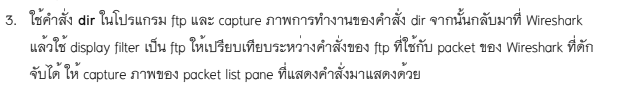
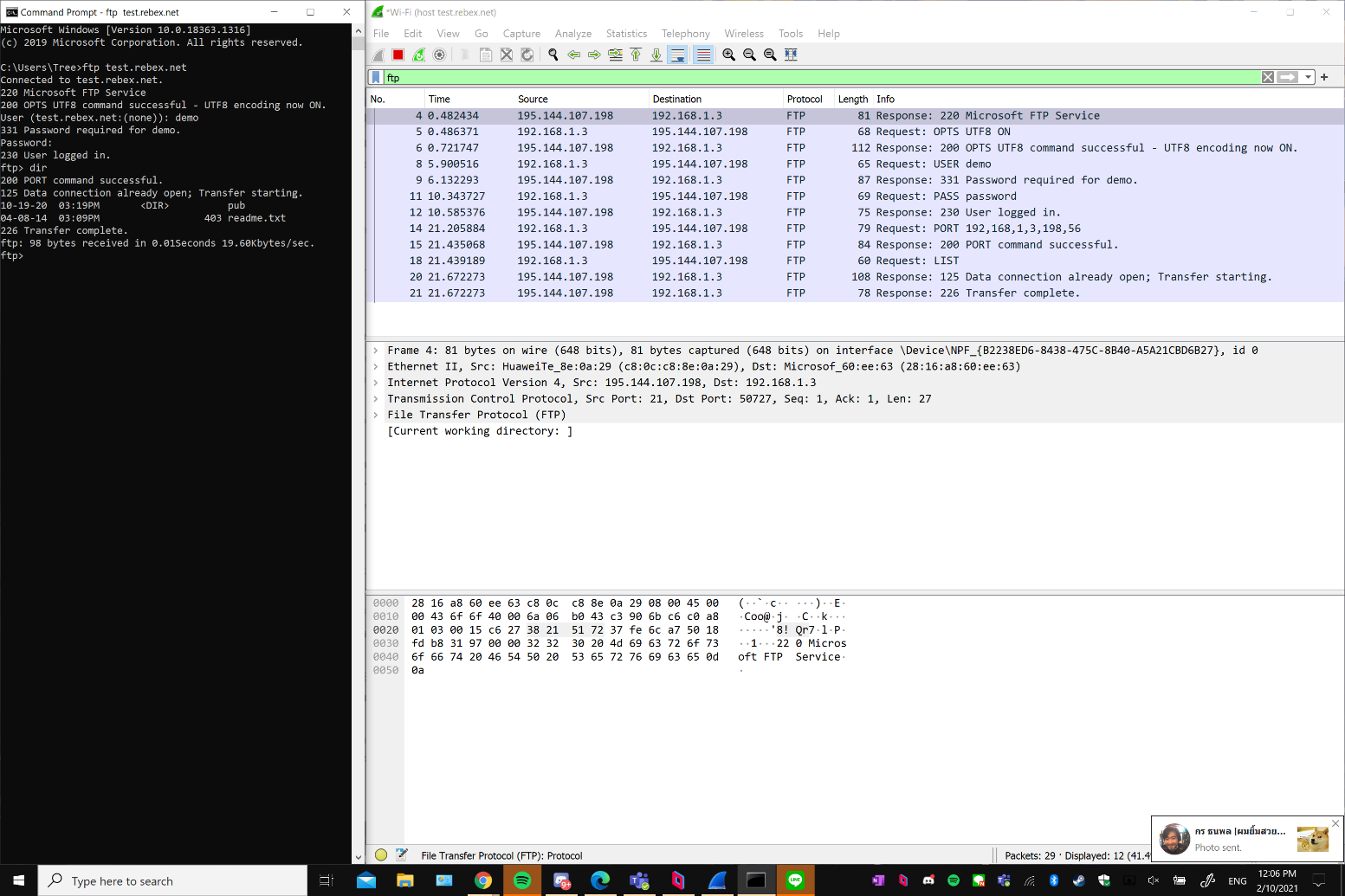
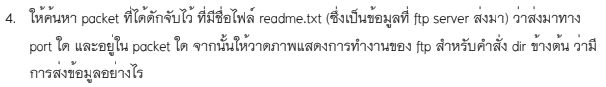
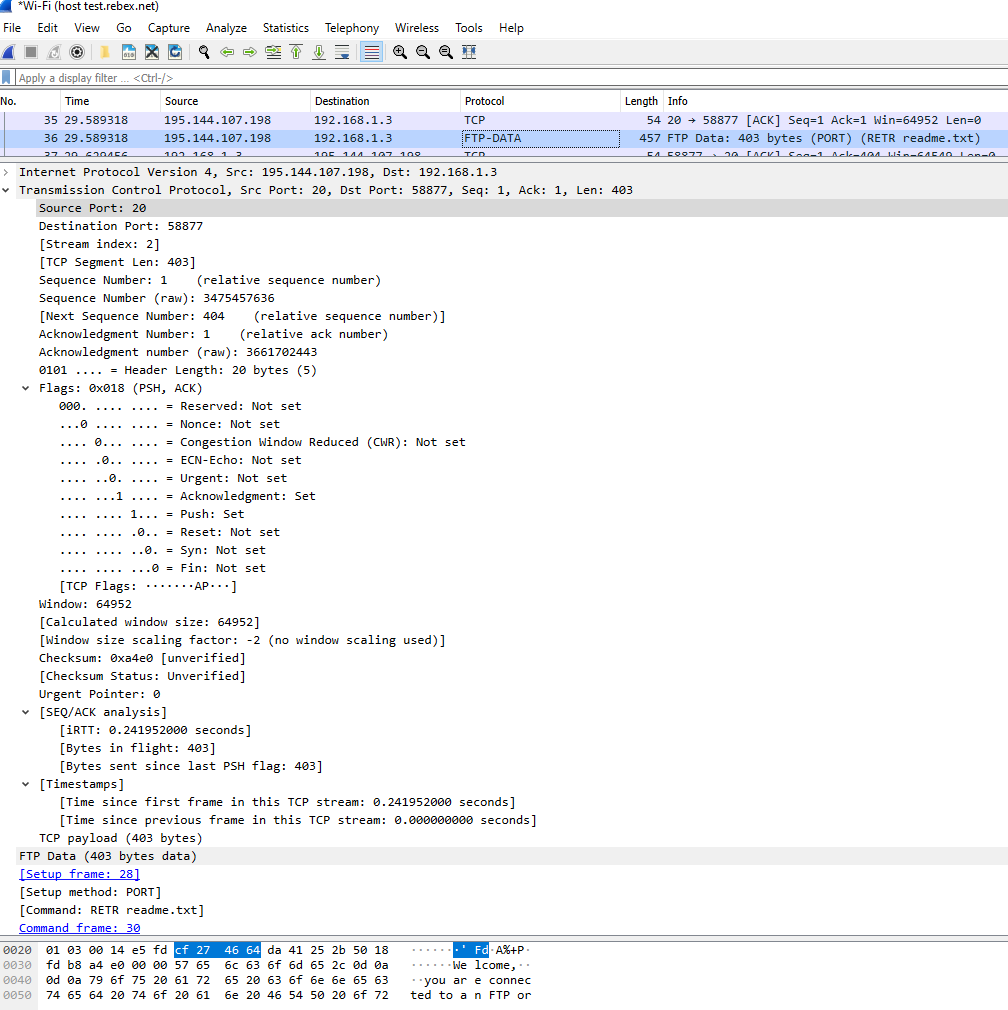
**นายภากรณ์ ธนประชานนท์ 62010694**

****

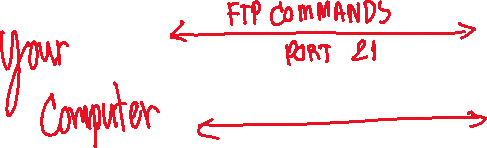
****

****

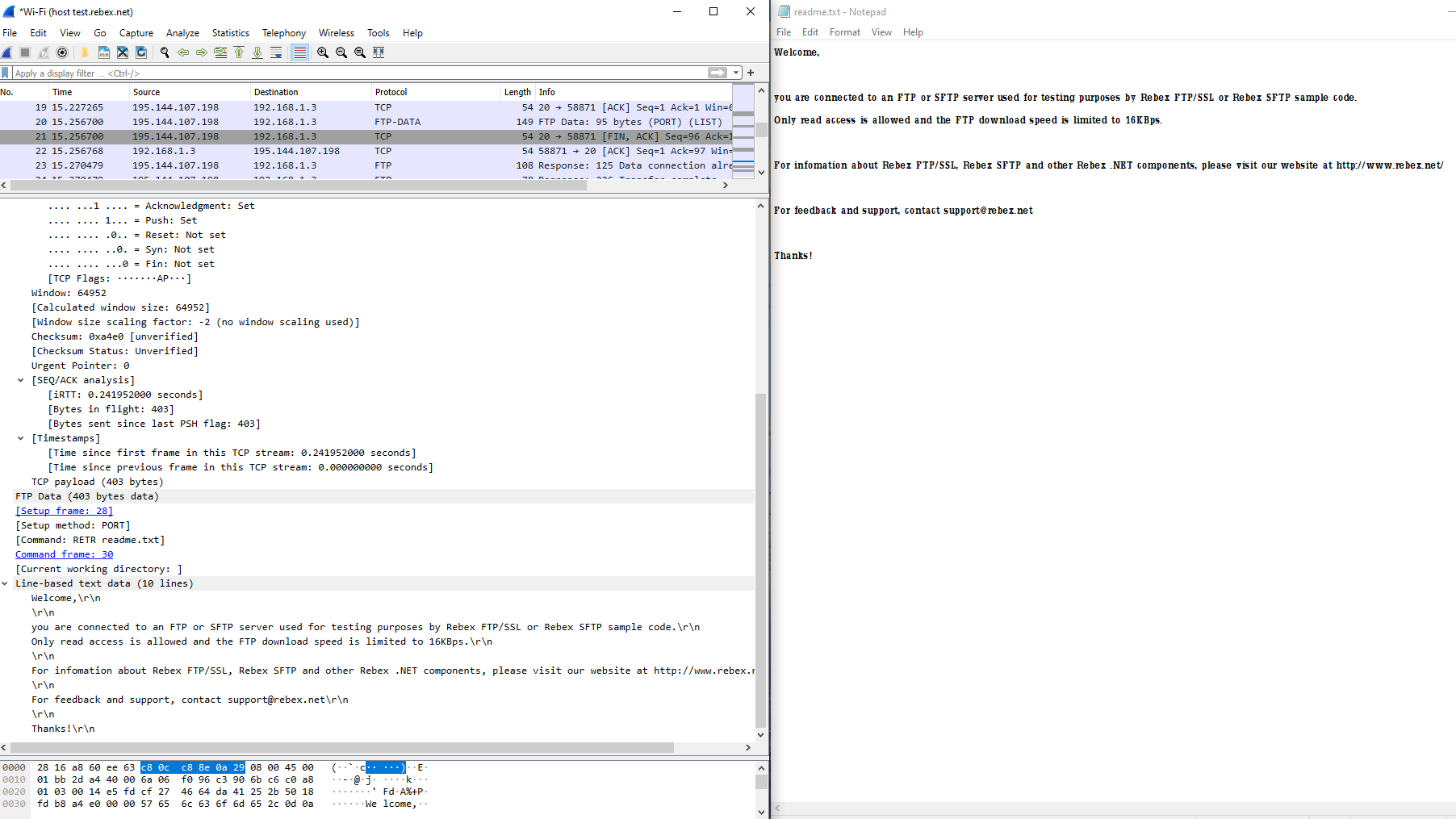
****

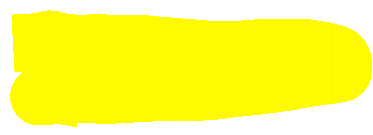


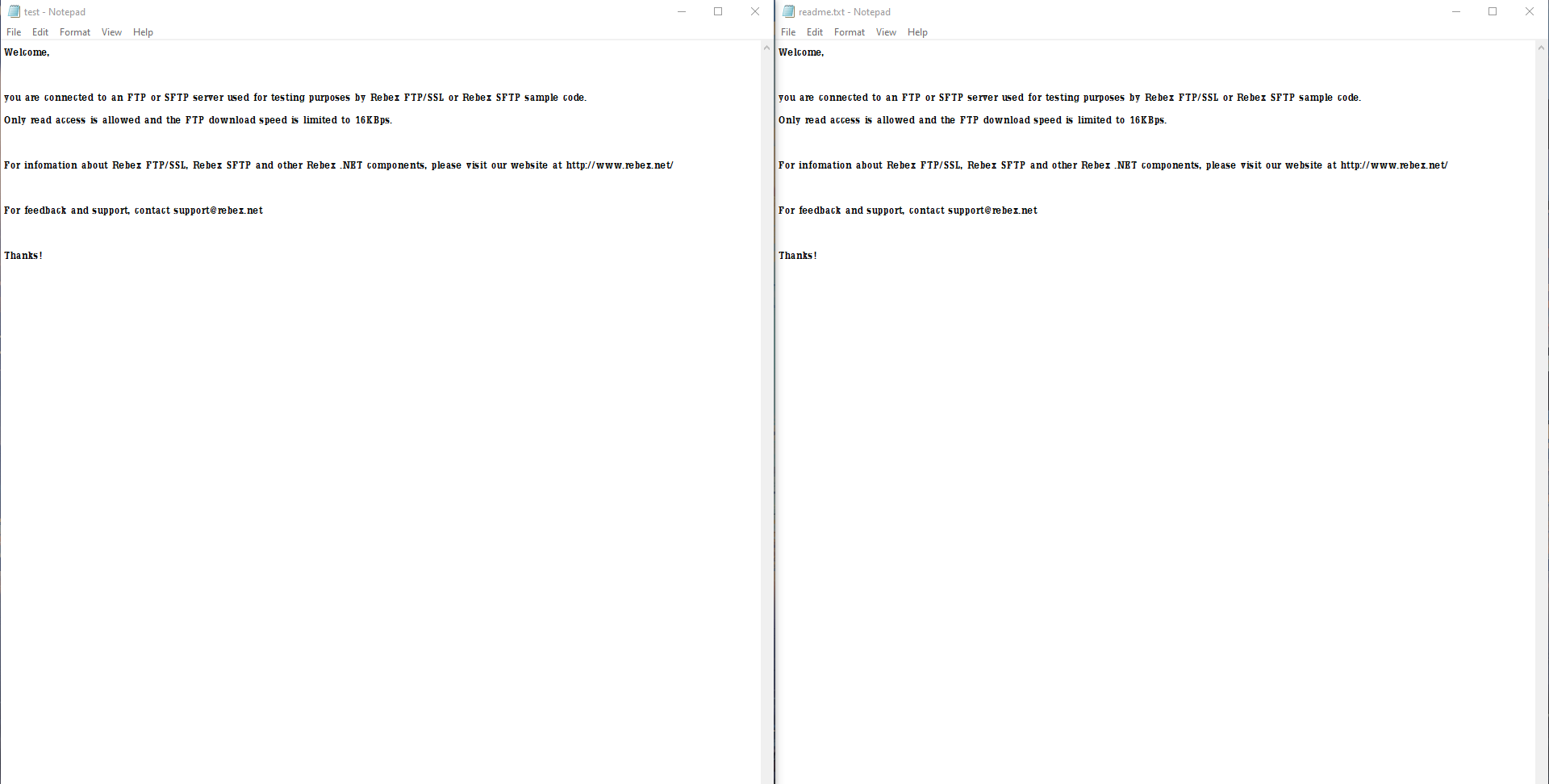
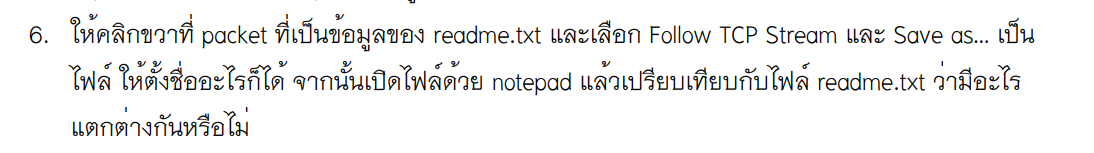
**มี Source Port เป็น 20 Destination Port เป็น 58877 อยู่ใน Packet ที่ 36 ซึ่งเป็นการ RETR readme.txt จาก 195.144.107.198 มาที่ 192.168.1.3 โดย Protocol FTP-DATA**



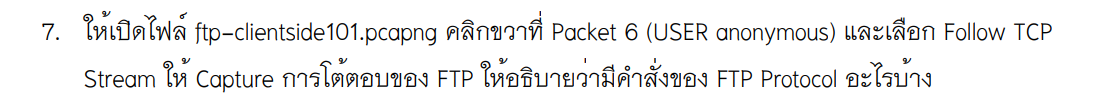
****

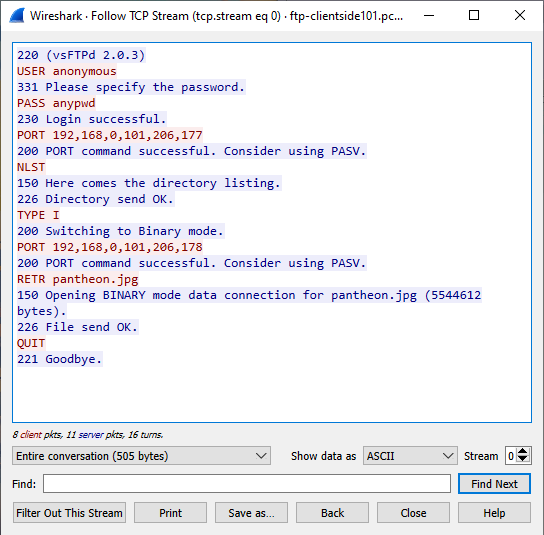
****



****

**เหมือนกัน**

****

****

**-USER ทำการส่ง User** **Identification ไปให้ Server (ชื่อผู้ใช้ anonymous)**

**-PASS ทำการส่ง User** **Password ไปให้ Server (รหัส anypwd)**

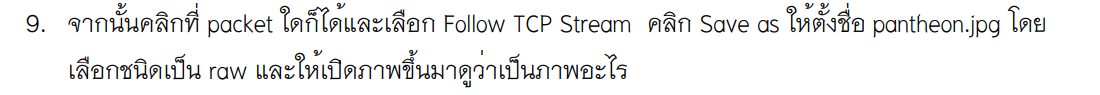
**-PORT สร้างการเชื่อมต่อกับผู้ใช้งานเพื่อส่งไฟล์ผ่าน Port 20**

**-NLST ส่ง List Directory ให้กับผู้ใช้**

**-TYPE บอกชนิดบอกไฟล์ที่ต้องการ**

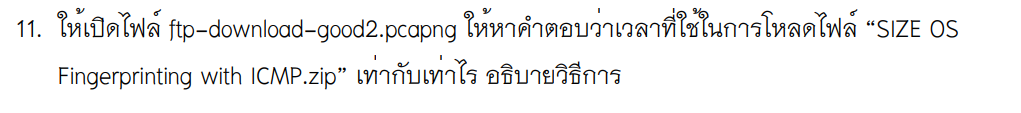
**-RETR ทำการร้องขอไฟล์จาก FTP Server (pantheon.jpg)**

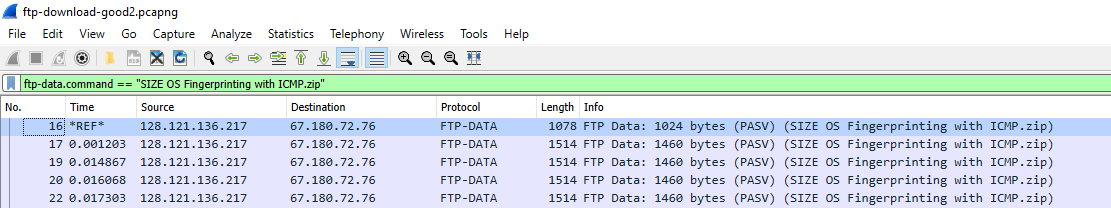
**-QUIT ออกจากการใช้งาน FTP พร้อมปิดการเชื่อมต่อ**

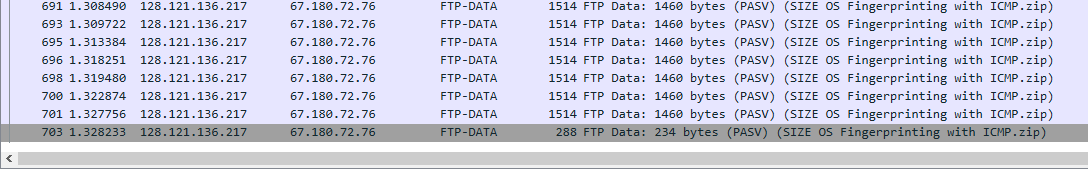
****

****

**เพื่อกรอง Packet TCP Stream ที่ไม่ต้องการเห็นออกด้วยเงื่อนไข !(tcp.stream eq 0) and !(tcp.stream eq 1) หลังจากนั้นจะได้ TCP Stream ที่เราทำการ Follow เอาไว้**

****

****

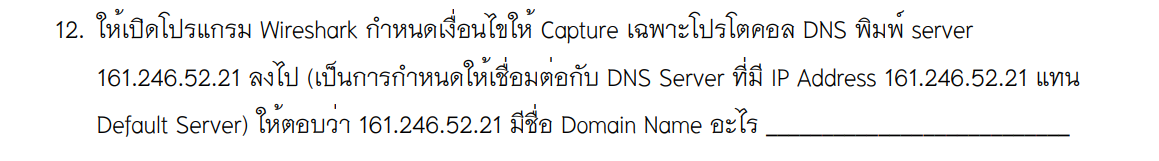
****

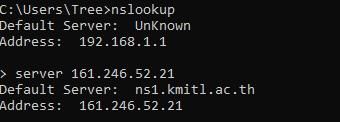


**Display Filter ใช้ “ftp-data.command == "SIZE OS Fingerprinting with ICMP.zip"”**

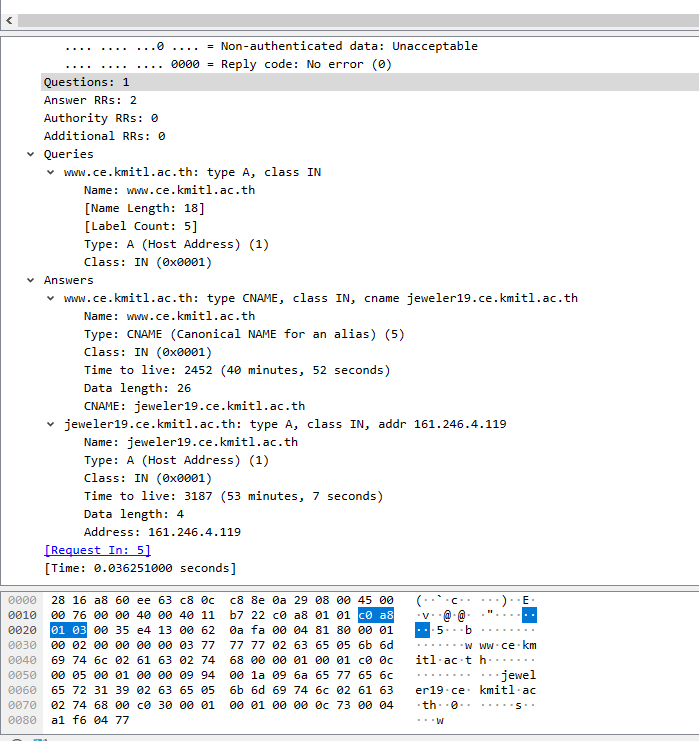
**Ctrl-T ที่ Packet แรกที่เริ่มโหลดMark เป็น Ref เวลา**

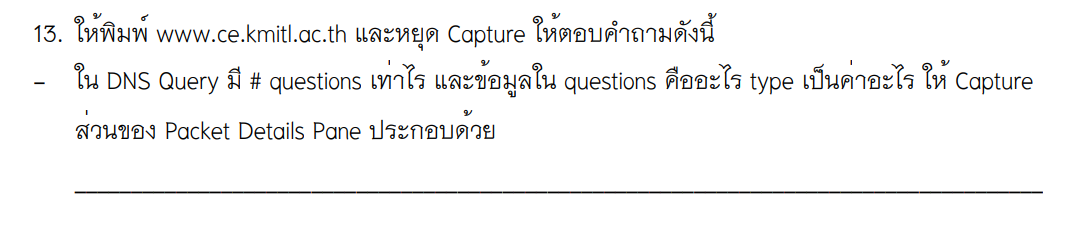
**หา Packet สุดท้ายที่โหลด และอ่านค่าเวลา ซึ่งอ่านได้ 1.328233 วินาที**

****

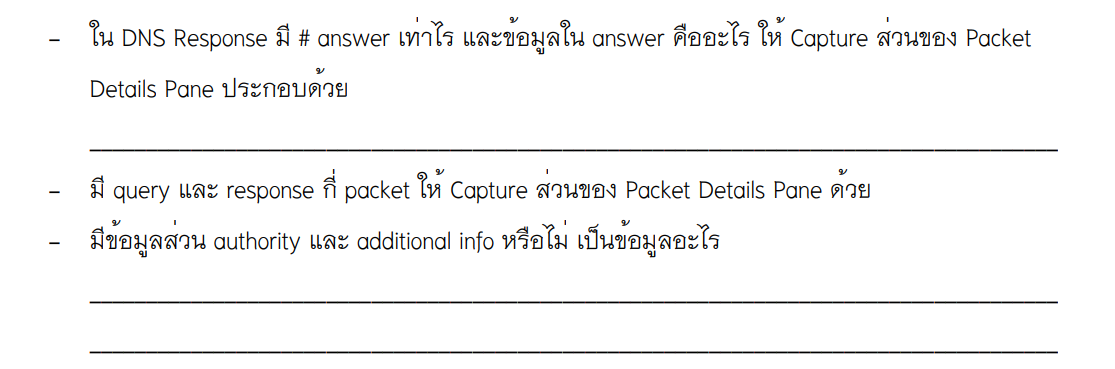
****

**ns1.kmitl.ac.th**

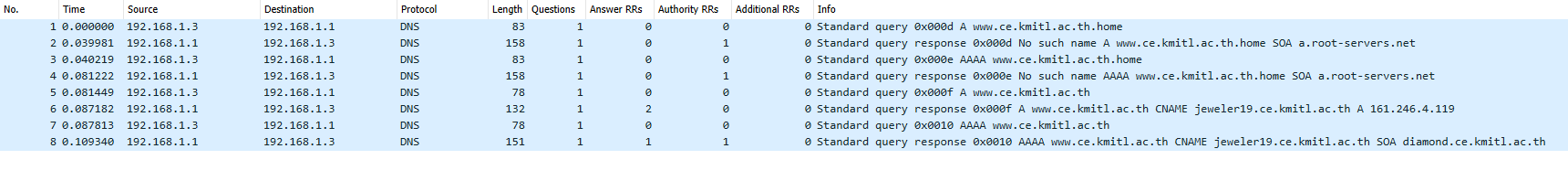
****

****

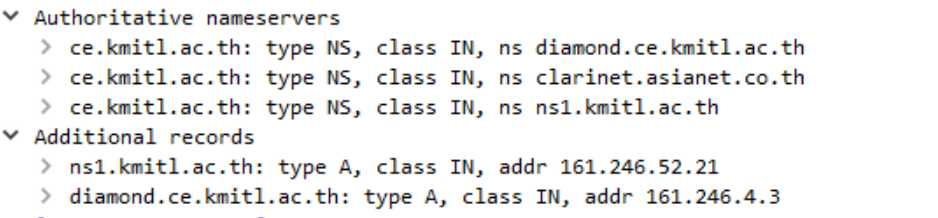
**1 Question ซึ่งมีข้อมูลเป็น www.ce.kmitl.ac.th, type A Class IN เป็น Type A**

****

**มี 2 Answer เป็น [www.ce.kmitl.ac.th](http://www.ce.kmitl.ac.th) : type CNAME , class IN , cname jeweler19.ce.kmitl.ac.th และ jeweler19.ce.kmitl.ac.th : type A , class IN , addr 161.246.4.119**

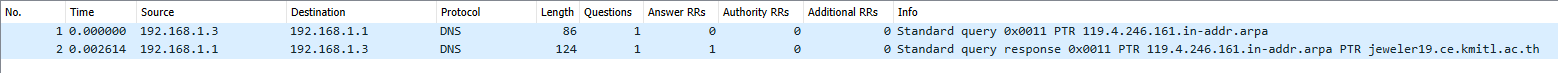
****

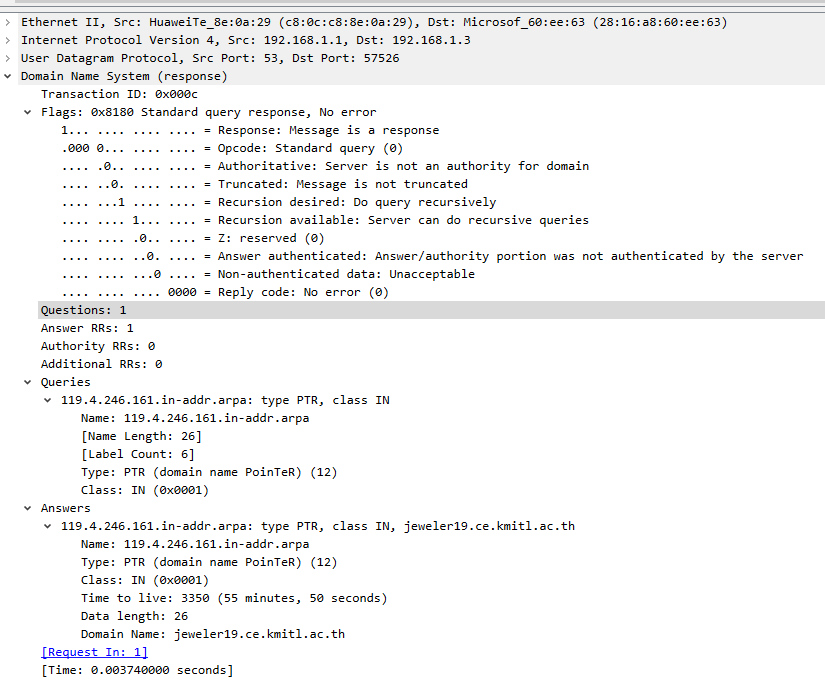
**มี 8 packet**

****

**มี เป็นข้อมูลตามในภาพซึ่งเป็น ชื่อของ server ทั้งหมด และ ip ทั้งหมดของ server ตามลำดับ**

****



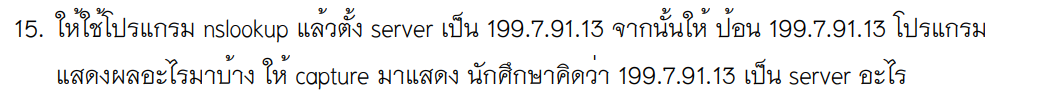
****

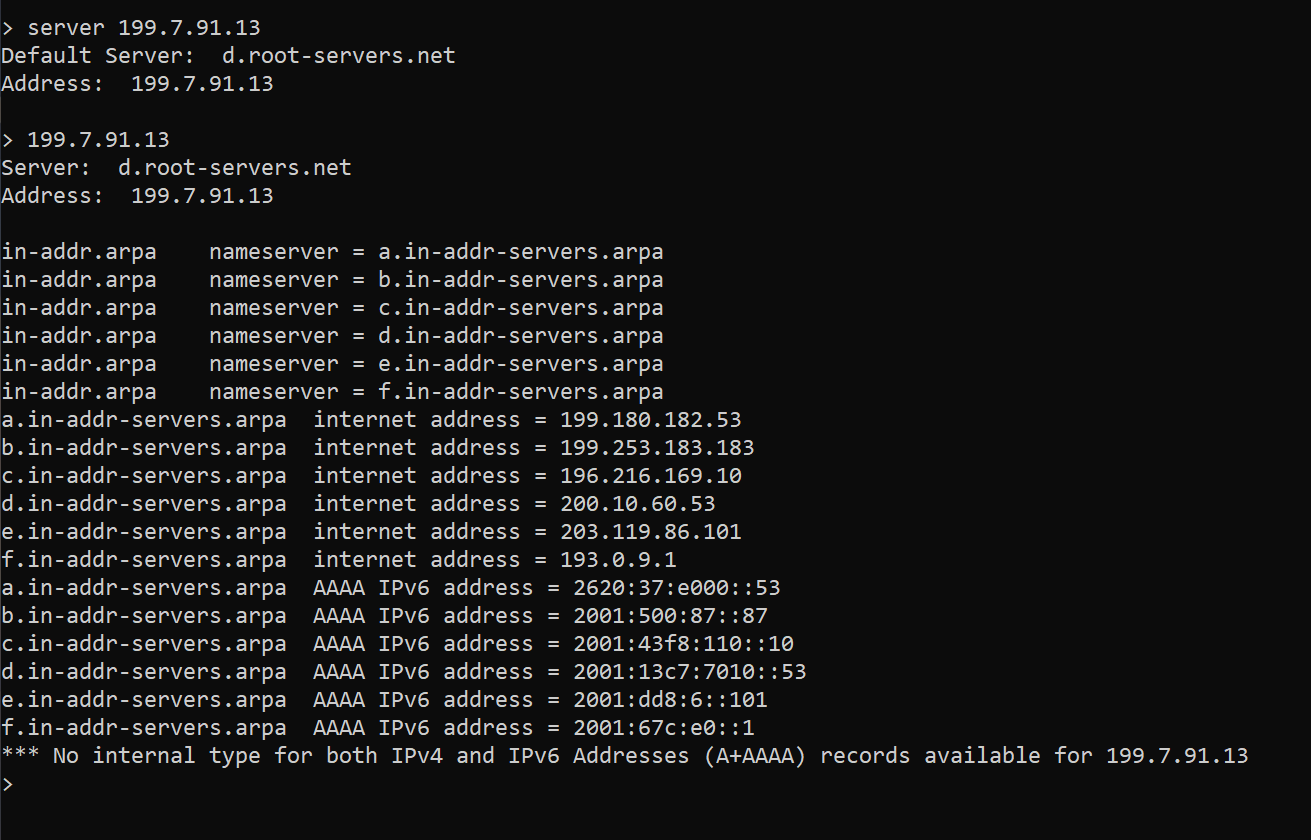
**มี 1 Question เป็น 119.4.246.161 ,type PTR ,class IN**

**มี 1 Answer เป็น 119.4.246.161 type PTR, class IN, jeweler19.ce.kmitl.ac.th**

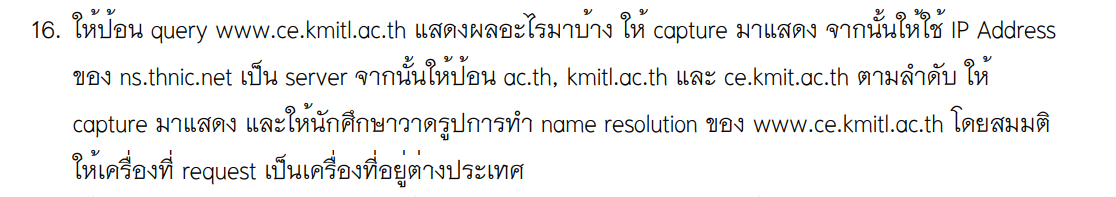
**มี 2 Packet**

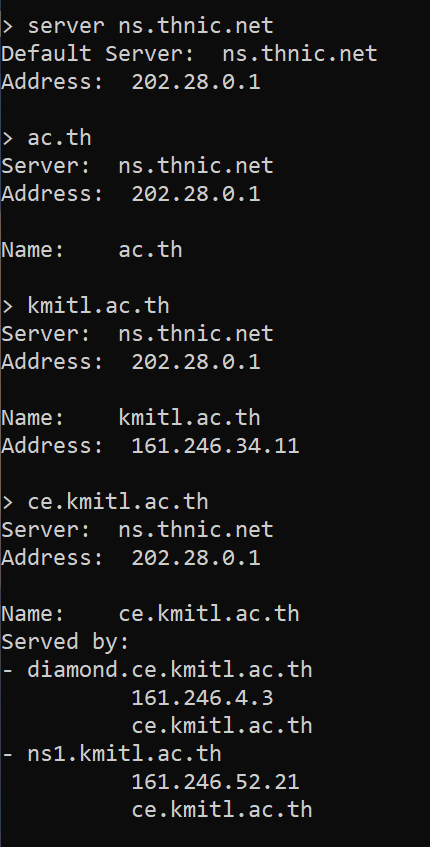
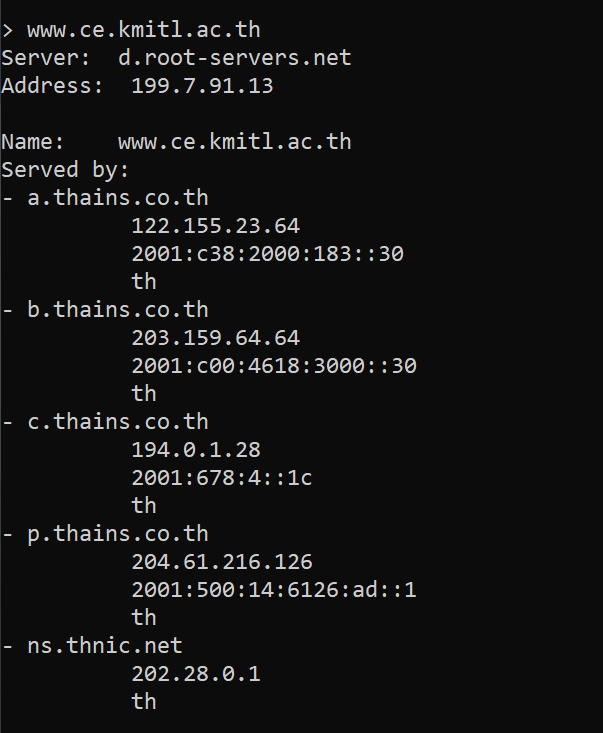
**ไม่มี Authority , Additional Info**

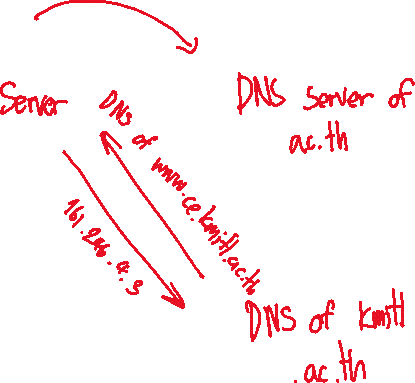
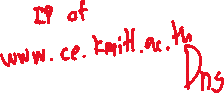
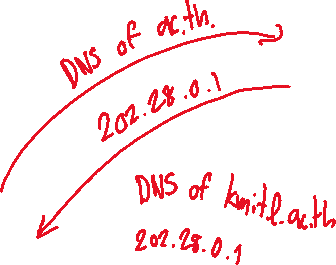
****

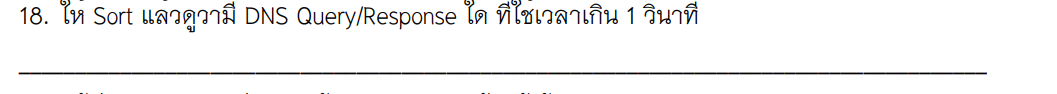
****

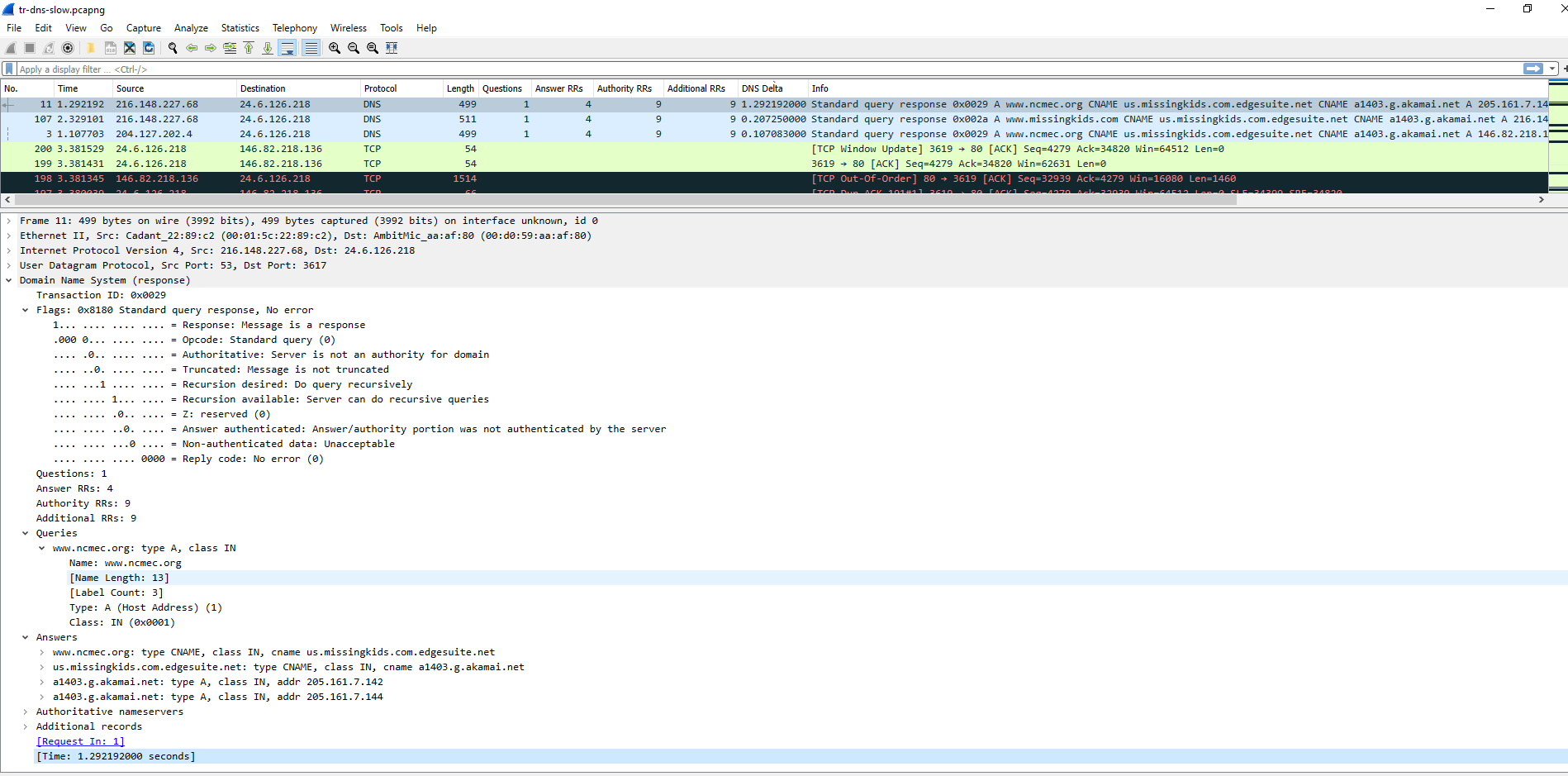
**คิอว่าเป็น d.root-servers.net**

****

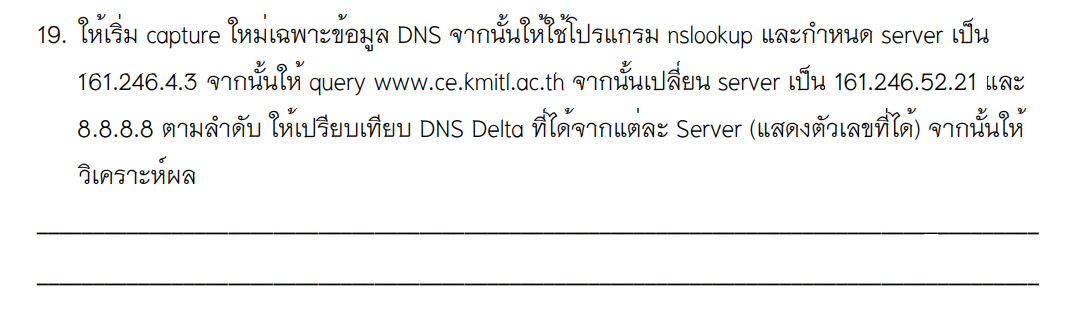
****

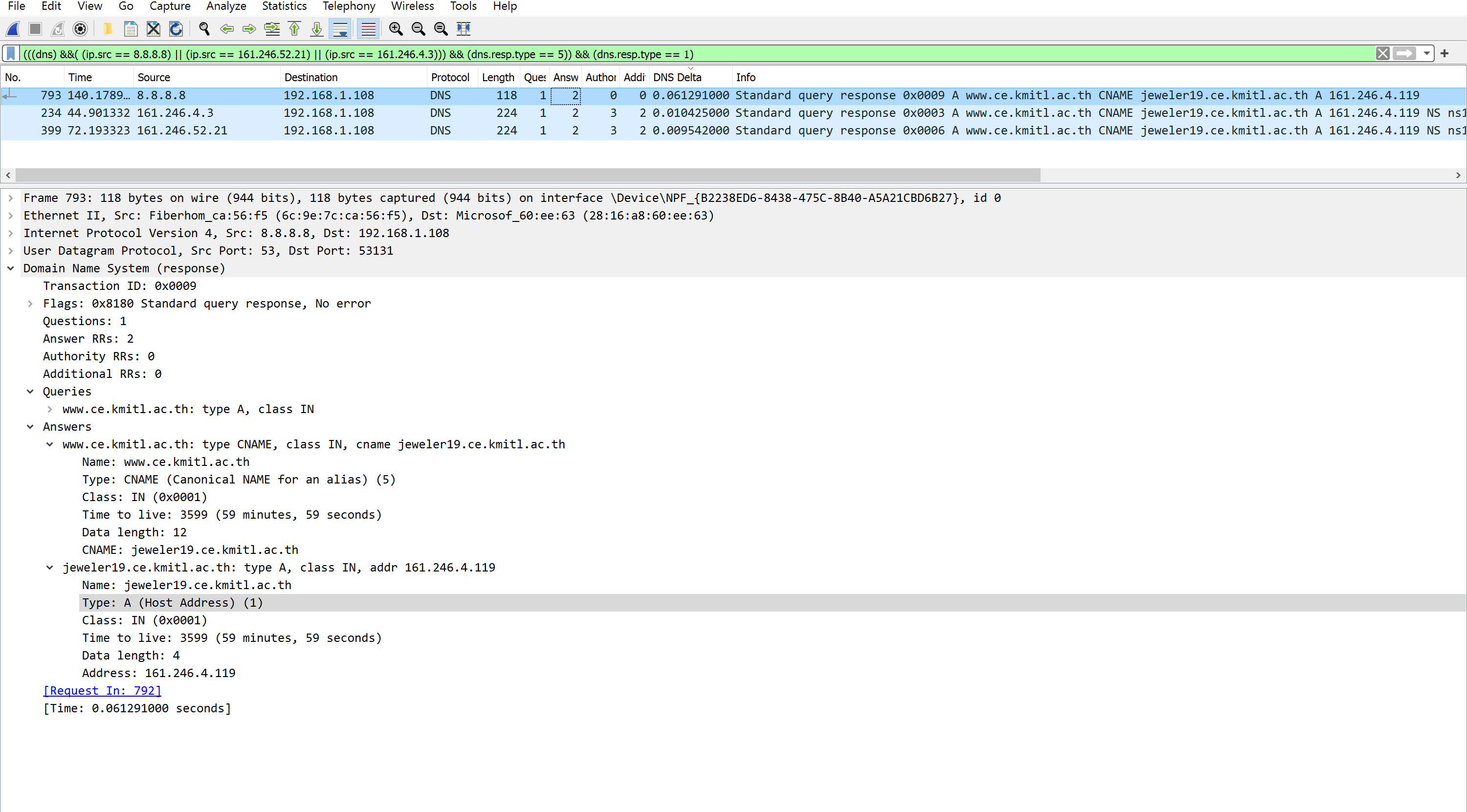


****

****

**Packet ที่ 11 ใช้เวลาไป 1.292192 วินาที**

****

****

**จาก Column DNS Delta จะพบว่า 8.8.8.8 มีเวลาเท่ากับ 0.061291 วินาที ซึ่งจะต่างจาก 161.246.4.3 และ 162.246.52.21 อย่างมากซึ่งมีเวลาเท่ากับ 0.010425 กับ 0.009542 เนื่องจากสอง DNS อยู่ใกล้ว่า 8.8.8.8 ซึ่งเป็น Public DNS ของ Google ,round trip time เลยมีค่าน้อยกว่านั่นเอง**