

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 command 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 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

เมื่อ ftp จะเริ่มการติดต่อ (packet ที่ 1-7)

เมื่อป้อน user name จะตรงกับ packet ที่ 8

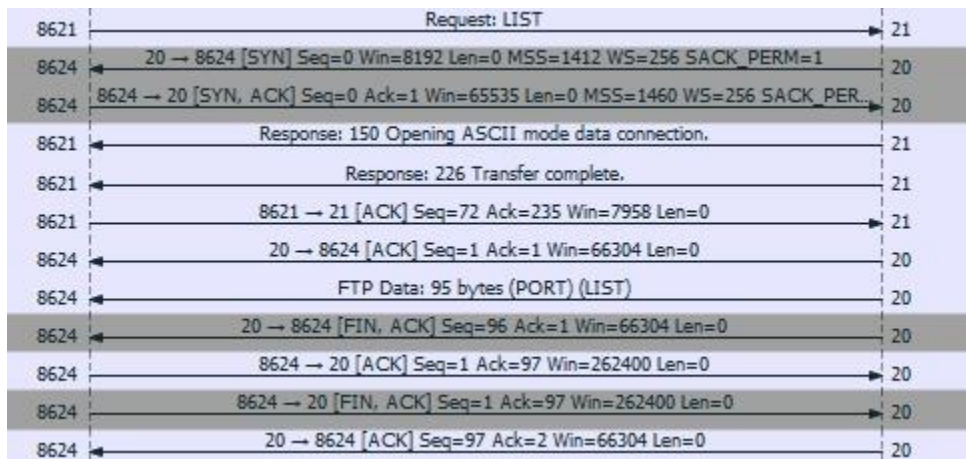
เมื่อป้อน password จะตรงกับ packet ที่ 11

เมื่อป้อน dir จะตรงกับ packet ที่ 16

Time	Destination	Protocol	Length	Host	Info
4 0.0000...	192.168.1.4	FTP	81		Response: 220 Microsoft FTP Service
5 0.0074...	195.144.107.198	FTP	68		Request: OPTS UTF8 ON
6 0.1670...	192.168.1.4	FTP	112		Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
8 2.6429...	195.144.107.198	FTP	65		Request: USER demo
9 0.1675...	192.168.1.4	FTP	87		Response: 331 Password required for demo.
11 2.4999...	195.144.107.198	FTP	69		Request: PASS password
12 0.1674...	192.168.1.4	FTP	75		Response: 230 User logged in.
14 10.792...	195.144.107.198	FTP	79		Request: PORT 192,168,1,4,33,176
15 0.1678...	192.168.1.4	FTP	84		Response: 200 PORT command successful.
16 0.0053...	195.144.107.198	FTP	60		Request: LIST
19 0.1670...	192.168.1.4	FTP	95		Response: 150 Opening ASCII mode data connection.
20 0.0350...	192.168.1.4	FTP	78		Response: 226 Transfer complete.

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

อยู่ใน packet ที่ 23 (FTP-DATA) พอร์ต 20



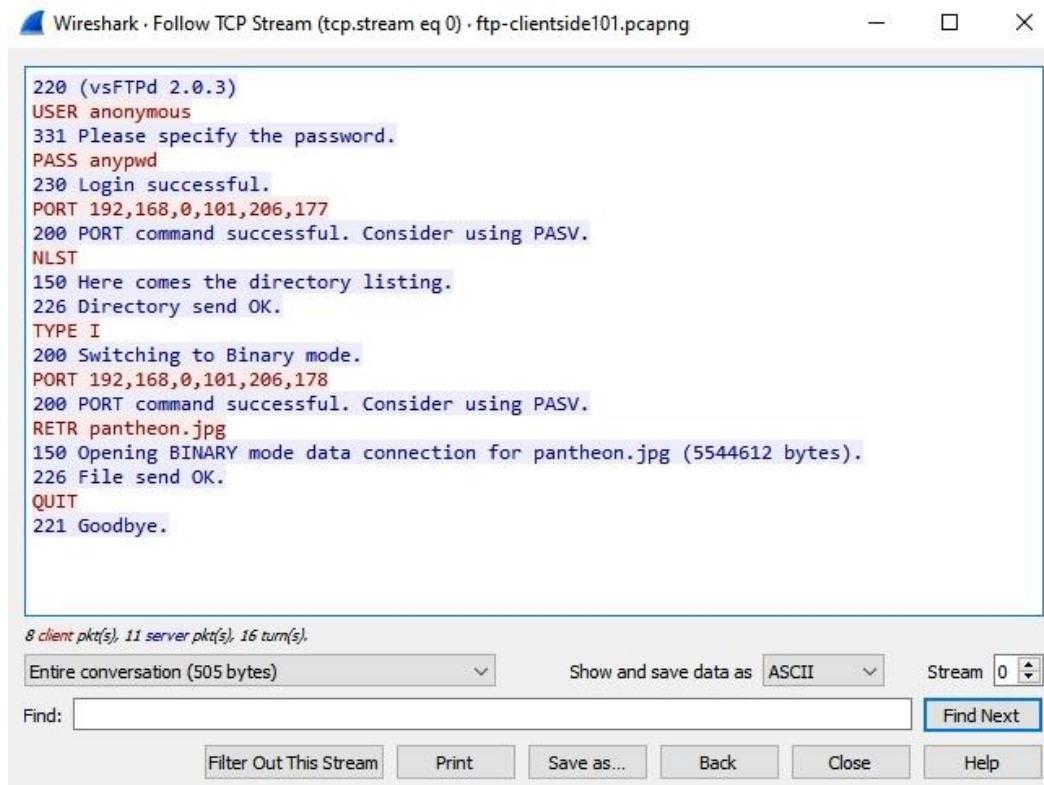
- 1) โปรแกรม FTP Client จะส่งคำสั่ง LIST ผ่านทาง Port 21
 - 2) โปรแกรม FTP Server จะ Open Connection กับ Port 20 (FTP-DATA) ผ่าน SYN ,SYN/ACK และ ACK (ในรูปเป็น packet ที่ 2,3 และ 4)
 - 3) โปรแกรม FTP Server จะส่งข้อความ Response มา 2 ข้อความผ่าน Port 21 (ในรูปจะมี Ack ตอบกลับว่าได้รับข้อความจาก Client ใน packet ที่ 6)
 - 4) เริ่มส่งข้อมูล ใน packet ที่ 8 เนื่องจากข้อมูลมีน้อยจึงส่งเพียง packet เดียว
 - 5) จากนั้น Server Close Connection กับ Client (packet ที่ 9-12)
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

ไม่แตกต่างกัน

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



The image shows the 'Follow TCP Stream' window in Wireshark for the file ftp-clientside101.pcapng. The window displays the text of the FTP session between a client (vsFTPD 2.0.3) and a server. The commands and responses are as follows:

```
220 (vsFTPD 2.0.3)
USER anonymous
331 Please specify the password.
PASS anypwd
230 Login successful.
PORT 192,168,0,101,206,177
200 PORT command successful. Consider using PASV.
NLST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,0,101,206,178
200 PORT command successful. Consider using PASV.
RETR pantheon.jpg
150 Opening BINARY mode data connection for pantheon.jpg (5544612 bytes).
226 File send OK.
QUIT
221 Goodbye.
```

Below the text, it shows statistics: 8 client pkt(s), 11 server pkt(s), 16 turn(s). The 'Entire conversation (505 bytes)' is selected. The 'Show and save data as' dropdown is set to 'ASCII'. The 'Stream' dropdown is set to '0'. There is a 'Find:' text box and a 'Find Next' button. At the bottom, there are buttons for 'Filter Out This Stream', 'Print', 'Save as...', 'Back', 'Close', and 'Help'.

คำสั่ง USER, PASS, NLST, TYPE I, PORT, RETR, QUIT

8. 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
9. จากนั้นคลิกที่ packet ใดก็ได้และเลือก Follow TCP Stream คลิก Save as ให้ตั้งชื่อ pantheon.jpg โดยเลือกชนิดเป็น raw และให้เปิดภาพขึ้นมาดูว่าเป็นภาพอะไร



10. ให้อธิบายว่าการทำงานในข้อ 8 ทำเพื่ออะไร

เพื่อ Filter เอา Stream ที่ไม่เกี่ยวกับข้อมูลภาพออกไปจากการแสดงผลใน Packet List Pane

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

วิธีที่ 1

ค้นหา Packet แรกที่มี SIZE OS Fingerprinting ซึ่งเป็น Packet ที่ Request ไฟล์ ซึ่งจะพบว่าอยู่ที่ Packet ที่ 14 จากนั้นคลิกขวาที่ Packet และเลือก Set Time Reference ซึ่งให้ข้อมูลเวลาของ Packet นี้เป็นจุดอ้างอิง คือ เริ่มจาก 0 (อาจนำเวลามาลบกันก็ได้ ไม่ต้อง Set Time Reference)
จากนั้นเลือก Follow TCP Stream หรือป้อน tcp.stream eq 1 ใน Wireshark เพื่อกรองเอาเฉพาะการส่งข้อมูลไฟล์นี้ ซึ่งจะพบว่าที่ Packet สุดท้าย คือ เวลาประมาณ 1.39 วินาที

วิธีที่ 2

ค้นหา Packet ที่มี SIZE OS Fingerprinting จากนั้นไปที่ Packet สุดท้าย แล้วดูที่ TCP | Timestamps ซึ่งจะมีข้อมูล เวลาซึ่งการหาโดยวิธีนี้จะได้ประมาณ 1.38 วินาที

```
▼ [Timestamps]
  [Time since first frame in this TCP stream: 1.382876000 seconds]
  [Time since previous frame in this TCP stream: 0.000447000 seconds]
```

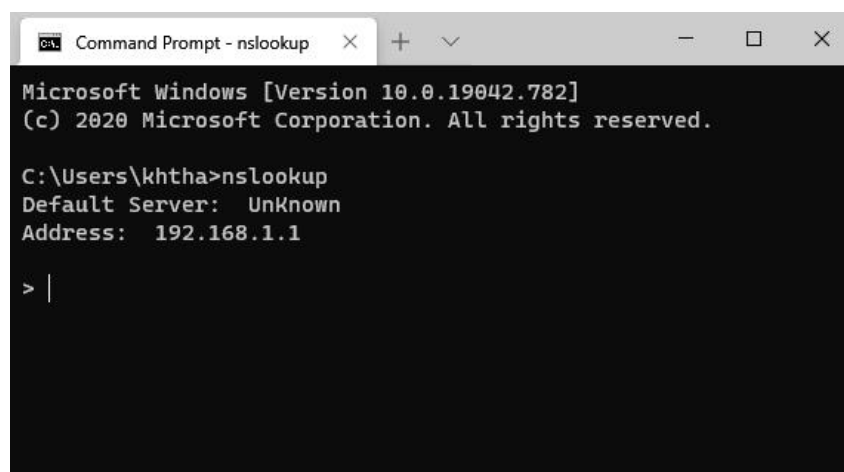
วิธีที่ 3

ดูใน packet ที่ 12 จะมีข้อมูล 1.328 วินาที

```
> File Transfer Protocol (FTP)
[Current working directory: /articlefarm/OS Fingerprinting with ICMP/]
[Command response frames: 419]
[Command response bytes: 610078]
[Command response first frame: 16]
[Command response last frame: 703]
[Response duration: 1328ms]
[Response bitrate: 3675Kbps]
[Setup frame: 8]
```

DNS (Domain Name System)

โปรโตคอล DNS จะใช้พอร์ต 53 โดยระบบปฏิบัติการส่วนใหญ่จะมีโปรแกรมที่ติดต่อกับ DNS ได้ มีชื่อว่า nslookup กรณีของ Windows ให้เรียก Command Prompt จากนั้นให้เรียกโปรแกรม nslookup (หากใช้ระบบปฏิบัติการอื่นก็ทำคล้ายกัน) จะปรากฏหน้าจอดังรูป

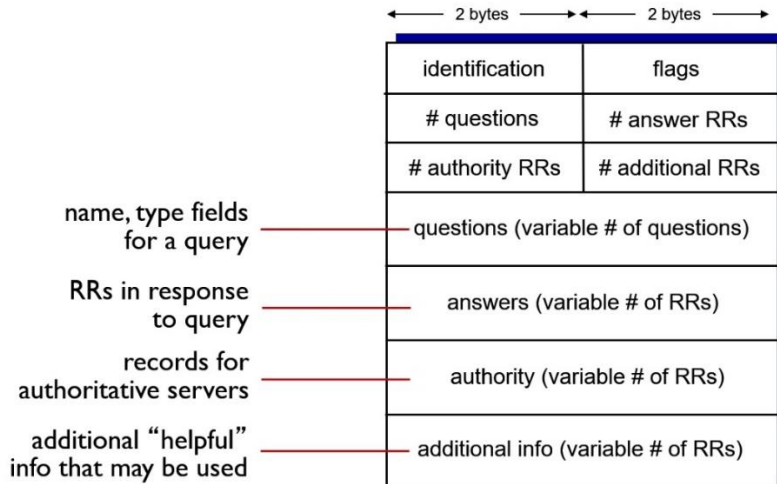


```
Microsoft Windows [Version 10.0.19042.782]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\khtha>nslookup
Default Server:  UnKnown
Address:  192.168.1.1

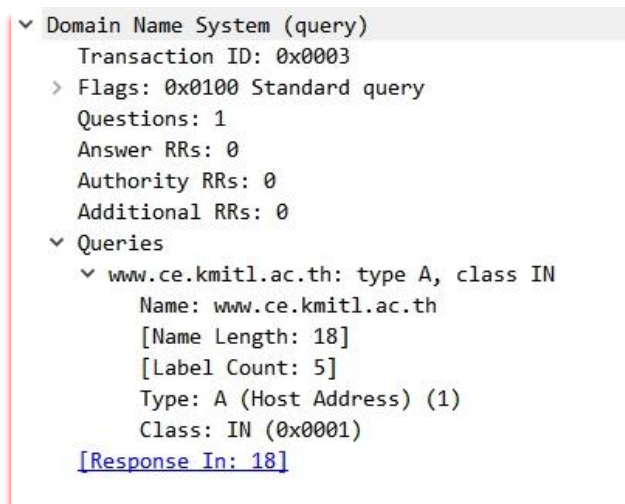
> |
```

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 **ns1.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 # query จำนวน 1 query โดยเป็น Address Mapping record (A Record) โดยส่งข้อมูลถาม **www.ce.kmitl.ac.th**



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

มี # answer จำนวน 2 answer โดยข้อมูล คือ

www.ce.kmitl.ac.th เป็น Canonical Name record (CNAME Record)

jewelwe19.ce.kmitl.ac.th เป็น Address Mapping record (A Record)


```

Domain Name System (response)
  Transaction ID: 0x0003
  > Flags: 0x8500 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 3
  Additional RRs: 2
  < Queries
    < www.ce.kmitl.ac.th: type A, class IN
      Name: www.ce.kmitl.ac.th
      [Name Length: 18]
      [Label Count: 5]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  < Answers
    > www.ce.kmitl.ac.th: type CNAME, class IN, cname jeweler19.ce.kmitl.ac.th
    > jeweler19.ce.kmitl.ac.th: type A, class IN, addr 161.246.4.119
  < Authoritative nameservers
  < Additional records
  [Request In: 17]
  [Time: 0.018792000 seconds]

```

- มี query และ response ที่ packet ให้ Capture ส่วนของ Packet Details Pane ด้วย
- มี 2 query และ 2 response (ข้อนี้เขียนผิดจริงๆ ควรจะให้ capture Packet List pane)

```

Domain Name System (response)
  Transaction ID: 0x0003
  > Flags: 0x8500 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 3
  Additional RRs: 2
  < Queries
    < www.ce.kmitl.ac.th: type A, class IN
      Name: www.ce.kmitl.ac.th
      [Name Length: 18]
      [Label Count: 5]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  < 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: 3600 (1 hour)
      Data length: 12
      CNAME: jeweler19.ce.kmitl.ac.th

```

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร
- มี, โดยในส่วน of authority เป็นข้อมูล name server ที่พบ record www.ce.kmitl.ac.th ส่วน of Additional records คือข้อมูลที่ไม่ได้ถามโดยตรง แต่มีความเกี่ยวข้อง

```

< Authoritative nameservers
  > ce.kmitl.ac.th: type NS, class IN, ns diamond.ce.kmitl.ac.th
  > ce.kmitl.ac.th: type NS, class IN, ns clarinet.asianet.co.th
  > ce.kmitl.ac.th: type NS, class IN, ns ns1.kmitl.ac.th
< Additional records
  > ns1.kmitl.ac.th: type A, class IN, addr 161.246.52.21
  > diamond.ce.kmitl.ac.th: type A, class IN, addr 161.246.4.3

```

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 # query จำนวน 1 query โดยเป็น Reverse-lookup Pointer records (PTR Record) โดยส่งข้อมูลถาม 161.246.4.119

```
Domain Name System (query)
Transaction ID: 0x0005
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
v Queries
  v 119.4.246.161.in-addr.arpa: type PTR, class IN
    Name: 119.4.246.161.in-addr.arpa
    [Name Length: 26]
    [Label Count: 6]
    Type: PTR (domain name PoinTeR) (12)
    Class: IN (0x0001)
    [Response In: 6]
```

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

มี # answer จำนวน 1 answer โดยข้อมูล คือ

119.4.246.161.in-addr.arpa เป็น Reverse-lookup Pointer records (PTR Record)

```
v Answers
  v 119.4.246.161.in-addr.arpa: type PTR, class IN, jeweler19.ce.kmitl.ac.th
    Name: 119.4.246.161.in-addr.arpa
    Type: PTR (domain name PoinTeR) (12)
    Class: IN (0x0001)
    Time to live: 3600 (1 hour)
    Data length: 26
    Domain Name: jeweler19.ce.kmitl.ac.th
```

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

มี, โดยในส่วนของ authority เป็นข้อมูล name server ที่พบ record 161.246.4.119

ส่วนของ Additional records คือข้อมูลที่ไม่ได้ถามโดยตรง แต่มีความเกี่ยวข้อง

```
v Authoritative nameservers
  > 4.246.161.in-addr.arpa: type NS, class IN, ns ns1.kmitl.ac.th
  > 4.246.161.in-addr.arpa: type NS, class IN, ns diamond.ce.kmitl.ac.th
v Additional records
  > ns1.kmitl.ac.th: type A, class IN, addr 161.246.52.21
  > diamond.ce.kmitl.ac.th: type A, class IN, addr 161.246.4.3
```

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

```
> 199.7.91.13
Server: [199.7.91.13]
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
```

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

ผลลัพธ์ของการป้อน www.ce.kmitl.ac.th

```
> www.ce.kmitl.ac.th
Server: [199.7.91.13]
Address: 199.7.91.13

Name: www.ce.kmitl.ac.th
Served by:
- a.thains.co.th
  122.155.23.64
  2001:c38:2000:183::30
  th
- b.thains.co.th
  203.159.64.64
  2001:c00:4618:3000::30
  th
- c.thains.co.th
  194.0.1.28
  2001:678:4::1c
  th
- p.thains.co.th
  204.61.216.126
  2001:500:14:6126:ad::1
  th
- ns.thnic.net
  202.28.0.1
  th
```


ผลลัพธ์เมื่อกำหนด server เป็น 202.28.0.1 และป้อน ac.th, kmitl.ac.th และ ce.kmitl.ac.th

```
> ac.th
Server: [202.28.0.1]
Address: 202.28.0.1

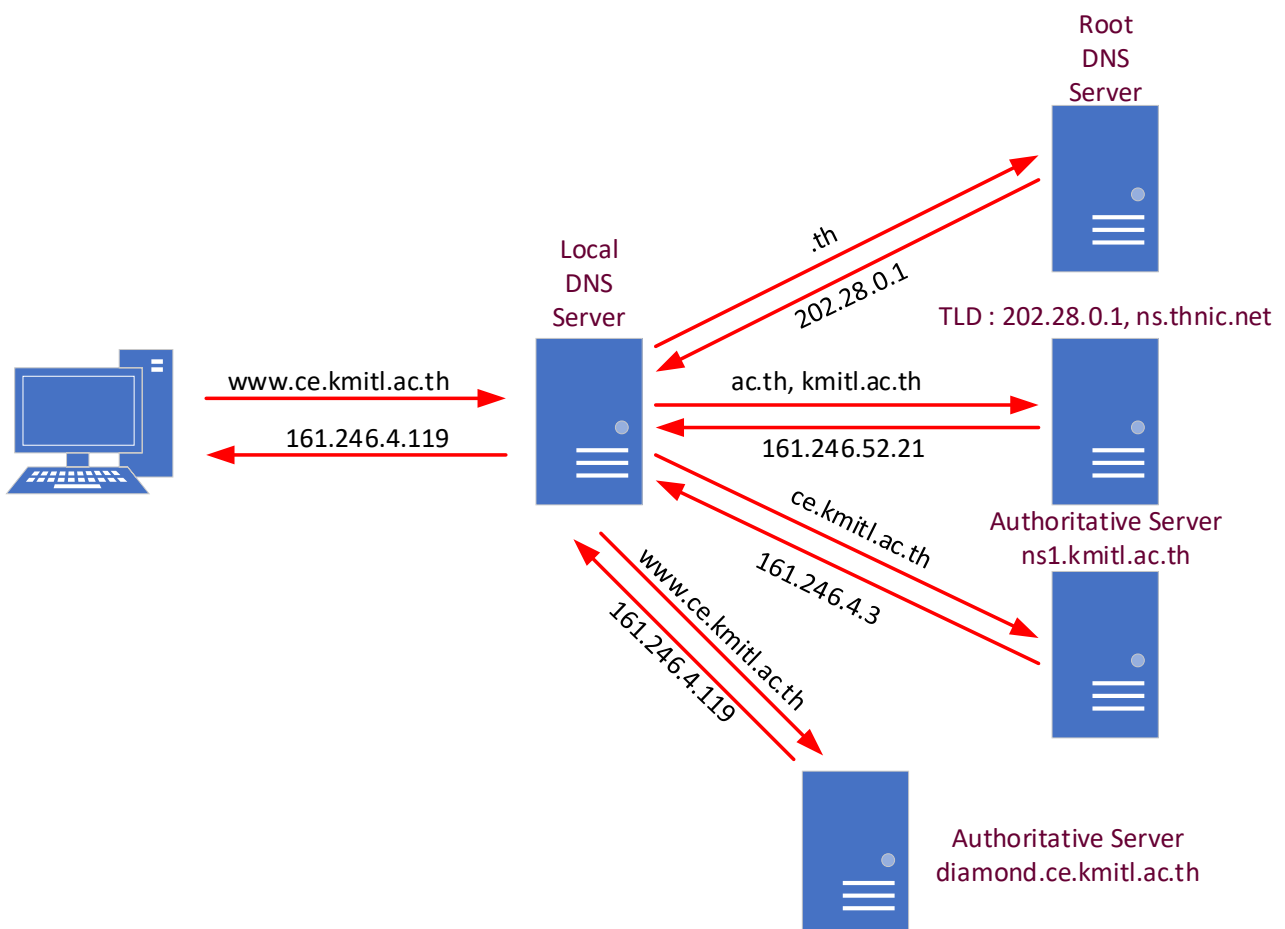
Name: ac.th

> kmitl.ac.th
Server: [202.28.0.1]
Address: 202.28.0.1

Name: kmitl.ac.th
Address: 161.246.34.11

> ce.kmitl.ac.th
Server: [202.28.0.1]
Address: 202.28.0.1

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



17. ให้เปิดไฟล์ tr-dns-slow.pcapng แล้วหา packet response ของ DNS แล้วขยายส่วนที่เป็น DNS หาข้อมูลเวลา จากนั้นให้สร้างเป็นคอลัมน์ ตั้งชื่อเป็น DNS Delta
18. ให้ Sort แล้วดูว่ามี DNS Query/Response ใด ที่ใช้เวลาเกิน 1 วินาที

มี 1 query

No.	Time	Destination	Protocol	Length	DNS Delta	Info
11	1.292192	24.6.126.218	DNS	499	1.292192000	Standard query response 0x0029 A www.ncmec.org

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

ค่าเวลาจะแตกต่างกันไป แต่โดยทั่วไป $161.246.4.3 < 161.246.52.21 < 8.8.8.8$

เนื่องจาก 161.246.4.3 เป็นเจ้าของข้อมูลจึงให้ข้อมูลได้เร็ว ส่วน 161.246.52.21 และ 8.8.8.8 จะต้องไปถามที่ name server ตัวอื่น จึงช้ากว่าตามจำนวน server ที่ต้องไปถามและระยะทาง