

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. เริ่ก Command Prompt และป้อนคำสั่ง `ftp ftp.cs.brown.edu test.rebex.net` โดยให้ใส่ user เป็น demo และใช้ password เป็น password
 3. ใช้คำสั่ง `dir` ในโปรแกรม ftp และบันทึก screenshot ภาพการทำงานของคำสั่ง `dir` จากนั้นกลับมาที่ Wireshark และใช้ display filter เป็น `ftp` ให้เปรียบเทียบแต่ละคำสั่งของ ftp ว่าตรงกับ packet ใดที่ Wireshark ดักจับได้ ให้บันทึก screenshot ภาพของ Packet List Pane ที่แสดงคำสั่งมาแสดงด้วย

ການອົງກວດນໍາ

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

- ข้อบกพร่อง fpt ที่ server ส่งมา อยู่ที่ packet ที่ 21 ถูกส่งมาทาง port หมายเลข 20

ขั้นตอนการทำงานของคำสั่ง dir

- client ຖ່ານໃສ request ດ້ວຍ dir ໃບໜາຟ, server ຕະຫຼອງ response ນັບນາວ່າ command successful ຖກນັ້ນຝຶ່ງ, client ກ່າວໃສ request List ໃບ server ກໍເຊີ: response list ນັບນາພໍໃຈວ່າ response ຈະ Transfer complete .

ข้อ 3)

ภาพที่ใช้คำสั่ง dir

```
C:\Users\bamby>ftp test.rebex.net
Connected to test.rebex.net.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (test.rebex.net:(none)): demo
331 Password required for demo.
Password:
230 User logged in.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
10-19-20 03:19PM <DIR> pub
12-17-21 11:58AM 405 readme.txt
226 Transfer complete.
ftp: 98 bytes received in 0.00Seconds 32.67Kbytes/sec.
ftp>
```

ภาพการ filter ดู ftp

No.	Time	Source	Destination	Protocol	Length	Host	HTTP delta	Info
18	15.371605	10.66.2.223	195.144.107.198	FTP	60			Request: LIST
5	0.432445	10.66.2.223	195.144.107.198	FTP	68			Request: OPTS UTF8 ON
11	9.587899	10.66.2.223	195.144.107.198	FTP	69			Request: PASS password
14	15.158573	10.66.2.223	195.144.107.198	FTP	79			Request: PORT 10.66.2.223
8	4.266261	10.66.2.223	195.144.107.198	FTP	65			Request: USER demo
19	15.577647	195.144.107.198	10.66.2.223	FTP	95			Response: 150 Opening A
6	0.637355	195.144.107.198	10.66.2.223	FTP	112			Response: 200 OPTS UTF8
16	15.365706	195.144.107.198	10.66.2.223	FTP	84			Response: 200 PORT comm
4	0.424848	195.144.107.198	10.66.2.223	FTP	81			Response: 220 Microsoft
24	15.578012	195.144.107.198	10.66.2.223	FTP	78			Response: 226 Transfer
12	9.793459	195.144.107.198	10.66.2.223	FTP	75			Response: 230 User logg
9	4.474295	195.144.107.198	10.66.2.223	FTP	87			Response: 331 Password

ข้อ 4)

21 15.577647 195.144.107.198 10.66.2.223 FTP-DA... 149 FTP Data: 95 bytes

> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (95 bytes)
FTP Data (95 bytes data)
[Setup frame: 14]
[Setup method: PORT]
[Command: PORT 10.66.2.223,215,95]
[Command frame: 14]
[Current working directory:]
▼ Line-based text data (2 lines)
10-19-20 03:19PM <DIR> pub\r\n
12-17-21 11:58AM 405 readme.txt\r\n

21 15.577647 195.144.107.198 10.66.2.223 FTP-DA... 149 FTP Data: 95 bytes

▼ Transmission Control Protocol, Src Port: 20, Dst Port: 55135, Seq: 1, Ack: 1, Len: 95
Source Port: 20
Destination Port: 55135
[Stream index: 1]
[Conversation completeness: Incomplete (30)]
[TCP Segment Len: 95]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3203044875
[Next Sequence Number: 96 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3566899621
0101 = Header Length: 20 bytes (5)

5. ใช้คำสั่ง **get readme.txt** เพื่อดownloadไฟล์ readme.txt จาก ftp server เมื่อดownloadเสร็จสิ้นให้เปิดไฟล์ดังกล่าวด้วยโปรแกรม notepad และบันทึกภาพ screenshot นำมาแสดง (หากไม่รู้ว่า path ของไฟล์ที่ดาวน์โหลดมาแล้วว่าอยู่ที่ path ใดบนเครื่อง ให้พิมพ์คำสั่ง **lcd** เพื่อแสดง current directory ของผู้client) พร้อมทั้งนำภาพ screenshot จากหน้าโปรแกรม Wireshark ส่วนที่แสดงข้อมูลในการส่งไฟล์ readme.txt มาเปรียบเทียบด้วย

* from notepad

```

readme - Notepad
File Edit Format View Help
Welcome,
You are connected to an FTP or SFTP server used for testing purposes by Rebex FTFS
Only read access is allowed and the FTP download speed is limited to 16KBps.
For information about Rebex FTP/SSL, Rebex SFTP and other Rebex .NET components,
For feedback and support, contact support@rebx.net
Thanks!

```

* from wireshark

Sequence Number	Source IP	Destination IP	Port	Protocol	Length
36	195.144.107.198	10.66.2.223	21	TCP	54
37	195.144.107.198	10.66.2.223	21	TCP	54
38	195.144.107.198	10.66.2.223	21	TCP	78
39	195.144.107.198	10.66.2.223	21	TCP	56
40	195.144.107.198	10.66.2.223	21	TCP	54
41	195.144.107.198	10.66.2.223	21	TCP	54
42	195.144.107.198	10.66.2.223	21	TCP	54
43	195.144.107.198	10.66.2.223	21	TCP	56
44	195.144.107.198	10.66.2.223	21	TCP	56

6. ให้คลิกขวาที่ packet ที่เป็นข้อมูลของ readme.txt และเลือก Follow TCP Stream และ Save as... เป็นไฟล์ ให้ดังชื่อไรก็ได้ จากนั้นเปิดไฟล์ด้วย notepad และเปรียบเทียบกับไฟล์ readme.txt ว่ามีอะไรแตกต่างกันหรือไม่

- ไม่ต่างกัน

7. พิมพ์คำสั่ง disconnect เพื่อให้โปรแกรม ftp client ตัดการเชื่อมต่อ กับ 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)

ภาพของข้อ 6

```

readme111 - Notepad
File Edit Format View Help
Welcome,
You are connected to an FTP or SFTP server used for testing purposes by Rebex FTFS
Only read access is allowed and the FTP download speed is limited to 16KBps.
For information about Rebex FTP/SSL, Rebex SFTP and other Rebex .NET components,
For feedback and support, contact support@rebx.net
Thanks!

```

สั่ง Username → server
 สั่ง password → server
 รับ port ที่ server ควรพัฒนา
 ขอ file ที่ directory
 set Transfer mode
 รับ port ที่ server ควรพัฒนา
 โอน file ที่รับ
 แล้วเชื่อมต่อ

```

220 (vsFTPd 2.0.3)
USER anonymous
331 Please specify the password.
PASS anypwd
230 Login successful.
PORT 192.168.0.101,206,178
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.

```

Packet 15. 8 client pkts, 11 server pkts, 16 turns. Click to select.

10. จากนั้นที่หน้าต่างของ Follow TCP Stream ให้เลือก Filter Out this Stream และให้ดูที่ display filter ว่า แสดงว่าอะไร จากนั้นคลิกขวาที่ packet 16 และเลือก Follow TCP Stream อีกครั้งแล้วเลือก Filter Out this Stream อีกครั้ง 

11. จากหน้าคลิกที่ packet ได้ก็ได้แล้วเลือก Follow TCP Stream คลิก Save as ให้ตั้งชื่อ pantheon.jpg โดยเลือกชนิดเป็น raw และให้เปิดภาพขึ้นมาดูว่าเป็นภาพอะไร

ການຂໍ້ 11 →



12. ให้คณิตฯ เวลาการทำงานในวันที่ 10 ทำเพิ่มอีก

filter 101 packet ที่เก็บข้อมูล packet 6,16 001

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

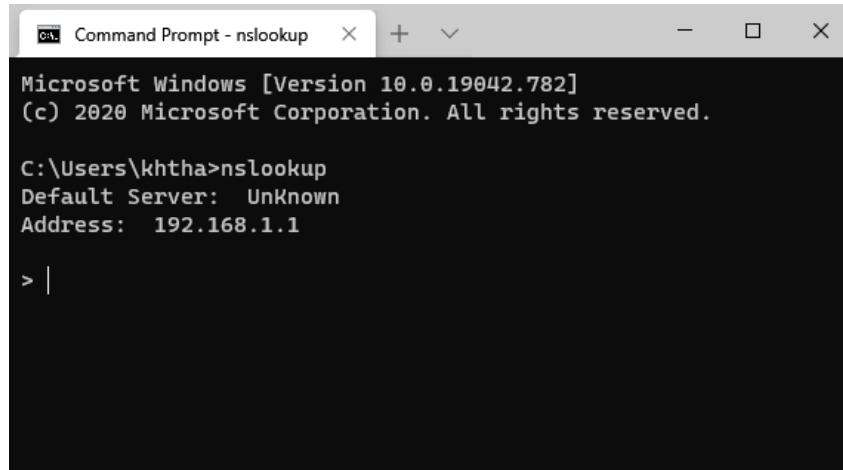
- ① หน้า pagket ที่ request : RERT OS Fingerprinting with ICMP.zip (= Packet ที่ 14)
 - ② คลิกขวาที่ packet → Follow → TCP Stream หากเราหักดักที่ขึ้นว่า 226 Transfer complete.
คลิกไปที่บรรทัดที่เบื้องบนว่า 226 Transfer complete.
 - ③ กลับไปที่หน้า packet จะเห็นว่ามี packet ที่ถูก Hightlight นั่นคือ packet ที่ 707
ซึ่งเป็นตัว response : 226 Transfer complete
 - ④ หมายเหตุ : รู้ว่าใช้เวลาในการ load ไฟล์ ได้จากการเวลา Time ของ packet 14 - packet 707

$$= 1.56556 - 1.550831$$

$$\underline{\text{ទឹករាយ}} = 0.014729 \text{ s}$$

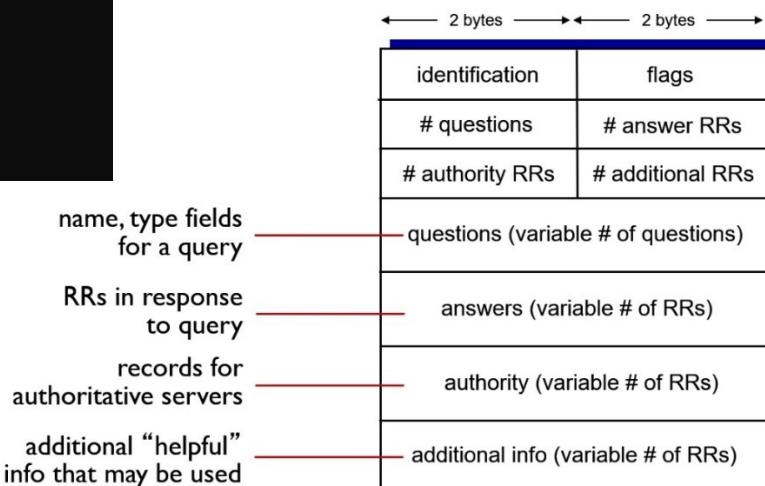
DNS (Domain Name System)

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



- ให้เปิดโปรแกรม Wireshark เพื่อ capture โดยกำหนดเงื่อนไขให้ capture เนพาะโปรโตคอล DNS จากนั้นในหน้าที่เรียก 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 ns1.kmitl.ac.th

```
C:\Users\bamby>nslookup
Default Server: ns1.kmitl.ac.th
Address: 16.252.98.21
> server 161.246.52.21
Default Server: ns1.kmitl.ac.th
Address: 161.246.52.21
>
```



- ให้พิมพ์ 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

* question = 1 , ข้อมูลใน question คือ Domain name : www.ce.kmitl.ac.th
type = type A

Idx	Source	Destination	Protocol	Length	HTTP Info
19	161.246.52.21	161.246.52.21	DNS	90	Standard query 0x0000 A www.ce.kmitl.ac.th.kmitl.ac.th
20	161.246.52.21	161.246.52.21	DNS	159	Standard query response 0x0003 No such name A www.ce.kmitl.ac.th.kmitl.ac.th 500
21	161.246.52.21	161.246.52.21	DNS	90	Standard query response 0x0003 No such name A www.ce.kmitl.ac.th.kmitl.ac.th 500
22	161.246.52.21	161.246.52.21	DNS	159	Standard query response 0x0003 No such name AAAA www.ce.kmitl.ac.th.kmitl.ac.th 500
23	161.246.52.21	161.246.52.21	DNS	90	Standard query response 0x0003 No such name AAAA www.ce.kmitl.ac.th.kmitl.ac.th 500
24	161.246.52.21	161.246.52.21	DNS	141	Standard query response 0x0003 No such name A www.ce.kmitl.ac.th.kmitl.ac.th 500 A.T
25	161.246.52.21	161.246.52.21	DNS	94	Standard query response 0x0003 No such name AAAA www.ce.kmitl.ac.th.kmitl.ac.th 500 A.T
26	161.246.52.21	161.246.52.21	DNS	141	Standard query response 0x0003 No such name AAAA www.ce.kmitl.ac.th.kmitl.ac.th 500 A.T
27	161.246.52.21	161.246.52.21	DNS	79	Standard query response 0x0003 No such name A www.ce.kmitl.ac.th.kmitl.ac.th 500
28	161.246.52.21	161.246.52.21	DNS	200	Standard query response 0x0003 AAAA www.ce.kmitl.ac.th.kmitl.ac.th 161.246.127.233 M.nsl.ku.
29	161.246.52.21	161.246.52.21	DNS	78	Standard query response 0x0003 AAAA www.ce.kmitl.ac.th.kmitl.ac.th 161.246.127.233 M.nsl.ku.
30	161.246.52.21	161.246.52.21	DNS	147	Standard query response 0x0003 AAAA www.ce.kmitl.ac.th.kmitl.ac.th 161.246.127.233 M.nsl.ku.

Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on Interface 'Device\NPF_{405D2C05-60B6-4084-9E41-ADCE0000C00F}', id 0					
Ethernet II, Src: Intel PRO/100 MT [16:09:21:40:44:43], Dst: HuaweiTe [00:0c:33:ba:b3:2f] (Broadcast)					
User Datagram Protocol, Src Port: 53199, Dst Port: 53 (DNS/Domain Name System)					
> Flags: question (Question)					
Answer RRs: 0 Additional RRs: 0					
> Questions					
Query:					
www.kmitl.ac.th.kmitl.ac.th. [16:09:21:40:44:43] type: A, class: IN					
Response:					
www.kmitl.ac.th.kmitl.ac.th. [16:09:21:40:44:43] type: A, class: IN					

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

Answer RRs : 1

ចុច្ចាស់ Answer : domain name , type , class , addr

```
  > www.ce.kmitl.ac.th: type A, class IN
  > Answers
    > www.ce.kmitl.ac.th: type A, class IN, addr 161.246.127.223
        Name: www.ce.kmitl.ac.th
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3600 (1 hour)
        Data length: 4
        Address: 161.246.127.223
```

- มี query และ response กี่ packet ให้บันทึก screenshot ส่วนของ Packet Details Pane ด้วย
 - 2 packet
 - response 2 packet

[ip.addr=161.246.52.21]							[ip.addr=161.246.52.21]										
No.	Time	Source	Destination	Protocol	Length	Host	HTTPc	Info	No.	Time	Source	Destination	Protocol	Length	Host	HTTPc	Info
9	30.245942	172.28.10.14	161.246.52.21	DNS	78			Standard query 0x0003 A www.ce.knctl.ac.th	9	30.245942	172.28.10.14	161.246.52.21	DNS	78			Standard query 0x0003 A www.ce.knctl.ac.th
10	30.355778	161.246.52.21	172.28.10.14	DNS	200			Standard query response 0x0003 A www.ce.km	10	30.355778	161.246.52.21	172.28.10.14	DNS	200			Standard query response 0x0003 A www.ce.km
11	30.356322	172.28.10.14	161.246.52.21	DNS	78			Standard query 0x0004 AAAA www.ce.knctl.ac	11	30.356322	172.28.10.14	161.246.52.21	DNS	78			Standard query 0x0004 AAAA www.ce.knctl.ac
12	30.415752	161.246.52.21	172.28.10.14	DNS	127			Standard query response 0x0004 AAAA www.ce	12	30.415752	161.246.52.21	172.28.10.14	DNS	127			Standard query response 0x0004 AAAA www.ce

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

authority : 3 = name server

additional info : 2 = IP v03 name server

```
权威性名字服务器
  ✓ ck.kmtil.ac.th: type NS, class IN, ns ns1.kmtil.ac.th
    Name: ck.kmtil.ac.th
    Type: NS (权威性名字服务器) (2)
    Class: IN (0x0001)
    Time to live: 36000 (1 hour)
    Data length: 6
    Name Server: ns1.kmtil.ac.th

  ✓ ck.kmtil.ac.th: type NS, class IN, ns diamond.cc.kmtil.ac.th
    Name: ck.kmtil.ac.th
    Type: NS (权威性名字服务器) (2)
    Class: IN (0x0001)
    Time to live: 36000 (1 hour)
    Data length: 6
    Name Server: diamond.cc.kmtil.ac.th

  ✓ ck.kmtil.ac.th: type NS, class IN, ns clarinet.asianet.co.th
    Name: ck.kmtil.ac.th
    Type: NS (权威性名字服务器) (2)
    Class: IN (0x0001)
    Time to live: 36000 (1 hour)
    Data length: 6
    Name Server: clarinet.asianet.co.th

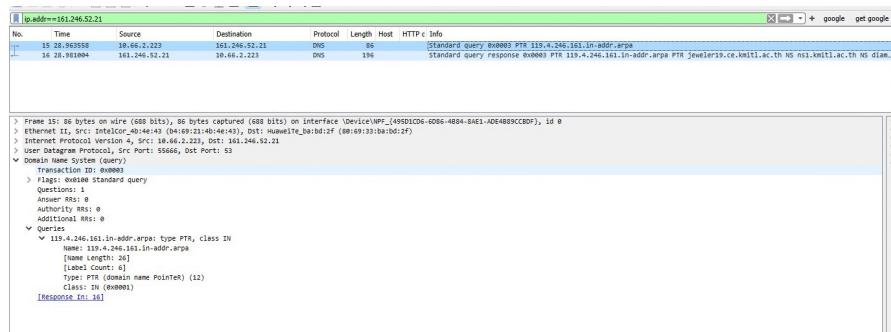
  ✓ Additional records
  ✓ ns1.kmtil.ac.th: type A, class IN, addr 161.246.52.21
    Name: ns1.kmtil.ac.th
    Type: A (主机地址) (1)
    Class: IN (0x0001)
    Time to live: 36000 (1 hour)
    Data length: 4
    Address: 161.246.52.21
  ✓ diamond.cc.kmtil.ac.th: type A, class IN, addr 161.246.4.3
    Name: diamond.cc.kmtil.ac.th
    Type: A (主机地址) (1)
    Class: IN (0x0001)
    Time to live: 36000 (1 hour)
    Data length: 4
    Address: 161.246.4.3
[Request In: 9]
[Time: 0.109836000 seconds]
```

16. ทำตามข้อ 15 อีกรั้ง แต่ใช้ 161.246.4.119 แทนที่จะใช้ www.ce.kmitl.ac.th

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

จำนวน questions : 1 = 119.4.246.161.in-addr.arpa

Type = type PTR



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

answer = 1

ข้อมูลใน answer

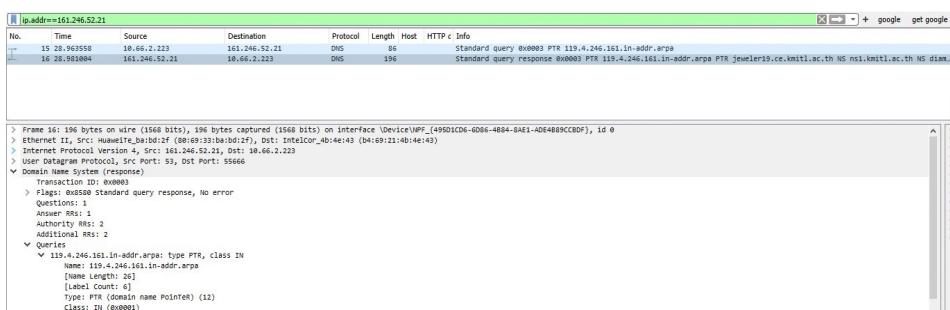
↓



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

query = 1

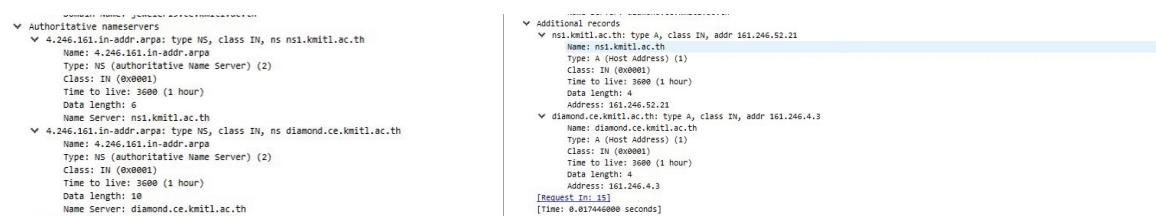
response = 1



- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

authority = 2 > IP von name server

additional = 2 > name server



17. ให้ใช้โปรแกรม nslookup และตั้ง server เป็น 199.7.91.13 จากนั้นให้ป้อน 199.7.91.13 โปรแกรมแสดงผลอะไรมาบ้าง ให้บันทึก screenshot มาแสดง นักศึกษาติดว่า 199.7.91.13 เป็น server อะไร
- root - server**

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

> 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 = 193.180.182.53
b.in-addr.servers.arpa internet address = 193.250.100.183
c.in-addr.servers.arpa internet address = 195.16.160.10
d.in-addr.servers.arpa internet address = 200.10.68.53
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:eb00::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:0::1
*** No internal type for both IPv4 and IPv6 Addresses (A+AAAA) records available for 199.7.91.13
>
```

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

```
> www.ce.kmitl.ac.th
Server: d.root-servers.net
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
  2405:3340:e011:3000::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

>
```

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

Name: ac.th

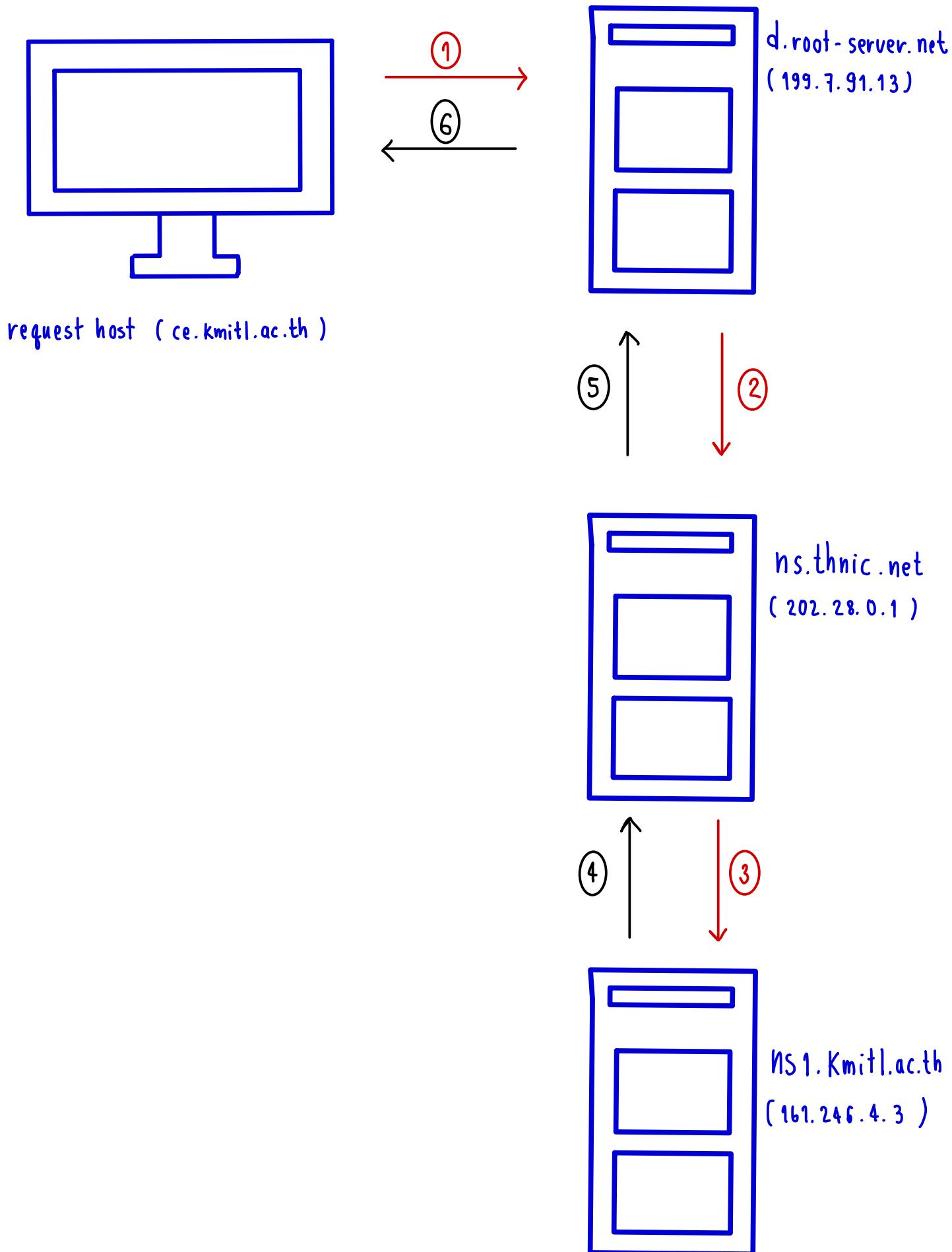
> kmitl.ac.th
Server: [202.28.0.1]
Address: 202.28.0.1

Name: kmitl.ac.th
Address: 161.246.127.182

> 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
```

name resolution



19. ให้เปิดไฟล์ tr-dns-slow.pcapng และหา 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

No.	Time	Source	Destination	Protocol	Length	Host	HTTP Info	DNS Delta	Info
1	13:20:53.045	216.149.227.68	24.4.126.248	DNS	499			0.202320008 Standard query response 0x0003 A www.ce.kmitl.ac.th.kmitl.ac.th	
2	13:20:53.045	216.149.227.68	24.4.126.248	DNS	131			0.202320008 Standard query response 0x0003 A www.ce.kmitl.ac.th.kmitl.ac.th	
3	13:20:53.045	204.127.202.4	24.4.126.248	DNS	499			0.202320008 Standard query response 0x0029 A www.nic.org.CNAME us.aitingdein.	

21. ให้เปิด Wireshark เพื่อ capture ใหม่ โดยให้ตัดกับเฉพาะข้อมูล 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 ให้เบริรย์บทเทียบ DNS Delta ที่ได้จากแต่ละ server (แสดงตัวเลขที่ได้) จากนั้นให้วิเคราะห์ผล

Server 161.246.4.3 ใช้งาน => 0.003975000

Server 161.246.52.21 ใช้งาน => 0.005832000

Server 8.8.8.8 ใช้งาน => 0.076470000

พบว่า server ทำการ response จากนั้นไปมากถึง 161.246.4.3 → 161.246.52.21 → 8.8.8.8 dns จะมี response เรื่อยๆ ขึ้นจนกว่า Host กับ DNS Server จะโกรล์ว Network มากเกิน

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

5	32.682600	10.66.2.223	161.246.4.3	DNS	90	Standard query 0x0003 A www.ce.kmitl.ac.th.kmitl.ac.th
6	32.686575	161.246.4.3	10.66.2.223	DNS	139	0.003975000 Standard query response 0x0003 No such name A www.ce.kmitl.ac.th.kmitl.ac.th
7	32.686776	10.66.2.223	161.246.4.3	DNS	90	Standard query 0x0004 AAAA www.ce.kmitl.ac.th.kmitl.ac.th
8	32.692715	161.246.4.3	10.66.2.223	DNS	139	0.005939000 Standard query response 0x0004 No such name AAAA www.ce.kmitl.ac.th.kmitl.ac.th
9	32.692715	10.66.2.223	161.246.4.3	DNS	91	Standard query 0x0005 AAAA www.ce.kmitl.ac.th.kmitl.ac.th

31	68.304892	10.66.2.223	161.246.52.21	DNS	78	Standard query 0x000e A www.ce.kmitl.ac.th
32	68.310724	161.246.52.21	10.66.2.223	DNS	200	0.005832000 Standard query response 0x000e A www.ce.kmitl.ac.th A 161.246.127.21
33	68.311494	10.66.2.223	161.246.52.21	DNS	78	Standard query 0x000f AAAA www.ce.kmitl.ac.th
34	68.315519	161.246.52.21	10.66.2.223	DNS	127	0.004025000 Standard query response 0x000f AAAA www.ce.kmitl.ac.th SOA diamond.c

41	108.708453	10.66.2.223	8.8.8.8	DNS	90	Standard query 0x0011 A www.ce.kmitl.ac.th.kmitl.ac.th
42	108.784923	8.8.8.8	10.66.2.223	DNS	139	0.076470000 Standard query response 0x0011 No such name A www.ce.kmitl.ac.th.kmitl.ac.th
43	108.785246	10.66.2.223	8.8.8.8	DNS	90	Standard query 0x0012 AAAA www.ce.kmitl.ac.th.kmitl.ac.th
44	108.854187	8.8.8.8	10.66.2.223	DNS	139	0.068941000 Standard query response 0x0012 No such name AAAA www.ce.kmitl.ac.th