62010694
นายภากร ชนประชานนท์

กิจกรรมที่ 1 : การติดตั้ง Wireshark และการใช้งานเบื้องต้น

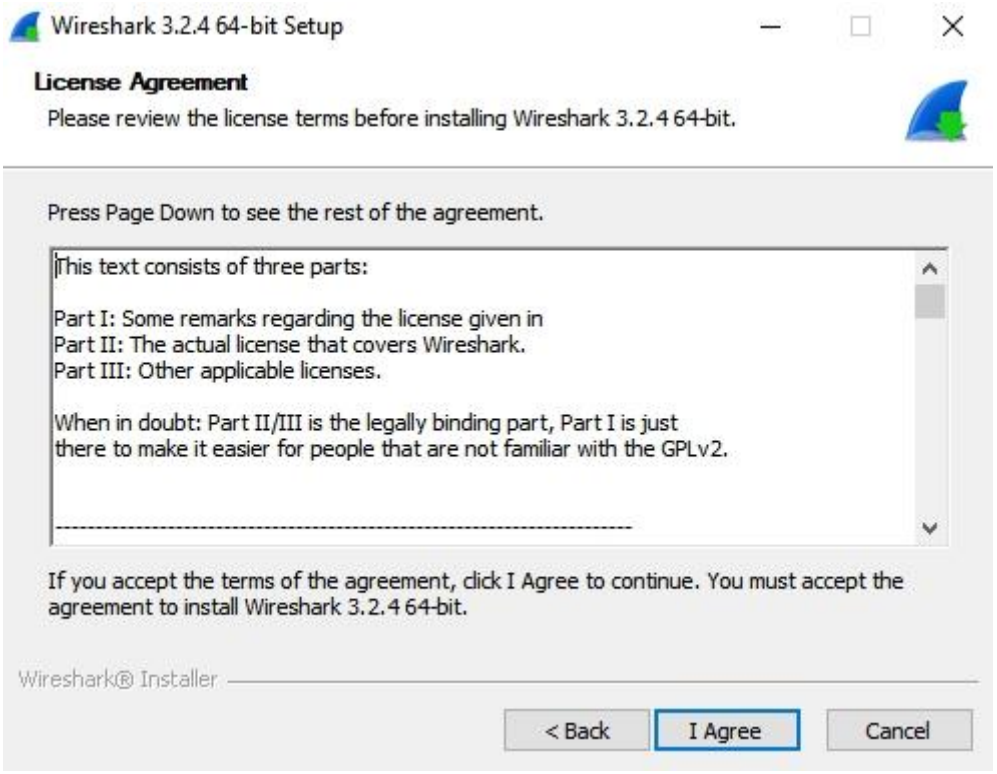
Wireshark เป็นโปรแกรมสำหรับวิเคราะห์ packet ในระบบเครือข่าย สามารถติดตั้งได้หลาย platform ทั้ง Linux, Unix หรือ Window โดยอาศัย pcap ในการจับ packet บน interface ของเครื่อง และมี TShark เป็น commnad line ด้วย

คุณสมบัติของ Wireshark

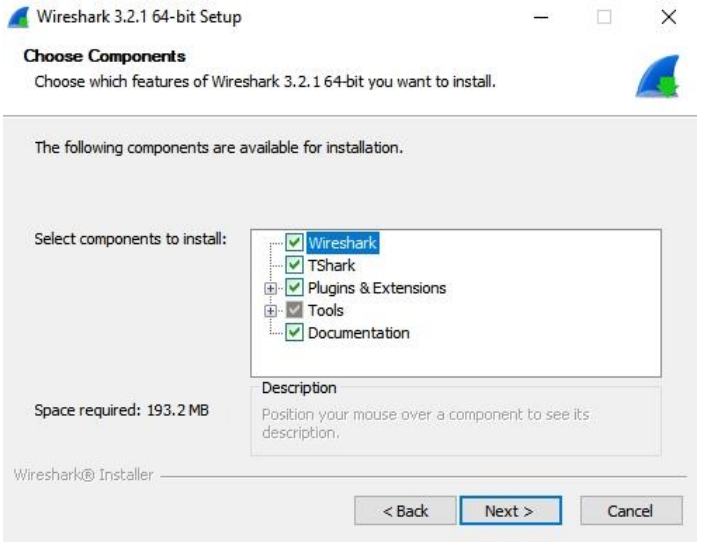
1. สามารถจับข้อมูลในระบบเครือข่าย network ได้ รวมถึงอ่านข้อมูล packet จากไฟล์มาวิเคราะห์ได้
2. สามารถดักจับข้อมูลได้หลายแบบทั้ง Ethernet, IEEE 802.11, PPP และ loopback
3. ใช้งานได้ทั้งบน GUI และ command line (TShark)
4. สามารถ filter ข้อมูลได้
5. มีเครื่องมือวิเคราะห์เครือข่ายให้ใช้งานค่อนข้างมาก
6.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

การติดตั้ง

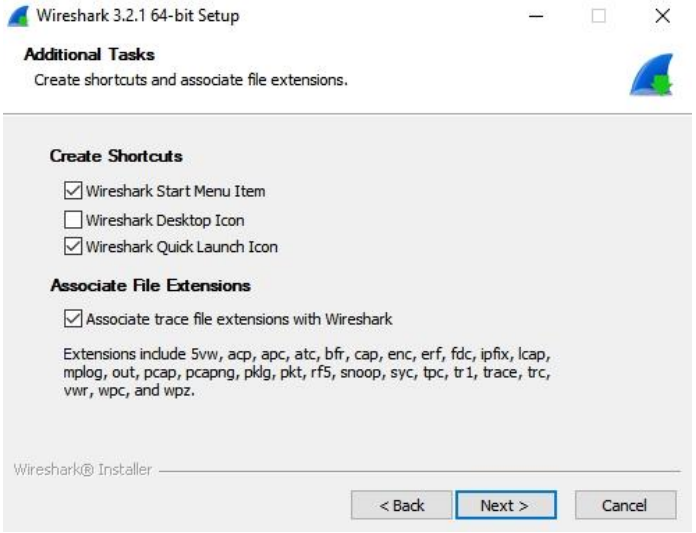
1. เข้าหน้าเว็บ https://www.wireshark.org/download.html
2. เลือก Windows Installer (64-bit) โหลดและติดตั้ง



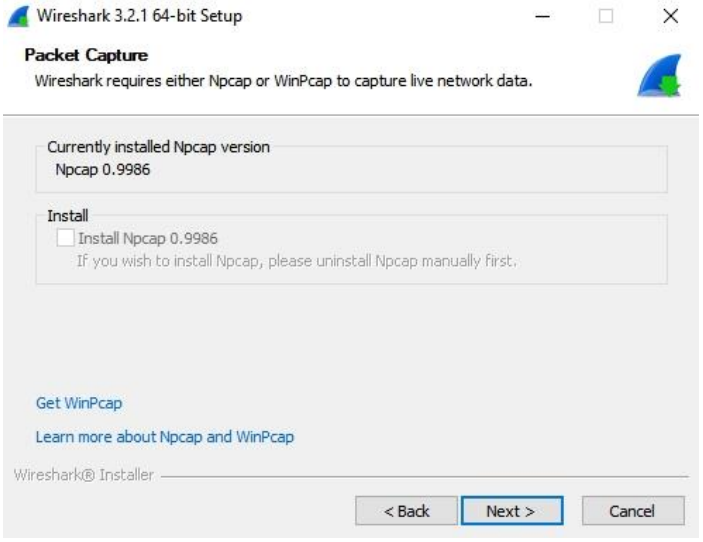
3. กด Next



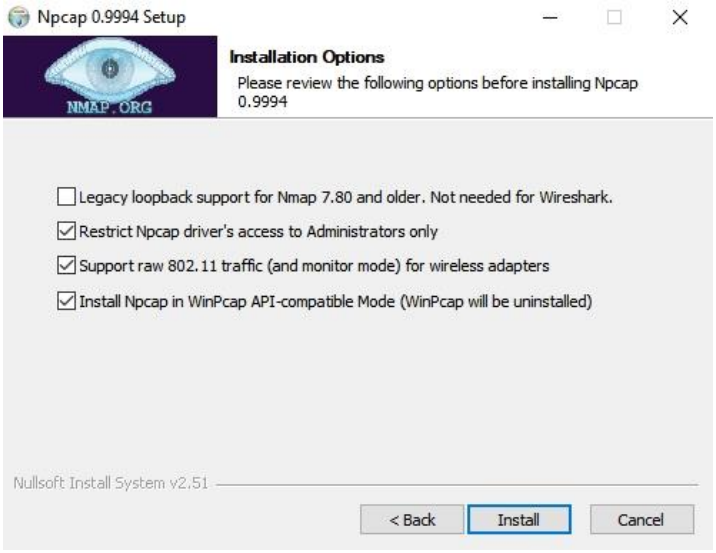
4. เลือกตามต้องการว่าจะเอา Desktop Icon หรือ Quick Launch หรือไม่



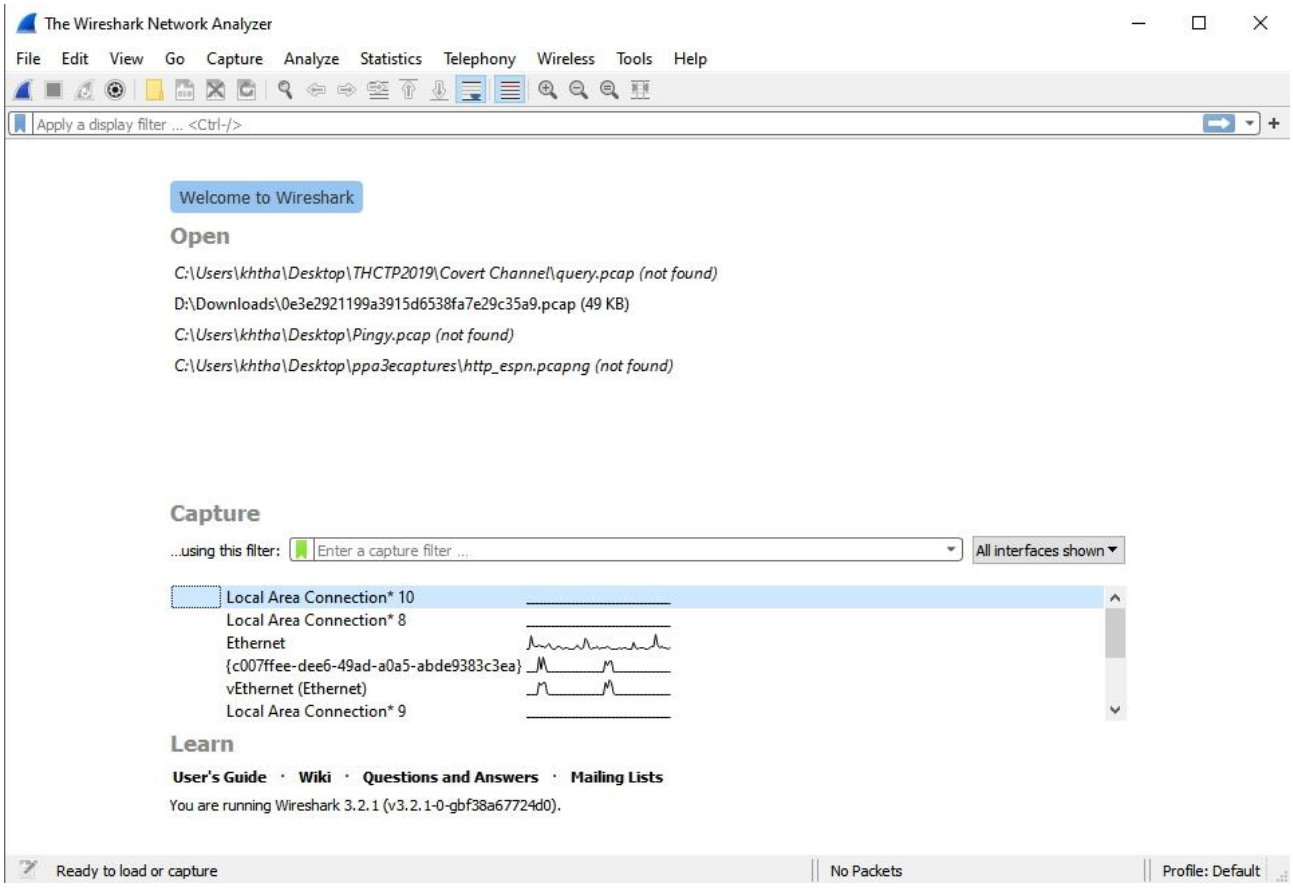
5. Next ไปเรื่อยๆ เลือกติดตั้ง Npcap ถ้ายังไม่ติดตั้ง



6. ในหน้าติดตั้ง Npcap ให้เลือกหมด ยกเว้นตัวแรก



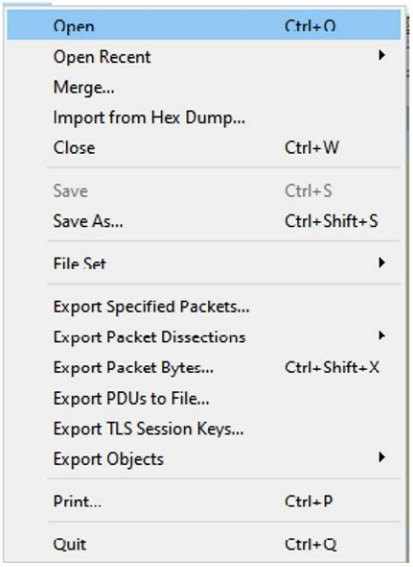
7. จากนั้นกด Next ไปเรื่อยๆ จนเสร็จ เมื่อเปิดโปรแกรมจะได้หน้าจอดังนี้ (การเปิดโปรแกรมให้คลิกขวา More –> Run as Administrator ไม่งั้นโปรแกรมจะถาม Admin Mode หลายครั้ง)



การใช้งานเบื้องต้น

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

- **เมนู File**

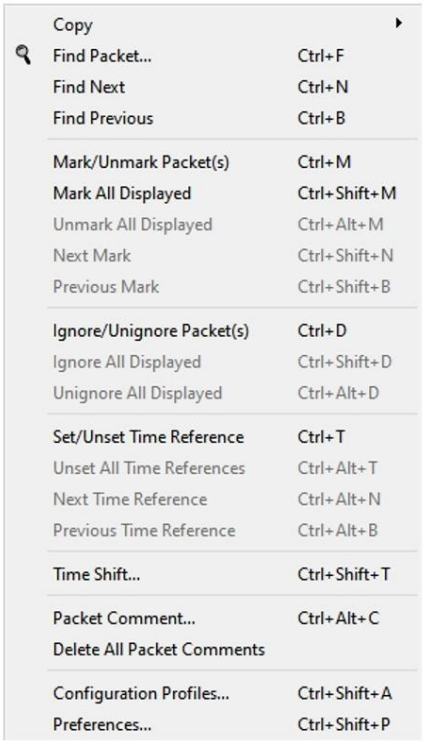


Merge สามารถรวมไฟล์ปัจจุบัน กับ ไฟล์อื่นได้

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

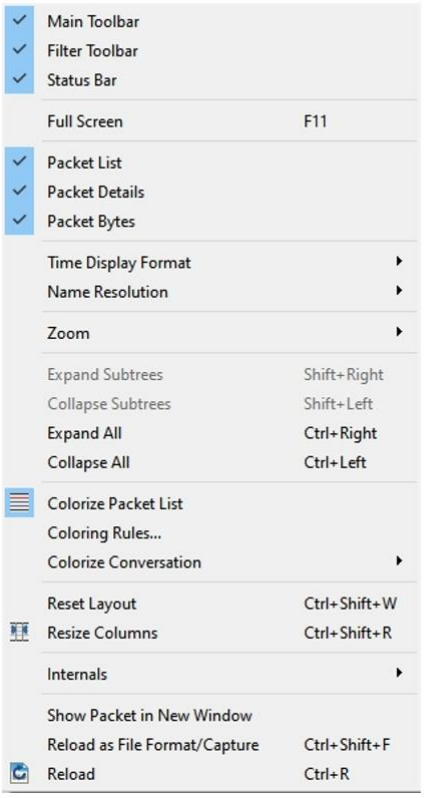
Find Previous ค้นหา Packet ก่อนหน้าตามเงื่อนไข

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

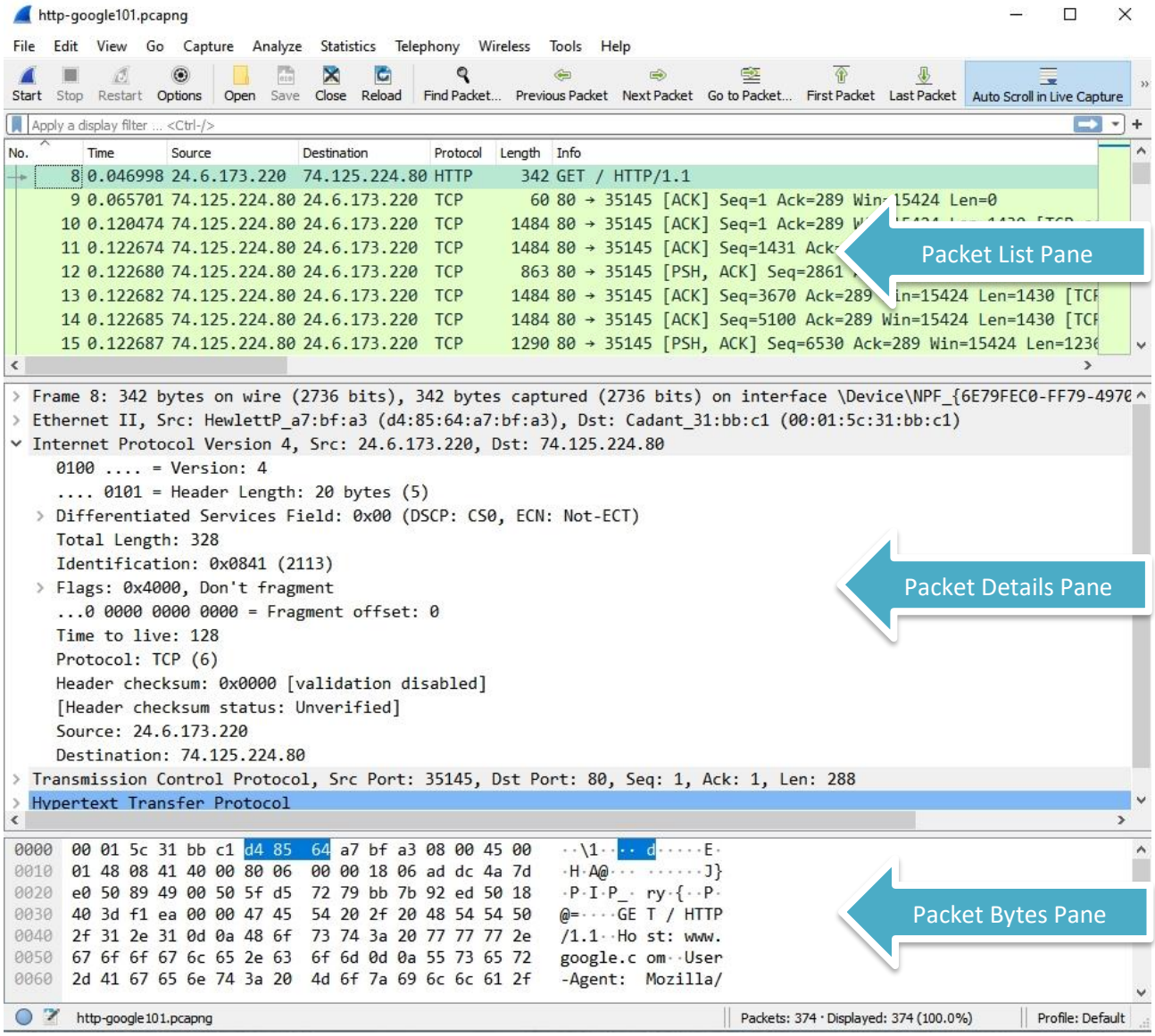
Start Capture	Open Capture File	Find Packet	Coloring	Zoom In
Stop Capture	Save Capture File	Go Back	Auto	Zoom Out
Restart Capture	Close Capture File	Forward	Scroll	Zoom 100%
Capture Option	Reload Capture File	Go to Number		Resize Column
		Go First		
		Go Last		

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 แสดงข้อมูลของ Packet แบบย่อๆ ที่สร้างขึ้นโดย Wireshark ซึ่งช่วยให้เห็นภาพรวมของไฟล์ได้อย่างดี

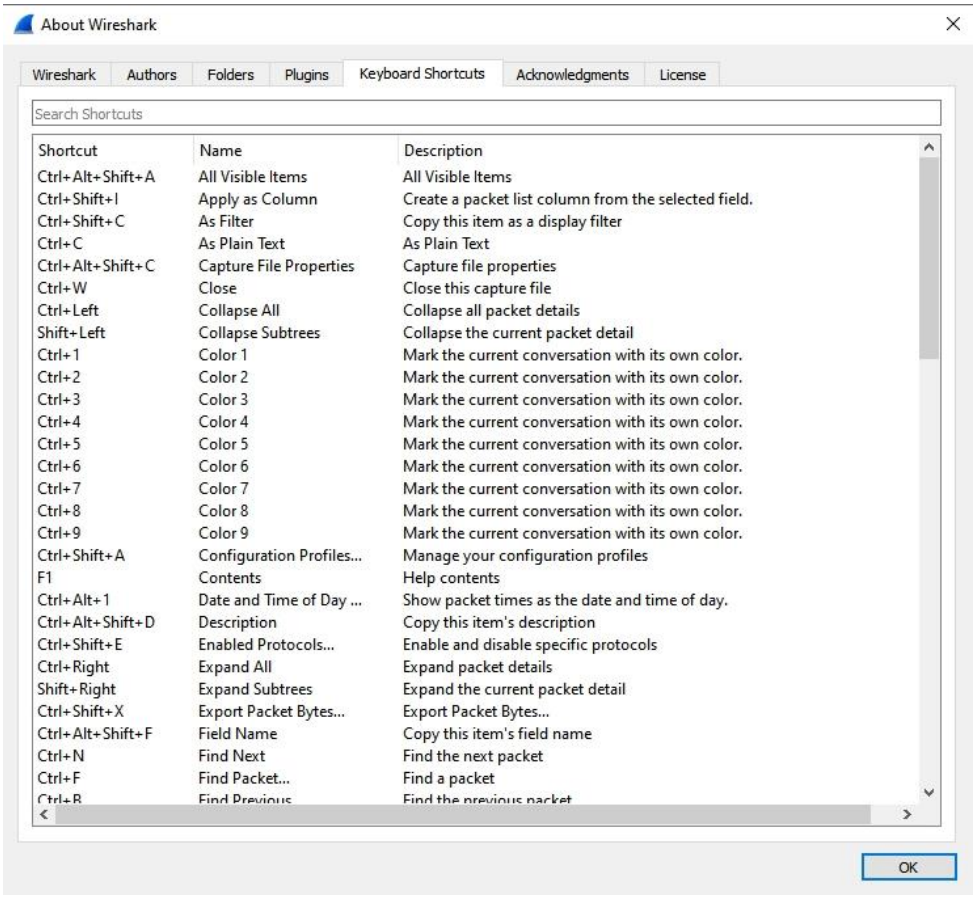
4. ให้ทดลองดังนี้

- กดที่ชื่อคอลัมน์ เกิดอะไรขึ้น ระบบ Sort ข้อมูลจากมากไปน้อย, น้อยไปมาก โดยอ้างอิงจากคอลัมน์ที่เรากด
- กดค้างที่ชื่อคอลัมน์แล้วเลื่อน เกิดอะไรขึ้น ระบบแสดงขนาดความกว้าง (Width) ของคอลัมน์ที่เรากด และสามารถย้ายคอลัมน์ไปไว้ที่แหน่งอื่นได้.

- คลิกขวาที่ชื่อคอลัมน์ เราสามารถทำอะไรได้บ้าง

ปรับแต่งคุณสมบัติของคอลัมน์ได้แก่ Align Left, Align Center, Align Right, Column Preferences, Edit Column, Resize to Contents, Resize Column to width, Resolve Names และเลือกแสดงผลคอลัมน์ได้แก่ No., Time, Source, Protocol, Length Info และสุดท้าย Remove This Column

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



6. ให้ค้นหา Packet ที่มีคำว่า GET และ Mark Packet (Ctrl-M หรือ คลิกขวา -> Mark) ทำไปเรื่อยๆ ให้ครบทั้งไฟล์ ให้ตอบคำถามว่ามีกี่ Packet ที่ Mark ไว้ (ดูได้จาก Status Bar ด้านล่าง) 11 (2.9%)
7. ให้ป้อน frame.marked==1 ลงในช่อง filter ด้านบน เกิดอะไรขึ้นให้อธิบายและ Capture ภาพไว้
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

Ctrl + Alt + Shift + H ,

www.google.com 10 ครั้ง , ssl.gstatic.com 1 ครั้ง

3. ให้นักศึกษาหาวิธีการเพิ่มคอลัมน์ที่ไม่ใช้วิธีการคลิกขวา

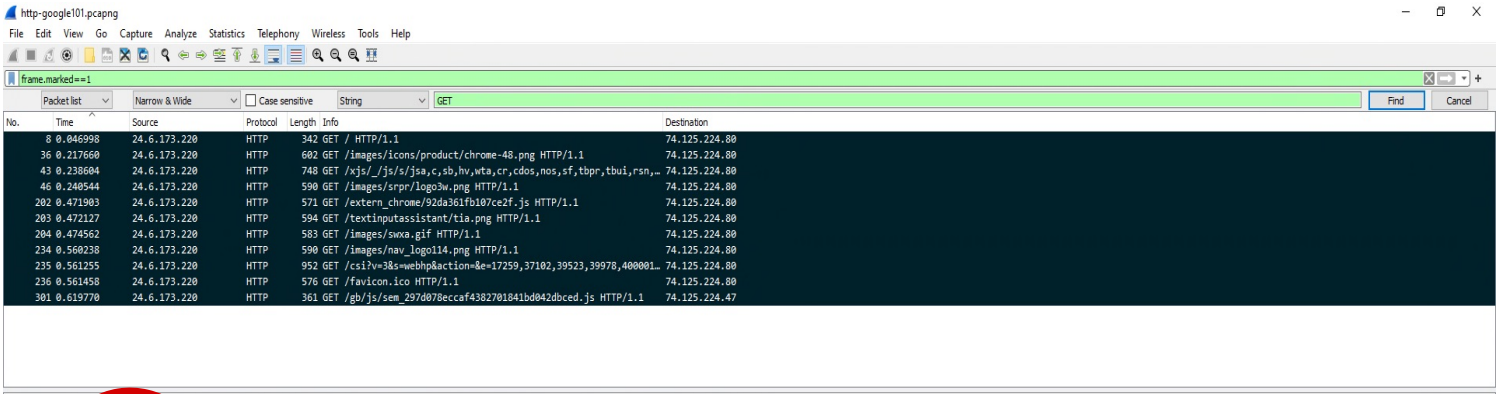
Ctrl + Shift + I

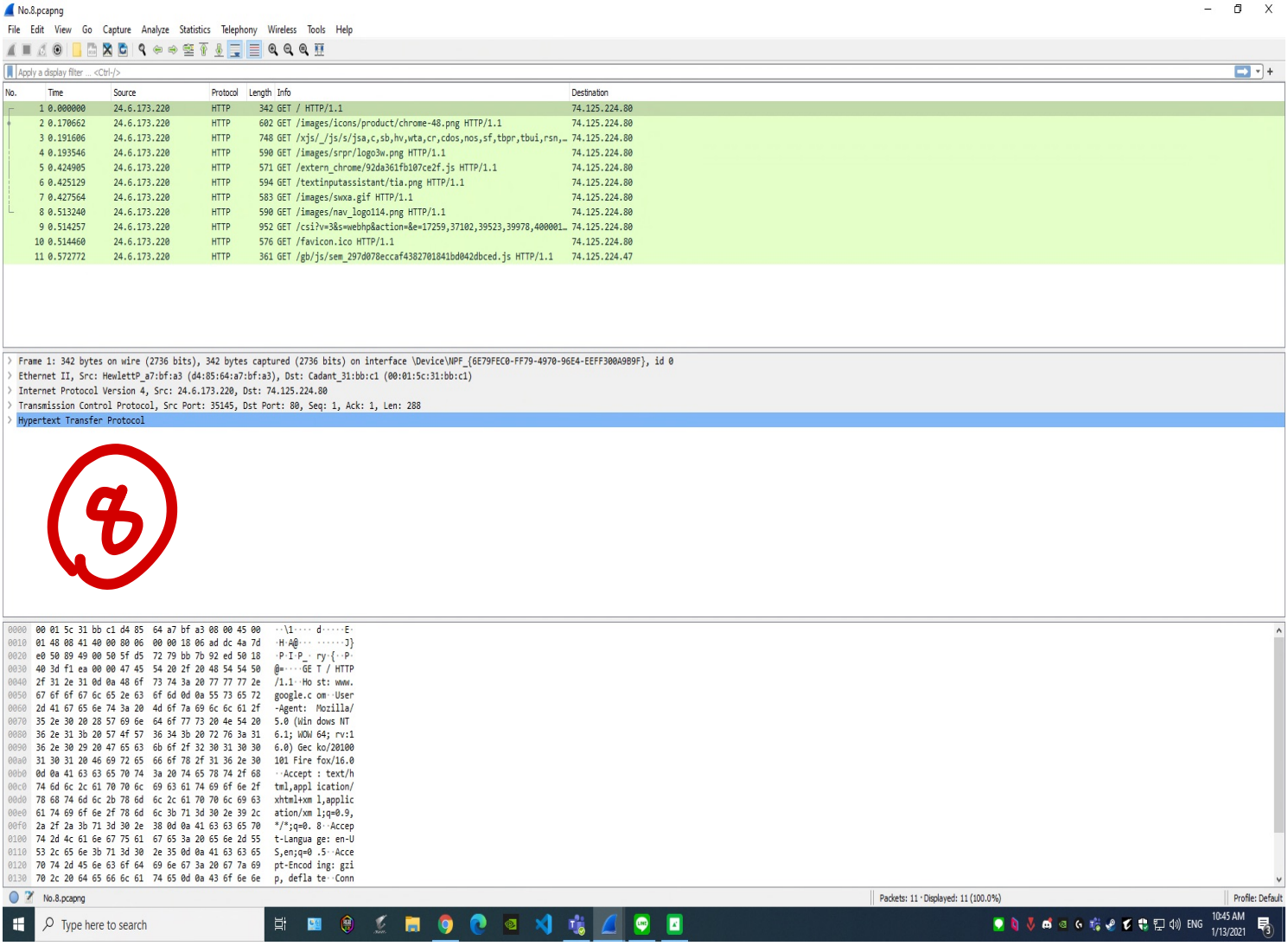
4. ให้ลบคอลัมน์ที่สร้าง

งานครั้งที่ 1

ให้ส่งข้อความที่ให้ตอบ (เขียนเรื่องและข้อด้วย) พร้อมภาพที่ให้ 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




No.8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Protocol Length Info Destination
1 0.000000 24.6.173.220 HTTP 342 GET / HTTP/1.1 74.125.224.80
2 0.170662 24.6.173.220 HTTP 602 GET /images/icons/product/chrome-48.png HTTP/1.1 74.125.224.80
3 0.191606 24.6.173.220 HTTP 748 GET /xjs/_/js/s/jsa,c,sb,hv,wta,cr,cdos,nos,sf,tbpr,tbui,rsn,… 74.125.224.80
4 0.193546 24.6.173.220 HTTP 590 GET /images/srpr/logo3w.png HTTP/1.1 74.125.224.80
5 0.424905 24.6.173.220 HTTP 571 GET /extern_chrome/92da361fb107ce2f.js HTTP/1.1 74.125.224.80
6 0.425129 24.6.173.220 HTTP 594 GET /textinputassistant/tia.png HTTP/1.1 74.125.224.80
7 0.427564 24.6.173.220 HTTP 583 GET /images/swxa.gif HTTP/1.1 74.125.224.80
8 0.513240 24.6.173.220 HTTP 590 GET /images/nav_logo114.png HTTP/1.1 74.125.224.80
9 0.514257 24.6.173.220 HTTP 952 GET /csi?v=3&s=webhp&action=&e=17259,37102,39523,39978,400001… 74.125.224.80
10 0.514460 24.6.173.220 HTTP 576 GET /favicon.ico HTTP/1.1 74.125.224.80
11 0.572772 24.6.173.220 HTTP 361 GET /gb/js/sem_297d078eccaf4382701841bd042dbced.js HTTP/1.1 74.125.224.47
Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 74.125.224.80
Transmission Control Protocol, Src Port: 35145, Dst Port: 80, Seq: 1, Ack: 1, Len: 288
Hypertext Transfer Protocol
8
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ··\1···· d·····E·
0010 01 48 08 41 40 00 80 06 00 00 18 06 ad dc 4a 7d ·H·A@··· ·····J}
0020 e0 50 89 49 00 50 5f d5 72 79 bb 7b 92 ed 50 18 ·P·I·P_· ry·{··P·
0030 40 3d f1 ea 00 00 47 45 54 20 2f 20 48 54 54 50 @=····GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1··Ho st: www.
0050 67 6f 6f 67 6c 65 2e 63 6f 6d 0d 0a 55 73 65 72 google.c om··User
0060 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
0070 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (Win dows NT
0080 36 2e 31 3b 20 57 4f 57 36 34 3b 20 72 76 3a 31 6.1; WOW 64; rv:1
0090 36 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 6.0) Gec ko/20100
00a0 31 30 31 20 46 69 72 65 66 6f 78 2f 31 36 2e 30 101 Fire fox/16.0
00b0 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 ··Accept : text/h
00c0 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f tml,appl ication/
00d0 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 xhtml+xm l,applic
00e0 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c ation/xm l;q=0.9,
00f0 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70 */*;q=0. 8··Accep
0100 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 t-Langua ge: en-U
0110 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 S,en;q=0 .5··Acce
0120 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encod ing: gzi
0130 70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e 6e p, defla te··Conn
No.8.pcapng
Packets: 11 · Displayed: 11 (100.0%)
Profile: Default
Type here to search
ENG
10:45 AM
1/13/2021