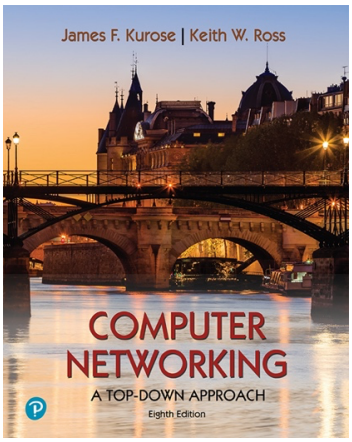
# Wireshark Lab: Getting Started v8.1

Supplement to *Computer Networking: A Top-Down Approach, 8th ed.,* J.F. Kurose and K.W. Ross

*"Tell me and I forget. Show me and I remember. Involve me and I understand."* Chinese proverb





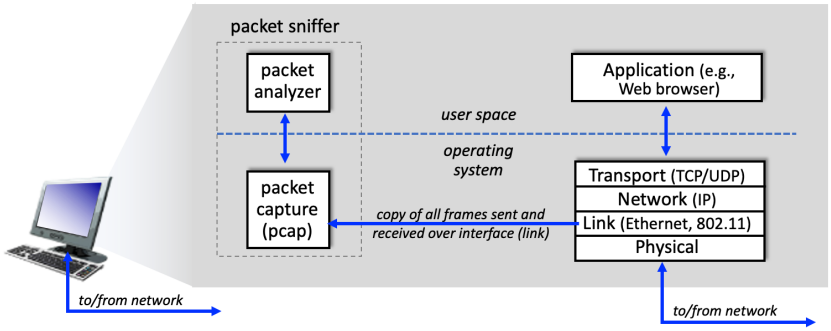

---

ความเข้าใจเกี่ยวกับโพรโทคอลเครือข่ายจะลึกซึ้งยิ่งขึ้นอย่างมากโดยการ "เห็นโพรโทคอลที่ใช้งานจริง" และ "เล่นกับโพรโทคอล" โดยสังเกตลำดับของข้อความที่แลกเปลี่ยนกัน ระหว่างโพรโทคอลจากไคลเอนต์และเซิร์ฟเวอร์ทั้งสองฝั่ง การเจาะลึกลงรายละเอียดของการดำเนินการของโพรโทคอล และทำให้โพรโทคอล ดำเนินการบางอย่าง แล้วสังเกตการกระทำเหล่านี้ และผลที่ตามมา ซึ่งสามารถทำได้ในสถานการณ์จำลอง หรือในสภาพแวดล้อมเครือข่าย "จริง" เช่น อินเทอร์เน็ต ในแบบฝึกหัดปฏิบัติการ Wireshark ที่นิสิตจะทำในวิชานี้ นิสิตจะใช้งานแอปพลิเคชันเครือข่ายต่างๆ ในสถานการณ์ที่แตกต่างกันโดยใช้คอมพิวเตอร์ของนิสิตเอง จะได้สังเกตโพรโทคอลเครือข่ายในคอมพิวเตอร์ของคุณ "กำลังทำงาน" โต้ตอบและแลกเปลี่ยนข้อความ กับโพรโทคอลที่ทำงานบนเครื่องที่อื่นในอินเทอร์เน็ต ดังนั้นคุณและคอมพิวเตอร์ของคุณจะเป็นส่วนสำคัญของแบบฝึกหัดปฏิบัติการ "สด" เหล่านี้ คุณจะสังเกตและเรียนรู้จากการลงมือทำในแล็บ Wireshark แรกนี้ คุณจะได้ทำความคุ้นเคยกับ Wireshark และทำการดักจับและสังเกตแพ็กเก็ตง่ายๆ

เครื่องมือพื้นฐานสำหรับการสังเกตข้อความที่แลกเปลี่ยนระหว่างโปรแกรมโพรโทคอล ที่เรียกใช้งานเรียกว่า packet sniffer ตามชื่อที่แนะนำ packet sniffer จะจับ ("ดมกลิ่น") ข้อความที่ส่ง/รับจาก/โดยคอมพิวเตอร์ของคุณ โดยทั่วไปจะจัดเก็บและ/หรือแสดงเนื้อหาของฟิลด์โพรโทคอลต่างๆ ในข้อความที่บันทึกไว้เหล่านี้ packet sniffer นั้นทำงานแบบ passive โดยจะคอยสังเกตข้อความที่ส่งและรับโดยแอปพลิเคชันและโพรโทคอลที่ทำงานบนคอมพิวเตอร์ของคุณ แต่จะไม่ส่งแพ็กเก็ตเองเลย ในทำนองเดียวกัน แพ็กเก็ตที่ได้รับจะไม่ถูกส่งไปยัง packet sniffer อย่างชัดเจน แต่ packet sniffer จะได้รับสำเนาของแพ็กเก็ตที่ส่ง/รับจาก/โดยแอปพลิเคชันและโพรโทคอลที่ทำงานบนเครื่องของคุณแทน

รูปที่ 1 แสดงโครงสร้างของ packet sniffer ทางด้านขวาของรูปที่ 1 คือโพรโทคอล (ในกรณีนี้คืออินเทอร์เน็ตโพรโทคอล) และแอปพลิเคชัน (เช่น เว็บเบราว์เซอร์หรือไคลเอนต์อีเมล) ที่ปกติทำงานบนคอมพิวเตอร์ของคุณ packet sniffer ที่แสดงภายในสี่เหลี่ยมเส้นประในรูปที่ 1 เป็นส่วนเพิ่มเติมจากซอฟต์แวร์ปกติในคอมพิวเตอร์ของคุณ และประกอบด้วยสองส่วนคือ ไลบรารีการจับแพ็กเก็ต ซึ่งจะได้รับสำเนาของเฟรมจากเลเยอร์ลิงก์ทุกเฟรมที่คอมพิวเตอร์ของคุณส่งหรือรับผ่านอินเทอร์เฟซที่กำหนด (เลเยอร์ลิงก์ เช่น Ethernet หรือ WiFi) ข้อความที่แลกเปลี่ยนโดยโพรโทคอลเลเยอร์ที่สูงกว่า เช่น HTTP, FTP, TCP, UDP, DNS หรือ IP ทั้งหมดจะถูกห่อหุ้มในเฟรมที่เลเยอร์ลิงก์ที่ถูกส่งผ่านสื่อทางกายภาพในที่สุด

เช่น สายอีเทอร์เน็ตหรือคลื่นวิทยุ WiFi 802.11 การจับเฟรมเลเยอร์ลิงก์ทั้งหมดจะทำให้คุณได้รับข้อความทั้งหมดที่ส่ง/รับผ่านลิงก์ที่ได้รับการตรวจสอบจาก/โดยโพรโทคอลและแอปพลิเคชันทั้งหมดที่ทำงานในคอมพิวเตอร์ของคุณ




**รูปที่ 1:** โครงสร้างของ packet sniffer

องค์ประกอบที่สองของ packet sniffer คือ **packet analyzer** ซึ่งแสดงเนื้อหาของฟิลด์ทั้งหมดภายในข้อความโพรโทคอล ในการทำเช่นนั้น **packet analyzer** จะต้อง "เข้าใจ" โครงสร้างของข้อความทั้งหมดที่แลกเปลี่ยนโดยโพรโทคอล ตัวอย่างเช่น สมมติว่าเราสนใจที่จะแสดงฟิลด์ต่างๆ ในข้อความที่แลกเปลี่ยนโดยโพรโทคอล HTTP ในรูปที่ 1 **packet analyzer** เข้าใจรูปแบบของอีเทอร์เน็ตเฟรม และสามารถระบุ IP ดาตาแกรม ภายในอีเทอร์เน็ตเฟรมได้ นอกจากนี้ยังเข้าใจรูปแบบ IP ดาตาแกรม เพื่อให้สามารถแยกส่วน ที่เป็น TCP ภายใน IP ดาตาแกรม ได้ในที่สุด และเข้าใจโครงสร้างของ TCP เซ็กเมนต์ จึงสามารถแยกข้อความ HTTP ที่มีอยู่ใน TCP เซ็กเมนต์ได้ ในที่สุด และเข้าใจโพรโทคอล HTTP และรู้ว่าไบต์แรกของข้อความ HTTP จะมีสตริง “GET” “POST” หรือ “HEAD”

เราจะใช้ packet sniffer Wireshark [http://www.wireshark.org/] สำหรับแล็บเหล่านี้ เพื่อให้เราสามารถแสดงเนื้อหาของข้อความที่ส่ง/รับจาก/โดยโพรโทคอลในระดับต่างๆ ของโพรโทคอลสแต็ก (ในทางเทคนิคแล้ว Wireshark คือเครื่องมือวิเคราะห์แพ็กเก็ตที่ใช้ไลบรารีการจับแพ็กเก็ตในคอมพิวเตอร์ของคุณ นอกจากนี้ ในทางเทคนิคแล้ว Wireshark ยังจับเฟรมของเลเยอร์ลิงก์ ดังแสดงในรูปที่ 1 แต่ใช้คำเรียกทั่วไปว่า “แพ็กเก็ต” เพื่ออ้างถึงเฟรมของเลเยอร์ลิงก์, ดาตาแกรมของเลเยอร์เครือข่าย, เซ็กเมนต์ของเลเยอร์ทรานสปอร์ต และข้อความในเลเยอร์แอปพลิเคชัน ดังนั้นเราจะใช้คำว่า "แพ็กเก็ต" ที่นี่เพื่อให้สอดคล้องกับแบบแผนของโปรแกรม Wireshark) Wireshark เป็นตัววิเคราะห์โพรโทคอลเครือข่ายฟรี ที่ทำงานบนคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Windows, Mac และ Linux/Unix จึงเป็นเครื่องมือวิเคราะห์แพ็กเก็ตที่ดีมากสำหรับการทำแล็บปฏิบัติการของเรา มีความเสถียร มีฐานผู้ใช้ขนาดใหญ่ และมีการสนับสนุนที่มีเอกสารประกอบการใช้งานอย่างดี ซึ่งรวมถึงคู่มือผู้ใช้ (http://www.wireshark.org/docs/wsug_html_chunked/) หน้าคู่มือ (http //www.wireshark.org/docs/man-pages/) และคำถามที่พบบ่อยโดยละเอียด (http://www.wireshark.org/faq.html) ฟังก์ชันการทำงานที่หลากหลายซึ่งรวมถึงความสามารถในการวิเคราะห์โพรโทคอลหลายร้อยรายการ และ ส่วนต่อประสานผู้ใช้ที่ออกแบบมาอย่างดี โดยทำงานในคอมพิวเตอร์ที่ใช้อีเทอร์เน็ต, เครือข่ายไร้สาย 802.11 (WiFi) และเทคโนโลยีลิงก์เลเยอร์อื่นๆ อีกมากมาย

# Getting Wireshark

หากต้องการเรียกใช้ Wireshark คุณจะต้องมีสิทธิ์เข้าถึงคอมพิวเตอร์ที่รองรับทั้ง Wireshark และไลบรารีการจับแพ็กเก็ต libpcap หรือ WinPCap เมื่อคุณติดตั้ง Wireshark ซอฟต์แวร์ libpcap จะถูกติดตั้งให้โดยอัตโนมัติถ้าหากเครื่องคุณไม่มีการติดตั้งไว้ก่อนแล้วภายในระบบปฏิบัติการ สามารถดู http://www.wireshark.org/download.html สำหรับรายการระบบปฏิบัติการที่รองรับและไซต์สำหรับดาวน์โหลด

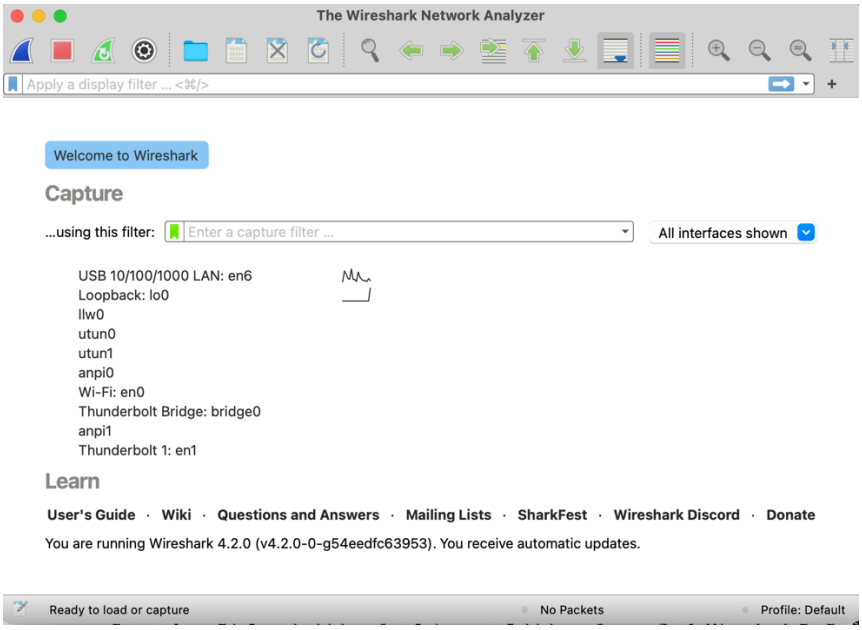
ดาวน์โหลดและติดตั้งซอฟต์แวร์ Wireshark:

• ไปที่ http://www.wireshark.org/download.html และดาวน์โหลดและติดตั้งโปรแกรม Wireshark

หน้าคำถามที่พบบ่อยเกี่ยวกับโปรแกรม Wireshark (FAQs) มีคำแนะนำที่เป็นประโยชน์และข้อมูลที่น่าสนใจมากมาย โดยเฉพาะอย่างยิ่งหากนิสิตมีปัญหาในการติดตั้งหรือใช้งานโปรแกรม Wireshark

# Running Wireshark

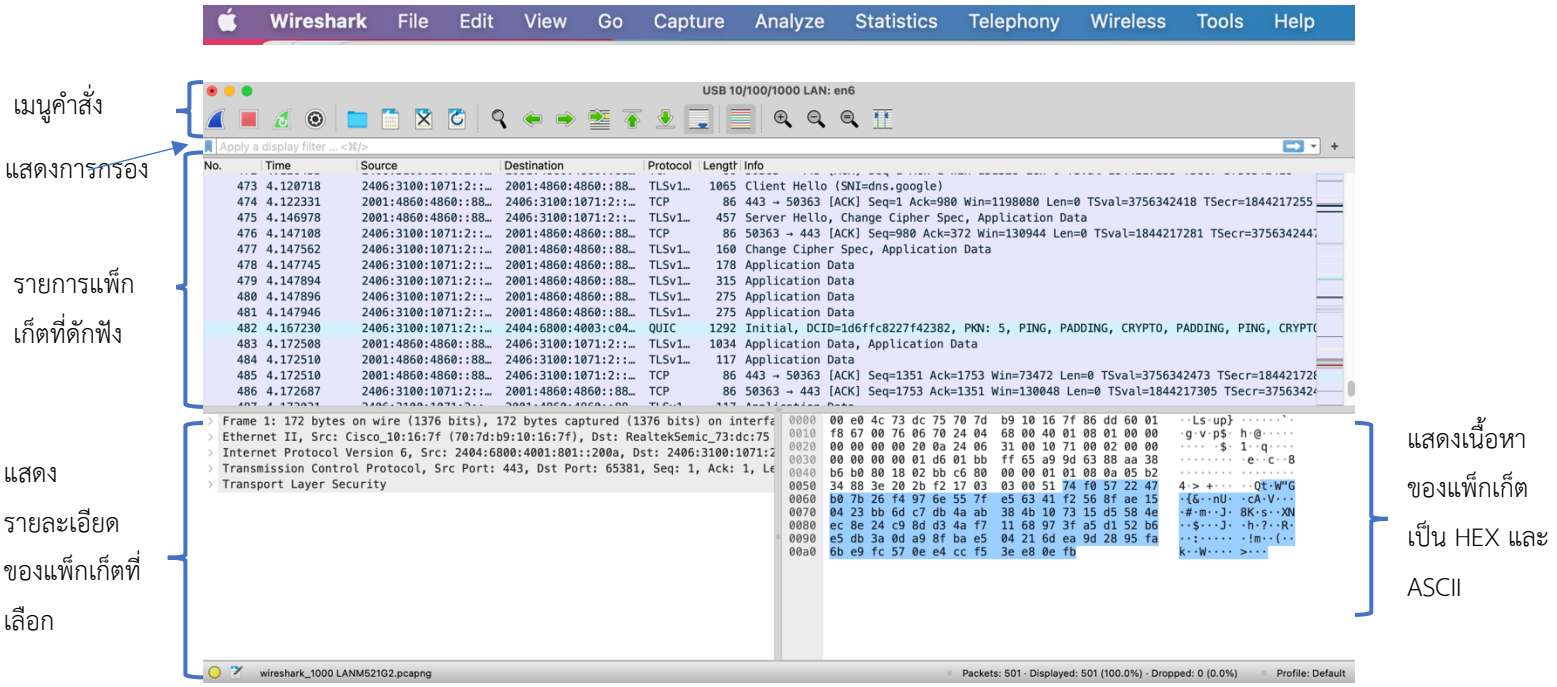
เมื่อคุณรันโปรแกรม Wireshark คุณจะได้หน้าจอเริ่มต้นที่มีลักษณะคล้ายกับหน้าจอด้านล่าง Wireshark เวอร์ชันต่างๆ จะมีหน้าจอเริ่มต้นที่แตกต่างกัน ดังนั้นอย่าแปลกใจหากหน้าจอของคุณไม่เหมือนกับหน้าจอด้านล่างทุกประการ! เอกสารของ Wireshark ระบุว่า “เนื่องจาก Wireshark ทำงานบนแพลตฟอร์มที่แตกต่างกันมากมายโดยมีตัวจัดการหน้าต่างที่แตกต่างกัน มีสไตล์ที่แตกต่างกัน และมีการใช้ชุดเครื่องมือ GUI เวอร์ชันที่แตกต่างกัน หน้าจอของคุณจึงอาจดูแตกต่างจากภาพหน้าจอที่ให้มา แต่เนื่องจากไม่มีความแตกต่างในฟังก์ชันการใช้งาน ภาพหน้าจอเหล่านี้ควรที่จะสามารถเข้าใจได้เป็นอย่างดี”




**รูปที่ 2:** หน้าจอเริ่มต้นเมื่อรันโปรแกรม Wireshark

บนหน้าจอนี้ไม่มีอะไรน่าสนใจมากนัก แต่จะสังเกตได้ว่าภายใต้ส่วนการจับภาพ (Capture) จะมีรายการของอินเทอร์เฟซต่างๆ ภาพนี้มาจากเครื่อง macbook ที่เราถ่ายภาพหน้าจอ มีอินเทอร์เฟซเพียงอินเทอร์เฟซเดียว นั่นคือ Ethernet "LAN en6" ซึ่งเป็นอินเทอร์เฟซสำหรับการเข้าถึงเครือข่าย LAN แพ็กเก็ตทั้งหมดที่เข้า/จากคอมพิวเตอร์เครื่องนี้จะถูกส่งผ่านอินเทอร์เฟซ LAN en6 ดังนั้นเราจึงต้องการจับแพ็กเก็ตที่นี่ บนเครื่อง macbook นี้ให้ดับเบิลคลิกที่อินเทอร์เฟซนี้ (หรือบนคอมพิวเตอร์เครื่องอื่น ให้ค้นหาอินเทอร์เฟซบนหน้าเริ่มต้นใช้งาน ที่คุณใช้เชื่อมต่ออินเทอร์เน็ต เช่น ส่วนใหญ่เป็นอินเทอร์เฟซ WiFi หรือ Ethernet และเลือกอินเทอร์เฟซนั้นในหน้าจอ Wireshark ที่คุณระบุอินเทอร์เฟซการจับแพ็กเก็ต)

หากคุณคลิกที่อินเทอร์เฟซใดอินเทอร์เฟซหนึ่งเหล่านี้เพื่อเริ่มการจับแพ็คเก็ต (เช่น เพื่อให้โปรแกรม Wireshark เริ่มจับแพ็กเก็ตทั้งหมดที่ถูกส่งไปยัง/จากอินเทอร์เฟซนั้น) หน้าจอเหมือนกับที่แสดงด้านล่างนี้จะปรากฏขึ้น โดยแสดงข้อมูลเกี่ยวกับแพ็คเก็ตที่ถูกจับ เมื่อคุณเริ่มการจับแพ็คเก็ต คุณสามารถหยุดได้โดยใช้เมนูแบบเลื่อนลง Capture และเลือก Stop (หรือโดยการคลิกที่ปุ่มสี่เหลี่ยมสีแดงถัดจากครีบ Wireshark ในรูปที่ 2)




**รูปที่ 3:** หน้าต่าง Wireshark, ระหว่างและหลังจากดักจับแพ็กเก็ต

อินเทอร์เฟซ Wireshark มีองค์ประกอบหลัก 5 ส่วน:

- เมนูคำสั่งคือเมนูแบบ drop-down ที่อยู่ด้านบนของหน้าต่างโปรแกรม Wireshark (และบนเครื่อง Mac ที่ด้านบนของหน้าจอเช่นกัน ภาพหน้าจอในรูปที่ 3 มาจากเครื่อง Mac) สิ่งที่น่าสนใจตอนนี้คือเมนู File และ Capture  เมนู File ช่วยให้คุณบันทึกข้อมูลแพ็กเก็ตที่บันทึกไว้ หรือเปิดไฟล์ที่มีข้อมูลแพ็กเก็ตที่บันทึกไว้ก่อน

หน้านี้ และออกจากแอปพลิเคชัน Wireshark เมนู Capture ช่วยให้คุณสามารถเริ่มและหยุดการจับแพ็กเก็ตได้

- หน้าต่างรายการแพ็กเก็ต จะแสดงข้อมูลสรุปหนึ่งบรรทัดสำหรับแต่ละแพ็กเก็ตที่จับ รวมถึงหมายเลขแพ็กเก็ต (กำหนดโดย โปรแกรม Wireshark ซึ่งไม่ใช่หมายเลขแพ็กเก็ต ที่มีอยู่ในส่วนหัวของโพรโทคอลใดๆ) เวลาที่แพ็กเก็ตถูกจับ หมายเลขที่อยู่ IP ของต้นทางและปลายทางของแพ็กเก็ต ประเภทโพรทคอลในระดับชั้นบน และข้อมูลเฉพาะโพรโทคอลที่มีอยู่ในแพ็กเก็ต รายการแพ็กเก็ต สามารถจัดเรียงตามหมวดหมู่เหล่านี้ได้ โดยคลิกที่ชื่อคอลัมน์ ช่องประเภทโพรโทคอลแสดงรายการโพรโทคอลระดับสูงสุดที่ส่งหรือรับแพ็กเก็ตนี้ กล่าวคือ โพรโทคอลที่เป็นแหล่งที่มา หรือช่องทางสุดท้ายสำหรับแพ็กเก็ตนี้
- หน้าต่างรายละเอียดส่วนหัวของแพ็กเก็ต ให้รายละเอียดเกี่ยวกับแพ็กเก็ตที่เลือก (ไฮไลต์) ในหน้าต่างรายการแพ็กเก็ต (หากต้องการเลือกแพ็กเก็ตในหน้าต่างรายการแพ็กเก็ต ให้วางเคอร์เซอร์บนบรรทัดสรุปบรรทัดเดียวของแพ็กเก็ตในหน้าต่างรายการแพ็กเก็ต แล้วคลิกด้วยปุ่มซ้ายของเมาส์) รายละเอียดเหล่านี้ ประกอบด้วยข้อมูลเกี่ยวกับเฟรมอีเทอร์เน็ต (สมมติว่าแพ็กเก็ตถูกส่ง/รับผ่านอินเทอร์เฟซอีเทอร์เน็ต) และ IP ดาตาแกรม ที่มีแพ็กเก็ตนี้ จำนวนอีเทอร์เน็ตและรายละเอียดระดับชั้น IP ที่แสดงสามารถขยายหรือย่อให้เล็กสุดได้โดยการคลิกที่กล่องบวก/ลบ หรือสามเหลี่ยมชี้ไปทางขวา/ล่าง ทางด้านซ้ายของอีเทอร์เน็ตเฟรม หรือบรรทัด IP ดาตาแกรม ในหน้าต่างรายละเอียดแพ็กเก็ต หากแพ็กเก็ตถูกส่งผ่านโพรโทคอล TCP หรือ UDP รายละเอียดของโพรโทคอล TCP หรือ UDP ก็จะปรากฏขึ้นเช่นกัน ซึ่งสามารถขยายหรือย่อให้เล็กสุดได้เช่นเดียวกัน สุดท้ายนี้จะมีการจัดเตรียมรายละเอียดเกี่ยวกับโพรโทคอลระดับสูงสุดที่ส่งหรือรับแพ็กเก็ตนี้ด้วย

- หน้าต่างเนื้อหาแพ็กเก็ต จะแสดงเนื้อหาทั้งหมดของดาตาเฟรมที่บันทึกไว้ ในรูปแบบ ASCII และ เลขฐานสิบหก (hexadecimal)
- ที่ด้านบนของอินเทอร์เฟซผู้ใช้แบบกราฟิก Wireshark คือฟิลด์ตัวกรองการแสดงผลแพ็กเก็ต ซึ่งสามารถป้อนชื่อโพรโทคอลหรือข้อมูลอื่น ๆ เพื่อกรองข้อมูลที่แสดงในหน้าต่างรายการแพ็กเก็ต (และด้วยเหตุนี้ส่วนหัวของแพ็กเก็ตและ หน้าต่างเนื้อหาแพ็กเก็ต) ในตัวอย่างด้านล่าง เราจะใช้ฟิลด์ตัวกรองการแสดงแพ็กเก็ตเพื่อให้ Wireshark ซ่อนแพ็กเก็ต (ไม่แสดง) ที่ไม่สอดคล้องกับข้อความ HTTP
- ที่ด้านบนของอินเทอร์เฟซผู้ใช้แบบกราฟิก Wireshark คือฟิลด์ตัวกรองการแสดงแพ็กเก็ต ซึ่งสามารถป้อนชื่อโพรโทคอลหรือข้อมูลอื่น ๆ เพื่อกรองข้อมูลที่แสดงในหน้าต่างรายการแพ็กเก็ต (และด้วยเหตุนี้ส่วนหัวของแพ็กเก็ตและ หน้าต่างเนื้อหาแพ็กเก็ต) ในตัวอย่างด้านล่าง เราจะใช้ฟิลด์ตัวกรองการแสดงแพ็กเก็ตเพื่อให้ Wireshark ซ่อนแพ็กเก็ต (ไม่แสดง) ที่ไม่สอดคล้องกับข้อความ HTTP

# Taking Wireshark for a Test Run

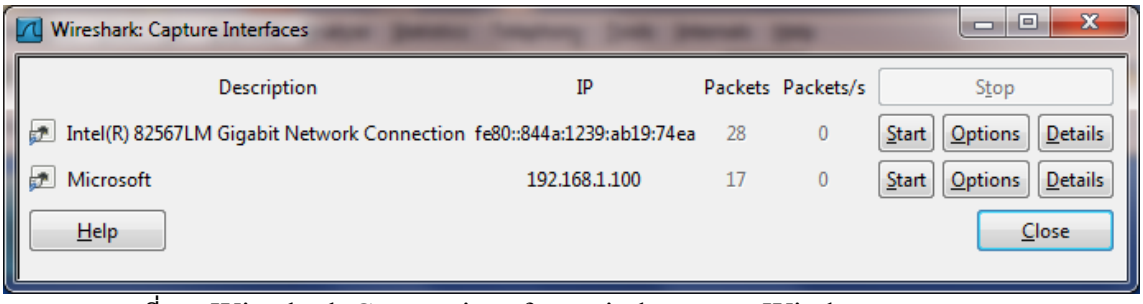
นำ Wireshark มาทดสอบการทำงาน

วิธีที่ดีที่สุดในการเรียนรู้เกี่ยวกับซอฟต์แวร์ชิ้นใหม่คือการทดลองใช้! เราจะถือว่าคอมพิวเตอร์ของคุณเชื่อมต่อกับอินเทอร์เน็ตผ่านอินเทอร์เฟซอีเทอร์เน็ตแบบมีสายหรืออินเทอร์เฟซ WiFi 802.11 ไร้สาย ทำสิ่งต่อไปนี้:

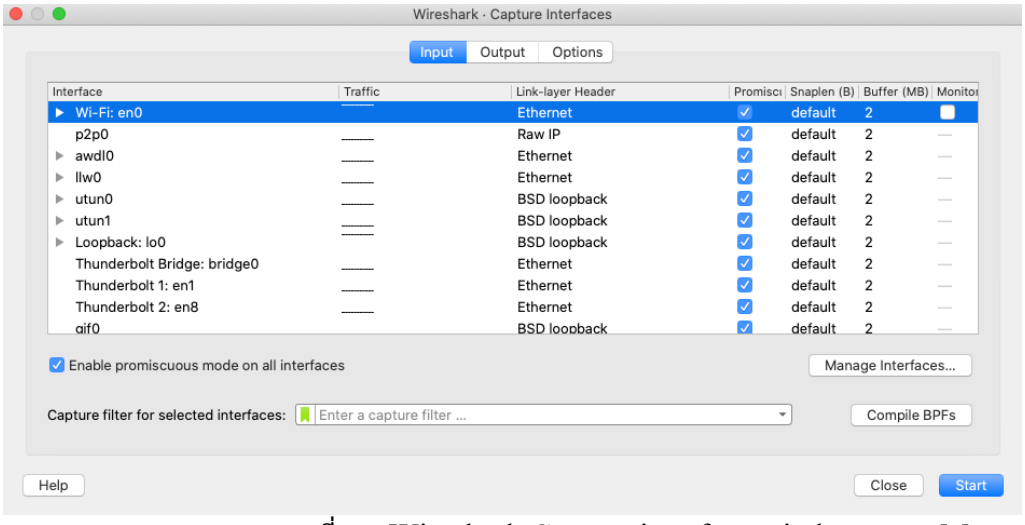
1. เปิดเว็บเบราว์เซอร์ที่คุณชื่นชอบ ซึ่งจะแสดงหน้าแรกที่คุณเลือก

2. เริ่มต้นซอฟต์แวร์ Wireshark ในตอนแรกคุณจะเห็นหน้าต่างคล้ายกับที่แสดงในรูปที่ 2 Wireshark ยังไม่ได้เริ่มจับแพ็กเก็ต

3. เพื่อเริ่มต้นการจับแพ็กเก็ต ให้เลือกเมนูดึงลงการจับภาพ และเลือกอินเทอร์เฟซ ซึ่งจะทำให้หน้าต่าง "Wireshark: Capture Interfaces" ปรากฏขึ้น (บนพีซี) หรือคุณสามารถเลือกตัวเลือกบน Mac ได้ คุณควรเห็นรายการอินเทอร์เฟซ ดังแสดงในรูปที่ 4a (Windows) และ 4b (Mac)

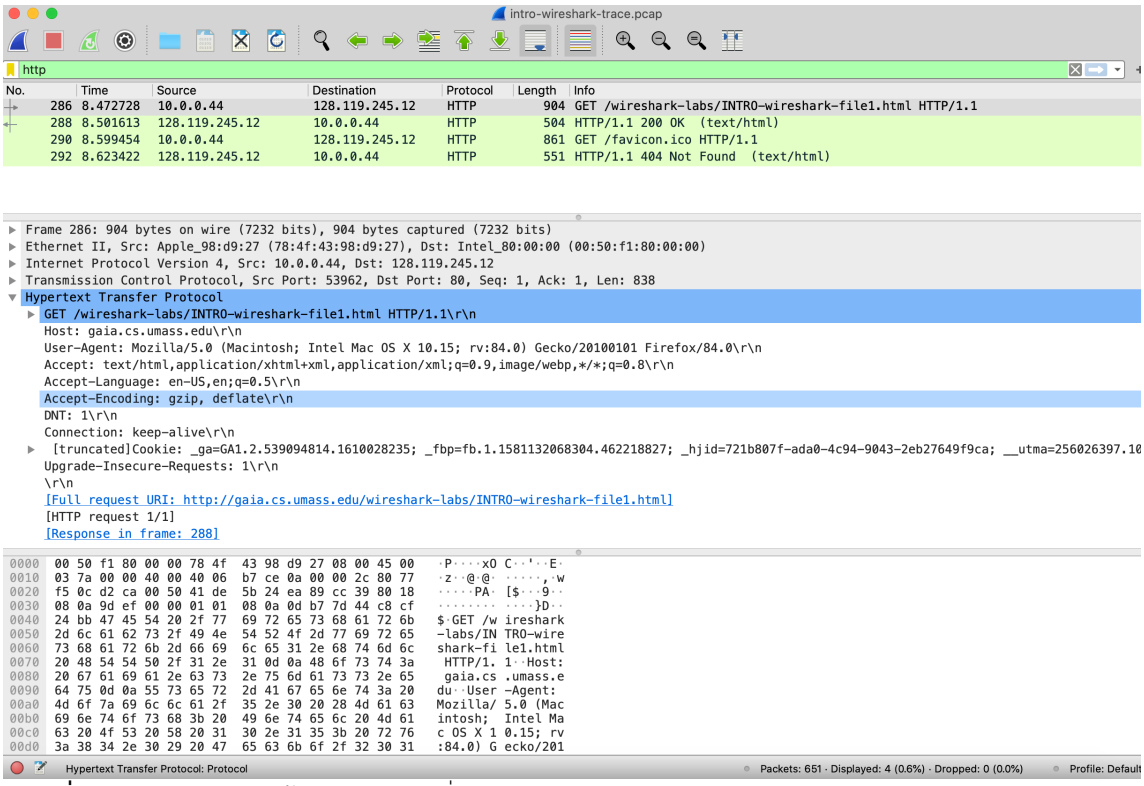



รูปที่ 4a: Wireshark Capture interface window, on a Windows computer




รูปที่ 4b: Wireshark Capture interface window, on a Mac computer

1. คุณจะเห็นรายการอินเทอร์เฟซบนคอมพิวเตอร์ของคุณ ตลอดจนจำนวนแพ็กเก็ตที่ถูกสังเกตบนอินเทอร์เฟซนั้นจนถึงตอนนี้ บนเครื่อง Windows ให้คลิกที่ Start สำหรับอินเทอร์เฟซที่คุณต้องการเริ่มการจับแพ็คเก็ต (ในกรณีในรูปที่ 4a คือ การเชื่อมต่อเครือข่าย Gigabit) บนเครื่อง Windows ให้เลือกอินเทอร์เฟซแล้วคลิกเริ่มที่ด้านล่างของหน้าต่าง) การจับแพ็คเก็ตจะเริ่มขึ้น - ตอนนี้ Wireshark กำลังจับแพ็คเก็ตทั้งหมดที่ส่ง/รับจาก/โดยคอมพิวเตอร์ของคุณ!
2. เมื่อคุณเริ่มการจับแพ็คเก็ต หน้าต่างที่คล้ายกับที่แสดงในรูปที่ 3 จะปรากฏขึ้น หน้าต่างนี้แสดงแพ็กเก็ตที่ถูกจับ โดยการเลือกเมนูแบบเลื่อนลง Capture และเลือก Stop หรือคลิกที่สี่เหลี่ยม Stop สีแดง คุณสามารถหยุดการจับแพ็คเก็ตได้ แต่อย่าเพิ่งหยุดการจับแพ็กเก็ต ให้มาจับแพ็กเก็ตที่น่าสนใจกันก่อน เพื่อที่จะทำเช่นนั้น เราจะต้องสร้างการรับส่งข้อมูลเครือข่ายบางอย่าง เรามาทำกันโดยใช้เว็บเบราว์เซอร์ซึ่งจะใช้โปรโตคอล HTTP ที่เราได้ศึกษาอย่างละเอียดในชั้นเรียน เพื่อดาวน์โหลดเนื้อหาจากเว็บไซต์
3. ขณะที่ Wireshark กำลังทำงาน ให้ป้อน URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html และให้เพจนั้นแสดงในเบราว์เซอร์ของคุณ ในการแสดงหน้านี้ เบราว์เซอร์ของคุณจะติดต่อกับเซิร์ฟเวอร์ HTTP ที่ gaia.cs.umass.edu และแลกเปลี่ยนข้อความ HTTP กับเซิร์ฟเวอร์เพื่อดาวน์โหลดหน้านี้ ตามที่กล่าวไว้ในหัวข้อ 2.2 ของข้อความ อีเทอร์เน็ตเฟรม หรือ WiFi ที่มีข้อความ HTTP เหล่านี้ (รวมถึงเฟรมอื่นๆ ทั้งหมดที่ส่งผ่านอีเทอร์เน็ต หรืออแด็ปเตอร์ WiFi ของคุณ) จะถูกบันทึกโดย Wireshark
4. หลังจากที่เบราว์เซอร์ของคุณแสดงหน้า INTRO-wireshark-file1.html (เป็นการแสดงข้อความความยินดีเพียงบรรทัดเดียว) ให้หยุดการจับแพ็กเก็ต Wireshark โดยเลือกหยุดในหน้าต่างการจับ Wireshark หน้าต่างหลักของ Wireshark ควรมีลักษณะคล้ายกับรูปที่ 3 ขณะนี้คุณมีข้อมูลแพ็กเก็ตสดที่มีข้อความโพรโทคอลทั้งหมดที่แลกเปลี่ยนระหว่างคอมพิวเตอร์ของคุณกับอุปกรณ์ในเครือข่ายอื่นๆ ข้อความ HTTP ที่แลกเปลี่ยนกับเว็บเซิร์ฟเวอร์ gaia.cs.umass.edu ควรปรากฏที่ไหนสักแห่งในรายการแพ็กเก็ตที่บันทึกไว้ แต่จะมีแพ็กเก็ตประเภทอื่น ๆ อีกมากมายที่แสดงเช่นกัน (ดู เช่น โพรโทคอลประเภทต่าง ๆ มากมายที่แสดงในคอลัมน์โพรโทคอลในรูปที่ 3) แม้ว่าการดำเนินการเดียวที่คุณทำคือการดาวน์โหลดหน้าเว็บ แต่ก็มีโพรโทคอลอื่น ๆ มากมายที่ทำงานบนคอมพิวเตอร์ของคุณ ซึ่งผู้ใช้งานมองไม่เห็น เราจะเรียนรู้เพิ่มเติมเกี่ยวกับโพรโทคอลเหล่านี้เมื่อเรากเรียนวิชานี้ไปตามลำดับ! สำหรับตอนนี้ คุณควรตระหนักว่ามักจะมีอะไรเกิดขึ้นมากกว่าแค่สิ่งที่คุณเห็น
5. พิมพ์ “http” (โดยไม่ต้องใส่เครื่องหมายคำพูด และในกรณีตัวพิมพ์เล็ก – ชื่อโพรโทคอลทั้งหมดจะเป็นตัวพิมพ์เล็กใน Wireshark และอย่าลืมกดปุ่ม enter/return ของคุณ) ลงในหน้าต่างข้อกำหนดตัวกรองการแสดงผลที่ด้านบนของหน้าหลัก หน้าต่าง Wireshark จากนั้นเลือก ใช้ (ทางด้านขวาของตำแหน่งที่คุณป้อน “http”) หรือเพียงแค่กด return ซึ่งจะทำให้เฉพาะข้อความ HTTP แสดงในหน้าต่างรายการแพ็กเก็ต รูปที่ 5 ด้านล่างแสดงภาพหน้าจอหลังจากใช้ตัวกรอง http กับหน้าต่างการจับแพ็คเก็ตที่แสดงก่อนหน้าในรูปที่ 3 นอกจากนี้ โปรดทราบว่าในหน้าต่างรายละเอียดแพ็คเก็ตที่เลือก เราได้เลือกที่จะแสดงเนื้อหาโดยละเอียดสำหรับข้อความแอปพลิเคชัน Hypertext Transfer Protocol ที่ พบภายในเซ็กเมนต์ TCP ซึ่งอยู่ภายใน IPv4 ดาตาแกรมที่อยู่ในเฟรม Ethernet หรือ (WiFi) การมุ่งเน้นไปที่เนื้อหาที่ข้อความ เซ็กเมนต์ เดตาแกรม และระดับเฟรมที่เฉพาะเจาะจงช่วยให้เรามุ่งเน้นไปที่สิ่งที่เราต้องการดู (ในกรณีนี้คือข้อความ HTTP)




**รูปที่ 5:** ดูรายละเอียดของข้อความ HTTP ที่มี GET ของ http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

6. ค้นหาข้อความ HTTP GET ที่ส่งจากคอมพิวเตอร์ของคุณไปยังเซิร์ฟเวอร์ HTTP gaia.cs.umass.edu (มองหาข้อความ HTTP GET ในส่วน “รายการแพ็กเก็ตที่บันทึกไว้” ของหน้าต่าง Wireshark (ดูรูปที่ 3 และ 5) ที่แสดง “GET” ตามด้วย URL gaia.cs.umass.edu ที่คุณป้อน เมื่อคุณเลือก ข้อความ HTTP GET, กรอบ Ethernet, ดาตาแกรม IP, ส่วน TCP และข้อมูลส่วนหัวของข้อความ HTTP จะถูกแสดงในหน้าต่างส่วนหัวของแพ็คเก็ต โดยการคลิกที่ '+' และ '-' และหัวลูกศรชี้ขวาและชี้ลงเพื่อ ทางด้านซ้ายของหน้าต่างรายละเอียดแพ็คเก็ต ลดจำนวนข้อมูล Frame, Ethernet, Internet Protocol และ Transmission Control Protocol ที่แสดง เพิ่มจำนวนข้อมูลที่แสดงเกี่ยวกับโปรโตคอล HTTP ให้สูงสุด จอแสดงผล Wireshark ของคุณควรมีลักษณะคร่าวๆ ดังแสดงในรูปที่ 5 (หมายเหตุ โดยเฉพาะอย่างยิ่ง จำนวนข้อมูลโพรทคอลที่น้อยที่สุดสำหรับโพรทคอลทั้งหมดยกเว้น HTTP และจำนวนข้อมูลโพรทคอลสูงสุดสำหรับ HTTP ในหน้าต่างส่วนหัวของแพ็กเก็ต)
7. ออกจากโปรแกรม Wireshark

ยินดีด้วย! ตอนนี้คุณทำแล็บแรกเสร็จแล้ว!

ตอนนี้ตอบคำถามด้านล่าง

1. โพรโทคอลใดต่อไปนี้ แสดงตามที่ปรากฏ (เช่น แสดงรายการอยู่ในคอลัมน์ “โพรโทคอล” ของ Wireshark) ในไฟล์การติดตามของคุณ: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2 ) (แสดงหลักฐานด้วยรูปที่ capture จาก Wireshark)

2. ใช้เวลานานเท่าใดในการส่งข้อความ HTTP GET จนกระทั่งได้รับการตอบกลับ HTTP OK (ตามค่าเริ่มต้น ค่าของคอลัมน์เวลาในหน้าต่างรายการแพ็กเก็ตคือระยะเวลาเป็นวินาทีนับตั้งแต่การติดตาม Wireshark เริ่มต้นขึ้น (หากคุณต้องการแสดงฟิลด์เวลาในรูปแบบเวลาของวัน ให้เลือก Wireshark ดูเมนูแบบเลื่อนลง จากนั้นเลือกรูปแบบการแสดงเวลา จากนั้นเลือกเวลาของวัน) (แสดงหลักฐานด้วยรูปที่ capture จาก Wireshark)

3. ที่อยู่อินเทอร์เน็ตของ gaia.cs.umass.edu (หรือที่เรียกว่า www-net.cs.umass.edu) คืออะไร ที่อยู่อินเทอร์เน็ตของคอมพิวเตอร์ของคุณคืออะไร ) (แสดงหลักฐานด้วยรูปที่ capture จาก Wireshark)

หากต้องการตอบคำถามสองข้อต่อไปนี้ คุณจะต้องเลือกแพ็กเก็ต TCP ที่มีคำขอ HTTP GET (คำใบ้: นี่คือหมายเลขแพ็กเก็ต 286) จุดประสงค์ของคำถามสองข้อถัดไปนี้คือเพื่อให้คุณคุ้นเคยกับการใช้ "รายละเอียดของหน้าต่างแพ็กเก็ตที่เลือก" ของ Wireshark; ดูรูปที่ 3 โดยคลิกที่แพ็คเก็ต 286 (หน้าจอของคุณควรมีลักษณะคล้ายกับรูปที่ 3) เพื่อตอบคำถามแรกด้านล่าง จากนั้นดูในหน้าต่าง “รายละเอียดของแพ็กเก็ตที่เลือก” เพื่อสลับสามเหลี่ยมสำหรับ HTTP (หน้าจอของคุณควรมีลักษณะคล้ายกับรูปที่ 5) สำหรับคำถามที่สองด้านล่าง คุณจะต้องขยายข้อมูลเกี่ยวกับส่วน Transmission Control Protocol (TCP) ของแพ็กเก็ตนี้

1. ขยายข้อมูลเกี่ยวกับข้อความ HTTP ในหน้าต่าง Wireshark “รายละเอียดของแพ็คเก็ตที่เลือก” (ดูรูปที่ 3 ด้านบน) เพื่อให้คุณสามารถดูช่องต่างๆ ในข้อความคำขอ HTTP GET เว็บเบราว์เซอร์ประเภทใดที่ออกคำขอ HTTP คำตอบจะแสดงที่ด้านขวาสุดของข้อมูลถัดจากช่อง “User-Agent:” ในการแสดงข้อความ HTTP แบบขยาย [ค่าฟิลด์นี้ในข้อความ HTTP คือวิธีที่เว็บเซิร์ฟเวอร์เรียนรู้ว่าคุณใช้เบราว์เซอร์ประเภทใด]
   • Firefox, Safari, Microsoft Internet Edge, อื่นๆ
2. ขยายข้อมูลเกี่ยวกับ Transmission Control Protocol สำหรับแพ็กเก็ตนี้ในหน้าต่าง Wireshark “รายละเอียดของแพ็กเก็ตที่เลือก” (ดูรูปที่ 3 ในการเขียนแล็บ) เพื่อให้คุณสามารถเห็นฟิลด์ในส่วน TCP ที่มีข้อความ HTTP หมายเลขพอร์ตปลายทางคืออะไร (หมายเลขต่อจาก "Dest Port:" สำหรับเซ็กเมนต์ TCP ที่มีคำขอ HTTP) ที่คำขอ HTTP นี้ถูกส่งไป

และในที่สุดก็ ...

1. พิมพ์ข้อความ HTTP สองข้อความ (GET และ OK) ที่อ้างถึงในคำถามที่ 2 ข้างต้น โดยเลือกพิมพ์จากเมนูคำสั่ง File ของ Wireshark และเลือกปุ่ม “Selected Packet Only” และ “Print as displayed” จากนั้นคลิก ok