจะถูก Admin Mode หลายครั้ง)



การใช้งานเบื้องต้น

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

• เมนู File

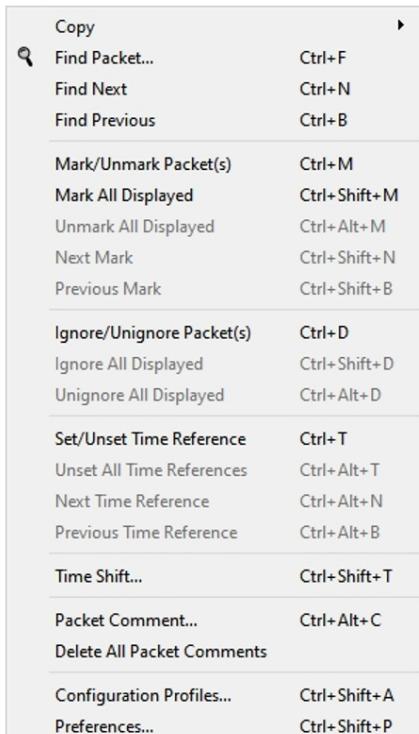


Merge สามารถรวมไฟล์ปัจจุบัน กับ ไฟล์อื่นได้

File Set เรียกคู่ไฟล์แบบเป็นชุด

Export ใช้ในการ Save บาง Packet หรือบางส่วน
ไปเป็นไฟล์

• เมนู Edit



Copy ใช้ copy packet ออกเป็นรูปแบบต่างๆ

Find Packet ค้นหา Packet ตามเงื่อนไข

Find Next ค้นหา Packet ถัดไปตามเงื่อนไข

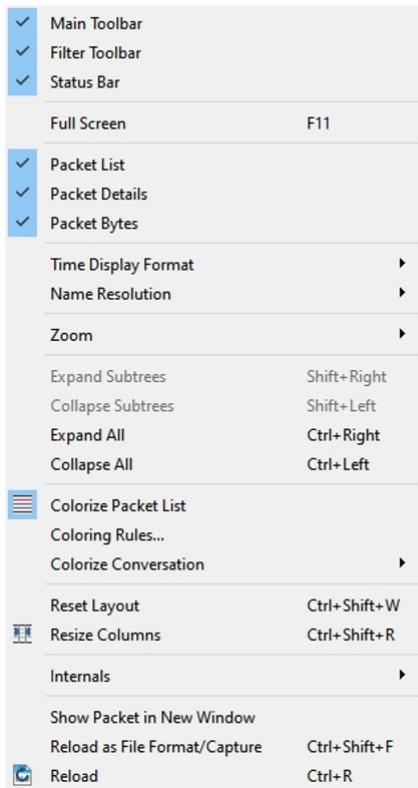
Find Previous ค้นหา Packet ก่อนหน้าตามเงื่อนไข

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



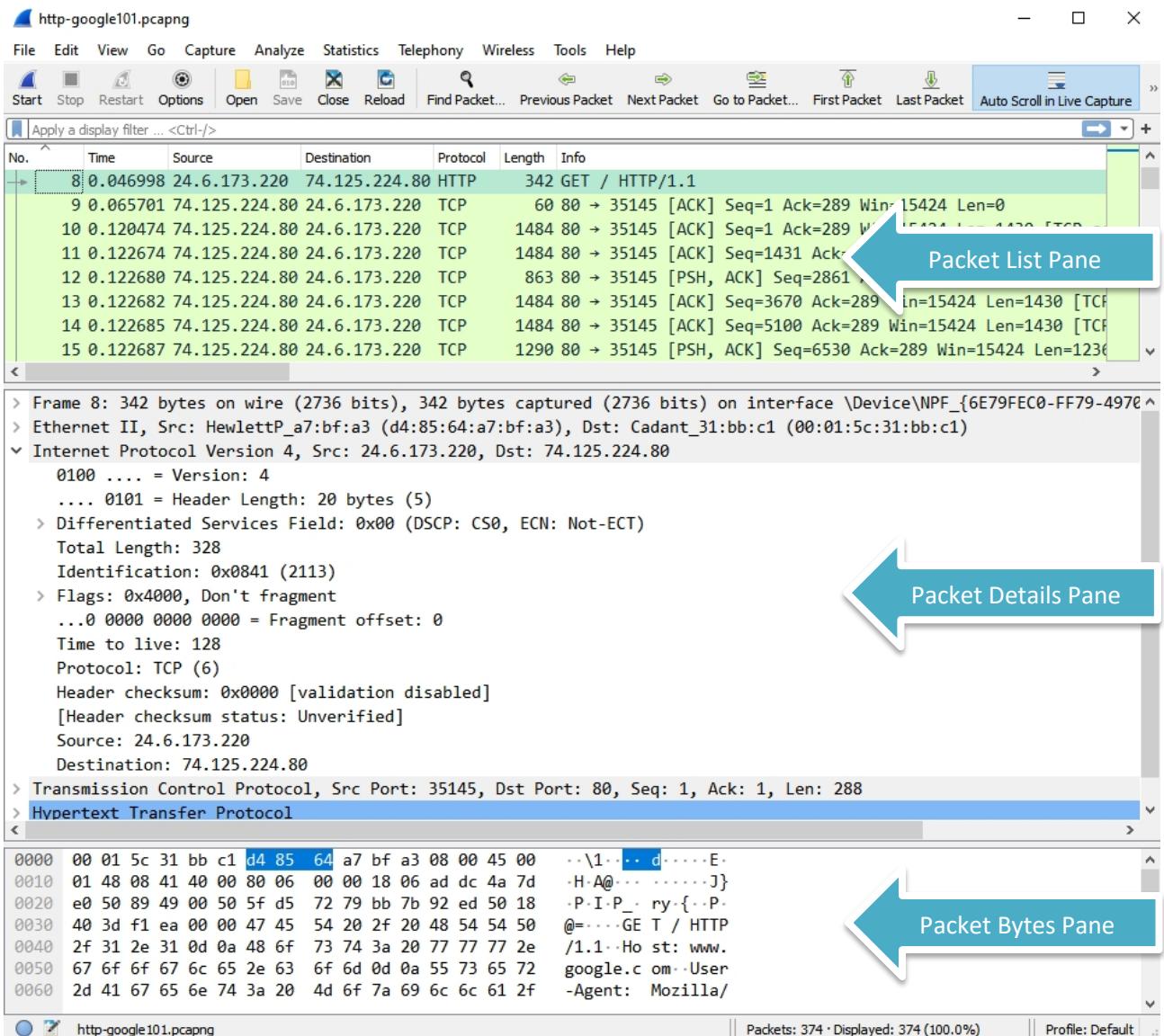
Start Capture	Open Capture File	Find Packet	Coloring	Zoom In
Stop Capture	Save Capture File	Go Back	Auto	Zoom Out
Restart Capture	Close Capture File	Forward	Scroll	Zoom 100%
Capture Option	Reload Capture	Go to Number		Resize Column
	File	Go First		
		Go Last		

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

Packet List Pane เป็นส่วนที่แสดงลำดับของ Packet ที่อยู่ในไฟล์ ตั้งนั้นสามารถดูจำนวน Packet และภาพรวมของข้อมูลที่อยู่ในไฟล์ได้ ถือเป็นส่วนที่มีความสำคัญที่จะใช้ในการวิเคราะห์

Packet Details Pane เป็นส่วนที่แสดงรายละเอียดของข้อมูลในเฟรม โดยจะมีข้อมูลบางส่วนที่ Wireshark ได้เพิ่มเข้าไป เพื่อความสะดวกต่อการใช้งานด้วย จะใช้ข้อมูลส่วนนี้ในการดูรายละเอียดของข้อมูลที่อยู่ภายใน Packet

Packet Bytes Pane เป็นส่วนที่เป็นข้อมูลจริง (Raw Data) ซึ่งหากข้อมูลที่ส่งเป็น Text และไม่มีการเข้ารหัส จะเห็นข้อมูลที่สามารถอ่านได้



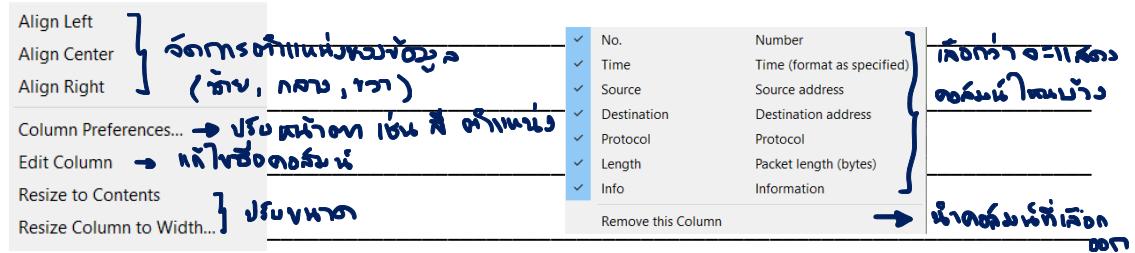
ໃນສ່ວນ Packet List Pane ຈະມີຂໍ້ມູນທີ່ແບ່ງອອກເປັນຄອລົມນ໌ ໂດຍມີຄອລົມນ໌ເປື່ອຕັ້ງນີ້

- No. ເປັນ Packet ທີ່ເກົ່າໄວໃນໄຟຣ໌
- Time ປັກຕິຈະແສດງເວລາທີ່ນັບຈາກ Packet ແຮກ ແຕ່ສາມາຮັກກຳຫຼຸດໃຫ້ແສດງເປັນແບບອື່ນໄດ້ຈາກ View
-> Time Display Format
- Source ແລະ Destination ແສດ ໄກສອນ IP Address ຕັ້ນທາງແລະປ່າຍທາງຂອງ Packet
- Protocol ແສດງວ່າໃນ Packet ສີ່ເປັນ Protocol ອະໄຮ
- Length ແສດງຄວາມຍາວຂອງ Packet
- Info ແສດງຂໍ້ມູນຂອງ Packet ແບບຍ່ອງທີ່ສ້າງຂຶ້ນໂດຍ Wireshark ຜຶ້ງຂ່າຍໃໝ່ເຫັນກາພຽມຂອງໄຟຣ໌ໄດ້
ອໝາງດີ

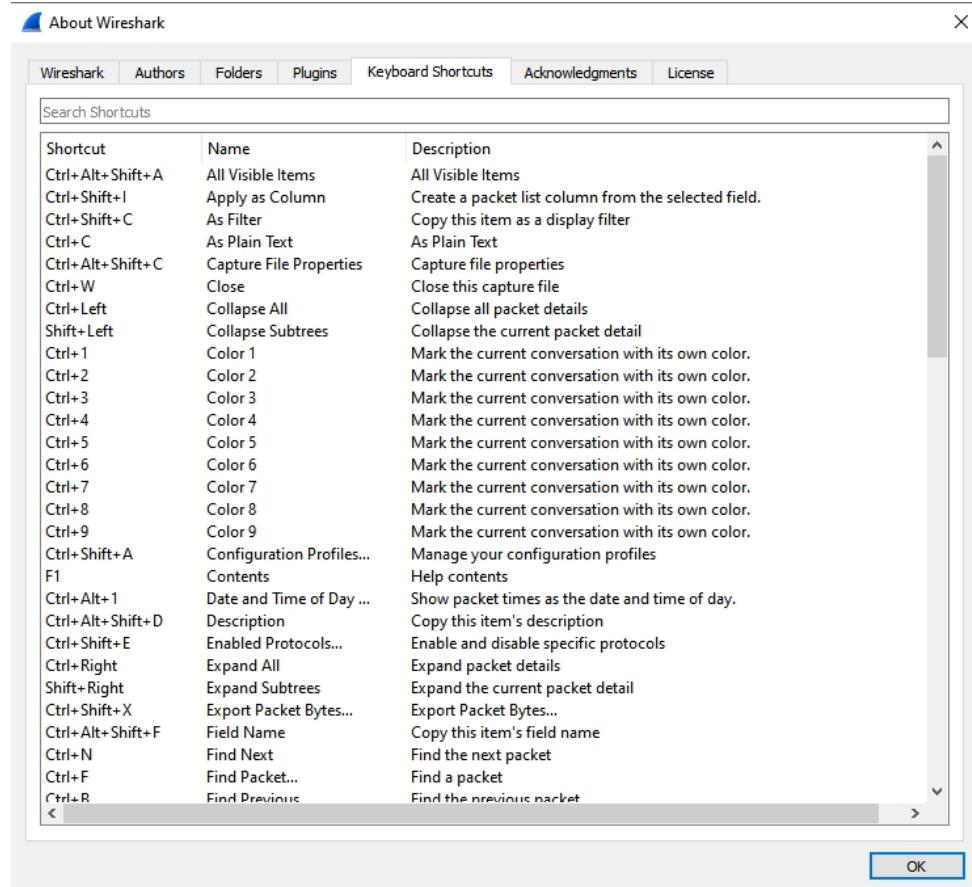
4. ໃຫ້ທົດລອງຕັ້ງນີ້

- ກົດທີ່ຊື່ຄອລົມນ໌ ເກີດອະໄຮເຊື້ນ ດ້າກທີ່ຄອລົມນ໌ໃໝ່ ຂ່າວະລະເບີນຕາມນັ້ນ-ນັກ ໜັ້ນ ມາກ-ນັ້ນ
- ກົດຄວາງທີ່ຊື່ຄອລົມນ໌ແລ້ວເລື່ອນ ເກີດອະໄຮເຊື້ນ ສາມາດຟັງທີ່ແນ່ງຕາມຄອລົມນ໌ໄປໄກໄລ

- คลิกขวาที่ชื่อคอลัมน์ เรากำarra ทำอะไรได้บ้าง



การใช้ Shortcut ใน Wireshark สามารถใช้ได้โดยดูมาจาก About -> Keyboard Shortcuts ตามรูป



- ให้คุณ Packet ที่มีคำว่า GET และ Mark Packet (Ctrl-M หรือ คลิกขวา -> Mark) ทำไปเรื่อยๆ ให้ครบทั้งไฟล์ ให้ตอบคำถามว่ามีกี่ Packet ที่ Mark ไว้ (ดูจาก Status Bar ด้านล่าง) _____ **11** ให้ป้อน frame.marked==1 ลงในช่อง filter ด้านบน เกิดอะไรขึ้นให้อธิบาย

Packet ที่แสดงมาจะเป็นต่อๆ กันๆ ที่ Mark ไว้

- ให้ File -> Export Specified Packet.. และเลือก Packet ที่ Mark เอาไว้ Save เป็นไฟล์ และเปิดไฟล์ที่ Save ให้บอกว่าสิ่งที่ Save คืออะไร

Save Packet ที่มีตัว Mark ไว้

การเพิ่มคอลัมน์

7. ให้ไปที่ Packet ที่ 8 เลื่อนไปที่ HTTP และขยาย ไปที่บรรทัด Host คลิกขวาแล้วเลือก Apply as Column และบอกรวบในไฟล์มีการใช้ HTTP ไปที่ Host ได้บ้าง

www.google.com และ ssl.gstatic.com

8. ให้หัวเรื่องการที่สามารถทราบรายชื่อ Host ตามข้อ 7 ให้เร็วที่สุด และให้บอกด้วยว่ามีการไป Request ที่ Host เหล่านั้นกี่ครั้ง

ล่องหนที่ Host บน packet ในวงกลมแล้วกด Ctrl + Shift + I host ของทุก packet ละปางๆ , Request ไปที่ host www.google.com 10 ครั้ง , ssl.gstatic.com 1 ครั้ง

9. ให้นักศึกษาหาวิธีการเพิ่มคอลัมน์ที่ไม่ใช้วิธีการคลิกขวา

วิธีที่ 1 ล่องหนที่ 8 = เพิ่มคอลัมน์แล้วกด Ctrl + Shift + I

วิธีที่ 2 edit → preferences → Appearance → Columns → สร้างชื่อ ประมาณ ตามต้องการ

10. ให้ลบคอลัมน์ที่สร้าง

งานครั้งที่ 1

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งโดยเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา
- กำหนดส่ง ภายในวันที่ 19 มกราคม 2564 โดยให้ส่งใน Microsoft Teams