

Table of Contents

Wireshark	3
ความสามารถของ Wireshark	3
คุณสมบัติของ Wireshark	4
ข้อมูลที่ควรรู้	4
Capture Point Selection	4
Promiscuous Mode	4
SPAN Port in Switch	4
Network Tap Device	5
Wireless Capture	5
Well known ports	5
3 Way Handshake	5
Wireshark Installation	6
Wireshark User Interface	7
แถบเมนูเบื้องต้น (MenuBar)	7
File	7
View	7
Edit	8
คีย์ลัดก้างหมุดในโปรแกรม (Keyboard Shortcuts)	8
แถบเครื่องมือ (ToolBar)	9
[ACT_01] ToolBar	9
How to use Wireshark101	10
การตั้งค่าพื้นฐาน (Initial Configuration)	11
สร้างไฟล์การใช้งานใหม่	12
การใช้งานพื้นฐาน	13
Mark & Export	13
Column Adding	13
Column Adjustment	14
[HW_01] Find 404 Error	14
[ACT_02] Split pcapng file	14
[ACT_03] Latency Inspection	15
[HW_02] Latency Inspection	17
Wireshark Filter	18
Capture Filter	18
ตัวอย่างการใช้ Capture Filter	18
Display Filter	19
ตัวอย่างการใช้ Display Filter	20
การเพิ่ม Filter ลงใน Toolbar	20
การเพิ่ม Filter ลงใน Bookmark	20
Display Filter Expression	21

Apply as Filter	21
[ACT_04] Filter101	21
[ACT_05] HTTP vs Port80	22
[ACT_06] DNS Filter	22
[HW_03] POST Method	22
ข้อควรระวังการตั้งเงื่อนไข Filter	23
สิ่งที่น่าสนใจของ Display Filter	23
[ACT_07] Contains in Filter	23
[ACT_08] Match in Filter	23

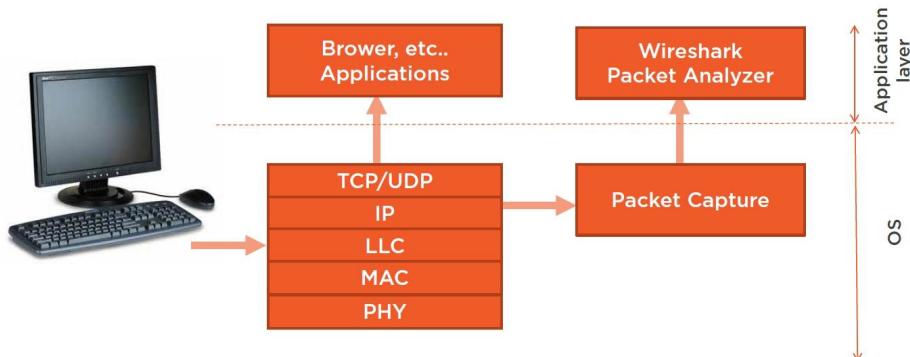
Wireshark

Wireshark ชื่อเดิม Ethereal เป็นโปรแกรม Open Source หรือ Freeware จำพวก Packet Sniffer ชนิดหนึ่ง ซึ่งประกอบไปด้วยส่วนของ Packet Capture และ Packet Analyzer ที่ค่อยทำหน้าที่ในการวิเคราะห์ระบบเครือข่าย โดยที่ Wireshark สามารถใช้งานบนระบบปฏิบัติการได้หลากหลาย เช่น Linux, Window และ OSX

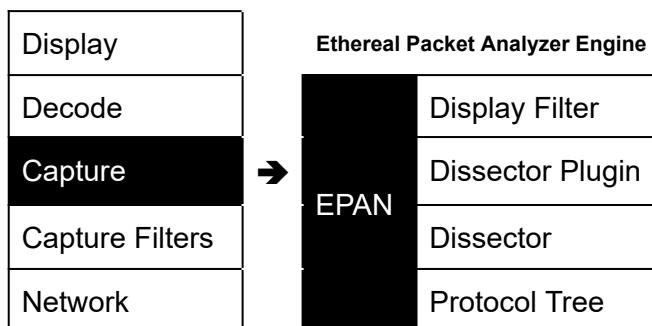
Wireshark จะใช้ Packet Capture เพื่อรับแพ็คเกตที่รีบบันอินเตอร์เฟดต่าง ๆ และข้อมูลดังกล่าวส่งผ่านไปยัง Packet Analyzer เพื่อใช้วิเคราะห์ โดยเครื่องมือสำหรับ Capture Packet ที่นิยมใช้กันมีดังนี้

- Libpcap ใช้ใน Unix/Linux
- WinPcap ใช้ใน Windows (ล่าสุดแล้ว)
- Npcap ใช้ใน Windows (ปัจจุบัน)

โปรแกรม Wireshark สามารถดาวน์โหลดได้ที่ www.wireshark.org/download.html นอกจากนี้ Wireshark ยังมี TShark เป็น Command Line Version อีกด้วย



รูปที่ 1 - Network Packet Analyzer Diagram



รูปที่ 2 - โครงสร้างของ Capture Engine

ความสามารถของ Wireshark

- ค้นหาปัญหาในระบบเครือข่าย
- ตรวจสอบพฤติกรรมที่ผิดปกติของระบบเครือข่าย
- ตรวจสอบพฤติกรรมของโปรแกรม
- ตรวจสอบโปรแกรมที่ไม่ประสงค์ดี
- ทำความเข้าใจกับ OSI Model
- ศึกษาและสำรวจการทำงานของ Protocol ต่าง ๆ
- เฝ้าดูการทำงานของระบบเครือข่าย
- ไม่สามารถส่ง Traffic หรือ Packet เข้าไปในเครือข่าย

คุณสมบัติของ Wireshark

โปรแกรม Wireshark สามารถดักจับข้อมูลที่รองรับได้หลากหลายโปรโตคอลที่มีอยู่ในปัจจุบัน ทำให้โปรแกรมนี้สามารถแปลงข้อมูลขึ้นมาแสดงแยกเป็น field แต่ละส่วนได้ เช่น

- สามารถจับข้อมูลในระบบเครือข่ายได้ รวมถึงอ่านข้อมูลแพ็คเกตจากไฟล์มาร์วิเคราะห์ได้
- สามารถดักจับข้อมูลได้หลายโปรโตคอลทั้ง Ethernet, IEEE 802.11, PPP และ loopback
- ใช้งานได้ทั้งบน GUI และ Command Line (TShark)
- สามารถ filter ข้อมูลได้
- เพิ่ม plugin สำหรับโปรโตคอลใหม่ ๆ ได้
- จับข้อมูล USB แบบ Raw data ได้
- ดักจับข้อมูลได้ทั้งแบบ มีสาย (Lan) และไร้สาย (Wireless)

ข้อมูลที่ควรรู้

Capture Point Selection

การเลือกจุดตรวจสอบปัญหาในระบบควรเลือกจุดที่ใกล้ปัญหาที่สุด ถ้าหากไม่แน่ใจให้ Capture จากหลาย ๆ จุด เช่น

- ปัญหาเกิดที่ผู้ใช้งานคนเดียว ก็จับที่ผู้ใช้งานคนนั้น หรือ Switch
- ปัญหาเกิดหลายคนอาจจะทำที่เราเตอร์ หรือ Switch
- ปัญหาเกิดที่ Service ตัวใด อาจจะทำที่เซิร์ฟเวอร์

Promiscuous Mode

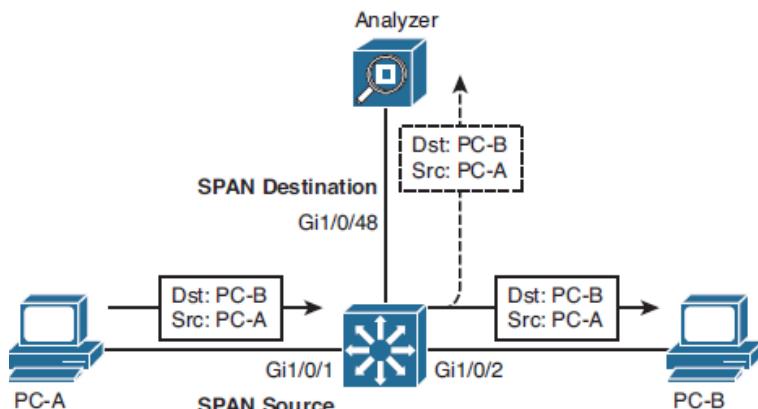
ปกติแล้วการส่งข้อมูลในระบบเครือข่าย ถ้าข้อมูลนั้นไม่ได้ ส่งถึงผู้รับ ผู้รับจะทำการ Discard / Drop แพ็คเกตเดินทางต่อไป แต่ ในโหมดนี้จะรับทุกแพ็คเกตไม่สนใจว่าแพ็คเก็ตนั้นจะส่งถึงใคร



SPAN Port in Switch

ย่อมาจาก Switch Port Analyzer Analyzer สามารถเรียก Port Mirroring ได้ ซึ่งพอร์ตนี้เป็น พอร์ตพิเศษที่จะส่งแพ็คเกตทั้งหมดที่วิ่งอยู่บน Switch หรือแพ็คเกตของพอร์ตที่กำหนดได้ โดยข้อเสีย คือจะต้องใช้ Switch ที่มีราคาสูงขึ้น และต้องทำการ Config เพิ่มเติม

ในการตรวจสอบความผิดปกติในเครือข่ายบางครั้งต้องใช้ SPAN เนื่องจากปกติแล้วในครั้งแรก ของการส่งแพ็คเกต Switch จะทำการเรียนรู้แล้วพอร์ตที่เชื่อมต่อกับตัว Switch เพื่อบรุ่งแต่ละพอร์ต คืออุปกรณ์ตัวไหน (เรียนรู้จาก MAC Address) และเมื่อส่งข้อมูลในครั้งต่อ ๆ ไป Switch จะส่งข้อมูลไปยังพอร์ตที่เชื่อมต่อกับผู้รับโดยตรง (ไม่ส่งแพ็คเกตที่ไม่เกี่ยวข้องไปที่พอร์ตอื่น)



รูปที่ 3 - การต่อ SPAN Port เพื่อใช้งานกับ Packet Analyzer

Network Tap Device

គីឡូក្រុងសំគាល់គីឡូក្រុងការបង្កើតរឹងរាល់



รูปที่ 4 - อปกรณใชสำหรับดักข้อมูลในระบบเครือข่าย และวิธีต่อใช้งาน

Wireless Capture

- โดยทั่วไปจะไม่สามารถตักฟิร์ม Beacon หรือ Probe ได้ จะตักได้เฉพาะเฟิร์มข้อมูลเท่านั้น
 - ไดร์เวอร์ NDIS (Network Driver Interface Specification) จะตัดส่วนหัวของ 802.11 ออกทำให้ไม่เห็นข้อมูลนี้
 - หากต้องการ Capture ส่วนหัวด้วย จะต้องใช้ฮาร์ดแวร์ช่วยเพิ่มเติม เช่น airpcap



รูปที่ 5 - AirPcap Nx

Well known ports

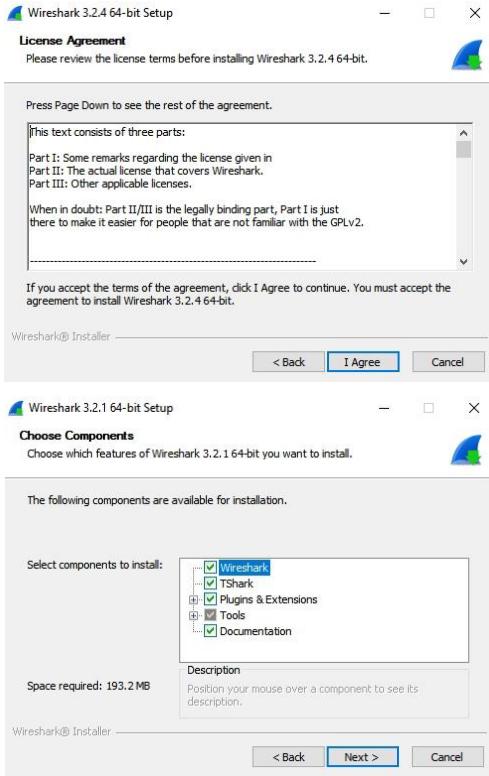
<u>TCP</u>		<u>UDP</u>	
Port	Application	Port	Application
20	FTP Data	53	DNS
21	FTP Control	67,68	DHCP
22	SSH	69	TFTP
23	Telnet	161	SNMP
25	SMTP		
53	DNS		
80	HTTP (WWW)		
110	POP3		
443	SSL		

3 Way Handshake

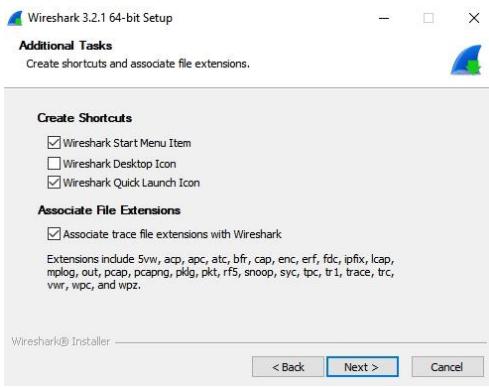


Wireshark Installation

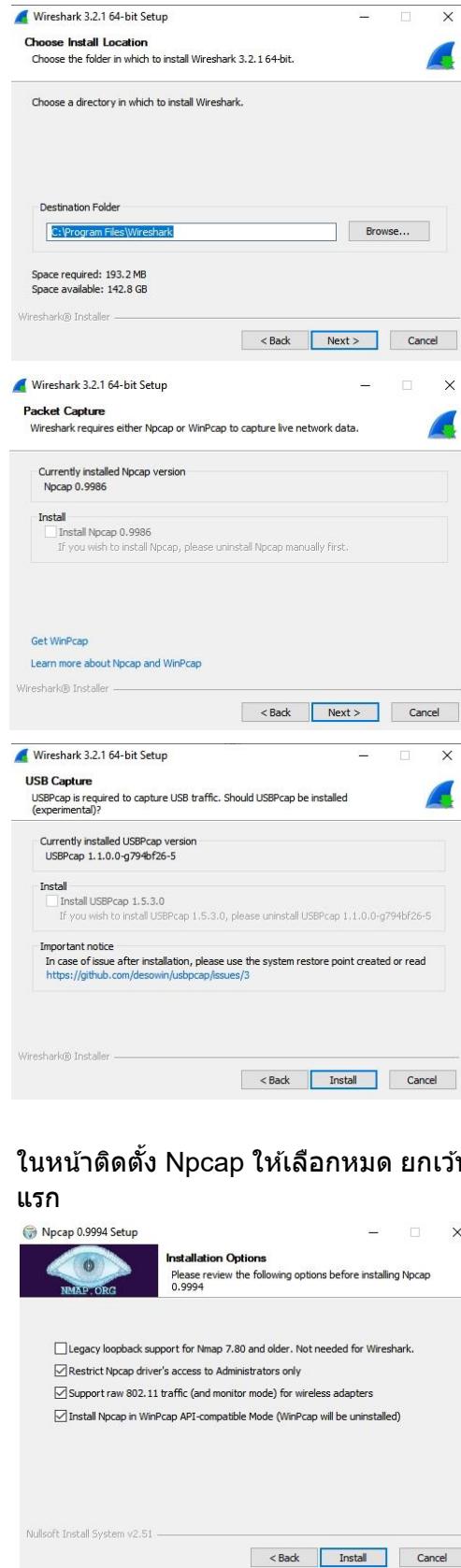
1. เลือก Windows Installer (64 bit) ให้หลด แล้วติดตั้ง



2. เลือกตามต้องการว่าจะเอา Desktop Icon หรือ Quick Launch หรือไม่



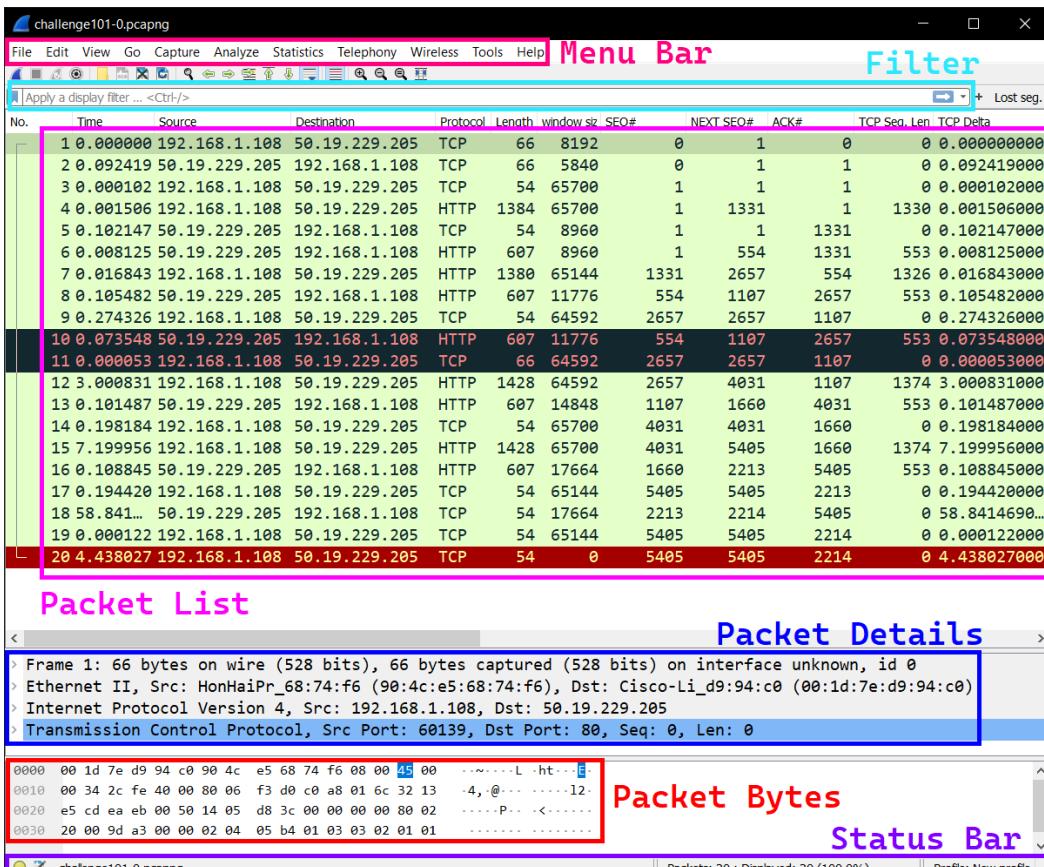
3. เลือกติดตั้ง Npcap ถ้ายังไม่ติดตั้ง และ ดำเนินการติดตั้งจนเสร็จ



Wireshark User Interface

ແຄນເມນຸເບື້ອງຕັ້ນ (Menu Bar)

ແຄນນີ້ຈະອູ່ດ້ານນົບຂອງໂປຣແກຣມ ມີໜ້າທີ່ຮັບຮັບພັງກຳຊັບກຳທຳການຫລັກ ຍ ອົງການທຳການຕ່າງ ຍ ທີ່ຈຳເປັນ ສໍາຮັບຂ່ອງສີຂາວດ້ານລ່າງເປັນຂ່ອງສໍາຮັບໃສ Filter ເພື່ອກຽນຂ້ອມລິ້ຫ້ອດາມທີ່ຕ້ອງການ



ຮູບທີ 6 - ໂຄງສ້າງພື້ນຖານຂອງໂປຣແກຣມ Wireshark

File

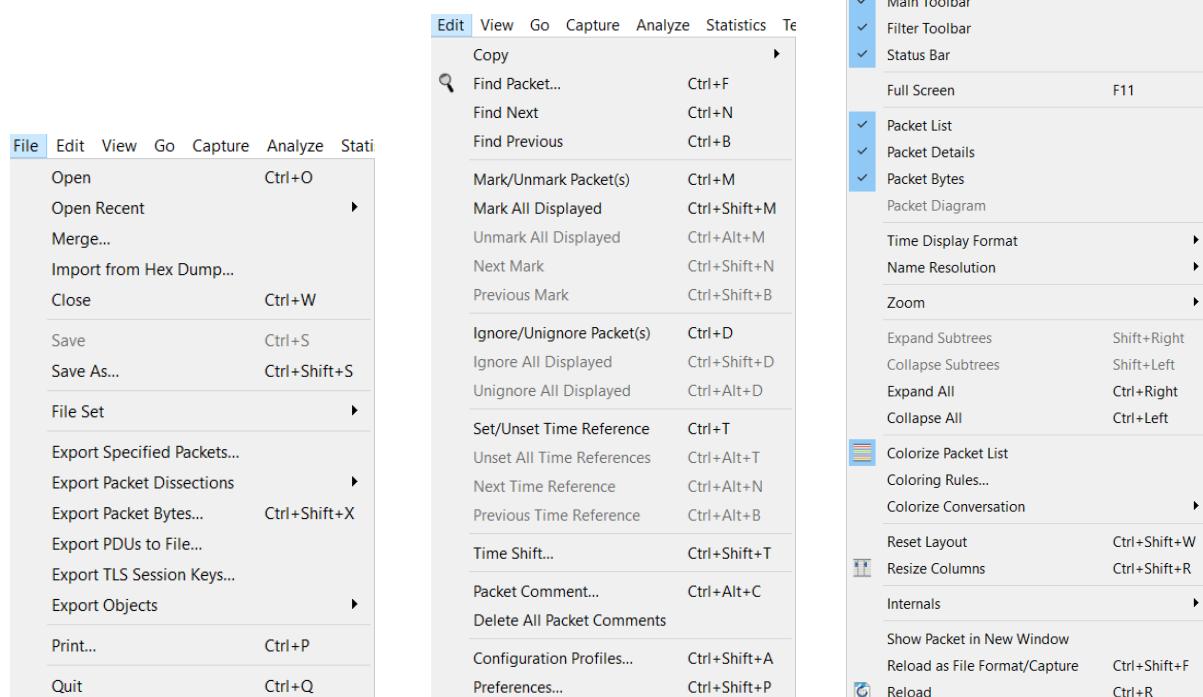
- Merge : ຮວມຂ້ອມລິ່ໄລທີ່ເປີດປັ້ງຈຸບັນ ແລະ ໄຟລີ່ທີ່ຈະ Merge ເປັນໄຟລີ່ເຕີຍກັນ
- File Set : ເຮັກດູໄຟລີ່ແບບເປັນຊຸດ
- Export : ໃນໃນການບັນທຶກນາງແພັກເກີດ ອົງບາງສ່ວນເປັນໄຟລີ່ໃໝ່

View

- Main Toolbar / Filter Toolbar / Status Bar : ໃຊ້ເພື່ອເລືອກແສດງ ອົງໄມ່ແສດງ ແຄນຕ່າງ ຍ
- Packet List / Packet Details / Packet Bytes : ເລືອກແສດງສ່ວນຕ່າງ ຍ ຂອງແພັກເກີດ
- Time Display Format : ເປົ້າຢູ່ນຮູ່ນແບບການຜລແສດງເວລາ
- Name Resolution : ສາມາດເລືອກແປ່ງຂ້ອມລ Physical Address, Network Address ແລະ Transport Address ເປັນໜີ້ໄດ້
- Zoom : ຍ່ອ ອົງຍາຍຂາດຕ້ວອັກຊີຣ
- Colorize Packet List : ສັງໂປຣແກຣມຮະບາຍສີພື້ນຫລັງຂອງ Packet List ຕາມເງື່ອນໄຂ
- Coloring Rules : ກຳນົດເງື່ອນໄຂຂອງສີແຕ່ລະສີທີ່ຈະຮະບາຍ
- Colorize Conversation : ກຳນົດສີທີ່ຈະຮະບາຍຕາມປະເທດ (Conversation)

Edit

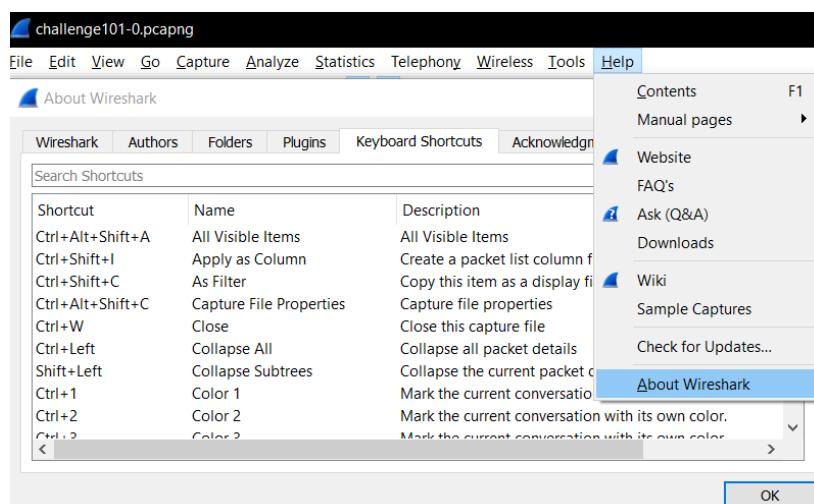
- Copy : ใช้คัดลอดแพ็คเกตออกเป็นรูปแบบต่างๆ
- Find Packet : ใช้ค้นหาแพ็คเกตตามเงื่อนไข
- Find Next : ค้นหาแพ็คเกตถัดไปตามเงื่อนไข
- Find Previous : ค้นหาแพ็คเกตก่อนหน้าตามเงื่อนไข
- Mark/Unmark : ทำเครื่องหมาย (คลิกขวาได้)
- Ignore : ไม่สนใจแพ็คเกตตอนวิเคราะห์
- Time Shift : เลื่อนเวลาของแพ็คเกต



รูปที่ 7 - เมนู File Edit และ View ที่อยู่ส่วนด้านบนของ Wireshark

คีย์ลัดทั้งหมดในโปรแกรม (Keyboard Shortcuts)

สามารถเข้าไปดูคีย์ลัดได้ในเมนู Help > About Wireshark > Keyboard Shortcuts



รูปที่ 8 - คีย์ลัดต่าง ๆ ของโปรแกรม Wireshark

แทบเครื่องมือ (ToolBar)



Start Capture

Stop Capture

Restart Capture

Capture Option

Open Capture File

Save Capture File

Close Capture File

Reload Capture File



เป็นกลุ่มเครื่องมือสำหรับหาแพ็คเกตต่าง ๆ



ปุ่มลัดสำหรับรายสีใน Packet List



ปุ่มเพิ่ม/ลด ขนาดตัวอักษร

[ACT_01] ToolBar

Guideline

1. เปิดไฟล์ <http://google101.pcapng>
2. ทดลองใช้ Toolbar ด้านบนในการค้นหาแพ็คเกต, ไปแพ็คเก็ตถัดไป, ถอยไปยังแพ็คเก็ตก่อนหน้า, แพ็คเก็ตแรกสุด, แพ็คเก็ตท้ายสุด, แพ็คเก็ตที่ 296



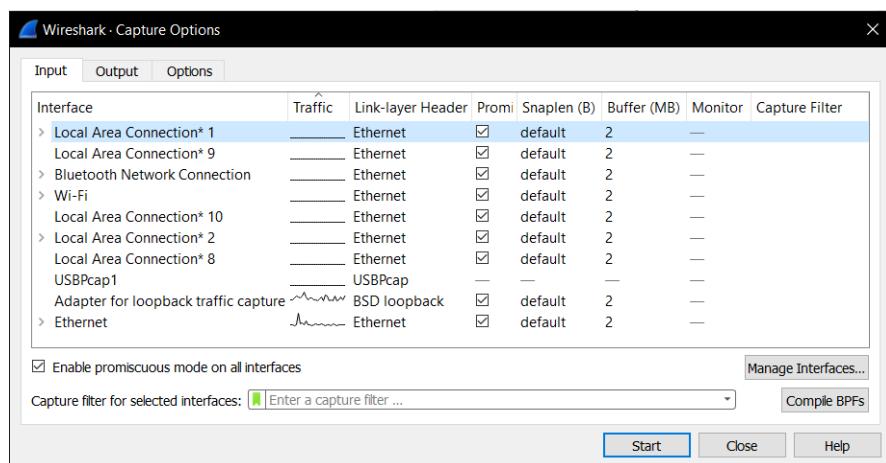
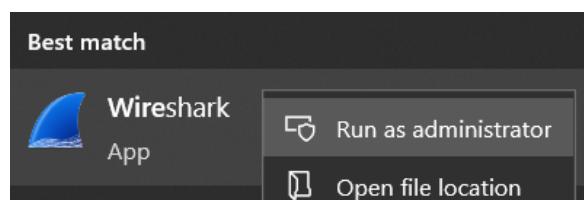
3. ทดลองค้นหาไฟล์รูปโดยเลือกค้นจาก String

Problem

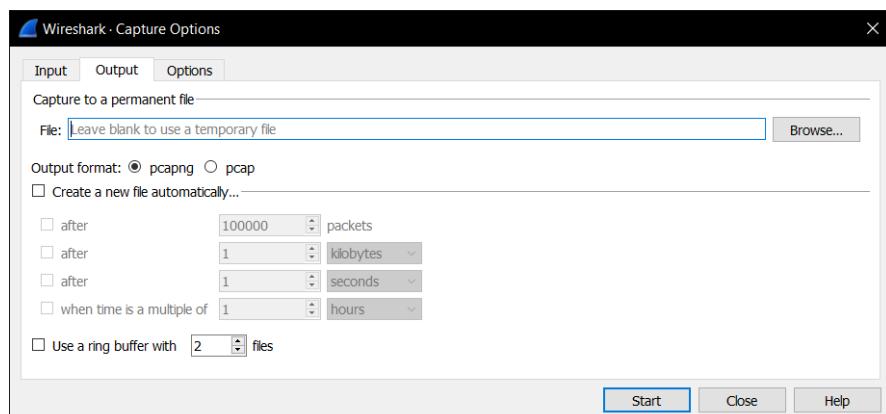
1. แพ็คเกตท้ายสุดคือแพ็คเก็ตที่เท่าไร
2. รายละเอียดแพ็คเก็ตที่ 296 แสดงอย่างไร
3. ในไฟล์นี้มีรูปกี่ไฟล์
4. ไฟล์รูปในข้อ 3 ชื่ออะไรบ้าง

How to use Wireshark101

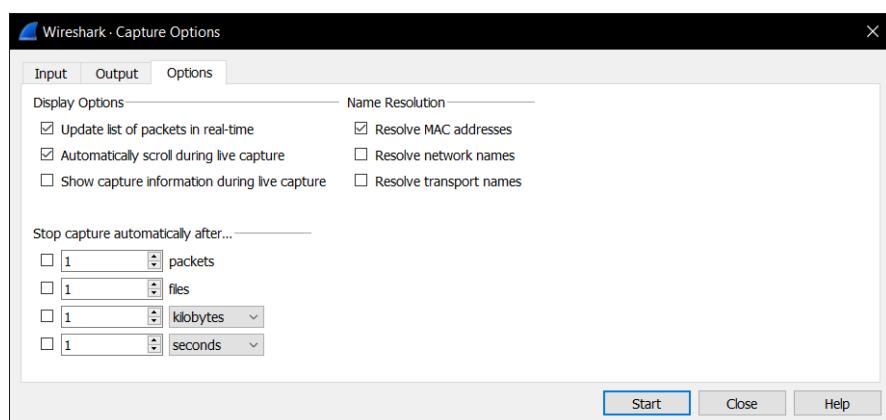
การเรียกใช้โปรแกรมควรใช้สิทธิ์ Admin ใน การเรียก เนื่องจากตัวโปรแกรมไม่สิทธิ์ในการเข้าถึง Interface ต่าง ๆ เพื่อดักแพ็คเกตไม่เช่นนั้นมีเมื่อเข้า โปรแกรม Wireshark จะทำการขอสิทธิ์ตามจำนวน Network Adaptor ที่มีอยู่ทั้งหมด (เช่น Ethernet1, Ethernet2, Wi-Fi,.....)



รูปที่ 9 - Network Adaptor ที่ต้องการจะดักแพ็คเกต



รูปที่ 10 - การตั้งค่าไฟล์ Output เช่น การแบ่งไฟล์ ประเภทไฟล์ที่บันทึก เป็นต้น

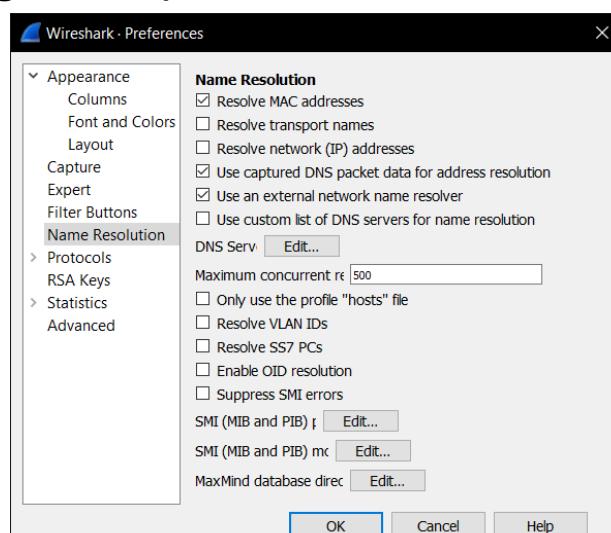


รูปที่ 11 - การตั้งค่าเพิ่มสำหรับไฟล์ Output ต่าง ๆ เช่น การ Resolve Name เป็นต้น

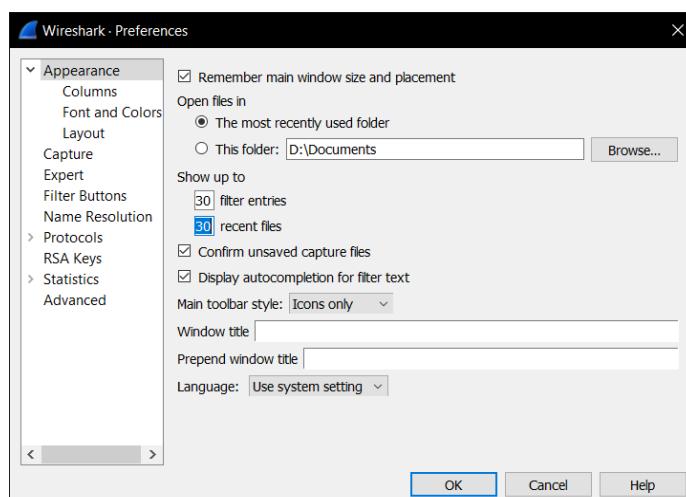
การตั้งค่าพื้นฐาน (Initial Configuration)

กรณีที่ต้องการตั้งค่าที่เกี่ยวข้องกับ Name Resolution โดยให้ Wireshark ทำการ Resolve Name ในระหว่างที่ดักแพ็คเกต (ต้องใช้ Traffic และ Processing ตั้งนั้นไม่ควรใช้โดยไม่จำเป็น) จะสามารถเลือก Resolve ได้ดังนี้

- MAC : ใช้ manuf file
- IP : ใช้ DNS
- Transport : ใช้ Service file

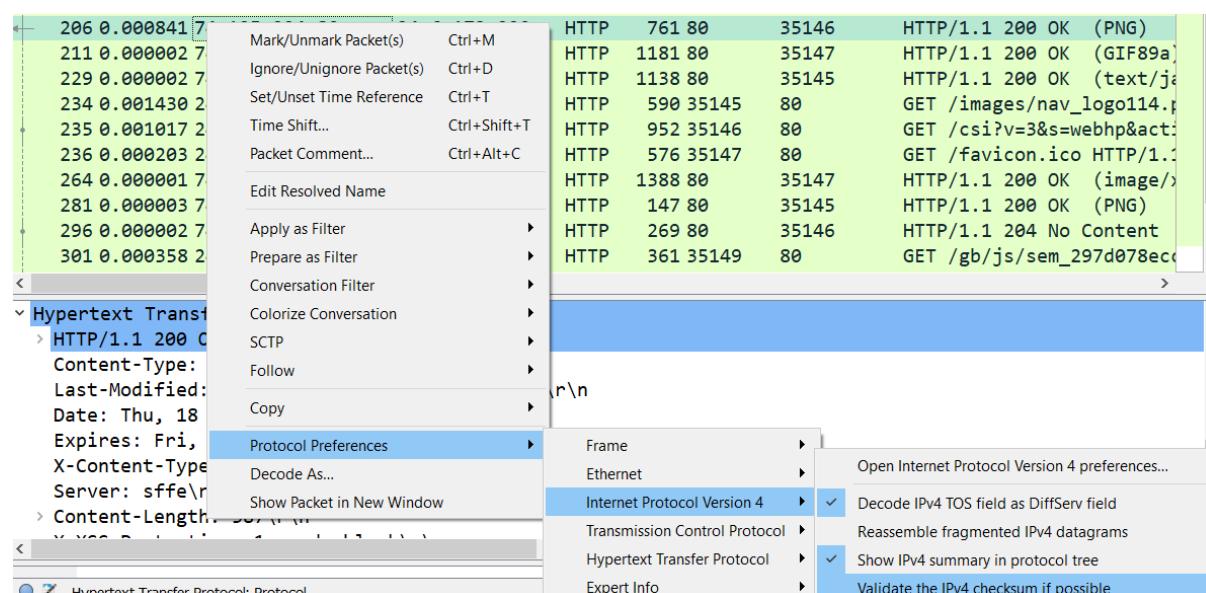


รูปที่ 12 - หน้าต่างการตั้งค่า Preference ในเมนู Edit

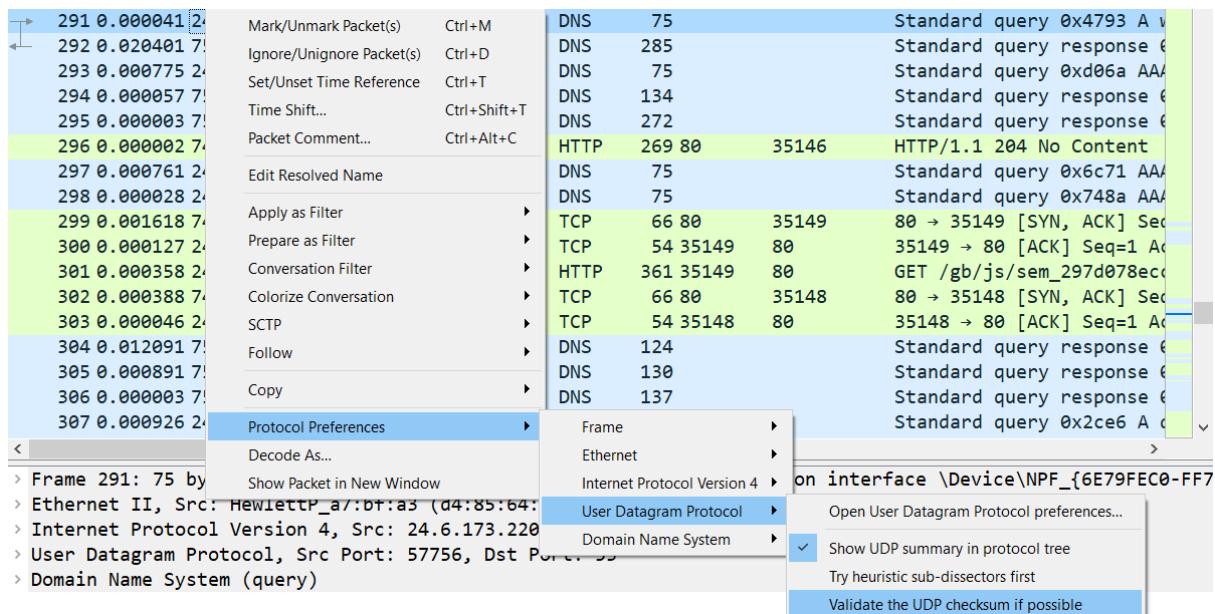


กำหนด filter entries และ recent files เป็น 30 เพื่อให้แสดงจำนวน filters และ recent files ให้มากขึ้น

ปิด Validate the IPv4 checksum if possible เพื่อให้ประมวลผลได้ไวขึ้น โดยคลิกขวาเลือกแพ็คเกตที่มีการใช้ Internet Protocol V.4



รูปที่ 13 - การปิดฟังก์ชัน Validate the IPv4 checksum



รูปที่ 14 - การปิดฟังก์ชัน Validate the UDP checksum

เลือกแพ็คเกตที่มีการทำงานผ่าน Transport Layer ในส่วนของ Packet list เช่น DNS Packet เป็นต้น จากนั้นคลิกขวา Transmission Control Protocol Protocol เลือก Protocol Preferences และตั้งค่าดังนี้

- disable Validate the TCP checksum if possible
- disable Allow subdissector to reassemble TCP streams
- enable Track number of bytes in flight
- enable Calculate conversation timestamps

การตั้งค่าพื้นฐานเหล่านี้ควรตั้งค่าแยกเป็นอึកໂປຣໜຶ່ງ ໄນគຽດຕັ້ງຄ່າທັນ Default Profile ທີ່ດິມາກັນໂປຣແກຣມໃນຕອນແຮກ ໂດຍການສ້າງໂປຣໜຶ່ງການຕັ້ງຄ່າສາມາຄສ້າງໄດ້ດາມຫ້ວຂອຄັດໄປ

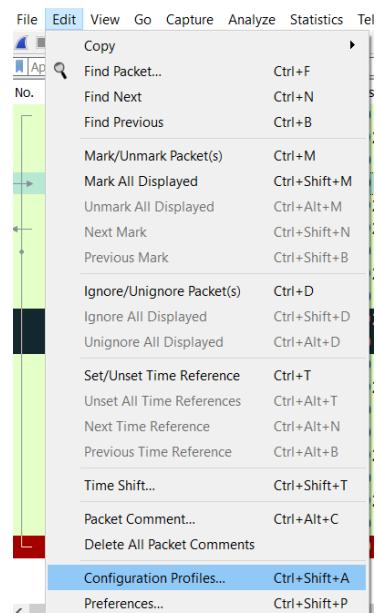
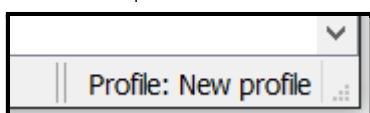
สร้างໂປຣການໃໝ່

ปกติแล้วเมื่อผู้ใช้งานทำการตั้งค่าໂປຣແກຣມ Wireshark ด้วย Configuration Profile (เก็บอยู่ในโฟลเดอร์ %APPDATA%\Wireshark) ดังนั้นผู้ใช้งานควรที่จะสร้างໂປຣແກຣມสำหรับการใช้งานแต่ละประเภทให้เหมาะสม และไม่ควรใช้ Default Profile เนื่องจากเป็นค่าพื้นฐานของ Wireshark เมื่อใช้งานไประยะหนึ่ง และต้องการกลับมาใช้การตั้งค่าตอนแรกอาจจำลืมได้ว่าผู้ใช้งานได้เปลี่ยนการตั้งค่าอะไรไปบ้าง

ตัวอย่างข้อมูลที่เก็บในໂປຣໜຶ່ງ Preference, Capture Filters, Display Filters, Coloring Rules, Disabled Protocols รวมถึงข้อมูลการแสดงผล เช่น ความกว้างคอลัมน์ เป็นต้น

การสร้างໂປຣໜຶ່ງມີວິທີ 2 ວິທີນັ້ນເຄື່ອງ

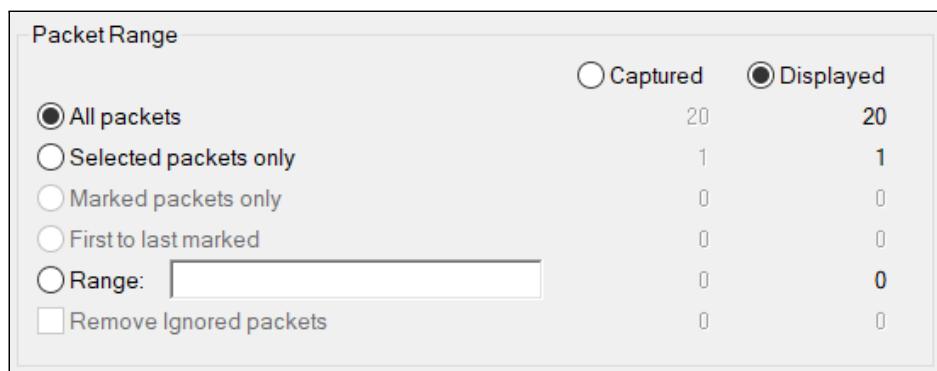
1. เข้า去ເມນຸ Edit > Configuration Profiles
2. ຄລິກຂາວທີ່ມີນຳຂາວລ່າງ ແລ້ວເລືອກ New



การใช้งานพื้นฐาน

Mark & Export

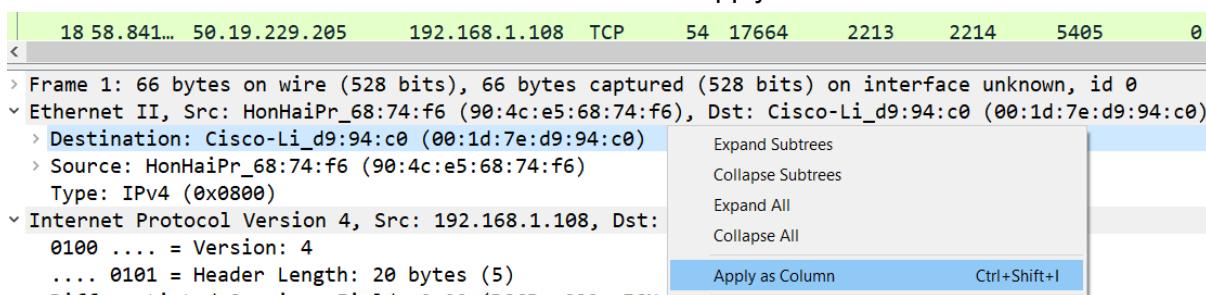
- คือการทำเครื่องหมายบนข้อมูล Packet ที่จับมาได้
- กด Ctrl + M หรือคลิกขวา → Mark
- ประโยชน์ของการ Mark คือ
 - ◆ เลื่อนกลับมาดูในภายหลังได้ง่ายขึ้น เพราะมีสีให้สังเกต
 - ◆ สามารถค้นหาได้ frame.marked == 1
 - ◆ สามารถ Export แยกออกเป็นไฟล์ได้ File → Export Specified Packet..



รูปที่ 15 - การตั้งค่าเมื่อ Export สามารถเลือกเฉพาะ Marked packets ได้

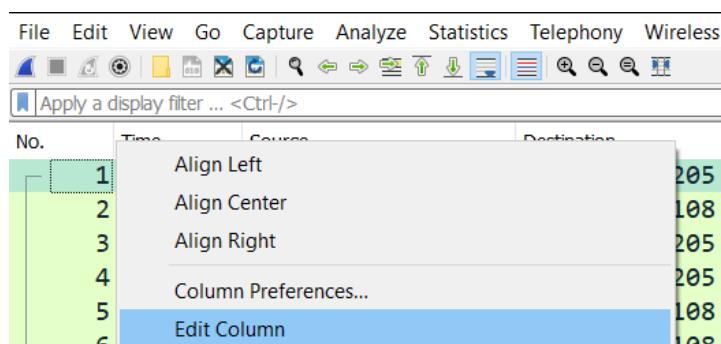
Column Adding

- สามารถเพิ่มค่าที่ต้องการใช้เคราะห์บอย ๆ เป็นคอลัมน์เพื่อง่ายต่อการค้นหา
- การเพิ่มคอลัมน์สามารถเพิ่มได้ 2 วิธี
 - ◆ เลือกส่วนที่จะเพิ่มเป็นคอลัมน์ คลิกขวา → Apply as Column



รูปที่ 16 - การเพิ่มคอลัมน์จากข้อมูลใน Packet Details

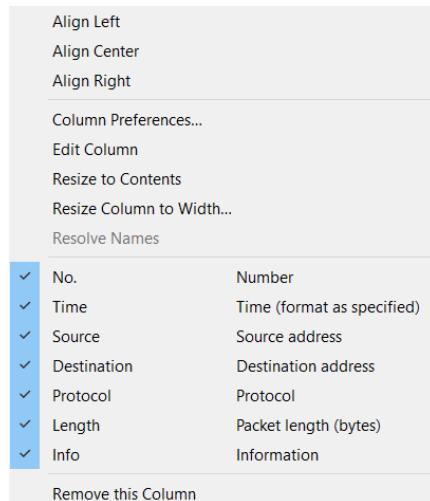
- ◆ คลิกขวาที่ Header ของตาราง Packet List → Edit Column



รูปที่ 17 - การเพิ่มคอลัมน์โดย Edit Column

Column Adjustment

- คลิกขวาที่ชื่อคอลัมน์เพื่อปรับค่าต่าง ๆ
 - ◆ ชิด ซ้าย ขวา กลาง
 - ◆ Edit Column (แก้ไขรายละเอียด)
 - ◆ Resize to Content (ปรับความกว้างตามข้อมูล)
 - ◆ Resize Column to Width (กำหนดความกว้าง)
- คลิกที่ชื่อคอลัมน์ จะเป็นการเรียง



[HW_01] Find 404 Error

Guideline

1. คลิก Capture Options ในแถบเมนูเลือก Adapter ที่ออกอินเตอร์เน็ต
2. ในแถบ Output กด Browse ตั้งชื่อไฟล์เป็น Find404NotFound.pcapng
3. ไปที่ www.chappellu.com/nothere.html และหยุด Capture
4. ให้ค้นหาเกี่ยวกับ 404 error ในไฟล์ที่บันทึกได้

Problem

1. เชิร์ฟเวอร์ www.chappellu.com/nothere.html ไอพีแอดเดรสอะไร
 2. เมื่อเข้าเว็บตั้งกล่าวเจอรายละเอียด 404 Error หรือไม่
 3. จากข้อ 1 ถ้าเจอ เจอในแพ็คเก็ตที่เท่าไร (ถ้าไม่เจอให้ตอบ -1)
 4. จากข้อ 1 ถ้าไม่เจอ เป็นเพราะสาเหตุอะไร (ถ้าเจอตอบ -)
-
-
-
-

[ACT_02] Split pcapng file

Guideline

1. คลิก Capture → Options ในแถบเมนูเลือก Adapter ที่ออกอินเตอร์เน็ต
2. ใน Tab Output กด Browse ตั้งชื่อไฟล์เป็น Kmitl.pcapng
3. กำหนดให้ชื่อไฟล์ใหม่ทุก 1 MB และ ทุก 10 วินาที และหยุดหลังจาก 3 ไฟล์
4. กด Start ไปที่ <https://www.kmitl.ac.th> ให้ดูผลที่เกิดขึ้น
5. สร้าง Configuration Profile ใหม่ (ห้ามใช้ Default Profile)
6. เข้าที่ File → File Set → List Files
7. สร้างคอลัมน์ Host เพิ่มเติมโดยเลือกแพ็คเก็ตที่มีโปรโตคอล HTTP
8. หาหมวดหมู่ Hypertext Transfer Protocol ในส่วนของ Packet Details
9. ขยายหมวดหมู่ Hypertext Transfer Protocol และหาแคล Host คลิกขวาเลือก Apply as Column

Problem

1. เมื่อเข้าไปในหน้า List Files ตารางจะแสดงรายละเอียดทั้งหมดกี่เค้า
2. แคปปูปหน้าจอหน้าต่าง List Files
3. แคปปูปหน้าจอส่วนของ Packet list หลังจากเพิ่มคอลัมน์แล้ว

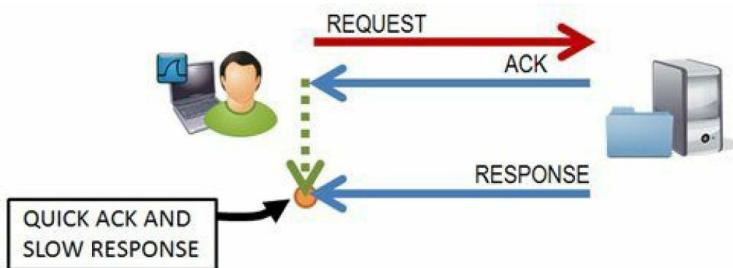
List File

Packet list

[ACT_03] Latency Inspection

Note

- Server Latency เกิดจากเซิร์ฟเวอร์ตอบสนองช้า อาจเกิดจากทรัพยากรไม่เพียงพอ หรือเป็นที่ตัวแอพพลิเคชัน ซึ่งสามารถดูได้จาก Quick Ack และ Slow Response



รูปที่ 18 - Quick Ack and Slow Response Situation

- ปกติคอลัมน์ Time จะแสดงข้อมูล Seconds Since Beginning of Capture ซึ่งจะเริ่มจาก 0
- แต่ถ้าต้องการให้เห็นเวลาระหว่างแพ็คเกต (Delta time) ให้เปลี่ยนการตั้งค่าดังนี้ เมนู View → Time Display Format → Seconds Since Previous Displayed Packet

No.	Time	Source	Destination	Protocol	Length	Info
6	0.226388	150.101.135.12	24.6.173.220	TCP	66 80	→ 21458 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=66 MSS=1460 SACK_PERM=1 WS=128
19	0.207913	150.101.135.12	24.6.173.220	TCP	1514 80	→ 21458 [ACK] Seq=10221 Ack=1166 Win=8192 Len=1460 [TCP segment of a reassembled PDU]
144	0.285086	24.6.173.220	150.101.135.12	TCP	54 21458	→ 80 [ACK] Seq=1166 Ack=143081 Win=65700 Len=0
14	0.195098	150.101.135.12	24.6.173.220	TCP	1514 80	→ 21458 [ACK] Seq=4381 Ack=1166 Win=8192 Len=1460 [TCP segment of a reassembled PDU]
43	0.193580	150.101.135.12	24.6.173.220	TCP	1514 80	→ 21458 [PSH, ACK] Seq=35041 Ack=1166 Win=8192 Len=1460 [TCP segment of a reassembled PDU]
25	0.193321	150.101.135.12	24.6.173.220	TCP	1514 80	→ 21458 [ACK] Seq=17521 Ack=1166 Win=8192 Len=1460 [TCP segment of a reassembled PDU]
9	0.193286	150.101.135.12	24.6.173.220	TCP	60 80	→ 21458 [ACK] Seq=1 Ack=1166 Win=8192 Len=0

รูปที่ 19 - เวลาตั้งแต่เริ่มตักแพ็คเกต (ค่าพื้นฐานของโปรแกรม)

No.	Time	Source	Destination	Protocol	Length	Info
17...	49.372097	150.101.135.12	24.6.173.220	TCP	1514 80	→ 21458 [ACK] Seq=17892301 Ack=1167 Win=8192 Len=1460 [TCP segment of a reassembled PDU]
17...	49.372094	150.101.135.12	24.6.173.220	TCP	1514 80	→ 21458 [ACK] Seq=17890841 Ack=1167 Win=8192 Len=1460 [TCP segment of a reassembled PDU]
17...	49.371253	150.101.135.12	24.6.173.220	TCP	1514 80	→ 21458 [ACK] Seq=17889381 Ack=1167 Win=8192 Len=1460 [TCP segment of a reassembled PDU]
17...	49.302023	150.101.135.12	24.6.173.220	TCP	1514 80	→ 21458 [PSH, ACK] Seq=17887921 Ack=1166 Win=8192 Len=1460 [TCP segment of a reassembled PDU]

รูปที่ 20 - เวลาระหว่างแพ็คเกตปัจจุบัน และแพ็คเกตก่อนหน้าที่ตักจับได้

Guideline

1. สร้างคอลัมน์ Delta time เพิ่มจากคอลัมน์ Time ปกติ <http://pcapnet101.pcapng>
2. หาหมวดหมู่ TCP ใน Packet Details → คลิกขวาที่ Time since previous frame in this TCP stream → เลือก Apply as Column

> Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFFF300A9B9F}, id 0
> Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)
> Internet Protocol Version 4, Src: 150.101.135.12, Dst: 24.6.173.220
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 21458, Seq: 0, Ack: 1, Len: 0
Source Port: 80 Destination Port: 21458 [Stream index: 0] [TCP Segment Len: 0] Sequence Number: 0 (relative sequence number) Sequence Number (raw): 4095395115 [Next Sequence Number: 1 (relative sequence number)] Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 2265659684 1000 = Header Length: 32 bytes (8) Flags: 0x012 (SYN, ACK) Window: 5840 [Calculated window size: 5840] Checksum: 0xa744 [unverified] [Checksum Status: Unverified] Urgent Pointer: 0 Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP) [SEQ/ACK analysis] [Timestamps] [Time since first frame in this TCP stream: 0.226388000 seconds] [Time since previous frame in this TCP stream: 0.226388000 seconds]

รูปที่ 21 - การเพิ่ม TCP Delta เป็นคอลัมน์

3. เปลี่ยนชื่อคอลัมน์ที่ได้ใหม่เป็น TCP Delta

Problem

1. แพ็คเกตที่ 470, 471 และ 458 ใช้เวลาเยอะผิดปกติหรือไม่ เพราะ
.....
2. แพ็คเกตที่ 398, 396 และ 397 ใช้เวลาเยอะผิดปกติหรือไม่ เพราะ
.....
3. แพ็คเกตที่ควรพิจารณาเนื่องจากอาจมีปัญหาเกี่ยวกับ Latency คือแพ็คเกตที่ และ.....
4. แคปรูปหน้าจอส่วนของ Packet list หลังจากเพิ่มคอลัมน์แล้ว

Packet list

[HW_02] Latency Inspection

Problem

1. ในไฟล์ [http-slow101.pcapng](#) แพ็คเกตใดบ้างที่อาจเกิดปัญหา Latency (ให้ตอบเรียงแพ็คเกตเลขน้อยไปทางเลขมาก โดยใช้ ", " คั่น)
.....
.....
2. ในคอลัมน์ Info จะสังเกตเห็นแพ็คเกตเหล่านี้มีบางสิ่งเหมือนกันนั่นคือ
.....
.....
3. จากข้อ 2 ให้อธิบายสิ่งนั้น
.....
.....

Wireshark Filter

Capture Filter

ใช้กรองเฉพาะแพ็คเกตที่ต้องการตอนตักจับข้อมูล ดังนั้นในไฟล์ที่ตักจับจะมีแค่แพ็คเกตที่ตรงเงื่อนไขที่กรองเท่านั้น ปกติแล้วสามารถแบ่งการกรองได้ดังนี้

- กรองด้วยชื่อ
 - ◆ Host name
 - ◆ Network Address
 - ◆ Port Number
- กรองตามเป้าหมายที่ต้องการ
 - ◆ Source (src)
 - ◆ Destination (dst)
- กรองตามโปรโตคอล
 - ◆ ARP, ICMP, IP, TCP, UDP, etc



รูปที่ 21 - ช่องใส่ Capture Filter ในหน้าแรกก่อนตักจับแพ็คเกต

ตัวอย่างการใช้ Capture Filter

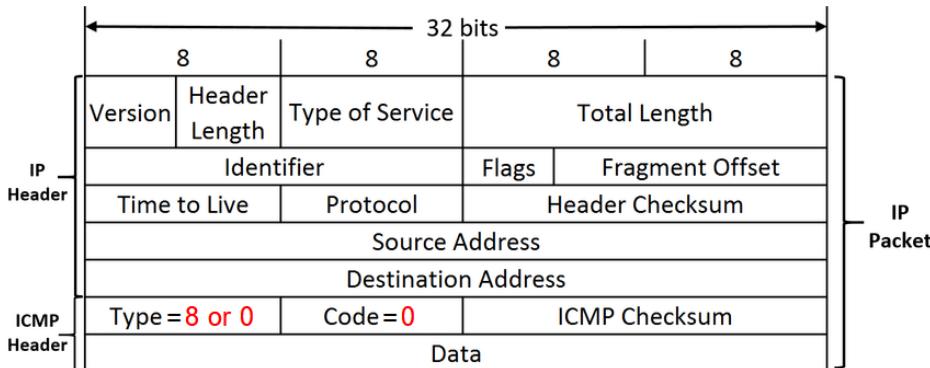
- host 10.3.1.1
- host 2406:da00:ff00::6b16:f02d
- not host 10.3.1.1
- src host 10.3.1.1
- dst host 10.3.1.1
- host www.espn.com
- net 10.3.0.0/16
- net 10.3.0.0 mask 255.255.0.0
- not dst net 10.3.0.0/16
- dst net 10.3.0.0/16
- src net 10.3.0.0/16
- ether host 00:08:15:00:08:15
- ether src 02:0A:42:23:41:AC
- not ether host 00:08:15:00:08:15:

- ★ tcp port 23
- ★ tcp dst port 80
- ★ host 161.246.5.100
- ★ net 161.246.5.0/24
- ★ src net 161.246.5.0/24
- ★ net 161.246.5.0 mask 255.255.255.0

- ❖ port 53
- ❖ not port 53
- ❖ udp port 67
- ❖ tcp port 21
- ❖ portrange 1-80
- ❖ tcp portrange 1-80

- กรณีมีหลายเงื่อนไขสามารถใช้ and or ได้ เช่น host 10.3.1.1 or host 10.3.1.2, port 20 or port 21, udp src port 68 and udp dst port 67 เป็นต้น
- กรณีต้องการระบุตำแหน่งของเงื่อนไขลงไปเพื่อให้ได้เฉพาะข้อมูลที่ต้องการ

- ◆ `icmp[0]==8` : กรองเฉพาะ Echo Request)
- ◆ `icmp[0]==17` : กรองเฉพาะ Address Mask Request
- ◆ `icmp[0]==8 or icmp[0]==0` : กรองทั้ง Echo Request และ Echo Reply
- ◆ `icmp[0]==3 and not icmp[1]==4` : กรองเฉพาะ ICMP Type 3 (Destination Unreachable) ยกเว้น ICMP Type 3/ Code 4 (Fragmentation Needed and Don't Fragment)



Type = 8 : Echo-request, Type = 0 : Echo-reply

รูปที่ 21 - เฟรม ICMP ที่อยู่ภายใน IP Packet

→ ตัวอย่างเพิ่มเติม

- ◆ `host 161.246.5.100 and not (port 80 or port 25)`
- ◆ `dst port 135 or dst port 445 or dst port 1433 and tcp[tcpflags] & (tcp-syn) != 0 and tcp[tcpflags] & (tcp-ack) = 0 and src net`
- ◆ `ip and (not ip[1] & 0xfc == 0x0) 192.168.0.0/24` (ip[1] คือไบต์ที่ 2)
- ◆ ไม่สามารถใช้ Filter เป็น Range ได้ (เช่น 192.168.1.1 - 192.168.1.50)

Display Filter

ใช้กรองเฉพาะแพ็คเกตที่ต้องการตอนค้นหาข้อมูล ดังนั้นในไฟล์ที่ดักจับที่มีทุกแพ็คเกตจะยังคงมีแพ็คเกตอยู่เหมือนเดิม แค่จำกัดการค้นหาเท่านั้น ข้อดีของการใช้ Display คือ ข้อมูลไม่หายสามารถเก็บข้อมูลได้ทุกแพ็คเกต ตั้งเงื่อนไขเปลี่ยนแปลงได้ในภายหลัง แต่ก็จะมีข้อเสียที่ต้องเล็กคือเปลี่ยนที่เก็บข้อมูล

No.	Field	Value	Delta	Source	Destination
1	http.response.code == 404	00000000	24.6.173.220	69.128.1.1	
2	http.response	00000000	24.6.173.220	69.128.1.1	
3	http.response.code	00000000	24.6.173.220	69.128.1.1	
4	http.response.code.desc	00000000	24.6.173.220	69.128.1.1	
5	http.response.line	00000000	24.6.173.220	69.128.1.1	
6	http.response.phrase	00000000	24.6.173.220	69.128.1.1	
7	http.response.version	00000000	24.6.173.220	69.128.1.1	
8	http.response_for.uri	00000000	24.6.173.220	69.128.1.1	
9	http.response_in	00000000	24.6.173.220	69.128.1.1	
10	http.response_number	095410000	69.4.231.53	24.6.173.220	

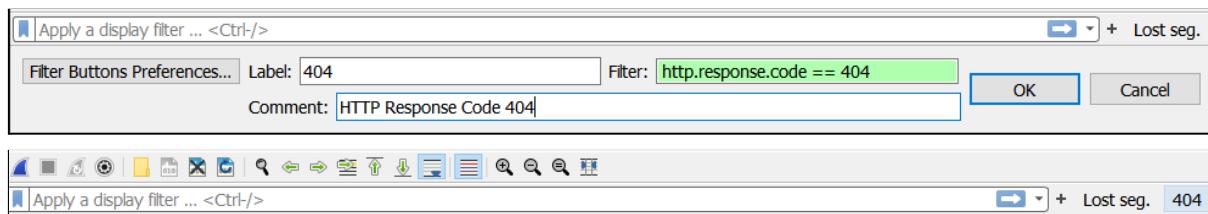
รูปที่ 21 - ช่องกรอก Display Filter ที่มี Auto Complete ในตัว และขึ้นพื้นหลังสีแดงถ้ารูปแบบ Filter ไม่ถูกต้อง

ตัวอย่างการใช้ Display Filter

- กรองเฉพาะโปรโตคอล เช่น arp, ip, tcp, dns, http, icmp
- กรองโปรโตคอลแบบกำหนดฟิลเตอร์ เช่น http.host, ftp.request.command, bootp.option.hostname
- กรองตามคุณลักษณะพิเศษ เช่น tcp.analysis.flags, tcp.analysis.zero_window
- กรองโดยใช้ตัวดำเนินการเปรียบเทียบเพิ่มเติม เช่น
 - ◆ == or eq เช่น ip.src == 10.2.2.2
 - ◆ != or ne เช่น tcp.srcport != 80
 - ◆ > or gt เช่น frame.time_relative > 1 (แสดงแพ็คเกตที่มาเกิน 1 วินาทีจากแพ็คเกตก่อนหน้า)
 - ◆ < or lt เช่น tcp.window_size < 1460
 - ◆ >= or ge เช่น dns.count.answers >= 10
 - ◆ <= or lt เช่น ip.ttl < 10
 - ◆ Contains เช่น http contains "GET"

การเพิ่ม Filter ลงใน Toolbar

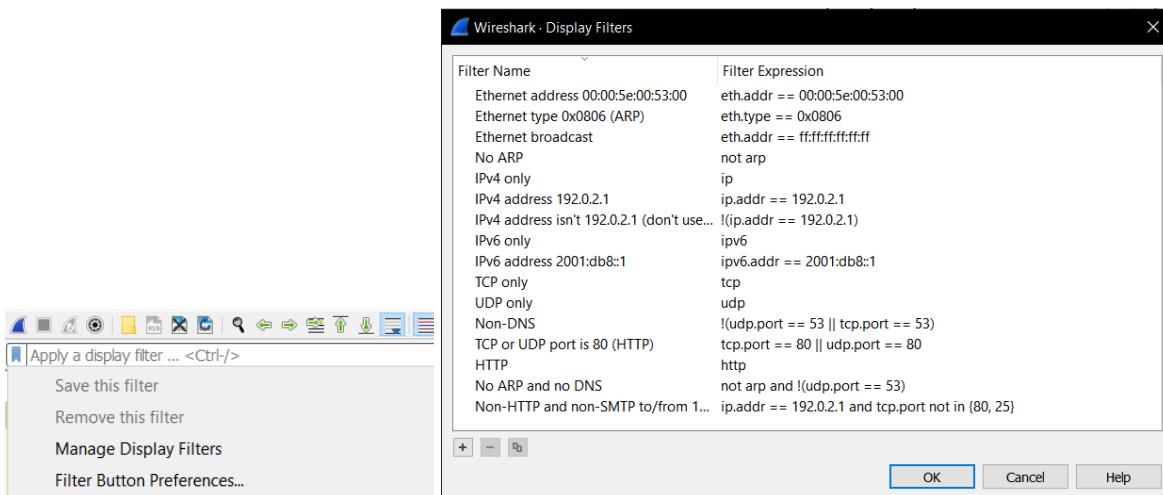
- หากมี Filter ที่ต้องใช้งานเป็นประจำ จะสามารถเพิ่ม Filter นั้นลงไปใน Toolbar ได้
- วิธีเพิ่มสามารถกดที่เครื่องหมาย + ทางด้านขวาสุดของช่องกรอก Display Filter และกรอกรายละเอียดของ Filter ที่ต้องการทำเป็นทางลัด



รูปที่ 22 - ปุ่ม + สำหรับการเพิ่ม Filter ลง Toolbar และผลลัพธ์หลังจากเพิ่ม Filter เรียบร้อยแล้ว

การเพิ่ม Filter ลงใน Bookmark

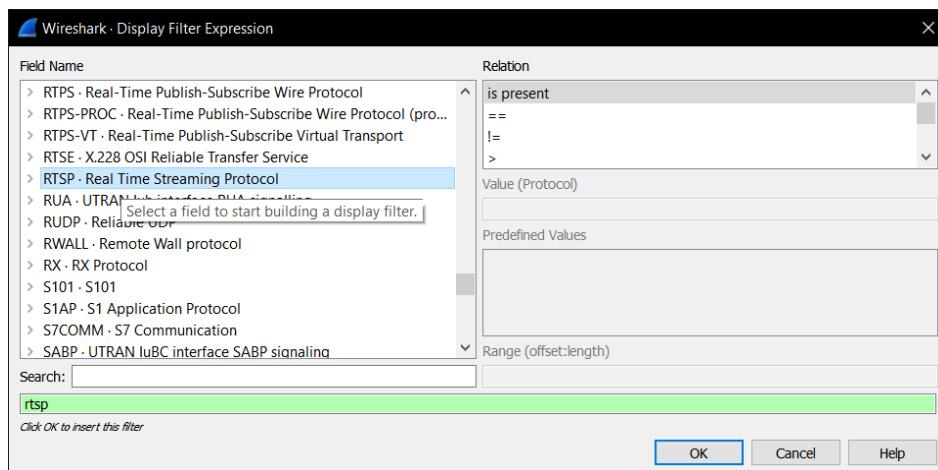
- หากมี Filter ที่ต้องการบันทึกไว้ใช้งานในครั้งถัดไปที่ไม่ได้มีความสำคัญมาก หรือ Filter มีเงื่อนไขขั้นช้อน จะสามารถเพิ่ม Filter นั้นลงไปใน Bookmark ได้
- วิธีเพิ่มสามารถกดที่เครื่องหมายรูปริบบิ้น ทางด้านซ้ายสุดของช่องกรอก Display Filter และเลือก Manage Display Filter หลังจากนั้นกด + เพื่อเพิ่ม



รูปที่ 22 - การเพิ่ม Filter ลงใน Bookmark

Display Filter Expression

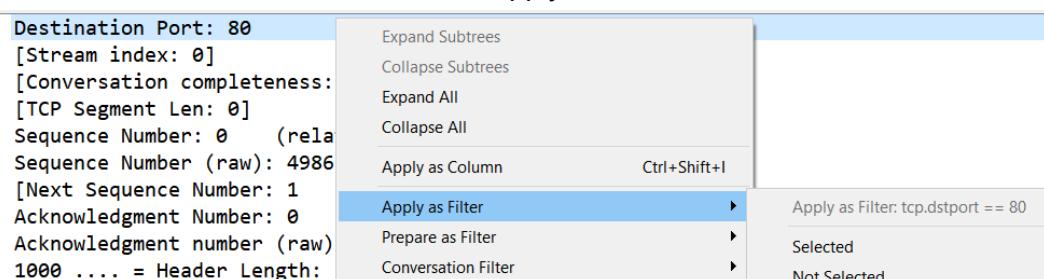
- เป็นเครื่องมือสำหรับช่วยสร้าง Display Filter
- สามารถใช้เครื่องมือนี้ได้โดยการคลิกขวาที่ช่อง Display Filter และเลือก Display Filter Expression



รูปที่ 23 - หน้าต่างช่วยสร้าง Display Filter โดยใช้ Display Filter Expression

Apply as Filter

- เป็นวิธีในการสร้าง Filter โดยเลือกฟิลเตอร์ที่ต้องการจะใช้จากหน้าต่าง Packet Detail
- เมื่อได้ฟิลเตอร์ที่ต้องการแล้ว คลิกขวาเลือก Apply as Filter



รูปที่ 24 - การสร้าง Filter จากฟิลเตอร์ที่ต้องการ

[ACT_04] Filter101

Guideline

- ทำการเชื่อมต่ออินเทอร์เน็ตสถาบัน และเริ่มดักจับแพคเกต
- ให้ทำการเคลียร์ DNS โดยการพิมพ์ `ipconfig /flushdns` ใน CMD
- Ping ไปยังเว็บไซต์ <https://www.kmitl.ac.th>
- เพิ่ม ICMP ลงใน Toolbar Filter และเรียกใช้
- สังเกตส่วน Packet Detail ทำการ Apply as Filter ในแท็บ Type ของแพคเกตที่เป็น Ping Request
- ทดลองเพิ่ม DNS เป็น Filter ลงใน Bookmark

Problem

- ไอพีแอดเดรสของเว็บสถาบันคือ
- Filter สำหรับใช้กรอง Ping Request คือ
- เมื่อทำการกรองเหลือแค่ Ping Request และจะขึ้นหนังหนาดกีแพคเกต (ถ้าหากใช้ CMD)

4. ในไฟล์ที่ดักแพ็คเกตได้มีการใช้งานโปรโตคอล DNS หรือไม่
5. แคปปูรูปหน้าจอให้เห็น Bookmark Filter และ Toolbar Filter

Bookmark & Toolbar Filter

[ACT_05] HTTP vs Port80

Guideline

1. เปิดไฟล์ [http-wiresharkdownload101.pcapng](#) และใช้ Filter เป็น `tcp.port == 80`
2. เปลี่ยน Filter เป็น `HTTP`

Problem

1. Filter ทั้งสองแบบต่างกันอย่างไร
-
-
-

[ACT_06] DNS Filter

Problem

1. ไฟล์ [mybackground101.pcapng](#) ถ้าหากต้องการให้ Filter เหลือแค่ DNS `api.memeo.info`, `api.memeo.com` และ `memeo.info` ซึ่งอยู่ที่ 216.115.74.x ต้องใช้ Filter อย่างไร
-

[HW_03] POST Method

Problem

1. ในไฟล์ [http-sfgate101.pcapng](#) ที่ใช้ Method POST ไปยัง `extras.sfgate.com` คือแพ็คเกตที่
2. จากข้อ 1 ใช้ Filter อะไรเพื่อกรองให้เหลือแค่ Method POST
3. จากข้อ 1 ใช้ Filter อะไรเพื่อกรองให้แสดงแพ็คเกตดังกล่าวเท่านั้น
4. จากไฟล์ดังกล่าวแพ็คเกตที่ใช้เวลามากที่สุด ใช้เวลาทั้งหมด วินาที (ตอบทศนิยม 2 ตำแหน่ง) ชื่องทำการ (คำตอบยาว 3 ตัวอักษร) ไฟล์
(ความยาว 16 ตัวอักษร)

5. จากไฟล์ดังกล่าวแพ็คเกตที่ Request ไป www.sfgate.com/feedback คือแพ็คเกตที่.....

ข้อควรระวังการตั้งเงื่อนไข Filter

- ✗ ip.addr != 10.2.2.2 จะแสดงทุกแพ็คเก็ต
- ✓ !ip.addr == 10.2.2.2
- ✗ !tcp.flags.syn == 1 จะแสดงโปรโตคอลอื่น ๆ เมื่อ้อนเดิม
- ✓ !tcp.flags.syn != 1
- ⚠ (tcp.port==80 && ip.src==10.2.2.2) || tcp.flags.syn==1
- ⚠ tcp.port==80 && (ip.src==10.2.2.2 || tcp.flags.syn==1)

สีพื้นหลังของ Display Filter

- สีแดง : Syntax ผิด
- สีเขียว : ใช้ได้ตามปกติ
- สีเหลือง : เตือนเนื่องจาก Syntax ถูกต้องแต่อาจไม่ได้ผลตามที่ต้องการ

[ACT_07] Contains in Filter

Note

- Contains เหมาะกับการใช้หาคำ
- สามารถใช้ (?i) เพื่อแทนตัวอักษรตัวเล็ก หรือตัวใหญ่ก็ได้

Guideline

1. เปิดไฟล์ http-pictures101.pcapng และใส่ Filter เป็น frame contains "sombrero"
2. เปลี่ยน Filter เป็น frame matches "(?i)(sombrero|football)"

Problem

1. สังเกตความต่างของ Filter ทั้ง 2 แบบ
.....
.....
.....

[ACT_08] Match in Filter

Note

- สามารถใช้ Regular Expression ช่วยได้

Guideline

1. เปิดไฟล์ http-pictures101.pcapng
2. ทดลองตั้งค่า Filter เป็น http.request.uri matches "baby.{1,3}smiling"
3. เปลี่ยน {1,3} เป็น {1,20}

Problem

1. หลังจากเปลี่ยน {1,3} เป็น {1,20} แตกต่างกันอย่างไร
.....
.....
.....