

## กิจกรรมที่ 5 : FTP และ DNS

กิจกรรมครั้งนี้จะเป็นการทำความเข้าใจกับโปรโตคอล FTP (File Transfer Protocol) และ DNS (Domain Name System) เพื่อเสริมสร้างความเข้าใจในการทำงานของโปรโตคอลทั้ง 2 ตัว

### FTP (File Transfer Protocol)

โปรโตคอล FTP จะใช้ 2 พอร์ต คือ พอร์ต 21 ใช้เป็น control channel คือเป็นช่องทางสำหรับรับส่งคำสั่ง และ พอร์ต 20 ใช้เป็น data channel ซึ่งใช้ในการรับส่งไฟล์

1. เปิดโปรแกรม Wireshark ให้กำหนดให้ capture เฉพาะ host test.rebex.net
2. เรียก Command Prompt แล้วป้อนคำสั่ง **ftp test.rebex.net** โดยให้ใส่ user เป็น demo และใช้ password เป็น password
3. ใช้คำสั่ง **dir** ในโปรแกรม ftp และบันทึก screenshot ภาพการทำงานของคำสั่ง dir จากนั้นกลับมาที่ Wireshark แล้วใช้ display filter เป็น ftp ให้เปรียบเทียบแต่ละคำสั่งของ ftp ว่าตรงกับ packet ใดที่ Wireshark ดักจับได้ ให้บันทึก screenshot ภาพของ Packet List Pane ที่แสดงคำสั่งมาแสดงด้วย

---

---

---

---

4. จาก packet ที่ได้ดักจับไว้ ให้ค้นหา packet ที่มีเนื้อหาระบุชื่อไฟล์ readme.txt (ซึ่งเป็นข้อมูลที่ ftp server ส่งมา) ว่าอยู่ใน packet ใด และส่งมาทางหมายเลข port ใด จากที่ระบุไว้ใน header ของ Transport Layer Protocol จากนั้นให้เปิดดูที่ Statistics -> Flow graph และนำมาอธิบายขั้นตอนการทำงานของคำสั่ง dir โดยละเอียด โดยอ้างอิงจาก Flow graph

---

---

---

---

---

---

---

---

5. ใช้คำสั่ง **get readme.txt** เพื่อดาวนโหลดไฟล์ readme.txt จาก ftp server เมื่อดาวนโหลดเสร็จสิ้นให้เปิดไฟล์ดังกล่าวด้วยโปรแกรม notepad และบันทึกภาพ screenshot นำมาแสดง (หากไม่รู้ path ของไฟล์ที่ดาวนโหลดมาแล้วว่าอยู่ที่ path ไบนเครื่อง ให้พิมพ์คำสั่ง **lcd** เพื่อแสดง current directory ของฝั่ง client) พร้อมทั้งนำภาพ screenshot จากหน้าโปรแกรม Wireshark ส่วนที่แสดงข้อมูลในการส่งไฟล์ readme.txt มาเปรียบเทียบด้วย

6. ให้คลิกขวาที่ packet ที่เป็นข้อมูลของ readme.txt และเลือก Follow TCP Stream และ Save as... เป็นไฟล์ ให้ตั้งชื่ออะไรก็ได้ จากนั้นเปิดไฟล์ด้วย notepad แล้วเปรียบเทียบกับไฟล์ readme.txt ว่ามีอะไรแตกต่างกันหรือไม่
- 

7. พิมพ์คำสั่ง disconnect เพื่อให้โปรแกรม ftp client ตัดการเชื่อมต่อกับ ftp server
8. พิมพ์คำสั่ง bye หรือ quit ก็ได้ เพื่อจบการทำงานของโปรแกรม ftp client
9. ให้เปิดไฟล์ ftp-clientside101.pcapng คลิกขวาที่ packet ที่ 6 (USER anonymous) และเลือก Follow TCP Stream ให้บันทึก screenshot หน้าต่าง Follow TCP Stream ที่แสดงการโต้ตอบของ FTP ให้อธิบายว่ามีคำสั่งของ FTP Protocol อะไรบ้าง (ระบุชื่อ FTP Commands ไม่ใช่คำสั่งของโปรแกรม)
- 
-

10. จากนั้นที่หน้าต่างของ Follow TCP Stream ให้เลือก Filter Out this Stream และให้ดูที่ display filter ว่าแสดงว่าอะไร จากนั้นคลิกขวาที่ packet 16 และเลือก Follow TCP Stream อีกครั้งและเลือก Filter Out this Stream อีกครั้ง
11. จากนั้นคลิกที่ packet ใดก็ได้และเลือก Follow TCP Stream คลิก Save as ให้ตั้งชื่อ pantheon.jpg โดยเลือกชนิดเป็น raw และให้เปิดภาพขึ้นมาดูว่าเป็นภาพอะไร

---

---

12. ให้อธิบายว่าการทำงานในข้อ 10. ทำเพื่ออะไร

---

---

13. ให้เปิดไฟล์ ftp-download-good2.pcapng ให้หาคำตอบว่าเวลาที่ใช้ในการโหลดไฟล์ "SIZE OS Fingerprinting with ICMP.zip" เท่ากับเท่าไร อธิบายวิธีการ

---

---

---

---

---

---

---

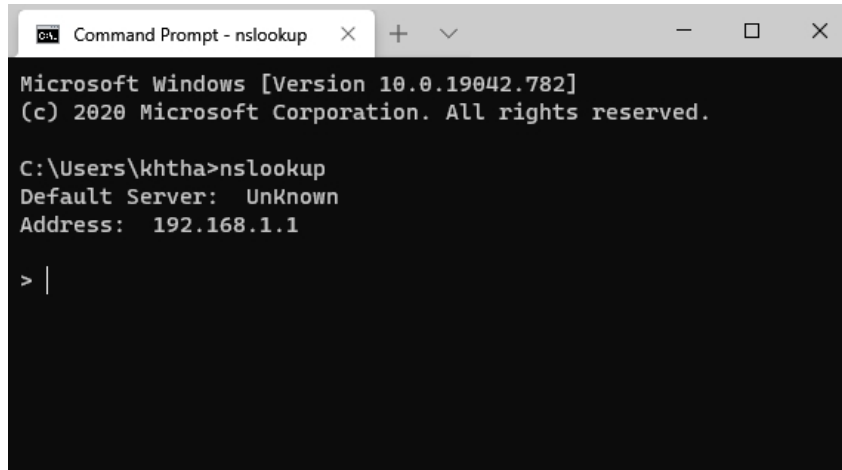
---

---

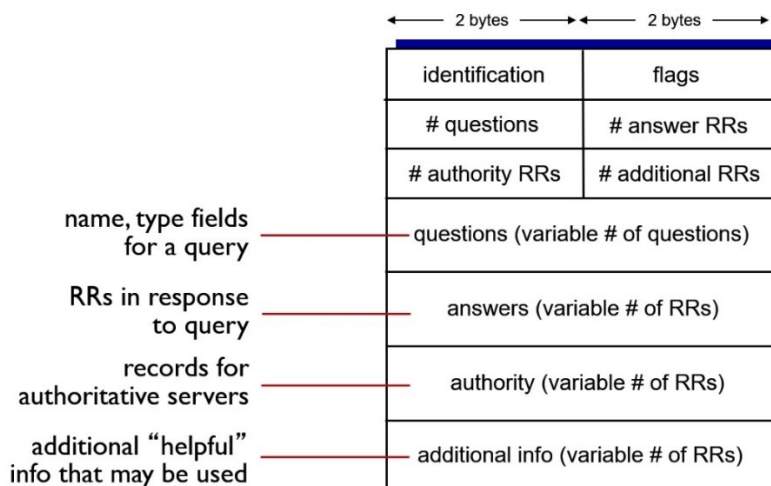
---

## DNS (Domain Name System)

โปรโตคอล DNS จะใช้พอร์ต 53 โดยระบบปฏิบัติการส่วนใหญ่จะมีโปรแกรมชื่อว่า nslookup ซึ่งสามารถใช้ติดต่อกับ DNS Server ได้ ในกรณีของ Windows ให้เรียก Command Prompt จากนั้นให้เรียกโปรแกรม nslookup (หากใช้ระบบปฏิบัติการอื่นก็ทำคล้ายกัน) จะปรากฏหน้าจอดังรูป



14. ให้เปิดโปรแกรม Wireshark เพื่อ capture โดยกำหนดเงื่อนไขให้ capture เฉพาะโปรโตคอล DNS จากนั้นในหน้าต่างที่เรียก nslookup ไว้แล้ว ให้พิมพ์ **server 161.246.52.21** ลงไป (เป็นการกำหนดให้เชื่อมต่อกับ DNS Server ที่มี IP Address 161.246.52.21 แทน Default Server) ให้ตอบว่า 161.246.52.21 มีชื่อ Domain Name อะไร \_\_\_\_\_



15. ให้พิมพ์ [www.ce.kmitl.ac.th](http://www.ce.kmitl.ac.th) ป้อนให้กับโปรแกรม nslookup จากนั้นหยุด capture และตอบคำถามดังนี้
- ใน DNS query มี # questions เท่าไร และข้อมูลใน questions คืออะไร type เป็นค่าอะไร ให้บันทึก screenshot ส่วนของ Packet Details Pane นำมาแสดงประกอบด้วย

---

---

- ใน DNS response มี # answer เท่าไร และข้อมูลใน answer คืออะไร ให้บันทึก screenshot ส่วนของ Packet Details Pane ประกอบด้วย

---

---

- มี query และ response กี่ packet ให้บันทึก screenshot ส่วนของ Packet Details Pane ด้วย

---

---

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

---

---

- ใน DNS query มี # questions เท่าไร และข้อมูลใน questions คืออะไร type เป็นค่าอะไร ให้นัก screenshot ส่วนของ Packet Details Pane นำมาแสดงประกอบด้วย

---

---

- ใน DNS response มี # answer เท่าไร และข้อมูลใน answer คืออะไร ให้นัก screenshot ส่วนของ Packet Details Pane ประกอบด้วย

---

---

- มี query และ response ที่ packet ให้นัก screenshot ส่วนของ Packet Details Pane ด้วย

---

---

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

---

---

17. ให้ใช้โปรแกรม nslookup แล้วตั้ง server เป็น 199.7.91.13 จากนั้นให้ บ้อน 199.7.91.13 โปรแกรมแสดงผลอะไรมาบ้าง ให้บันทึก screenshot มาแสดง นักศึกษาคิดว่า 199.7.91.13 เป็น server อะไร
- 

18. ให้บ้อน query เป็น www.ce.kmitl.ac.th แสดงผลอะไรมาบ้าง ให้บันทึก screenshot มาแสดง จากนั้นให้ใช้ IP Address ของ ns.thnic.net เป็น server และบ้อน query เป็น ac.th, kmitl.ac.th และ ce.kmit.ac.th ตามลำดับ ให้บันทึก screenshot มาแสดง และให้นักศึกษาวาดรูปการทำ name resolution ของ www.ce.kmitl.ac.th โดยสมมติให้เครื่องที่ request เป็นเครื่องที่อยู่ต่างประเทศ





19. ให้เปิดไฟล์ tr-dns-slow.pcapng แล้วหา packet response ของ DNS แล้วขยายส่วนที่เป็น DNS หาข้อมูลเวลา จากนั้นให้สร้างเป็นคอลัมน์ ตั้งชื่อเป็น DNS Delta
  20. ให้ sort แล้วดูว่ามี DNS query/response ใด ที่ใช้เวลาเกิน 1 วินาที ให้บันทึก screenshot มาแสดง
- 

21. ให้เปิด Wireshark เพื่อ capture ใหม่ โดยให้ดักจับเฉพาะข้อมูล DNS จากนั้นให้ใช้โปรแกรม nslookup โดยให้กำหนด server เป็น 161.246.4.3 จากนั้นให้ query www.ce.kmitl.ac.th จากนั้นเปลี่ยน server เป็น 161.246.52.21 และ 8.8.8.8 ตามลำดับ ให้เปรียบเทียบ DNS Delta ที่ได้จากแต่ละ server (แสดงตัวเลขที่ได้) จากนั้นให้วิเคราะห์ผล
- 
- 
- 
- 

#### งานครั้งที่ 5

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา ตามด้วย section และ \_lab05 ตามตัวอย่างต่อไปนี้  
64019999\_sec20\_lab05.pdf
- กำหนดส่ง ภายในวันที่ 17 กุมภาพันธ์ 2566 โดยให้ส่งใน Microsoft Teams ของรายวิชา