

## Lab 4: Basics Wireshark

### จุดประสงค์การทดลอง

- เพื่อศึกษาวิธีดักจับข้อมูลเชิงรหัสผ่านที่ส่งผ่านเว็บไซต์ http ด้วยโปรแกรม Wireshark

### บทนำ

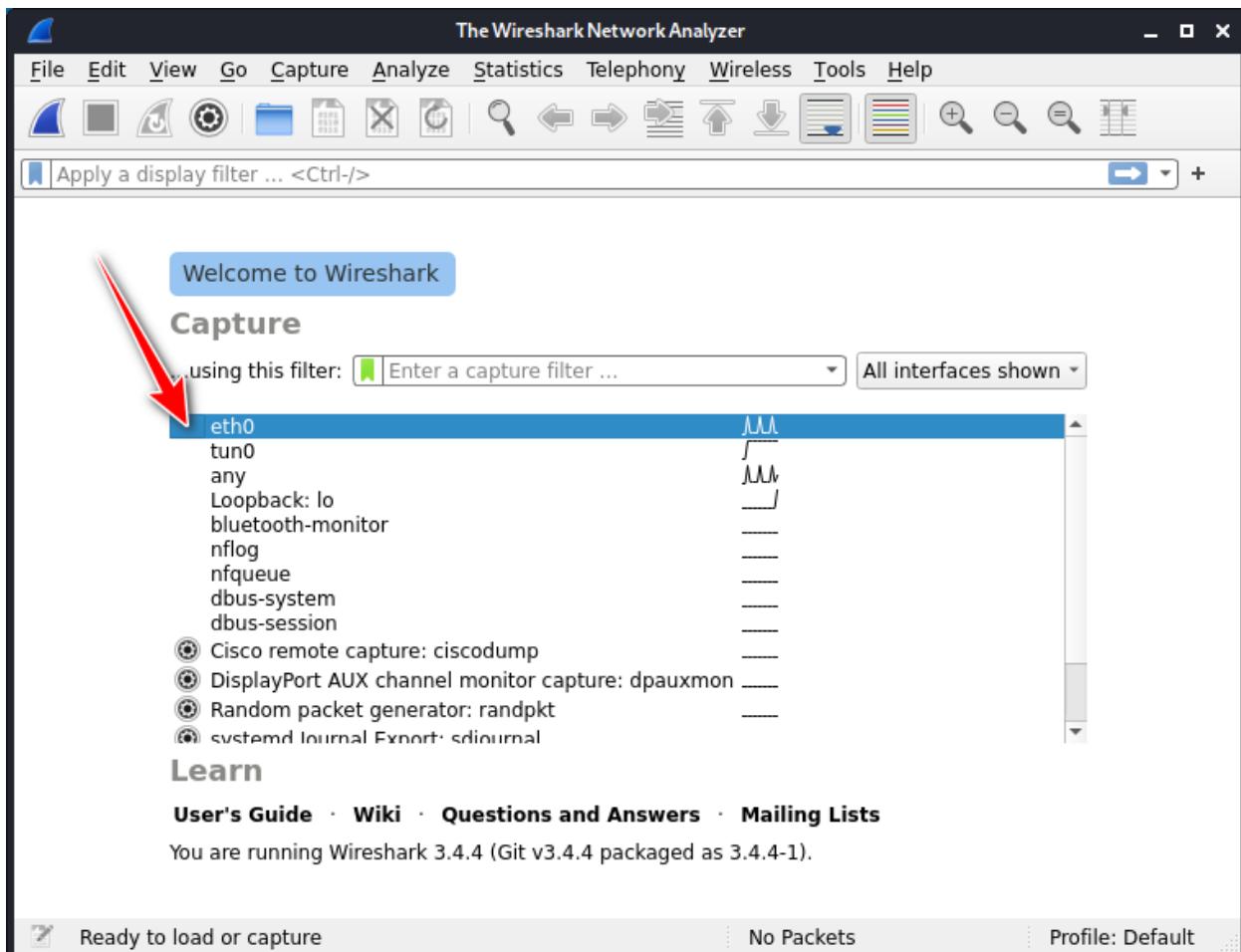
Wireshark เป็นเครื่องมือวิเคราะห์ Packet แบบโอเพ่นซอร์สที่ใช้สำหรับการวิเคราะห์การทำงานของไฟร์wall การตรวจสอบปัญหาของระบบเครือข่าย

### เครื่องมือ

Kali Linux

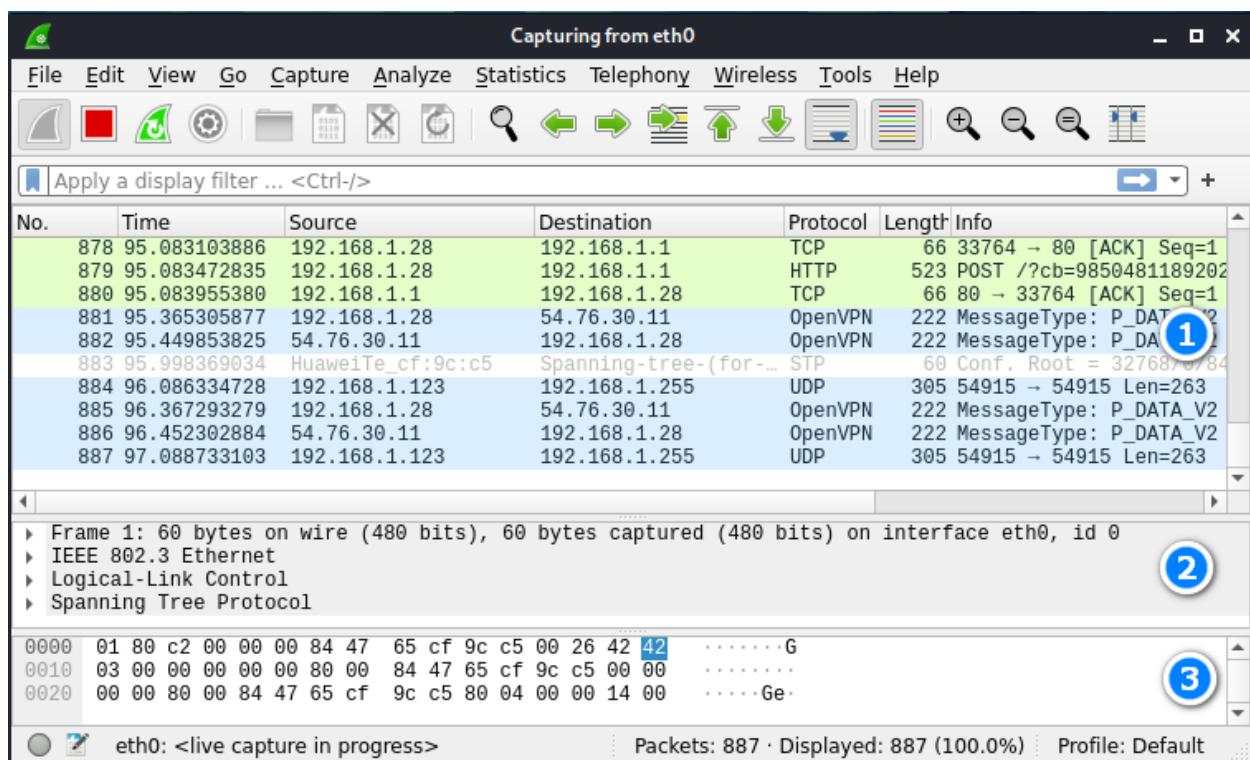
### ขั้นตอนการทดลอง

- เปิดโปรแกรม Wireshark จากหัวข้อ Sniffing & Spoofing โปรแกรมจะถามว่าต้องการใช้อินเทอร์เฟซใดในการจับแพ็กเก็ตสำหรับแล็บนี้เราจะใช้อินเทอร์เฟซ "eth0" (สังเกตว่าจะมี Traffic)



จากนั้นจะพบรากบหน้าต่างที่แบ่งออกเป็น 3 ส่วน

- ส่วนบนสุดจะแสดงรายการแพ็คเก็ตที่จับได้เป็นตาราง ซึ่งจะประกอบด้วยข้อมูล เช่น หมายเลขแพ็คเก็ต ต้นทางและปลายทางของแพ็คเก็ต เวลาที่จับได้ และโพรโทคอลของแพ็คเก็ต เป็นต้น
- ส่วนที่สองอธิบายการแสดงข้อมูลตามลำดับขั้นที่รวมอยู่ในแพ็คเก็ต สามารถขยายส่วนต่างๆ เพื่อดูข้อมูลที่แตกต่างกันเกี่ยวกับแต่ละแพ็คเก็ตเฉพาะได้
- ส่วนที่สามจะแสดงข้อมูลแพ็คเก็ตที่เข้ารหัส



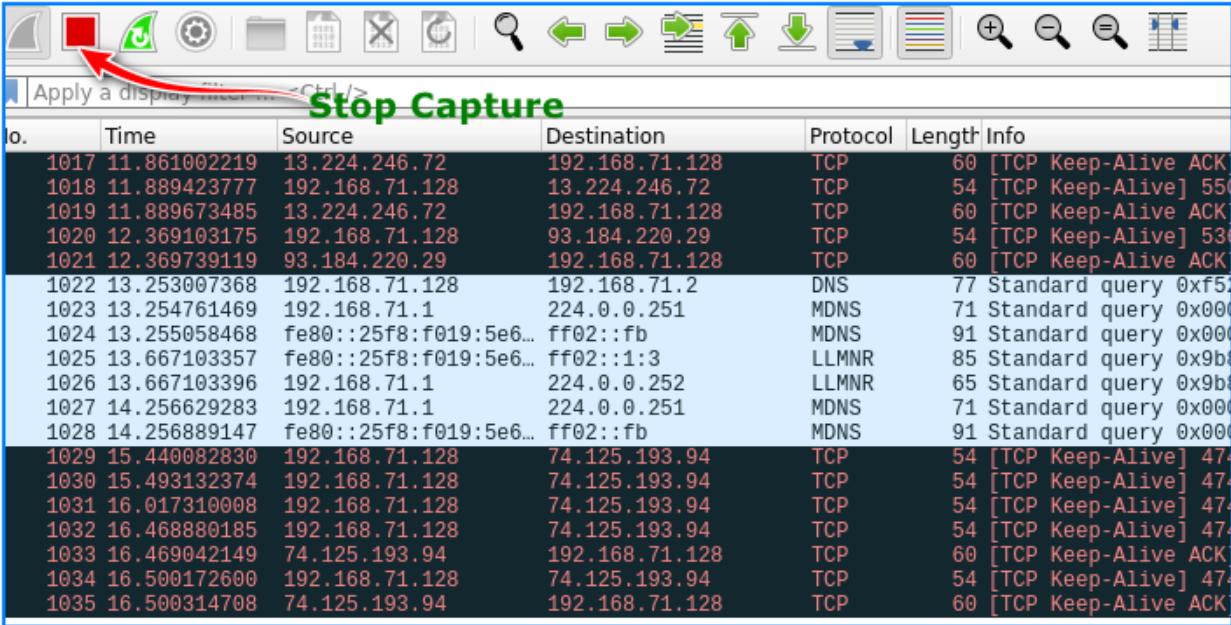
2. ใช้ Browser firefox ในเครื่อง Kali เข้าเว็บไซต์ <http://testphp.vulnweb.com/login.php> จะพบหน้าเข้าสู่ระบบสังเกตแม่กุญแจที่มีเส้นสีแดงที่ด้านซ้ายบนซึ่งระบุว่าหน้านี้กำลังสื่อสารผ่านโพรโทคอล http ซึ่งหมายความว่าข้อมูลใดๆ ที่ส่งมาที่นี่จะไม่ได้รับการเข้ารหัส

If you are already registered please enter your login information below:

Username :	<input type="text"/>
Password :	<input type="password"/>
<input type="button" value="login"/>	

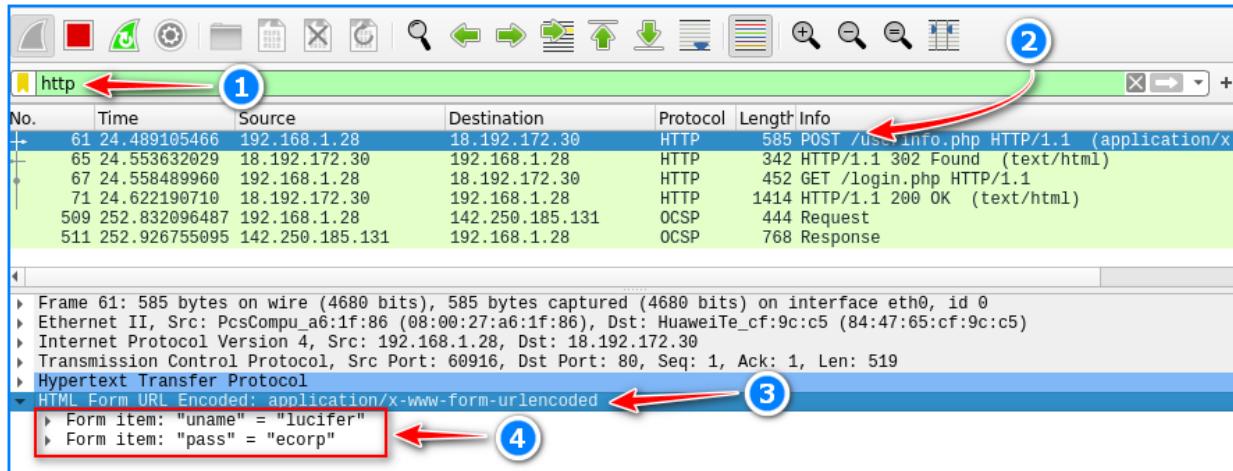
You can also signup here.  
Signup disabled. Please use the username **test** and the password **test**.

ทดลองกรอก Username และ Password แบบสุ่ม จากนั้นให้กดปุ่ม Stop Capturing Packets



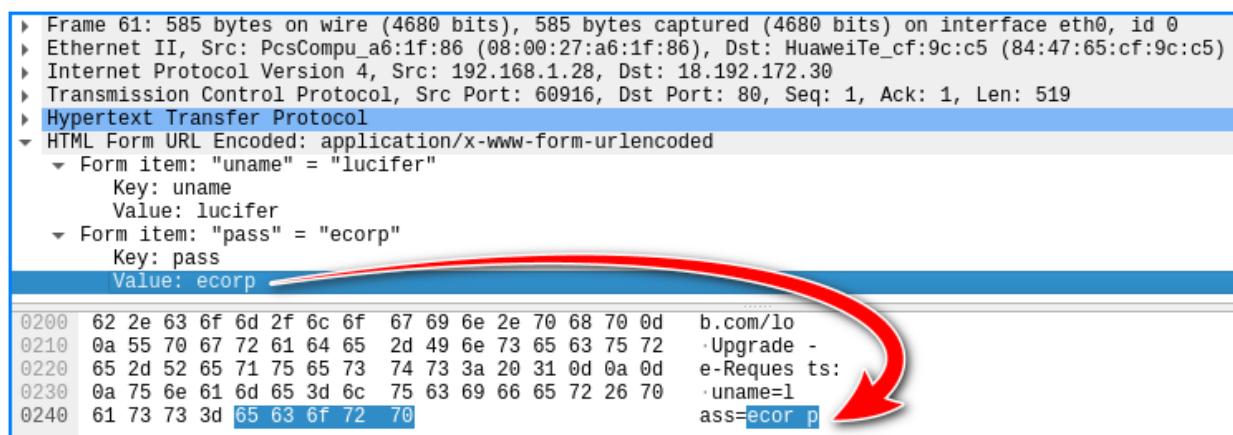
No.	Time	Source	Destination	Protocol	Length	Info
1017	11.861002219	13.224.246.72	192.168.71.128	TCP	60	[TCP Keep-Alive ACK]
1018	11.889423777	192.168.71.128	13.224.246.72	TCP	54	[TCP Keep-Alive] 550
1019	11.889673485	13.224.246.72	192.168.71.128	TCP	60	[TCP Keep-Alive ACK]
1020	12.369103175	192.168.71.128	93.184.220.29	TCP	54	[TCP Keep-Alive] 530
1021	12.369739119	93.184.220.29	192.168.71.128	TCP	60	[TCP Keep-Alive ACK]
1022	13.253007368	192.168.71.128	192.168.71.2	DNS	77	Standard query 0xf51
1023	13.254761469	192.168.71.1	224.0.0.251	MDNS	71	Standard query 0x000
1024	13.255058468	fe80::25f8:f019:5e6...	ff02::fb	MDNS	91	Standard query 0x000
1025	13.667103357	fe80::25f8:f019:5e6...	ff02::1:3	LLMNR	85	Standard query 0x9b1
1026	13.667103396	192.168.71.1	224.0.0.252	LLMNR	65	Standard query 0x9b1
1027	14.256629283	192.168.71.1	224.0.0.251	MDNS	71	Standard query 0x000
1028	14.256889147	fe80::25f8:f019:5e6...	ff02::fb	MDNS	91	Standard query 0x000
1029	15.440082830	192.168.71.128	74.125.193.94	TCP	54	[TCP Keep-Alive] 47
1030	15.493132374	192.168.71.128	74.125.193.94	TCP	54	[TCP Keep-Alive] 47
1031	16.017310008	192.168.71.128	74.125.193.94	TCP	54	[TCP Keep-Alive] 47
1032	16.468880185	192.168.71.128	74.125.193.94	TCP	54	[TCP Keep-Alive] 47
1033	16.469042149	74.125.193.94	192.168.71.128	TCP	60	[TCP Keep-Alive ACK]
1034	16.500172600	192.168.71.128	74.125.193.94	TCP	54	[TCP Keep-Alive] 47
1035	16.500314708	74.125.193.94	192.168.71.128	TCP	60	[TCP Keep-Alive ACK]

ในช่อง Apply a display filter ให้กรอกคำว่า http เพื่อให้โปรแกรม Wireshark แสดงข้อมูลเฉพาะไฟล์ protocol http จากนั้นกด Enter จะสังเกตเห็นว่าจำนวนแพ็กเก็ตที่จับได้ลดลงอย่างมาก เหลือเฉพาะข้อมูลที่เป็นไฟล์ protocol http เท่านั้น (ข้อมูลของ Destination อาจจะไม่ตรงกับตัวอย่าง)



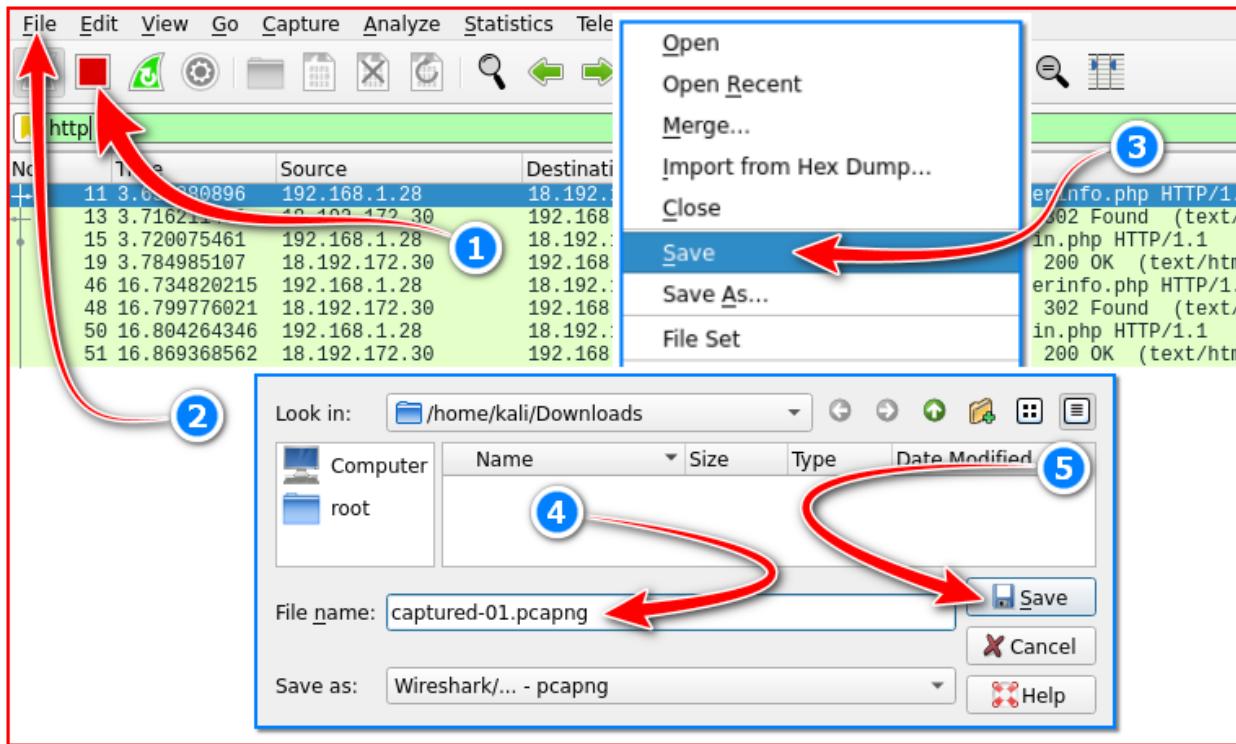
ค้นหาแพ็กเก็ตที่มี POST รวมอยู่ในส่วนข้อมูล (2) เมื่อพับแล้วให้เลือกแพ็กเก็ตนี้ จากนั้น ดูที่บานหน้าต่างที่สองและส่วนที่เรียกว่า Hypertext Transfer Protocol (http) คลิกที่ส่วนนี้และขยายเพื่อดูข้อมูลที่มี (3) จากนั้นคลิกที่ส่วน URL Encoded ของแบบฟอร์ม HTML เพื่อขยายข้อมูลภายในแท็บนี้ จากนั้นจะเห็นชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ที่ป้อนในแบบฟอร์มบนเว็บไซต์ http (4)

- เราสามารถดูข้อมูลของชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในรูปแบบเลขฐาน 16 (Hex code) ได้ในหน้าต่างที่ 3

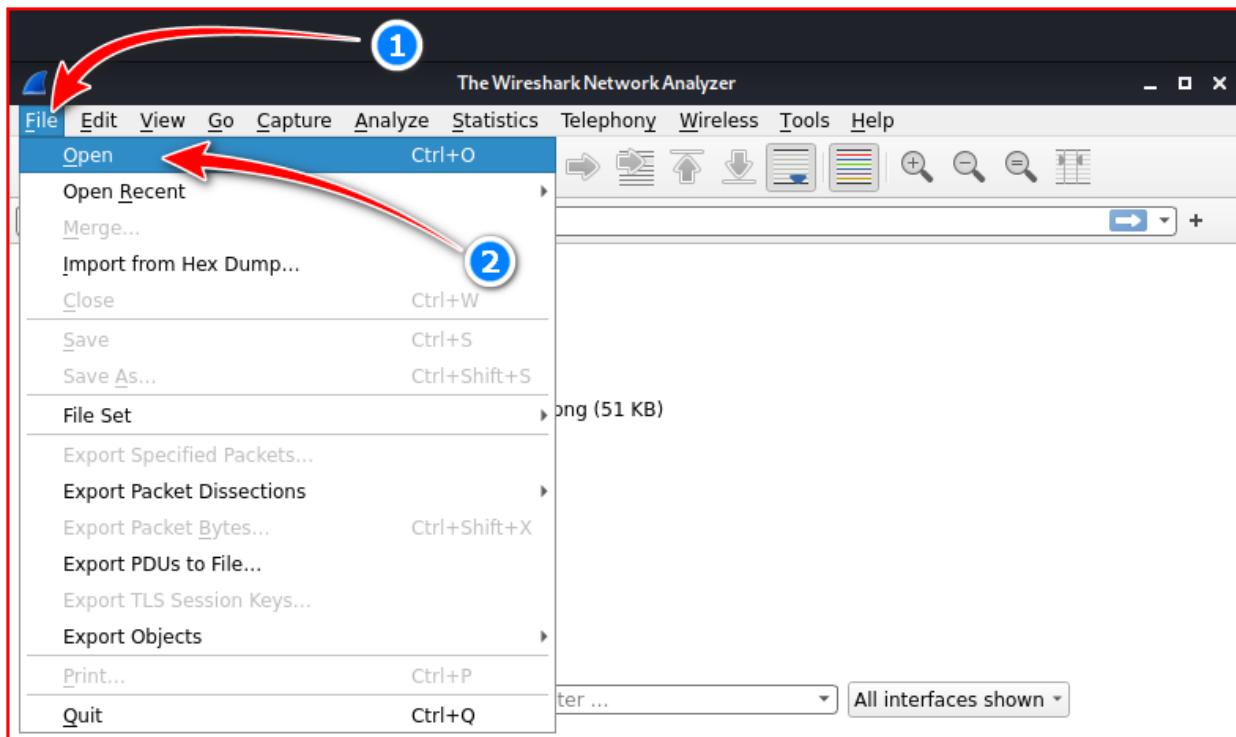


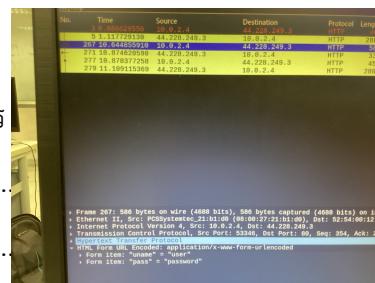
4. โปรแกรม Wireshark สามารถ Save เพื่อส่งไปให้เครื่องทำการวิเคราะห์ได้ด้วยขั้นตอนตามภาพ

- ขั้นตอนการ Save ข้อมูล

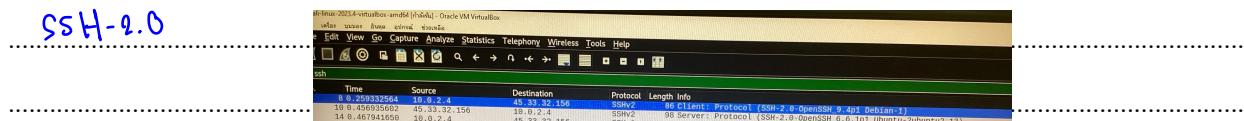


- ขั้นตอนการ Import ข้อมูล



บันทึกผลIP Address ของ <http://testphp.vulnweb.com/login.php> คือ เบอร์อะไร44.228.249.3

ทดลองใช้ ssh ไปที่ scanme.nmap.org และใช้ Wireshark วิเคราะห์ว่าเครื่อง scanme.nmap.org ใช้ SSH version อะไรในการให้บริการ

SSH-2.0

ให้นักศึกษาสรุปความรู้ที่ได้จากการทดลอง Lab 4 - Basic Wireshark นี้

ทดลองใช้ Wireshark ในการ分析 SSH ในการ分析ว่าเราสามารถ intercept packet ที่ต้องการจะมีลักษณะ filter ใด capture แล้ว save ใน Wireshark ของเราลองใช้ port ของ google คือ nslookup www.google.ca 8.8.8.8 ที่ port 53ดูใน protocol TLSv1.3