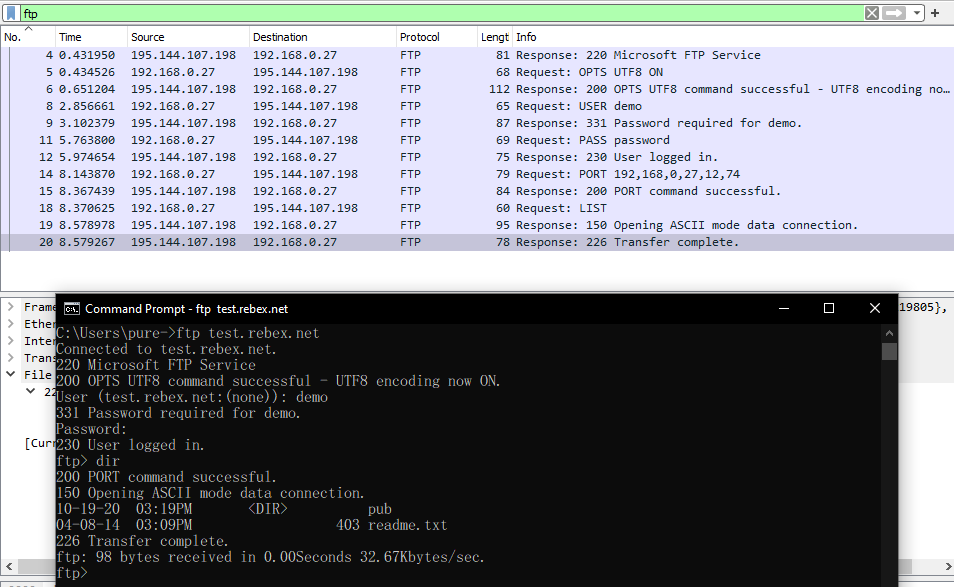
3. ใช้คำสั่ง dir ในโปรแกรม ftp และ capture ภาพการทำงานของคำสั่ง dir จากนั้นกลับมาที่ Wireshark แล้วใช้ display filter เป็น ftp ให้เปรียบเทียบระหว่างคำสั่งของ ftp ที่ใช้กับ packet ของ Wireshark ที่ดักจับได้ ให้ capture ภาพของ packet list pane ที่แสดงคำสั่งมาแสดงด้วย



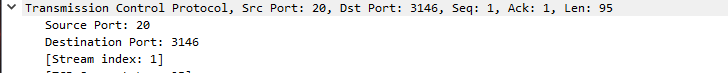
เปรียบเทีบคำสั่งในโปรแกรม ftp กับ wireshark

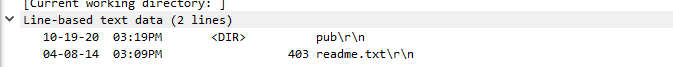
คำสั่ง dir (ftp) จะแปลงเป็นคำสั่ง LIST (wireshark)

คำสั่ง User เป็น USER

คำสั่ง Password เป็น PASS

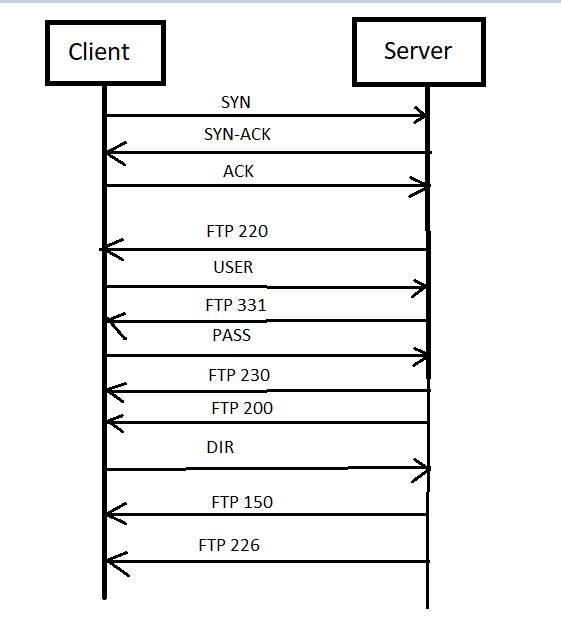
4. ให้ค้นหา packet ที่ได้ดักจับไว้ ที่มีชื่อไฟล์ readme.txt (ซึ่งเป็นข้อมูลที่ ftp server ส่งมา) ว่าส่งมาทาง port ใด และอยู่ใน packet ใด จากนั้นให้วาดภาพแสดงการทำงานของ ftp สำหรับคำสั่ง dir ข้างต้น ว่ามีการส่งข้อมูลอย่างไร 





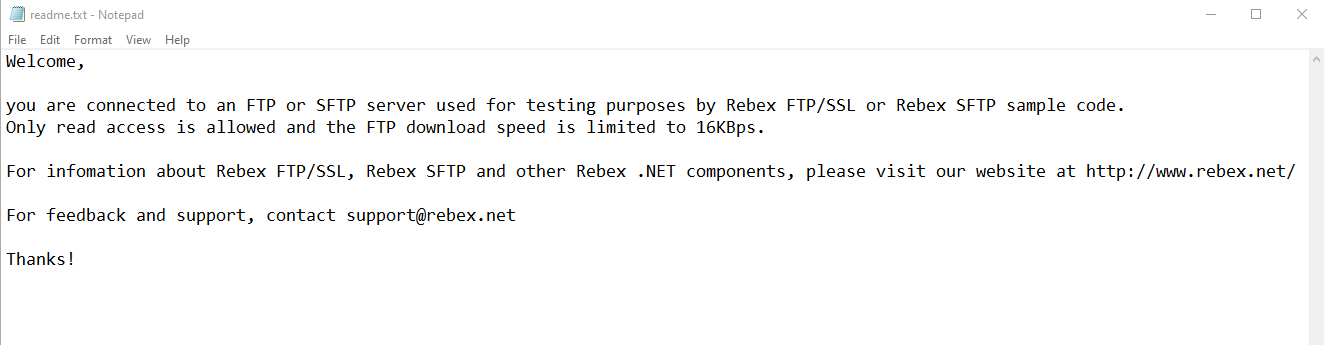
ส่งมาทาง port : 20

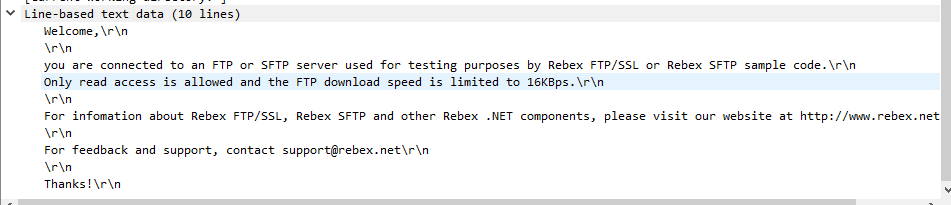
อยู่ใน packet ที่ 22



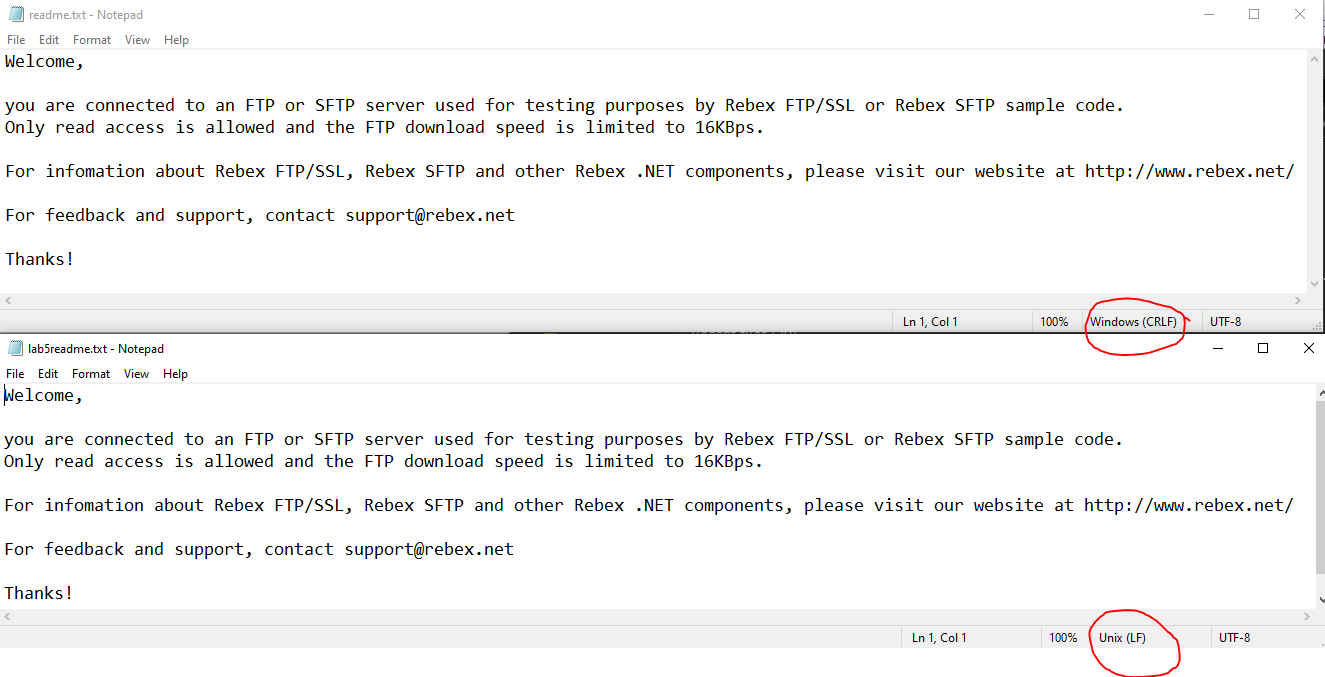
ภาพแสดงการทำงาน

5. ใช้คำสั่ง get readme.txt เพื่อรับไฟล์ readme.txt จาก ftp server จากนั้นให้เปิดไฟล์ใน notepad และ capture มาแสดง และ capture ข้อมูลใน Wireshark ที่เป็นการส่งไฟล์ readme.txt มาเปรียบเทียบ



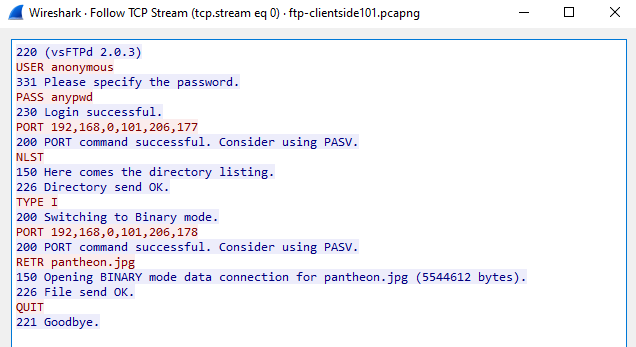


6. ให้คลิกขวาที่ packet ที่เป็นข้อมูลของ readme.txt และเลือก Follow TCP Stream และ Save as… เป็นไฟล์ ให้ตั้งชื่ออะไรก็ได้ จากนั้นเปิดไฟล์ด้วย notepad แล้วเปรียบเทียบกับไฟล์ readme.txt ว่ามีอะไรแตกต่างกันหรือไม่



ข้อความเหมือนกัน แต่ต่างกันที่ที่วงสีแดงไว้

7. ให้เปิดไฟล์ ftp-clientside101.pcapng คลิกขวาที่ Packet 6 (USER anonymous) และเลือก Follow TCP Stream ให้ Capture การโต้ตอบของ FTP ให้อธิบายว่ามีคำสั่งของ FTP Protocol อะไรบ้าง



มีคำสั่งของ FTP Protocol

USER - ชื่อผู้ใช้เพื่อเข้าสู่เซิร์ฟเวอร์

PASS - รหัสผ่าน

PORT - เข้าสู่โหมดใช้งาน

NLST  - ส่งคืนรายการไฟล์ไดเร็กทอรีในรูปแบบที่สั้นกว่า LIST รายการจะถูกส่งผ่านการเชื่อมต่อข้อมูล

TYPE I - ตั้งค่าประเภทการถ่ายโอนไฟล์

RETR - ดาวน์โหลดไฟล์

QUIT – ตัดการเชื่อมต่อ

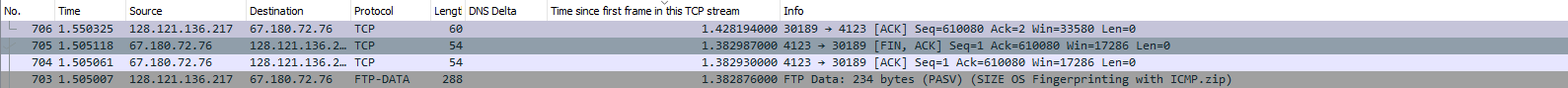
9. จากนั้นคลิกที่ packet ใดก็ได้และเลือก Follow TCP Stream คลิก Save as ให้ตั้งชื่อ pantheon.jpg โดยเลือกชนิดเป็น raw และให้เปิดภาพขึ้นมาดูว่าเป็นภาพอะไร



10. ให้อธิบายว่าการทำงานในข้อ 8 ทำเพื่ออะไร

ทำเพื่อกรองเฉพาะ packet ที่เกี่ยวข้องกับไฟล์ pantheon.png

11. ให้เปิดไฟล์ ftp-download-good2.pcapng ให้หาคำตอบว่าเวลาที่ใช้ในการโหลดไฟล์ “SIZE OS Fingerprinting with ICMP.zip” เท่ากับเท่าไร อธิบายวิธีการ



เวลาที่ใช้ในการโหลดไฟล์ 1.428194000 วินาที

วิธีการ

1.กด ctrl+f หาคำว่า SIZE OS Fingerprinting with ICMP.zip

2.กดที่ packet เลือก follow TCP Stream

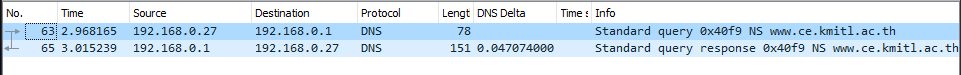
3.ไปที่ timestamp กดที่ Time since first frame in this TCP stream เลือก apply as column

4.กด sort ที่คอลัมน์ Time since first frame in this TCP stream แล้วดูเวลาที่มากที่สุด

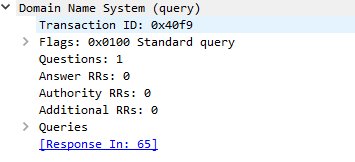
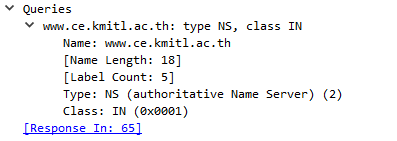
12. ให้เปิดโปรแกรม Wireshark กำหนดเงื่อนไขให้ Capture เฉพาะโปรโตคอล DNS พิมพ์ server 161.246.52.21 ลงไป (เป็นการกำหนดให้เชื่อมต่อกับ DNS Server ที่มี IP Address 161.246.52.21 แทน Default Server) ให้ตอบว่า 161.246.52.21 มีชื่อ Domain Name อะไร 

มีชื่อ Domain Name : nsl.kmitl.ac.th

13. ให้พิมพ์ www.ce.kmitl.ac.th และหยุด Capture ให้ตอบคำถามดังนี้



- ใน DNS Query มี # questions เท่าไร และข้อมูลใน questions คืออะไร type เป็นค่าอะไร ให้ Capture ส่วนของ Packet Details Pane ประกอบด้วย

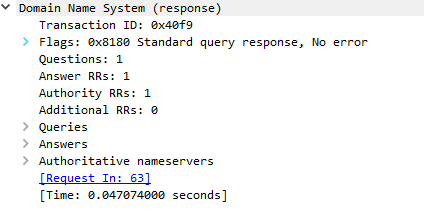
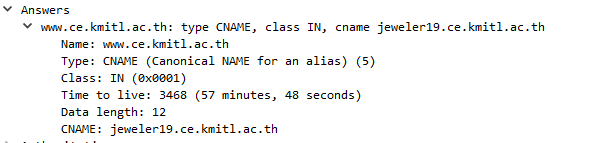
 

มี 1 question

ข้อมูลใน questions

Name : [www.ce.kmitl.ac.th](http://www.ce.kmitl.ac.th) , Type: NS , Class: IN

- ใน DNS Response มี # answer เท่าไร และข้อมูลใน answer คืออะไร ให้ Capture ส่วนของ Packet Details Pane ประกอบด้วย

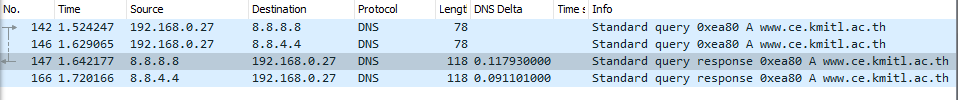
 

มี 1 answer

ข้อมูลใน answer

1. Name : www.ce.kmitl.ac.th , Type : CNAME, Class : IN, CNAME : jeweler19.ce.kmitl.ac.th
2. Name : jeweler19.ce.kmitl.ac.th , Type: A , Class : IN, Address : 161.246.4.119

- มี query และ response กี่ packet ให้ Capture ส่วนของ Packet Details Pane ด้วย



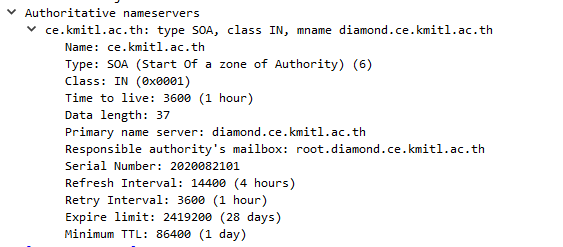
มี query 1 packet

มี response 1 packet

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

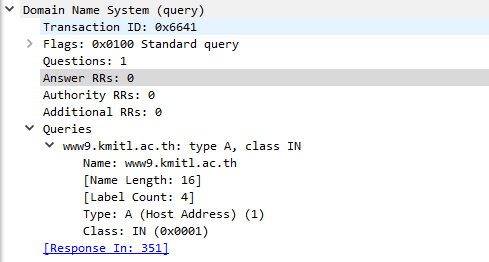
มี authority

มีข้อมูลตามรูป



14. ทำตามข้อ 13 อีกครั้ง แต่ใช้ 161.246.4.119 แทนที่จะใช้ [www.ce.kmitl.ac.th](http://www.ce.kmitl.ac.th)

- ใน DNS Query มี # questions เท่าไร และข้อมูลใน questions คืออะไร type เป็นค่าอะไร ให้ Capture ส่วนของ Packet Details Pane ประกอบด้วย



มี 1 question

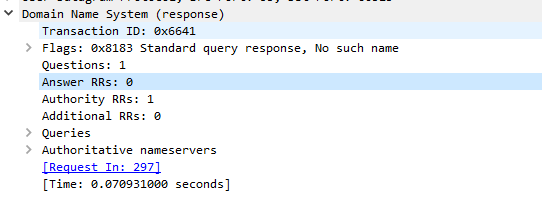
ข้อมูลใน questions

Name : www9.kmitl.ac.th

Type: A (IPv4)

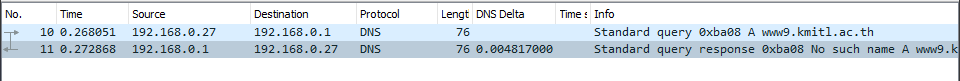
Class: IN

- ใน DNS Response มี # answer เท่าไร และข้อมูลใน answer คืออะไร ให้ Capture ส่วนของ Packet Details Pane ประกอบด้วย



มี 0 answer

- มี query และ response กี่ packet ให้ Capture ส่วนของ Packet Details Pane ด้วย



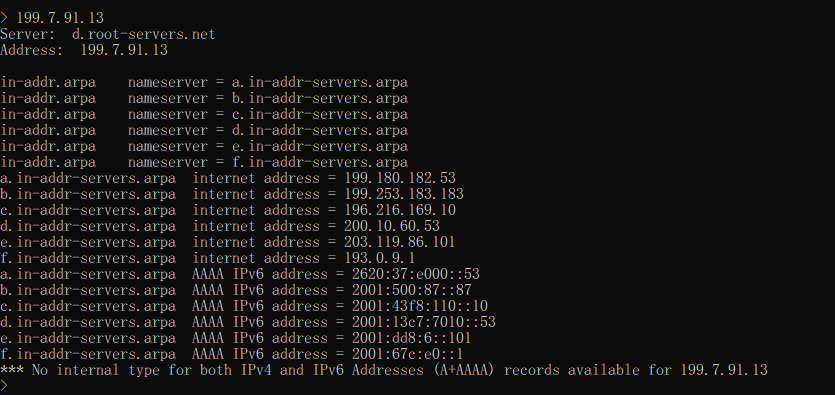
มี query 1 packet

มี response 1 packet

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

ไม่มี

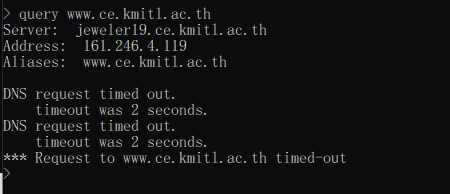
15. ให้ใช้โปรแกรม nslookup แล้วตั้ง server เป็น 199.7.91.13 จากนั้นให้ ป้อน 199.7.91.13 โปรแกรมแสดงผลอะไรมาบ้าง ให้ capture มาแสดง นักศึกษาคิดว่า 199.7.91.13 เป็น server อะไร



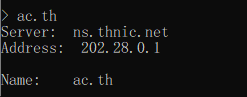
เป็น root server

16. ให้ป้อน query www.ce.kmitl.ac.th แสดงผลอะไรมาบ้าง ให้ capture มาแสดง จากนั้นให้ใช้ IP Address ของ ns.thnic.net เป็น server จากนั้นให้ป้อน ac.th, kmitl.ac.th และ ce.kmit.ac.th ตามลำดับ ให้ capture มาแสดง และให้นักศึกษาวาดรูปการทำ name resolution ของ www.ce.kmitl.ac.th โดยสมมติให้เครื่องที่ request เป็นเครื่องที่อยู่ต่างประเทศ

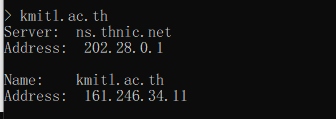
ป้อน query www.ce.kmitl.ac.th



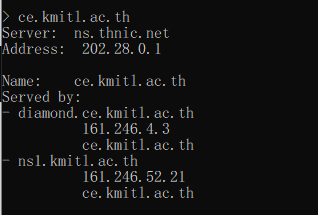
ป้อน ac.th

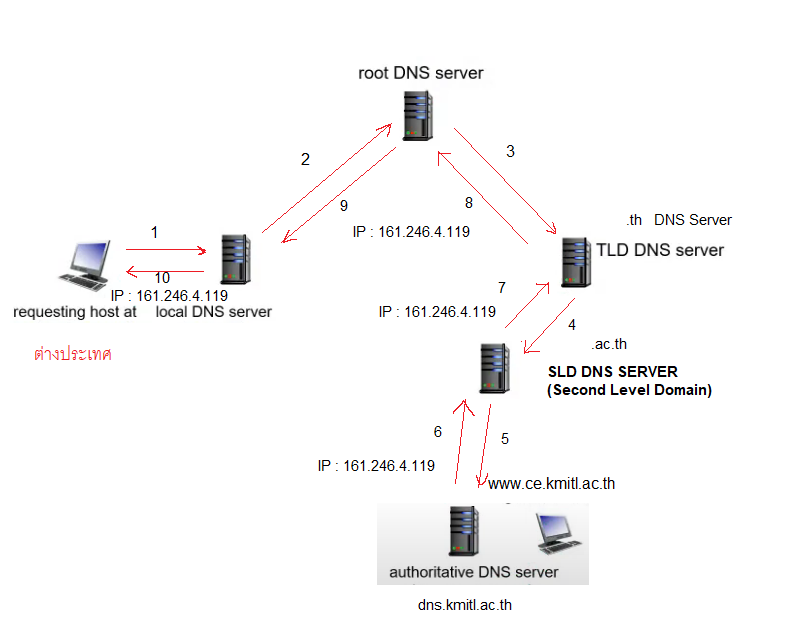


ป้อน kmitl.ac.th



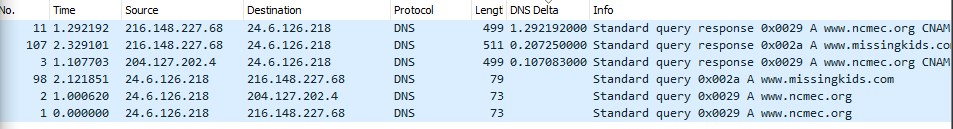
ป้อน ce.kmitl.ac.th





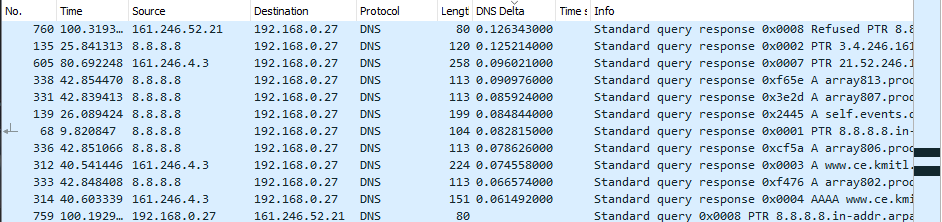
name resolution

18. ให้ Sort แล้วดูว่ามี DNS Query/Response ใด ที่ใช้เวลาเกิน 1 วินาที



มี 1 response packet ที่ 11 ใช้เวลา 1.292192000

19. ให้เริ่ม capture ใหม่เฉพาะข้อมูล DNS จากนั้นให้ใช้โปรแกรม nslookup และกำหนด 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



1. 161.246.52.21 (0.126343000)
2. 8.8.8.8 (0.125214000)
3. 161.246.4.3 (0.096021000)

วิเคราะห์

จาก DNS Delta ที่ได้ server 161.246.52.21 จะใช้เวลาเยอะที่สุด server 8.8.8.8 ลองลงมา และ 161.246.52.21 ใช้เวลาน้อยที่สุด