การใช้งาน Wireshark เบื้องต้น

งานนี้จะแนะนำนักศึกษาให้รู้จักกับ network analyzer ที่ฟรี สามารถดาวน์โหลดมาใช้งานได้โดยไม่เสียค่าใช้จ่าย ซึ่ง Network analyzers เป็นเครื่องมือที่มีประโยชน์มากในการสร้างความเข้าใจในเรื่องการสื่อสารข้อมูลและเครือข่าย โดยจะสแกนลิงก์ข้อมูลต่างๆ ที่เชื่อมต่อกับคอมพิวเตอร์และสร้างมุมมองของแพ็กเก็ต (packets) ต่างๆ ขณะที่มีการไหลผ่านคอมพิวเตอร์เครื่องนั้น เราจะใช้ Wireshark ซึ่งก็เป็น sniffer ตัวหนึ่งที่สามารถดาวน์โหลดได้ฟรีจาก www.wireshark.org

เป้าหมายของงานชิ้นนี้มี 2 ประเด็น คือ (1) เพื่อให้ นศ. ได้ทำความรู้จักและสามารถใช้งาน network analyzer และ (2) เพื่อให้ นศ. สามารถเห็นแพ็กเก็ตข้อมูลที่มีการส่งรับจริงและทำให้สามารถเข้าใจหัวข้อที่สอนในชั้นเรียนได้จากเครือข่ายที่ใช้งานอยู่จริง

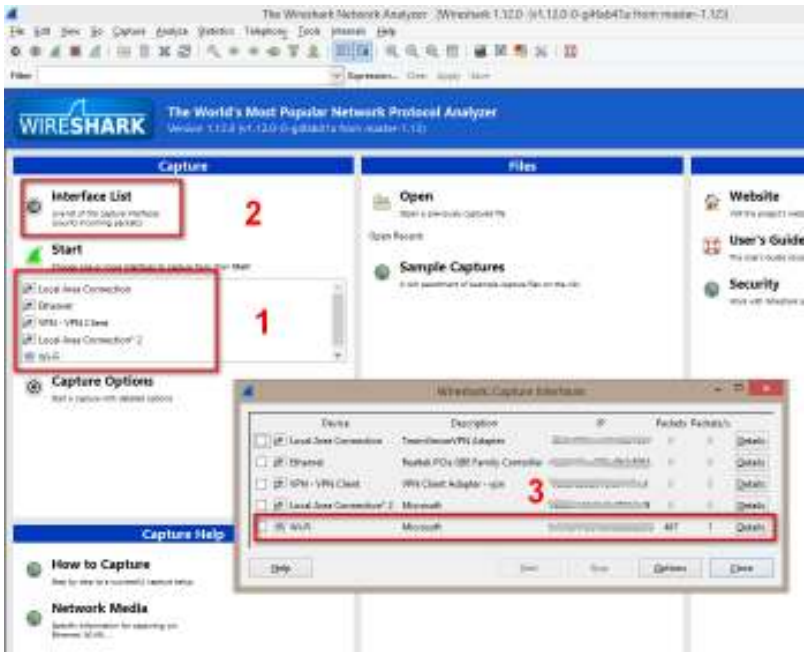
การใช้งานโปรแกรมนี้นั้นง่ายและซับซ้อนพอๆ กับการใช้งานโปรแกรมทั่วไป เช่น word processor หรือ spreadsheet

จงปฏิบัติตามคำสั่งดังต่อไปนี้ให้ครบถ้วน

ส่งงานภายในวันอังคาร ที่ 11 เดือน พฤศจิกายน พ.ศ. 2557 ก่อน 16.00 น. ณ ห้อง T-211 (กล่องรับงาน)

การใช้งาน Wireshark เบื้องต้น

1. ดาวน์โหลดไฟล์จาก www.wireshark.org, และติดตั้งโปรแกรมบนคอมพิวเตอร์ หลังจากนั้นเปิดโปรแกรมขึ้นมา
2. ในเมนูจะมี features ต่างๆมากมาย แต่ในงานนี้เราจะสนใจ options ต่างๆ ที่อยู่ใน “Capture” เท่านั้น หากสนใจเมนูต่างๆ สามารถอ่านรายละเอียดเพิ่มเติมได้ที่ http://www.wireshark.org/download/docs/user-guide-us.pdf.
3. เพื่อที่จะ capture packets ให้เลือก Start โดยคอมพิวเตอร์ที่ใช้อยู่นั้นอาจจะมีการ interface ที่หลากหลายเช่น wireless card หรือ wired card ดังรูปที่ 1. ในกรอบหมายเลข (1) โดย นศ. ควรเลือกการ Interface ที่กำลังใช้งานเชื่อมต่อ Internet อยู่ ณ ขณะนั้น จาก Interface List ดังรูปที่ 1. ในกรอบหมายเลข (2) จากนั้นเลือก Start จาก รูปที่ 1. ในกรอบหมายเลข (3) เพื่อที่เริ่มทำการ capture แพ็กเก็ตทุกแพ็กเก็ตที่วิ่งผ่าน Interface ที่เราเลือก

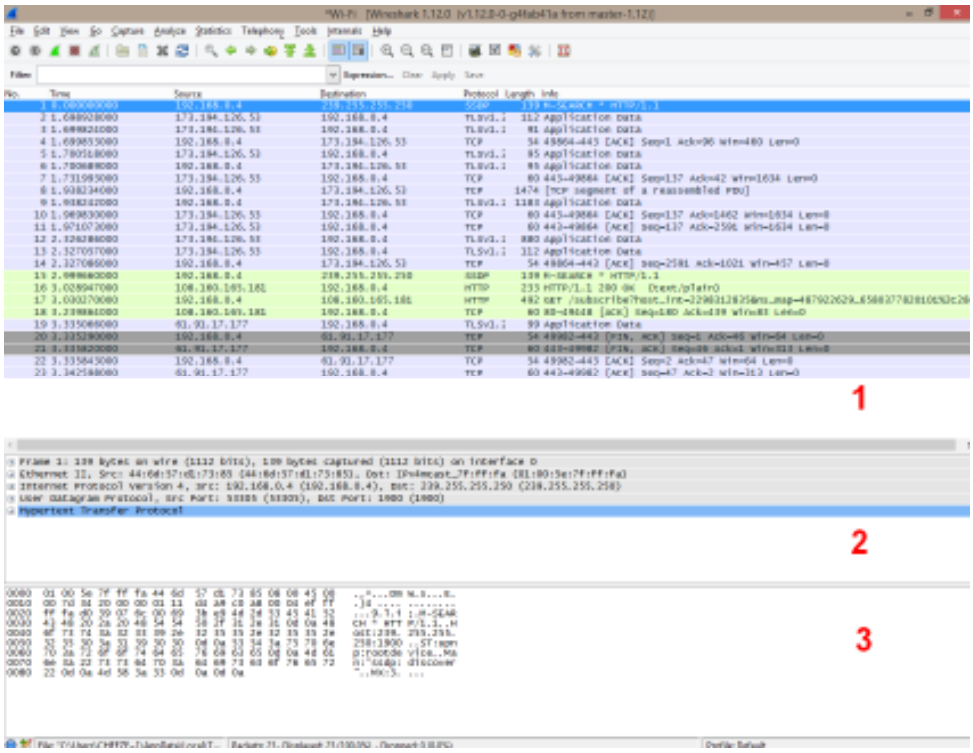


รูปที่ 1.

4. เมื่อเริ่มทำการ Capture ,Wireshark จะแสดงให้เห็นการรับส่งแพ็กเก็ตแบบ real time ในหน้าต่าง Capturing และหากต้องการหยุดการ capture ก็ทำได้ด้วยการคลิกปุ่ม stop ใน menu bar ดังรูปที่ 2. แต่ก่อนที่จะหยุดการ capture ให้แน่ใจว่าได้โหลดเว็บเพจในเว็บเบราเซอร์จนเสร็จสิ้นแล้ว นศ.สามารถดูรายละเอียดของการ รับ/ส่ง ทุกแพ็กเก็ตในการเข้าชมเว็บเพจนั้นได้ทันที

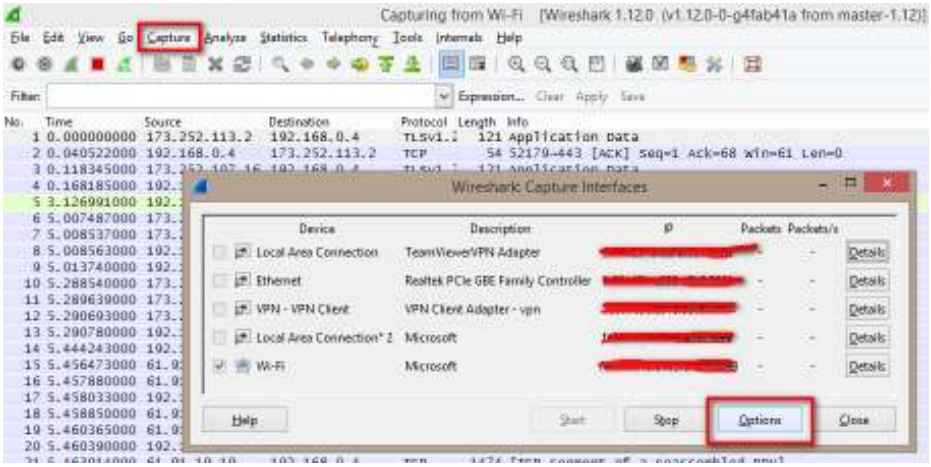
รูปที่ 2.

5. หน้าต่างหลักของ Wireshark ประกอบไปด้วย 3 ส่วน ดังรูปที่ 3. ได้แก่ (1) จะลิสท์ทุกแพ็กเก็ตที่จับได้ในขณะนั้น (2) แสดงรายละเอียดของแพ็กเก็ตที่ได้รับการเลือกไว้จากส่วนแรก และส่วนสุดท้าย (3) จะให้รายละเอียด bit-level ของแพ็กเก็ตตัวที่เลือกไว้ ดังนั้น การเลือกแพ็กเก็ตในส่วนชั้นบนของหน้าต่างนั้นจะมีการให้รายละเอียดในส่วนล่างนั่นเอง



รูปที่ 3.

6. ให้ นศ. เข้าไปที่ Capture Options จากนั้นให้ Disable Name resolution features ทั้งหมด โดยเข้าจากหน้า Live capture ดังนี้ Capture ⟶ Interfaces ดังรูปที่ 4. จากนั้นให้ Enable Name resolution เพื่อที่ capture.

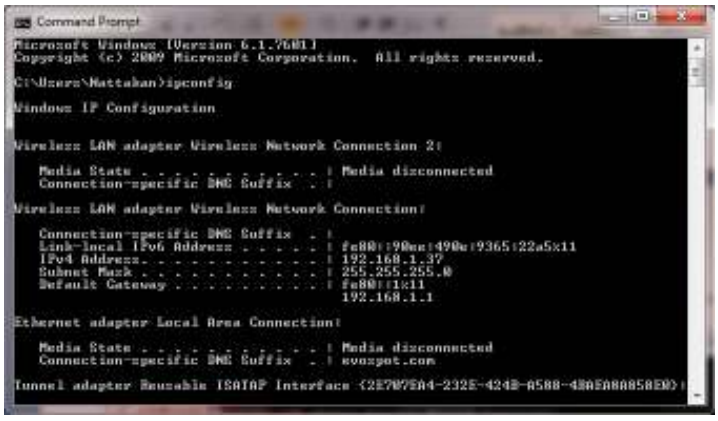


รูปที่ 4.

คำถาม 1: ข้อแตกต่างคืออะไร ? (Look at the source and destination areas) ตอบพร้อม capture หน้าจอของทั้งสองแบบมาเปรียบเทียบให้ดูด้วย

7. จะสังเกตได้ว่า เราสามารถเห็นแพ็กเก็ตที่สร้างมาจากอุปกรณ์ต่างๆ ในเครือข่ายของเรานอกเหนือจากอุปกรณ์ของเราเอง ซึ่งเป็นสิ่งที่เกิดขึ้นในเครือข่ายการกระจายข้อมูล หากพบว่า destination คือ ff:ff:ff:ff:ff:ff หรือ Broadcast IP นั่นหมายความว่า มันคือ การกระจายข้อมูลให้แก่ทุกคน ทุกเครื่อง

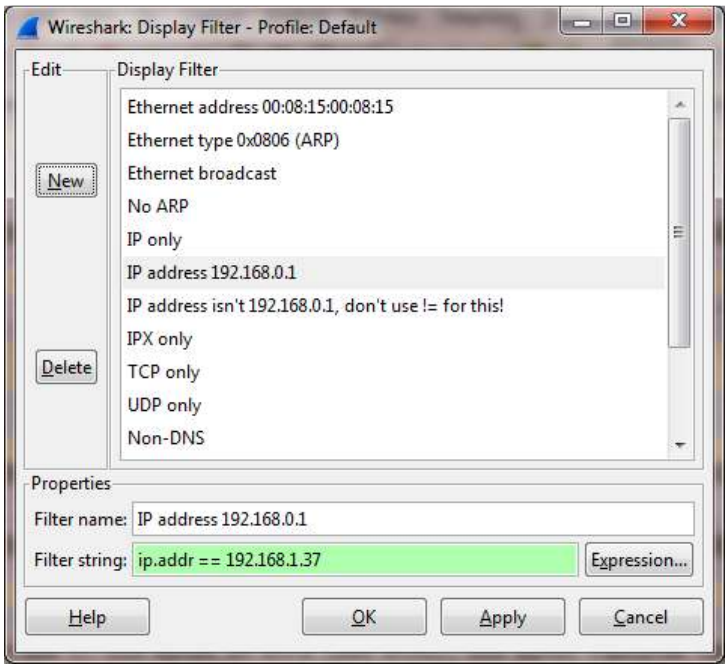
8. จากนั้นให้หาค่า IP ของเครื่องนอง นศ. โดยไปที่ Start Menu บนคอมพิวเตอร์ ⟶ Accessories ⟶ Command Prompt. ใช่คำสั่ง ipconfig ดังรูป



รูปที่ 5.

คำถาม 2: หมายเลขไอพีของเครื่องคอมพิวเตอร์ที่ใช้ คือ ?

9. ตอนนี้กลับไปที่โปรแกรม Wireshark และใช้ filter option โดยการเข้าไปที่ Analyze ⟶ Display Filters.



รูปที่ 6.

ให้กรอกหมายเลขไอพีที่เช็กได้จากข้อ 9 และกลับไปสังเกตผลการจัดแพ็กเก็ตในหน้าต่างหลักของ Wireshark

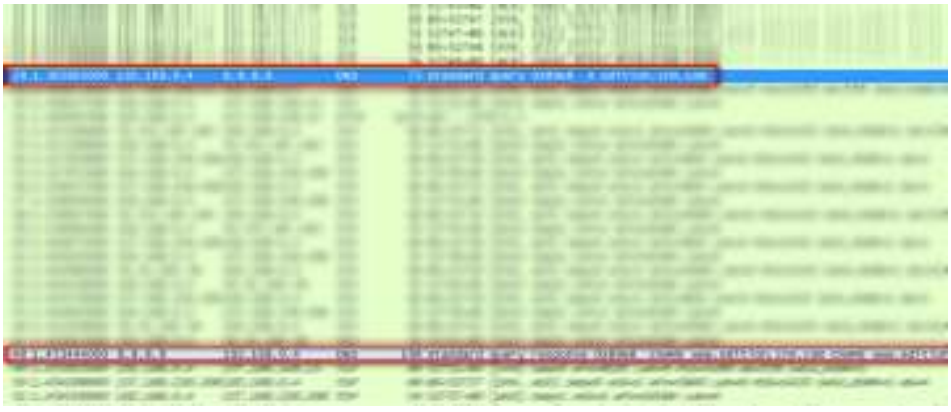
คำถาม 3:ผลที่ได้ คือ ? จงอธิบาย

10. จากนั้นให้ Restart การ capture ใหม่ โดยระหว่างเริ่มการ capture แล้วให้เข้าเว็บไซต์ http://www.cnn.com ด้วยเบราเซอร์และหยุดการ capture เมื่อเข้าสู่เว็บไซต์สำเร็จเรียบร้อยแล้ว

11. สังเกตส่วนบนสุดของหน้าต่างพบว่าบางแพ็กเก็ตเป็นโปรโตคอล DNS ให้คลิกที่ DNS ตัวแรกที่จับได้ ซึ่งเป็นการร้องขอจากเครื่องคอมพิวเตอร์เพื่อให้ทราบว่าหมายเลขไอพีของ cnn.com คืออะไร จากนั้น คลิกดูรายละเอียดด้านล่างว่าหมายเลขไอพีถูกต้องหรือไม่ จากนั้นให้หาและคลิกที่ DNS packet response ซึ่งจะบอกให้เราการตอบสนองกลับของ DNS และคอมพิวเตอร์จะทราบหมายเลขไอพีแล้วจากรายละเอียดในส่วนด้านล่าง

คำถาม 4: หมายเลขไอพีที่คอมพิวเตอร์ได้รับเพื่อใช้เข้าสู่ cnn.com คือ ?

(ในหลายๆเว็บไซต์นั้นอาจมีหลาย IP address เพื่อที่จะช่วยกระจายภาระ และในบางกรณีที่ บาง IP นั้นใช้ไม่ได้ เช่น google.com youtube.com เป็นต้น)



รูปที่ 7.

จากนั้นให้ คลิกที่เครื่องหมายในส่วนที่สองของรูปที่ 3. “+” เพื่อดูรายละเอียดของข้อมูล

12. คลิกแพ็กเก็ตแรกที่มีหมายเลขไอพีของ cnn.com ที่แสดงอยู่ในส่วนของ destination และเป็น Protocol HTTP ซึ่งเราจะเห็นส่วนหัว (heading) ของแพ็กเก็ต ส่วนหัวอันแรกคือข้อมูลจาก Wireshark. เช่น “Frame 459 (509 bytes on wire, 509 bytes captured)” ซึ่งจะบอกเราเกี่ยวกับตำแหน่งของแพ็กเก็ตนี้จากจำนวนแพ็กเก็ตทั้งหมดที่ Wireshark จับได้

คำถาม 5: สังเกตส่วนหัวที่เหลือ Ethernet Protocol? Internet Protocol? Transmission Control Protocol? Hypertext Transfer protocol? ทำไมใน message เดียวกันนี้ถึงแสดง protocols ที่แตกต่างกัน จงอธิบาย ?

คำถาม 6: โปรโตคอลทั้งสี่นี้สัมพันธ์กันอย่างไร ? จง Capture หน้าต่างที่แสดงแพ็กเก็ตที่มีทั้ง 4 โปรโตคอลนี้

13. คลิกดูรายละเอียดของ Hyper Text Transfer Protocol เพื่อตอบคำถามต่อไปนี้

คำถาม 7: ข้อมูลใดในแพ็กเก็ตนี้ที่แสดงให้ทราบเกี่ยวกับ browser ที่ใช้และระบบปฏิบัติการที่ใช้ด้วย? มันแสดงว่าเรากำลังส่ง cookie หรือไม่?

14. หาบรรทัดที่มี HTTP protocol จาก CNN ซึ่งอาจจะอยู่ในบรรทัดที่ 1, 2, หรือ 3 จาก cnn เนื่องจาก เราอาจถูกเลื่อนไปใช้ server ที่แตกต่างกันได้เพื่อให้การร้องขอการใช้งานเว็บไซต์ยังคงอยู่ เปิด Hypertext Transfer Protocol line ในส่วนที่สองของหน้าต่างโดยการคลิก จากนั้นคลิกบรรทัดที่บอกว่าคือ Data สังเกตตัวอักษรที่ได้รับการ highlight ไว้ในส่วนล่างของหน้าต่าง

คำถาม 8: ข้อความนี้คืออะไร?