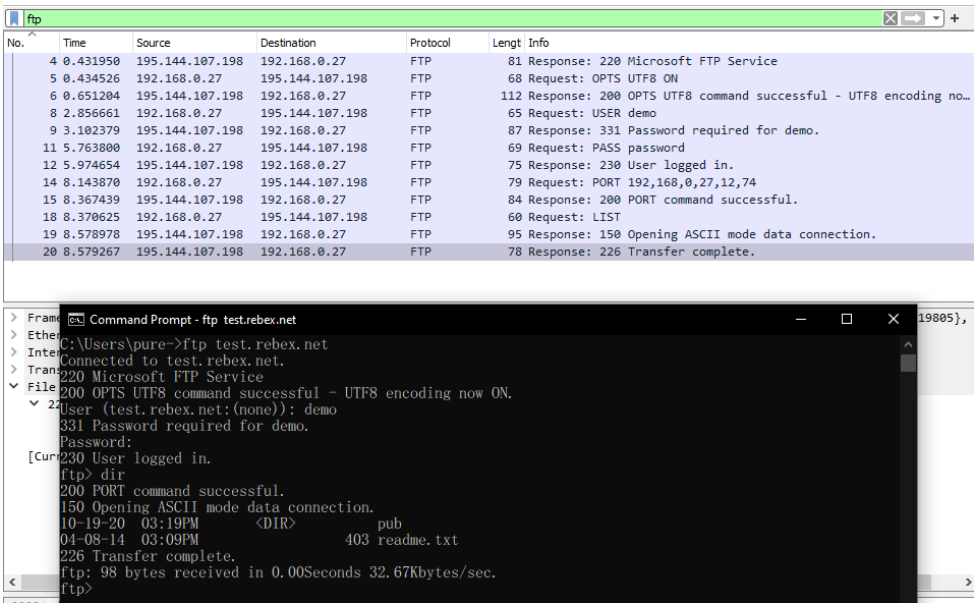
3. ใช้คำสั่ง dir ในโปรแกรม ftp และ capture ภาพการทำงานของคำสั่ง dir จากนั้นกลับมาที่ Wireshark แล้วใช้ display filter เป็น ftp ให้เปรียบเทียบระหว่างคำสั่งของ ftp ที่ใช้กับ packet ของ Wireshark ที่ดักจับได้ ให้ capture ภาพของ packet list pane ที่แสดงคำสั่งมาแสดงด้วย



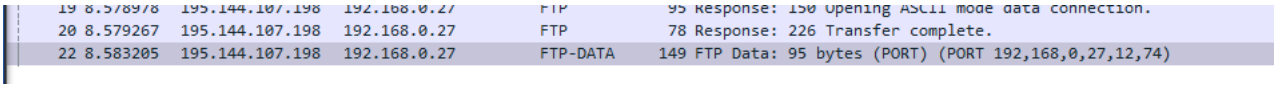
เปรียบเทียบคำสั่งในโปรแกรม ftp กับ wireshark

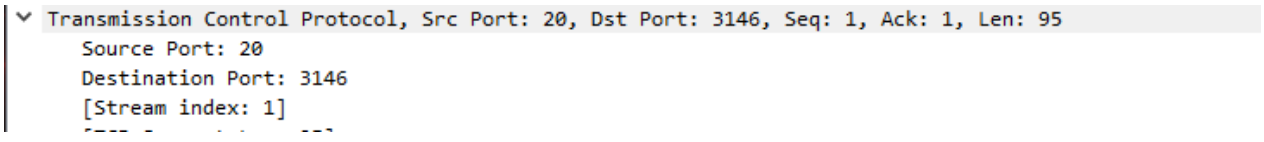
คำสั่ง dir (ftp) จะแปลงเป็นคำสั่ง LIST (wireshark)

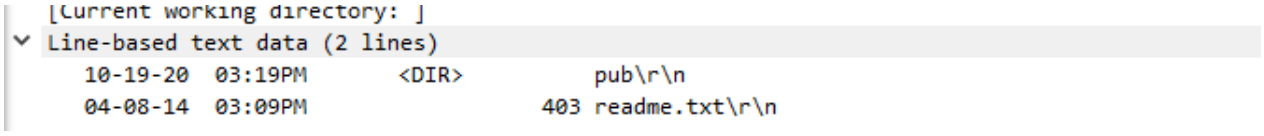
คำสั่ง User เป็น USER

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

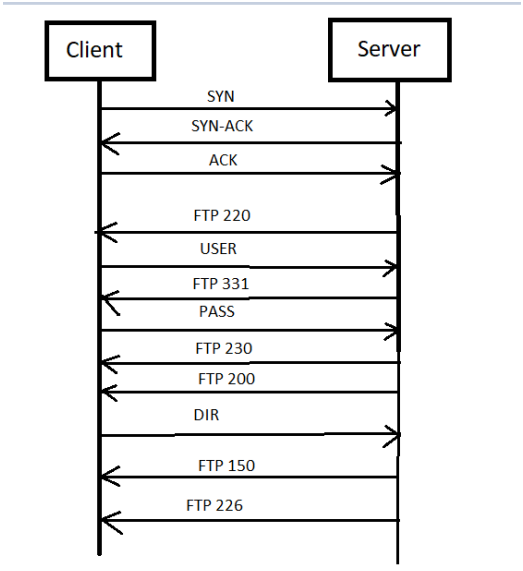






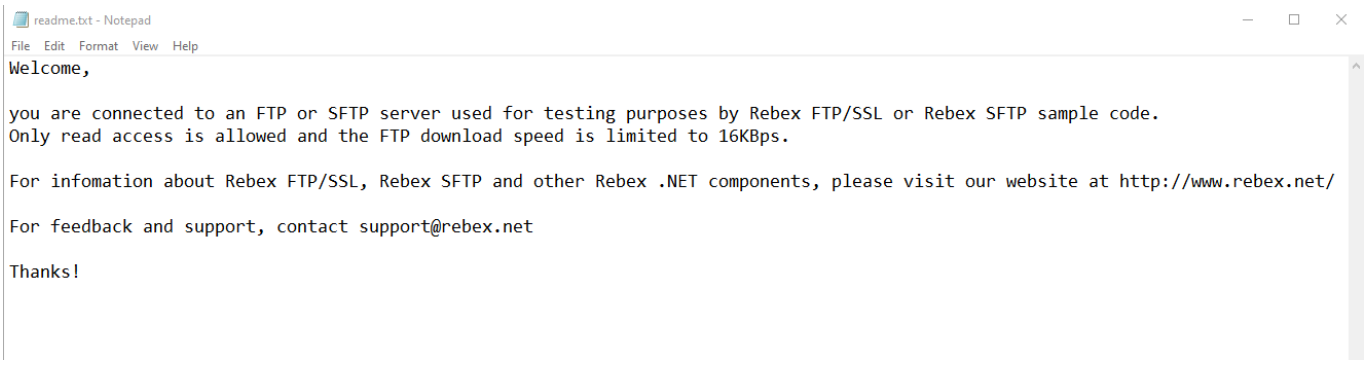
ส่งมาทาง port : 20

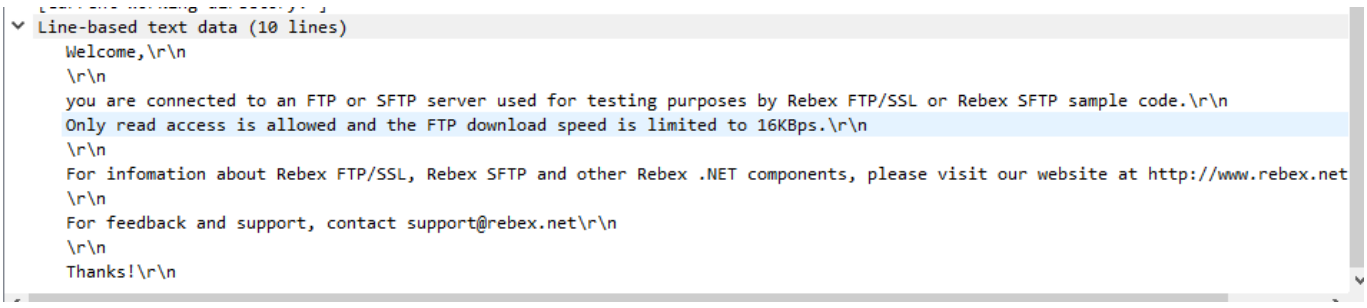
อยู่ใน packet ที่ 22



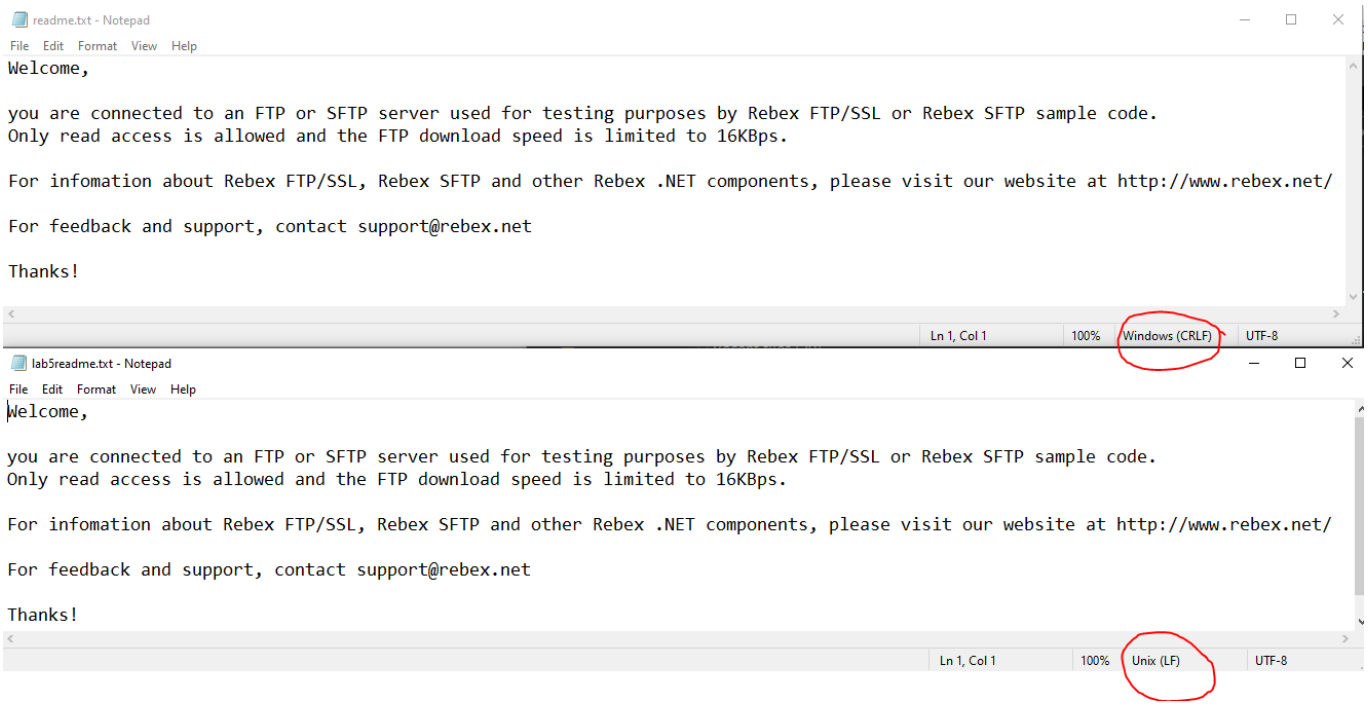
ภาพแสดงการทำงาน

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



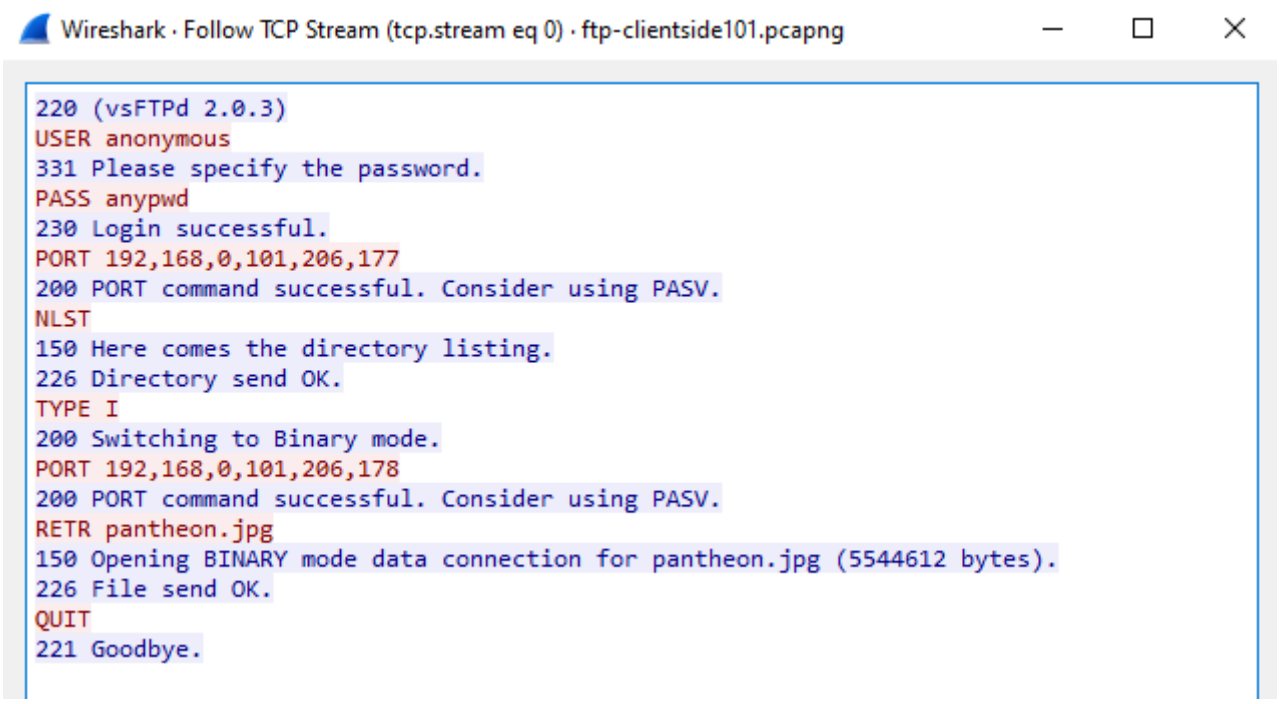


6. ให้คลิกขวาที่ packet ที่เป็นข้อมูลของ readme.txt และเลือก Follow TCP Stream และ Save as… เป็นไฟล์ ให้ตั้งชื่ออะไรก็ได้ จากนั้นเปิดไฟล์ด้วย notepad แล้วเปรียบเทียบกับไฟล์ readme.txt ว่ามีอะไรแตกต่างกันหรือไม่



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

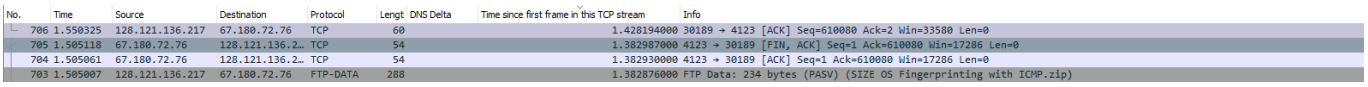
QUIT – ตัดการเชื่อมต่อ

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



No.	Time	Source	Destination	Protocol	Lengt	DNS Delta	Time since first frame in this TCP stream	Info
706	1.550325	128.121.136.217	67.180.72.76	TCP	60		1.428194000	30189 → 4123 [ACK] Seq=610080 Ack=2 Win=33580 Len=0
705	1.505118	67.180.72.76	128.121.136.2…	TCP	54		1.382987000	4123 → 30189 [FIN, ACK] Seq=1 Ack=610080 Win=17286 Len=0
704	1.505061	67.180.72.76	128.121.136.2…	TCP	54		1.382930000	4123 → 30189 [ACK] Seq=1 Ack=610080 Win=17286 Len=0
703	1.505007	128.121.136.217	67.180.72.76	FTP-DATA	288		1.382876000	FTP Data: 234 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)

เวลาที่ใช้ในการโหลดไฟล์ 1.428194000 วินาที

วิธีการ

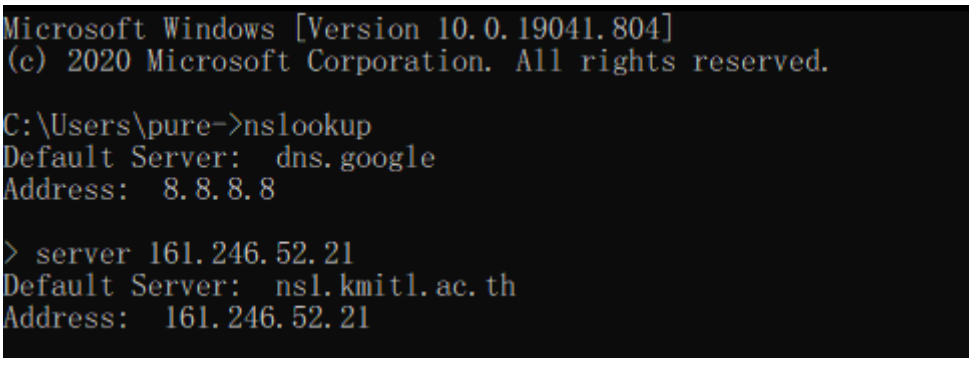
1.กด ctrl+f หาคำว่า SIZE OS Fingerprinting with ICMP.zip

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

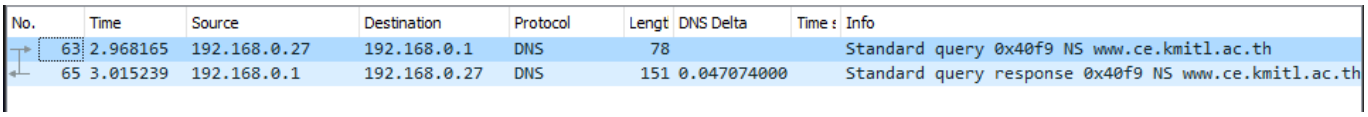
12. ให้เปิดโปรแกรม Wireshark กำหนดเงื่อนไขให้ Capture เฉพาะโปรโตคอล DNS พิมพ์ server 161.246.52.21 ลงไป (เป็นการกำหนดให้เชื่อมต่อกับ DNS Server ที่มี IP Address 161.246.52.21 แทน Default Server) ให้ตอบว่า 161.246.52.21 มีชื่อ Domain Name อะไร



```
Microsoft Windows [Version 10.0.19041.804]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\pure->nslookup
Default Server:  dns.google
Address:  8.8.8.8

> server 161.246.52.21
Default Server:  nsl.kmitl.ac.th
Address:  161.246.52.21
```

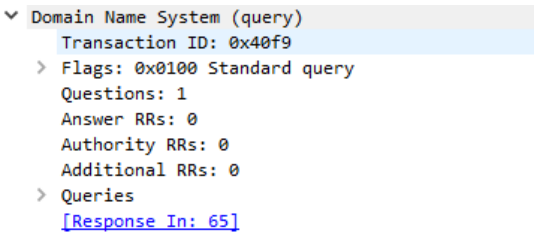
มีชื่อ Domain Name : nsl.kmitl.ac.th

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

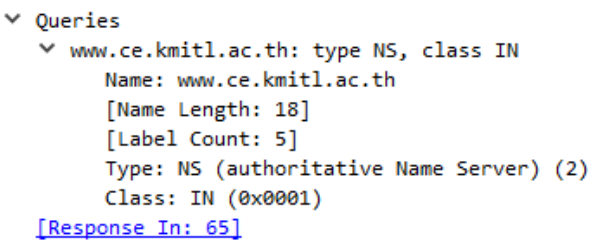


No.	Time	Source	Destination	Protocol	Lengt	DNS Delta	Time	Info
63	2.968165	192.168.0.27	192.168.0.1	DNS	78			Standard query 0x40f9 NS www.ce.kmitl.ac.th
65	3.015239	192.168.0.1	192.168.0.27	DNS	151	0.047074000		Standard query response 0x40f9 NS www.ce.kmitl.ac.th

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



```
Domain Name System (query)
    Transaction ID: 0x40f9
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 65]
```



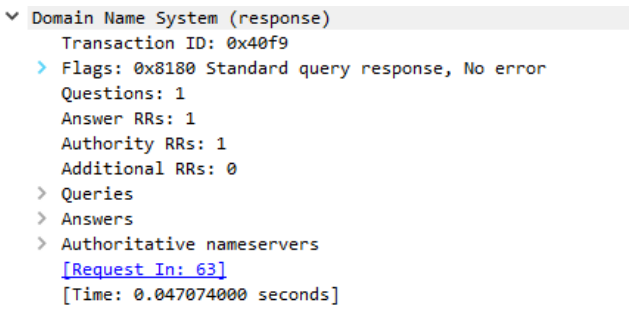
```
Queries
  www.ce.kmitl.ac.th: type NS, class IN
      Name: www.ce.kmitl.ac.th
      [Name Length: 18]
      [Label Count: 5]
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
[Response In: 65]
```

มี 1 question

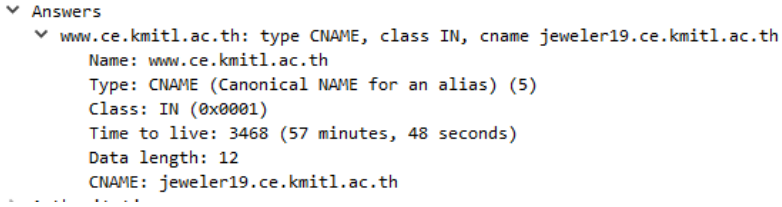
ข้อมูลใน questions

Name : 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



```
Domain Name System (response)
    Transaction ID: 0x40f9
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 0
  > Queries
  > Answers
  > Authoritative nameservers
    [Request In: 63]
    [Time: 0.047074000 seconds]
```



```
Answers
  www.ce.kmitl.ac.th: type CNAME, class IN, cname jeweler19.ce.kmitl.ac.th
      Name: www.ce.kmitl.ac.th
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 3468 (57 minutes, 48 seconds)
      Data length: 12
      CNAME: jeweler19.ce.kmitl.ac.th
```

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

No.	Time	Source	Destination	Protocol	Lengt	DNS Delta	Time s	Info
142	1.524247	192.168.0.27	8.8.8.8	DNS	78			Standard query 0xea80 A www.ce.kmitl.ac.th
146	1.629065	192.168.0.27	8.8.4.4	DNS	78			Standard query 0xea80 A www.ce.kmitl.ac.th
147	1.642177	8.8.8.8	192.168.0.27	DNS	118	0.117930000		Standard query response 0xea80 A www.ce.kmitl.ac.th
166	1.720166	8.8.4.4	192.168.0.27	DNS	118	0.091101000		Standard query response 0xea80 A www.ce.kmitl.ac.th

มี query 1 packet

มี response 1 packet

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

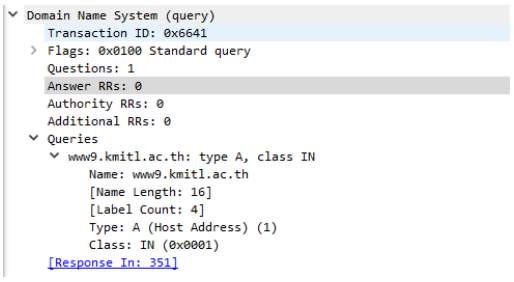
มี authority

มีข้อมูลตามรูป

```
Authoritative nameservers
  ce.kmitl.ac.th: type SOA, class IN, mname diamond.ce.kmitl.ac.th
      Name: ce.kmitl.ac.th
      Type: SOA (Start Of a zone of Authority) (6)
      Class: IN (0x0001)
      Time to live: 3600 (1 hour)
      Data length: 37
      Primary name server: diamond.ce.kmitl.ac.th
      Responsible authority's mailbox: root.diamond.ce.kmitl.ac.th
      Serial Number: 2020082101
      Refresh Interval: 14400 (4 hours)
      Retry Interval: 3600 (1 hour)
      Expire limit: 2419200 (28 days)
      Minimum TTL: 86400 (1 day)
```

14. ทำตามข้อ 13 อีกครั้ง แต่ใช้ 161.246.4.119 แทนที่จะใช้ 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

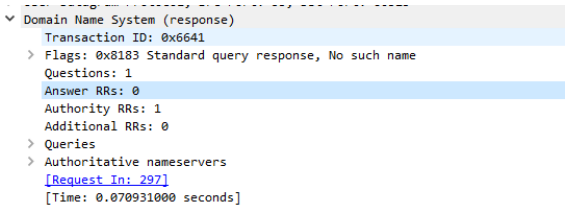
ข้อมูลใน questions

Name : www9.kmitl.ac.th

Type: A (IPv4)

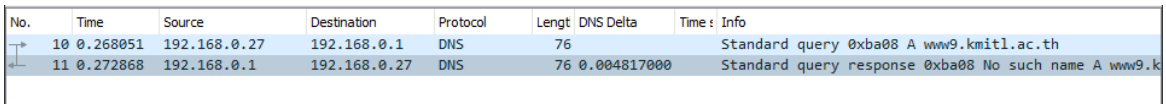
Class: IN

- 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



No.	Time	Source	Destination	Protocol	Lengt	DNS Delta	Time s	Info
10	0.268051	192.168.0.27	192.168.0.1	DNS	76			Standard query 0xba08 A www9.kmitl.ac.th
11	0.272868	192.168.0.1	192.168.0.27	DNS	76	0.004817000		Standard query response 0xba08 No such name A www9.k

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

```
> 199.7.91.13
Server:  d.root-servers.net
Address:  199.7.91.13

in-addr.arpa    nameserver = a.in-addr-servers.arpa
in-addr.arpa    nameserver = b.in-addr-servers.arpa
in-addr.arpa    nameserver = c.in-addr-servers.arpa
in-addr.arpa    nameserver = d.in-addr-servers.arpa
in-addr.arpa    nameserver = e.in-addr-servers.arpa
in-addr.arpa    nameserver = f.in-addr-servers.arpa
a.in-addr-servers.arpa  internet address = 199.180.182.53
b.in-addr-servers.arpa  internet address = 199.253.183.183
c.in-addr-servers.arpa  internet address = 196.216.169.10
d.in-addr-servers.arpa  internet address = 200.10.60.53
e.in-addr-servers.arpa  internet address = 203.119.86.101
f.in-addr-servers.arpa  internet address = 193.0.9.1
a.in-addr-servers.arpa  AAAA IPv6 address = 2620:37:e000::53
b.in-addr-servers.arpa  AAAA IPv6 address = 2001:500:87::87
c.in-addr-servers.arpa  AAAA IPv6 address = 2001:43f8:110::10
d.in-addr-servers.arpa  AAAA IPv6 address = 2001:13c7:7010::53
e.in-addr-servers.arpa  AAAA IPv6 address = 2001:dd8:6::101
f.in-addr-servers.arpa  AAAA IPv6 address = 2001:67c:e0::1
*** No internal type for both IPv4 and IPv6 Addresses (A+AAAA) records available for 199.7.91.13
>
```

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

```
> query www.ce.kmitl.ac.th
Server:  jeweler19.ce.kmitl.ac.th
Address:  161.246.4.119
Aliases:  www.ce.kmitl.ac.th

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to www.ce.kmitl.ac.th timed-out
>
```

ป้อน ac.th

```
> ac.th
Server:  ns.thnic.net
Address:  202.28.0.1

Name:    ac.th
```

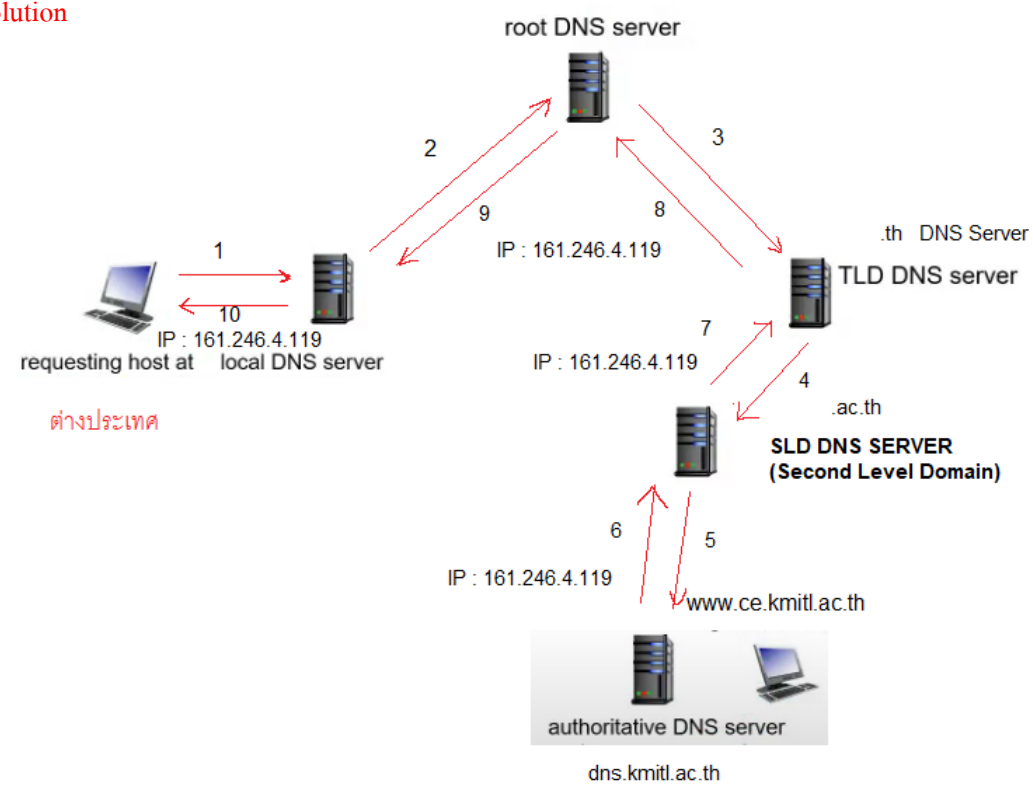
ป้อน kmitl.ac.th

```
> kmitl.ac.th
Server:  ns.thnic.net
Address:  202.28.0.1

Name:    kmitl.ac.th
Address:  161.246.34.11
```

ป้อน ce.kmitl.ac.th

```
> ce.kmitl.ac.th
Server:  ns.thnic.net
Address:  202.28.0.1

Name:    ce.kmitl.ac.th
Served by:
- diamond.ce.kmitl.ac.th
          161.246.4.3
          ce.kmitl.ac.th
- ns1.kmitl.ac.th
          161.246.52.21
          ce.kmitl.ac.th
```

name resolution



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

No.	Time	Source	Destination	Protocol	Lengt	DNS Delta	Info
11	1.292192	216.148.227.68	24.6.126.218	DNS	499	1.292192000	Standard query response 0x0029 A www.ncmec.org CNAM
107	2.329101	216.148.227.68	24.6.126.218	DNS	511	0.207250000	Standard query response 0x002a A www.missingkids.co
3	1.107703	204.127.202.4	24.6.126.218	DNS	499	0.107083000	Standard query response 0x0029 A www.ncmec.org CNAM
98	2.121851	24.6.126.218	216.148.227.68	DNS	79		Standard query 0x002a A www.missingkids.com
2	1.000620	24.6.126.218	204.127.202.4	DNS	73		Standard query 0x0029 A www.ncmec.org
1	0.000000	24.6.126.218	216.148.227.68	DNS	73		Standard query 0x0029 A www.ncmec.org

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

No.	Time	Source	Destination	Protocol	Lengt	DNS Delta	Time s	Info
760	100.3193…	161.246.52.21	192.168.0.27	DNS	80	0.126343000		Standard query response 0x0008 Refused PTR 8.8
135	25.841313	8.8.8.8	192.168.0.27	DNS	120	0.125214000		Standard query response 0x0002 PTR 3.4.246.161
605	80.692248	161.246.4.3	192.168.0.27	DNS	258	0.096021000		Standard query response 0x0007 PTR 21.52.246.1
338	42.854470	8.8.8.8	192.168.0.27	DNS	113	0.090976000		Standard query response 0xf65e A array813.proc
331	42.839413	8.8.8.8	192.168.0.27	DNS	113	0.085924000		Standard query response 0x3e2d A array807.proc
139	26.089424	8.8.8.8	192.168.0.27	DNS	199	0.084844000		Standard query response 0x2445 A self.events.d
68	9.820847	8.8.8.8	192.168.0.27	DNS	104	0.082815000		Standard query response 0x0001 PTR 8.8.8.8.in-
336	42.851066	8.8.8.8	192.168.0.27	DNS	113	0.078626000		Standard query response 0xcf5a A array806.proc
312	40.541446	161.246.4.3	192.168.0.27	DNS	224	0.074558000		Standard query response 0x0003 A www.ce.kmitl.
333	42.848408	8.8.8.8	192.168.0.27	DNS	113	0.066574000		Standard query response 0xf476 A array802.proc
314	40.603339	161.246.4.3	192.168.0.27	DNS	151	0.061492000		Standard query response 0x0004 AAAA www.ce.kmi
759	100.1929…	192.168.0.27	161.246.52.21	DNS	80			Standard query 0x0008 PTR 8.8.8.8.in-addr.arpa

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