Lab 4: Basics Wireshark

จุดประสงค์การทดลอง

1. เพื่อศึกษาวิธีดักจับชื่อผู้ใช้และรหัสผ่านที่ส่งผ่านเว็บไซต์ http ด้วยโปรแกรม Wireshark

บทนำ

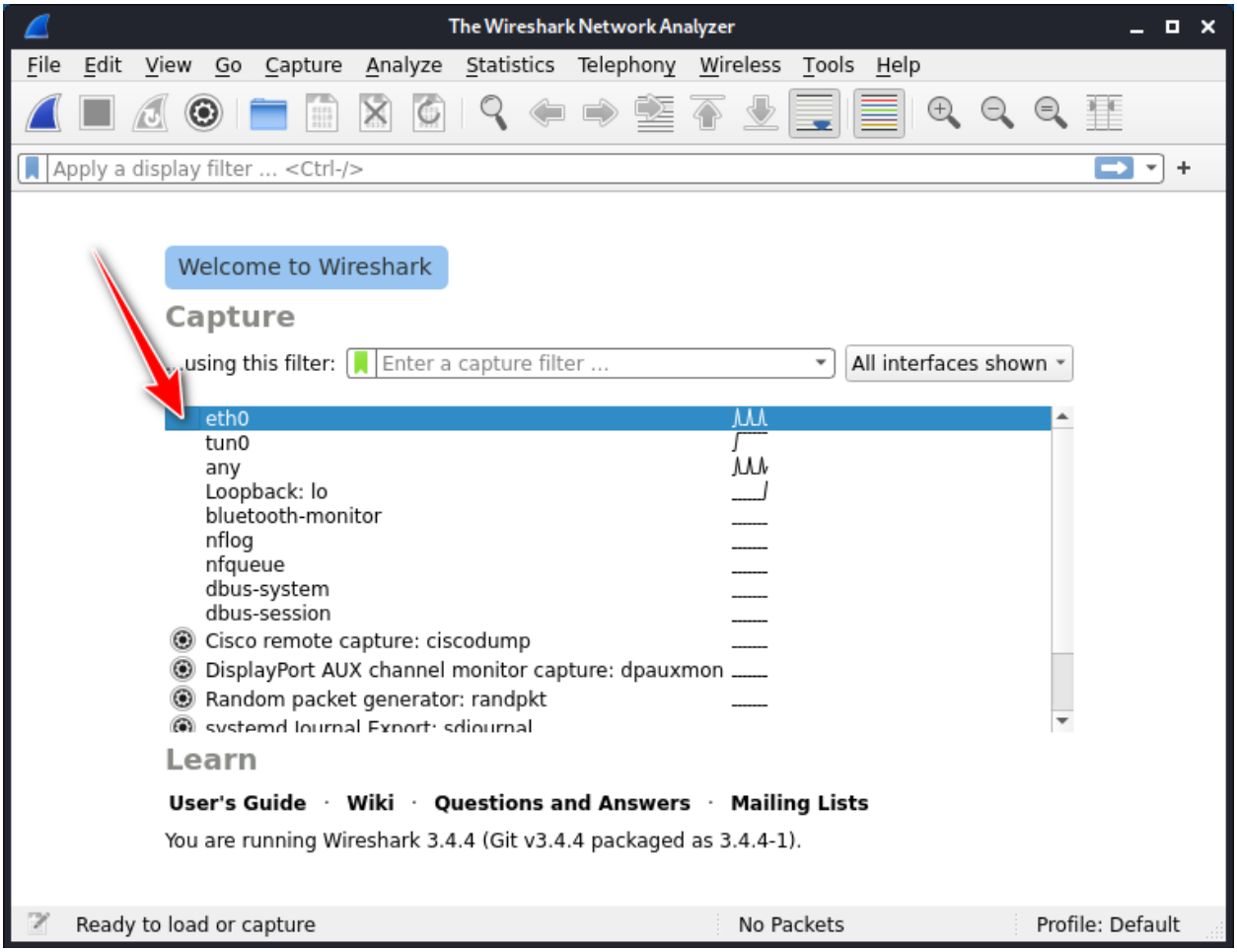
Wireshark เป็นเครื่องมือวิเคราะห์ Packet แบบโอเพ่นซอร์สที่ใช้สำหรับการวิเคราะห์การทำงานของโพรโทคอล การตรวจสอบปัญหาของระบบเครือข่าย

เครื่องมือ

Kali Linux

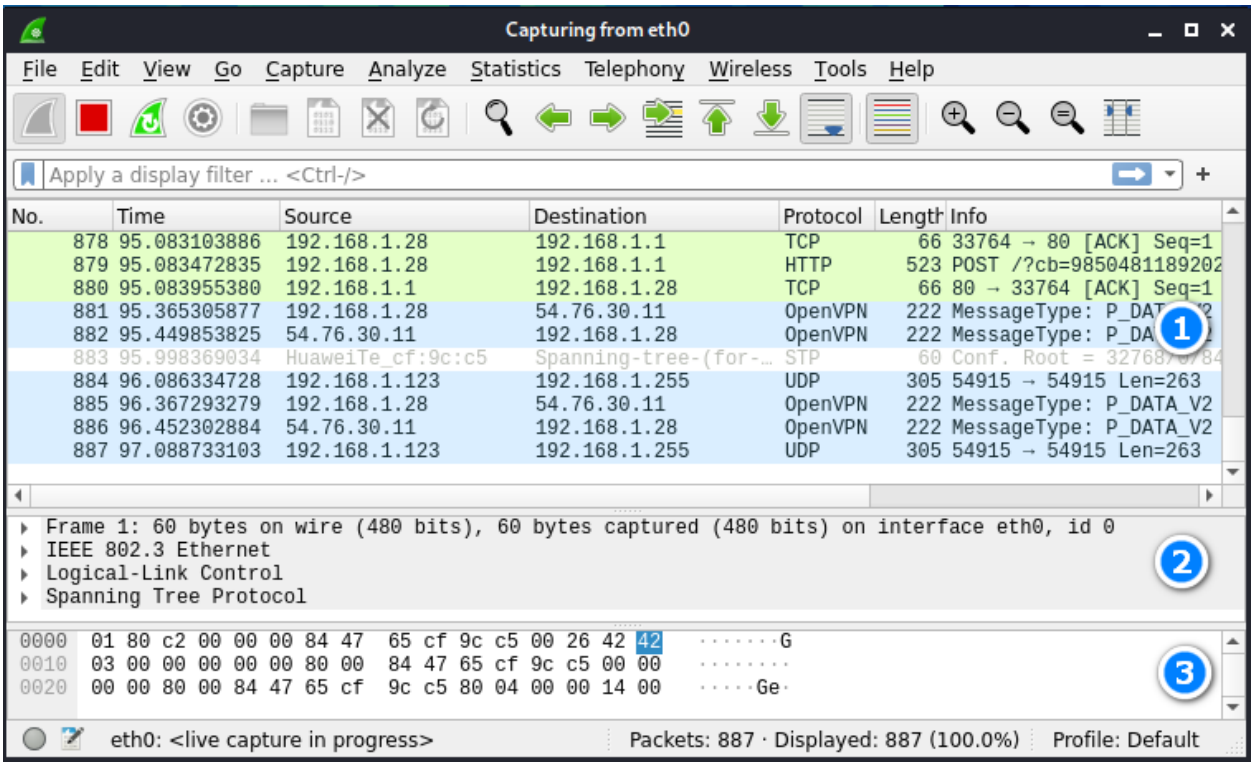
ขั้นตอนการทดลอง

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

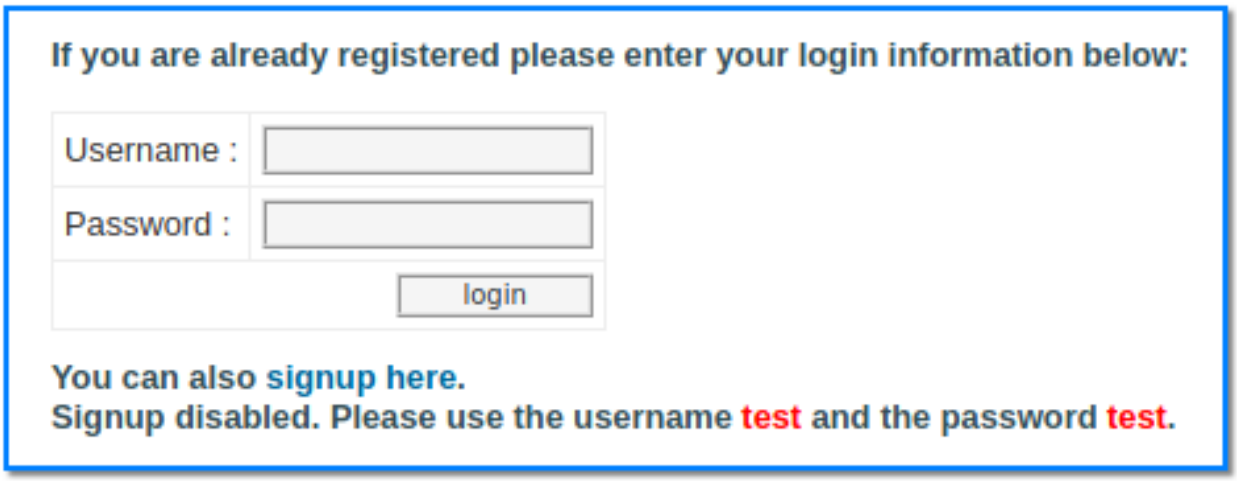


จากนั้นจะพบกับหน้าต่างที่แบ่งออกเป็น 3 ส่วน

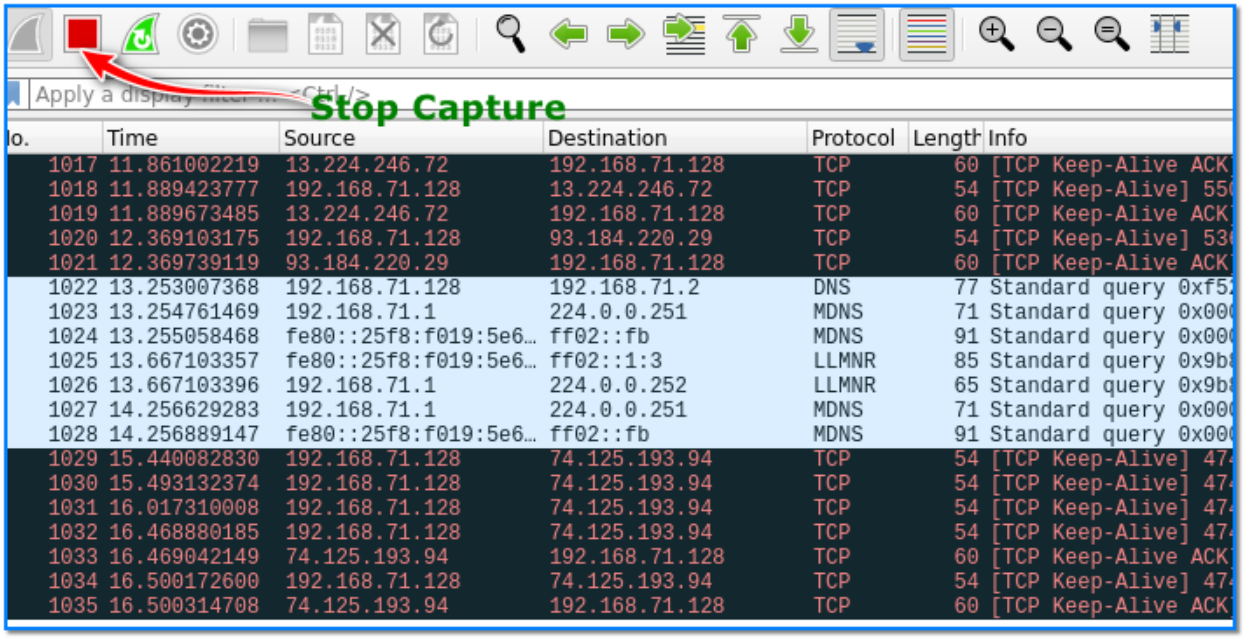
- ส่วนบนสุดจะแสดงรายการแพ็กเก็ตที่จับได้เป็นตาราง ซึ่งจะประกอบด้วยข้อมูล เช่น หมายเลขแพ็กเก็ต ต้นทางและปลายทางของแพ็กเก็ต เวลาที่จับได้ และโพรโทคอลของแพ็กเก็ต เป็นต้น
- ส่วนที่สองอธิบายการแสดงข้อมูลตามลำดับชั้นที่รวมอยู่ในแพ็กเก็ต สามารถขยายส่วนต่างๆ เพื่อดูข้อมูลที่แตกต่างกันเกี่ยวกับแต่ละแพ็กเก็ตเฉพาะได้
- ส่วนที่สามจะแสดงข้อมูลแพ็กเก็ตที่เข้ารหัส



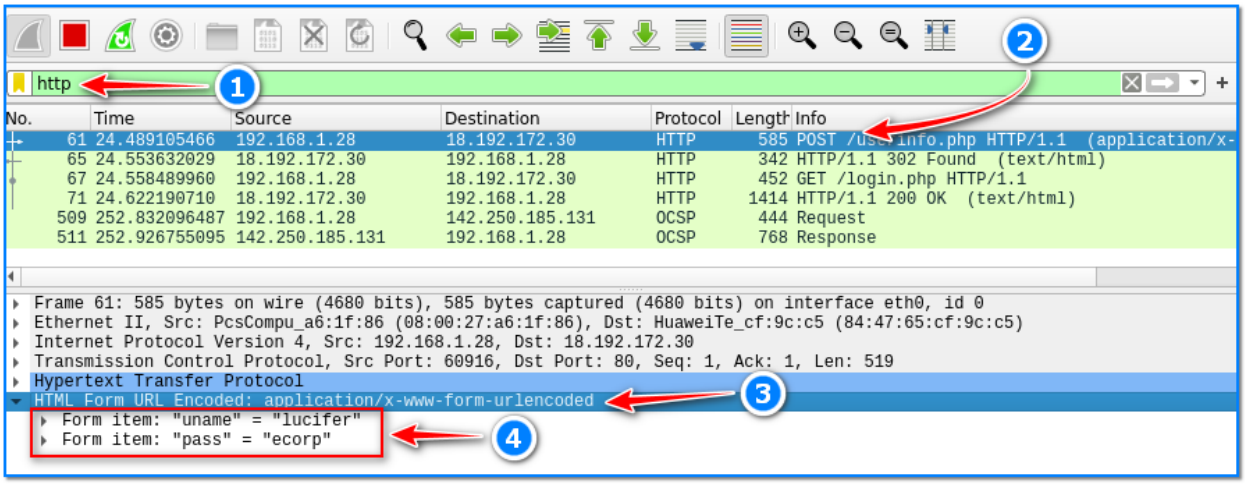
2. ใช้ Browser firefox ในเครื่อง Kali เข้าเว็บไซต์ http://testphp.vulnweb.com/login.php จะพบหน้าเข้าสู่ระบบสังเกตแม่กุญแจที่มีเส้นสีแดงที่ด้านซ้ายบนซึ่งระบุว่าหน้านี้กำลังสื่อสารผ่านโพรโทคอล http ซึ่งหมายความว่าข้อมูลใดๆ ที่ส่งมาที่นี่จะไม่ได้รับการเข้ารหัส



ทดลองกรอง Username และ Password แบบสุ่ม จากนั้นให้กดปุ่ม Stop Capturing Packets

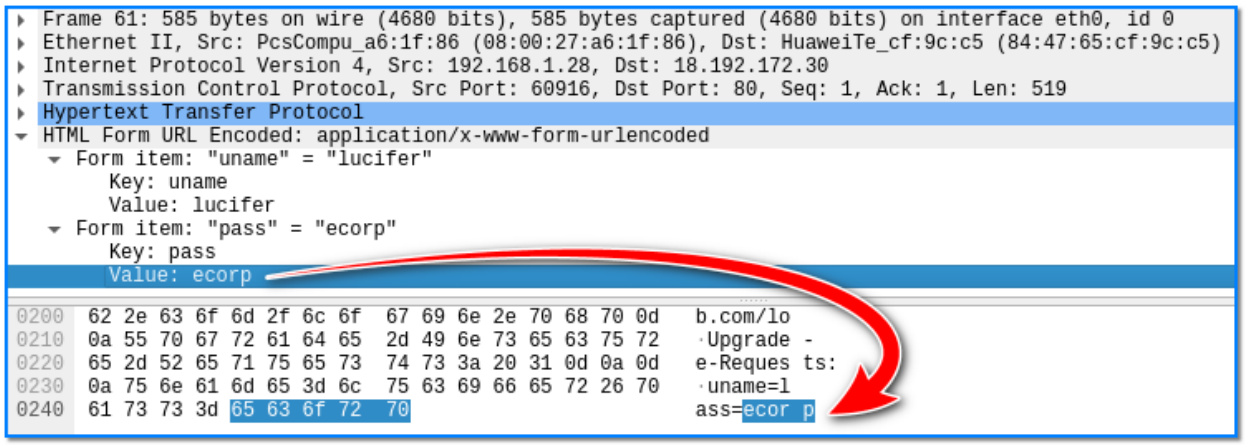


ในช่อง Apply a display filter ให้กรอกคำว่า http เพื่อให้โปรแกรม Wireshark แสดงข้อมูลเฉพาะโพรโทคอล http จากนั้นกด Enter จะสังเกตเห็นว่าจำนวนแพ็กเก็ตที่จับได้ลดลงอย่างมาก เหลือเฉพาะข้อมูลที่เป็นโพรโทคอล http เท่านั้น (ข้อมูลของ Destination อาจจะไม่ตรงกับตัวอย่าง)



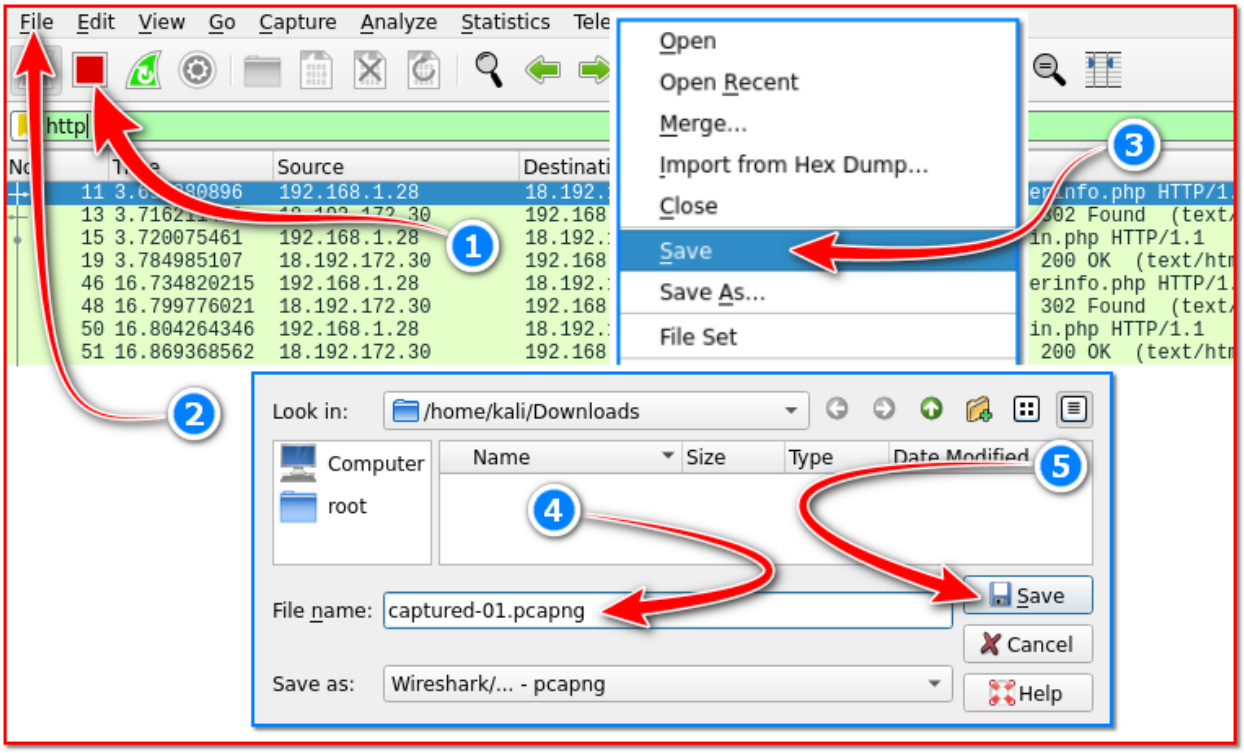
ค้นหาแพ็กเก็ตที่มี POST รวมอยู่ในส่วนข้อมูล (2) เมื่อพบแล้วให้เลือกแพ็กเก็ตนี้ จากนั้น ดูที่บานหน้าต่างที่สองและส่วนที่เรียกว่า Hypertext Transfer Protocol (http) คลิกที่ส่วนนี้และขยายเพื่อดูข้อมูลที่มี (3) จากนั้นคลิกที่ส่วน URL Encoded ของแบบฟอร์ม HTML เพื่อขยายข้อมูลภายในแท็บนี้ จากนั้นจะเห็นชื่อผู้ใช้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

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

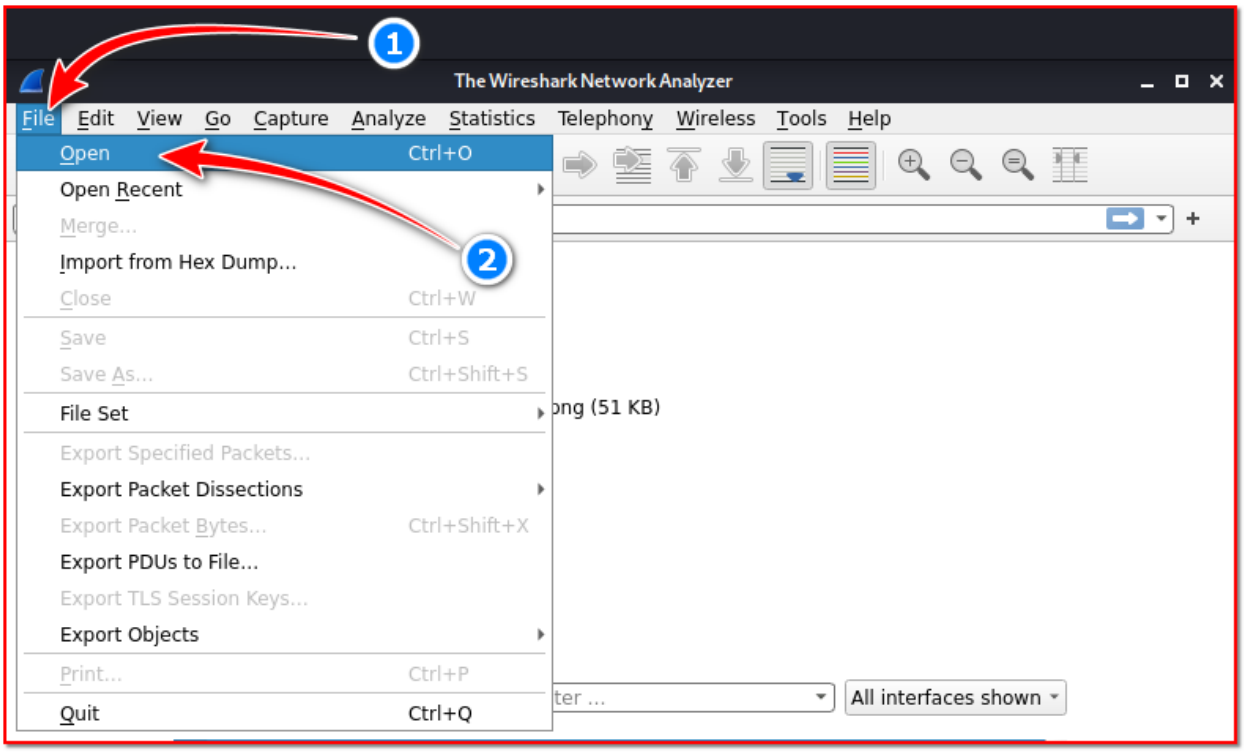


4. โปรแกรม Wireshark สามารถ Save เพื่อส่งไปให้เครื่องทำการวิเคราะห์ได้ด้วยขั้นตอนตามภาพ

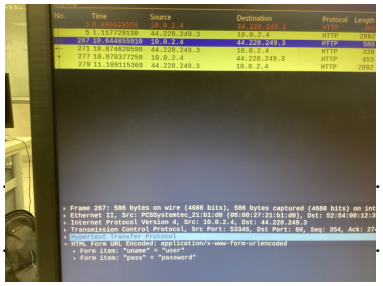
- ขั้นตอนการ Save ข้อมูล



- ขั้นตอนการ Import ข้อมูล



บันทึกผล

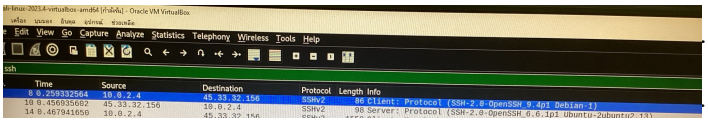


IP Address ของ http://testphp.vulnweb.com/login.php คือ เบอร์อะไร

44.228.249.3

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

ได้รู้วิธีใช้ wireshark และการใช้ SSH ในการเข้าถึงอุปกรณ์เพื่อดู packet ที่ส่งไป
ของอุปกรณ์ได้รู้วิธีใช้ filter และ capture หรือ Save ใน wireshark ด้วย
และได้รู้ port ของคำสั่ง nslookup www.google.com 8.8.8.8 ใช้ port 53
ดูผ่าน Protocol TLSv1.3