

01076010 เครือข่ายคอมพิวเตอร์ : 2/2564

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

กิจกรรมที่ 5 : FTP และ DNS

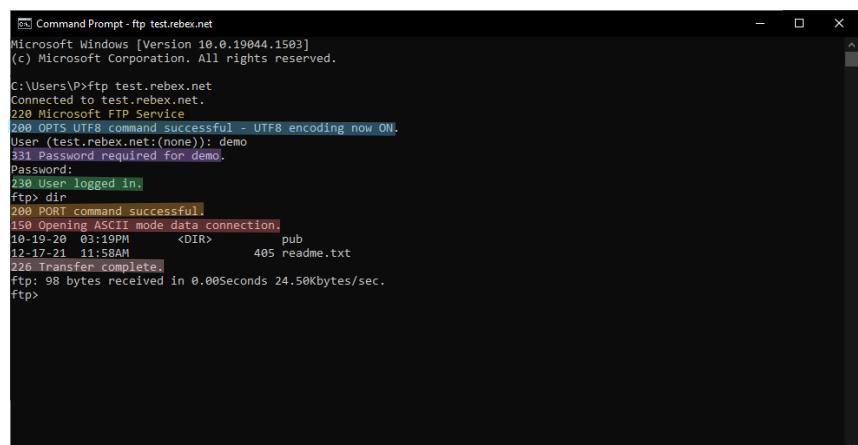
กิจกรรมครั้งนี้จะเป็นการทำความเข้าใจกับโปรโตคอล FTP (File Transfer Protocol) และ DNS (Domain Name System) เพื่อเสริมสร้างความเข้าใจในการทำงานของโปรโตคอลทั้ง 2 ตัว

FTP (File Transfer Protocol)

โปรโตคอล FTP จะใช้ 2 พอร์ต คือ พอร์ต 21 ใช้เป็น command channel คือเป็นช่องทางสำหรับส่งคำสั่ง และ พอร์ต 20 ใช้เป็น data channel ซึ่งใช้ในการรับส่งไฟล์

1. เปิดโปรแกรม wireshark ให้กำหนดให้ capture เฉพาะ host test.rebex.net
2. เรียก Command Prompt และป้อนคำสั่ง ftp test.rebex.net โดยให้ใส่ user เป็น demo และใช้ password เป็น password
3. ใช้คำสั่ง dir ในโปรแกรม ftp และ capture ภาพของผลการทำงานของคำสั่ง dir จากนั้นกลับมาที่ Wireshark และใช้ display filter เป็น ftp ให้เบริยบเทียบระหว่าง แต่ละคำสั่งของ ftp ว่าตรงกับ packet ใดของ Wireshark ที่ตัดจับ โดยให้ capture ภาพของ packet list pane ที่แสดงคำสั่งมาแสดงด้วย

ftp នៃគណន៍ទាំងពីរ នៃ wireshark ពាយិល់ តាត់បាន សាស្ត្របាន



```

C:\Users\P>ftp test.rebex.net
Microsoft Windows [Version 10.0.19044.1503]
(c) Microsoft Corporation. All rights reserved.

C:\Users\P>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.
150 Opening ASCII mode data connection.
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 24.50Kbytes/sec.
ftp>

```

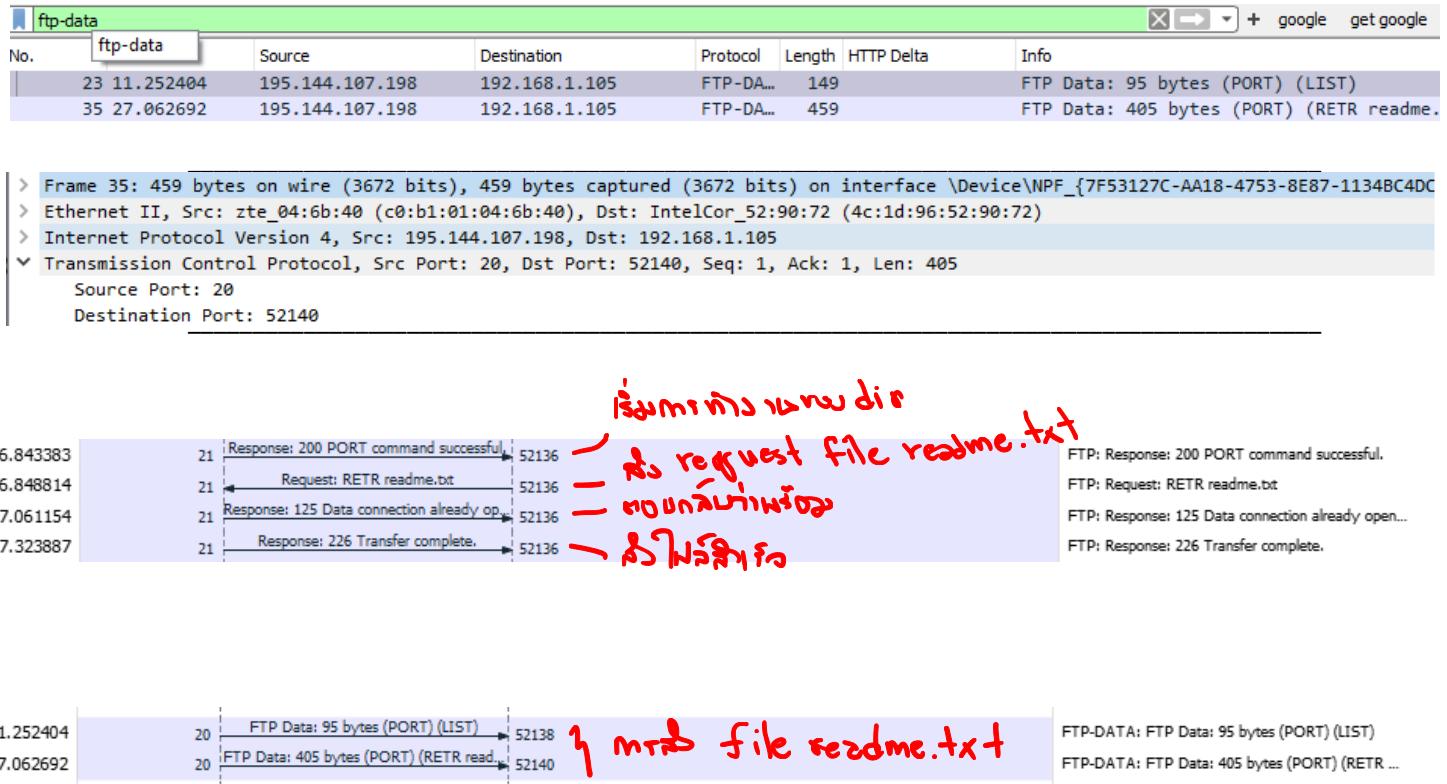
No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Info
4	0.428956	195.144.107.198	192.168.1.105	FTP	81		Response: 220 Microsoft FTP Service
5	0.433930	192.168.1.105	195.144.107.198	FTP	68		Request: OPTS UTF8 ON
6	0.648407	195.144.107.198	192.168.1.105	FTP	112		Response: 200 OPTS UTF8 command successful - UTF8 encoding
8	4.126417	192.168.1.105	195.144.107.198	FTP	65		Request: USER demo
9	4.340338	195.144.107.198	192.168.1.105	FTP	87		Response: 331 Password required for demo.
11	8.845640	192.168.1.105	195.144.107.198	FTP	69		Request: PASS password
12	9.060050	195.144.107.198	192.168.1.105	FTP	75		Response: 230 User logged in.
14	11.918259	192.168.1.105	195.144.107.198	FTP	81		Request: PORT 192,168,1,105,193,80
15	12.132543	195.144.107.198	192.168.1.105	FTP	84		Response: 200 PORT command successful.
18	12.138285	192.168.1.105	195.144.107.198	FTP	60		Request: LIST
19	12.368318	195.144.107.198	192.168.1.105	FTP	95		Response: 150 Opening ASCII mode data connection.
24	12.368690	195.144.107.198	192.168.1.105	FTP	78		Response: 226 Transfer complete.

4. ให้ค้นหา packet ที่ได้ดักจับไว้ ที่มีชื่อไฟล์ readme.txt (ซึ่งเป็นข้อมูลที่ ftp server ส่งมา) ว่าส่งมาทาง port ใด และอยู่ใน packet ใด จากนั้นให้เบิดดูที่ Statistics -> Flow graph และนำมาอธิบายขั้นตอนการทำงานของคำสั่ง dir โดยละเอียด โดยอ้างอิงจาก Flow graph

packet # 35

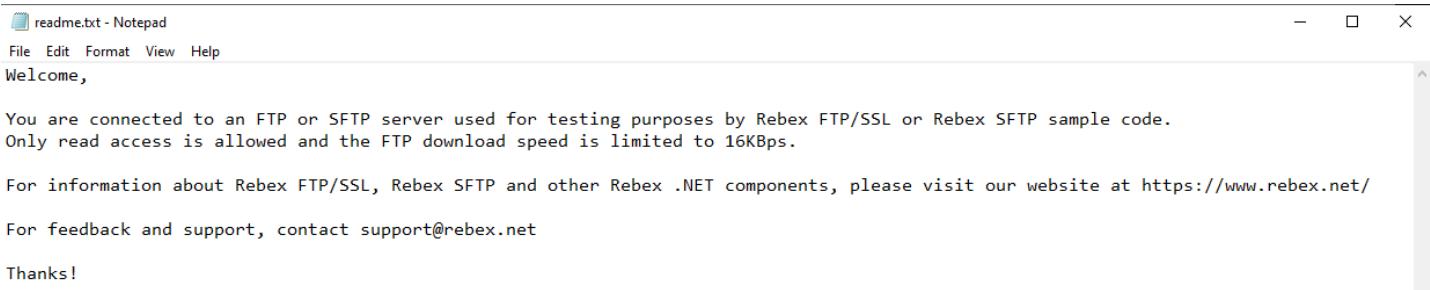
source port : 20

destination port : 52140



5. ใช้คำสั่ง get readme.txt เพื่อรับไฟล์ readme.txt จาก ftp server จากนั้นให้เบิดไฟล์ใน notepad และ capture มาแสดง และ capture ข้อมูลใน Wireshark ล้วนที่เป็นการส่งไฟล์ readme.txt มาเปลี่ยนเที่ยบ

readme.txt



Wireshark

```
Line-based text data (10 lines)
Welcome,\r\n
\r\n
You are connected to an FTP or SFTP server used for testing purposes by Rebex FTP/SSL or Rebex SFTP sample code.\r\n
Only read access is allowed and the FTP download speed is limited to 16Kbps.\r\n
\r\n
For information about Rebex FTP/SSL, Rebex SFTP and other Rebex .NET components, please visit our website at https://www.rebex.n
\r\n
For feedback and support, contact support@rebex.net\r\n
\r\n
Thanks!\r\n
```

0000 4c 1d 96 52 90 72 c0 b1 01 04 6b 40 08 00 45 00 L R r... k@ E...
0010 01 bd 64 f8 40 00 69 06 b9 da c3 90 6b c6 c0 a8 -d @ i... k...
0020 01 69 00 14 cb ac 2d 05 ad 34 e5 4b 60 1c 50 18 -i... 4 K P...
0030 01 04 94 2c 00 00 57 65 6c 63 6f 6d 65 2c 0d 0aWe lcome,.
0040 0d 0a 59 6f 75 20 61 72 65 20 63 6f 6e 6e 65 63 .. You are connec...
0050 74 65 64 20 74 6f 20 61 6e 20 46 54 50 20 6f 72 ted to a n FTP or ...
0060 28 53 46 54 50 20 73 65 72 76 65 72 20 75 73 65 SFTP se rver use...
0070 64 20 66 6f 72 20 74 65 73 74 66 6e 67 20 70 75 d for te sting pu...
0080 72 70 6f 73 65 73 20 62 79 20 52 65 62 65 78 20 rposes b y Rebex ...
0090 46 54 50 2f 53 53 4c 20 6f 72 20 52 65 62 65 78 FTP/SSL or Rebex ...
00a0 20 53 46 54 50 20 73 61 6d 70 65 65 20 63 6f 64 SFTP sa mple cod...
00b0 65 2e 0d 0a 4f 6e 6c 79 20 72 65 61 64 20 61 63 e.. Only read ac...
00c0 63 65 73 73 20 69 73 20 61 6c 6c 6f 77 65 64 20 cess is allowed...
00d0 61 6e 64 20 74 68 65 20 46 54 50 20 64 6f 77 6e and the FTP down...
00e0 62 6f 61 64 20 73 70 65 65 64 20 69 73 20 66 69 load spe ed is li...
00f0 6d 69 74 65 64 20 74 6f 20 31 36 4b 42 70 73 2e mited to 16KBps.
0100 00 0a 0d 0a 46 6f 72 20 69 6e 66 6f 72 6d 61 74 ... For informat...
0110 69 6f 60 20 61 62 6f 75 74 20 52 65 62 65 78 20 ion abou t Rebex ...
0120 46 54 50 2f 53 53 4c 2c 20 52 65 62 65 78 20 53 FTP/SSL, Rebex S...
0130 46 54 50 20 61 6e 64 20 6f 74 68 65 72 20 52 65 FTP and other Re...
0140 62 65 78 20 2e 4e 45 54 20 63 6f 6d 70 6f 6e 65 hex .NET compone...
0150 66 74 73 2c 20 70 6c 65 61 73 65 20 76 69 73 69 nts, ple ase visi...
0160 74 20 6f 75 72 20 77 65 62 73 69 74 65 20 61 74 t our we bsite at ...
0170 20 68 74 74 70 73 3a 2f 2f 77 77 77 2e 72 65 62 https://www.reb...
0180 65 78 2e 6e 65 74 2f 0d 0d 0d 0a 46 6f 72 20 66 ex.net/ ... For f...

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

เนื้อหาที่นักเรียนต้องรู้

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

```
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.
```

USER: สำหรับ user identification

PORT: กำหนดป้อมต่อไปนี้จะมา

PASS: ทำการส่ง user password

NLST: สำหรับ server (รหัส anypwd)

QUIT: ออกจากโปรแกรม

RETR: สำหรับ download file จาก FTP server

(pantheon.jpg)

QUIT: ออกจากโปรแกรม FTP

พร้อมปิดโปรแกรมต่อ

8. จากนั้นที่หน้าต่างของ Follow TCP Stream ให้เลือก Filter Out this Stream และให้ดูที่ display filter ว่าแสดงอะไร จากนั้นคลิกขวาที่ Packet 16 และเลือก Follow TCP Stream อีกครั้งและเลือก Filter Out this Stream อีกครั้ง **!(tcp.stream eq 0)**

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



10. ให้อธิบายว่าการทำงานในข้อ 8 ทำเพื่ออะไร

ผู้สอน packet ตอบว่า packet ที่มี TCP stream บนตัวเราต้องทั้ง 2 ไม่ซ้อนในปัจจุบันต้อง !!(tcp.stream eq 0) and !(tcp.stream eq 1)

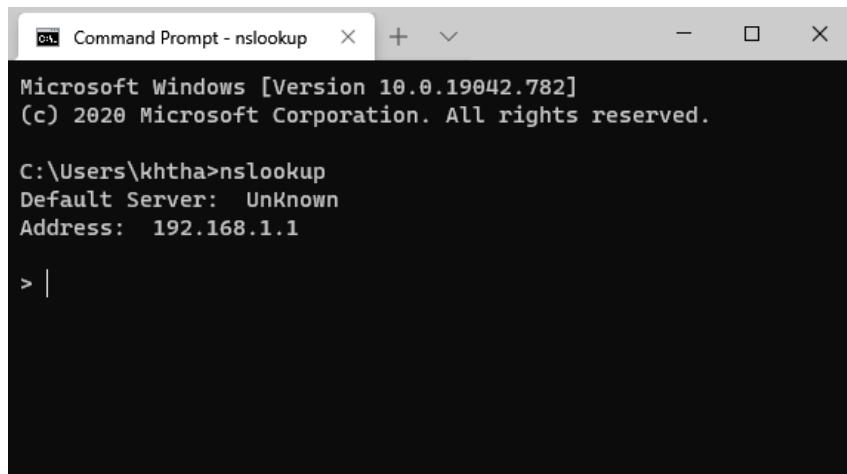
11. ให้เปิดไฟล์ ftp-download-good2.pcapng ให้หาคำต่อว่าเวลาที่ใช้ในการโหลดไฟล์ “SIZE OS Fingerprinting with ICMP.zip” เท่ากับเท่าไร อธิบายวิธีการ

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Info
16	"REF*	128.121.136.217	67.180.72.76	FTP-DATA	1078		FTP Data: 1024 bytes (PASV) (SIZE
17	0.001203	128.121.136.217	67.180.72.76	FTP-DATA	1514		FTP Data: 1460 bytes (PASV) (SIZE
19	0.014867	128.121.136.217	67.180.72.76	FTP-DATA	1514		FTP Data: 1460 bytes (PASV) (SIZE
20	0.016668	128.121.136.217	67.180.72.76	FTP-DATA	1514		FTP Data: 1460 bytes (PASV) (SIZE
698	1.319480	128.121.136.217	67.180.72.76	FTP-DATA	1514		FTP Data: 1460 bytes (PASV) (SIZE
700	1.322874	128.121.136.217	67.180.72.76	FTP-DATA	1514		FTP Data: 1460 bytes (PASV) (SIZE
701	1.327756	128.121.136.217	67.180.72.76	FTP-DATA	1514		FTP Data: 1460 bytes (PASV) (SIZE
703	1.328233	128.121.136.217	67.180.72.76	FTP-DATA	288		FTP Data: 234 bytes (PASV) (SIZE

Display filter : "ftp-data.command == "SIZE OS Fingerprinting with ICMP.zip" แล้วเลือก packet อย่างที่ปั๊ม ctrl-T เพื่อตั้งค่า filer ที่แรกที่มี (REF เท่า = 0) จึงจะมีปัญหา packet จุดท้าย จะต้องใช้เวลา 1.328233 วินาที

DNS (Domain Name System)

ໂປຣໂຕຄອລ DNS ຈະໃຊ້ພອਰົດ 53 ໂດຍຮະບບປົງບັດການສ່ວນໃໝ່ຈະມີໂປຣແກຣມທີ່ຕິດຕ່ອກນ DNS ໄດ້ ມີເລື່ອວ່າ nslookup ກຣນີຂອງ Windows ໃຫ້ເຮັດ Command Prompt ຈາກນັ້ນໃຫ້ເຮັດໂປຣແກຣມ nslookup (ຫາກໃຊ້ຮະບບປົງບັດການຂຶ້ນເກີ້ກຳຄລ້າຍເກີນ) ຈະປາກງູ້ທ່າງຈົດຕັ້ງຮູບ



```
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

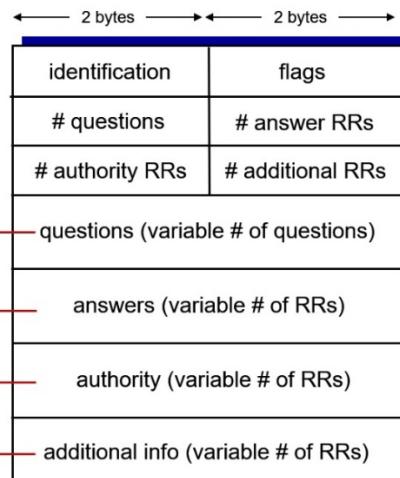
> |
```

12. ໃຫ້ເປີດໂປຣແກຣມ Wireshark ກຳນົດເງື່ອນໄຂໃຫ້ Capture ເລັກະໂປຣໂຕຄອລ DNS ພິມພໍ server 161.246.52.21 ລົງໄປ (ເປັນການກຳນົດໃຫ້ເຂື່ອມຕ່ອກນ DNS Server ທີ່ມີ IP Address 161.246.52.21 ແລ້ວ Default Server) ໃຫ້ຕອບວ່າ 161.246.52.21 ມີເລື່ອ Domain Name ອະໄໄ ns1.kmitl.ac.th

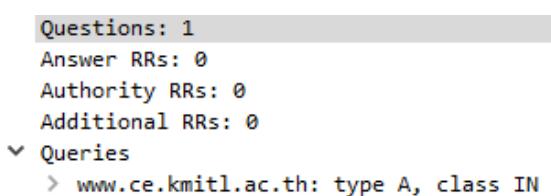
```
C:\Users\P>nslookup
Default Server: Unknown
Address: 2405:9800:a::2:26

> server 161.246.52.21
Default Server: ns1.kmitl.ac.th
Address: 161.246.52.21
```

name, type fields
for a query
RRs in response
to query
records for
authoritative servers
additional “helpful”
info that may be used



13. ໃຫ້ພິມພໍ www.ce.kmitl.ac.th ແລະໜູ້ດ Capture ໃຫ້ຕອບຄໍາຖາມຕັ້ງນີ້
- ໃນ DNS Query ມີ # questions ເທົ່າໄວ ແລະຂໍ້ມູນໃນ questions ດີວ່າວ່າ type ເປັນຄ່າວ່າໃຫ້ Capture ສ່ວນຂອງ Packet Details Pane ປະກອບດວຍ
- 1 question ຂັ້ນມູນຄົວ [www.ce.kmitl.ac.th : type A, class IN]
type A



```
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
  > www.ce.kmitl.ac.th: type A, class IN
```

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

2 Answers ใน Answers คือ

- 1) www.ce.kmitl.ac.th : type CNAME, class IN, cname jeweler19.ce.kmitl.ac.th
- 2) jeweler19.ce.kmitl.ac.th : type A, class IN, addr 161.246.4.119

```

Answer RRs: 2
Authority RRs: 3
Additional RRs: 2
> Queries
< 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
  < jeweler19.ce.kmitl.ac.th: type A, class IN, addr 161.246.4.119
    Name: jeweler19.ce.kmitl.ac.th
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 3600 (1 hour)
    Data length: 4
    Address: 161.246.4.119

```

- มี query และ response ที่ packet ให้ Capture ส่วนของ Packet Details Pane ดูรายละเอียด

มี query และ response ที่ packet ให้ Capture ส่วนของ Packet Details Pane ดูรายละเอียด

161.246.52.21	DNS	94	1	0 Standard query 0x0003 A www.ce.kmitl.ac.th.ZXHN H267A V1.0
192.168.1.105	DNS	94	1	0 Standard query response 0x0003 Refused A www.ce.kmitl.ac.th.ZXHN H267A V1.0
161.246.52.21	DNS	94	1	0 Standard query 0x0004 AAAA www.ce.kmitl.ac.th.ZXHN H267A V1.0
192.168.1.105	DNS	94	1	0 Standard query response 0x0004 Refused AAAA www.ce.kmitl.ac.th.ZXHN H267A V1.0
161.246.52.21	DNS	78	1	0 Standard query 0x0005 A www.ce.kmitl.ac.th
192.168.1.105	DNS	224	1	2 Standard query response 0x0005 A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th
161.246.52.21	DNS	78	1	0 Standard query 0x0006 AAAA www.ce.kmitl.ac.th
192.168.1.105	DNS	151	1	1 Standard query response 0x0006 AAAA www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th

< Domain Name System (response)

Transaction ID: 0x0005

> 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

< 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

> 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

[Request In: 11208]

[Time: 0.036592000 seconds]

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

วิธีดูจากงานรุป เป็นชื่อ server หรือ ip

```

▼ 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

1 question ตัวอย่าง [119.4.246.161.in-addr.arpa: type PTR
class IN] type PTR

```

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ▼ 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)

```

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

1 Answer ตัวอย่าง [119.4.246.161.in-addr.arpa: type PTR,
class IN ,jeweler19.ce.kmitl.ac.th]

```

Answer RRs: 1
Authority RRs: 2
Additional RRs: 2
> Queries
▼ Answers
  ▼ 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

```

- มี query และ response ใน packet ให้ Capture ส่วนของ Packet Details Pane ดู呀

มี 2 packet

18961	99.148266	192.168.1.105	161.246.52.21	DNS	86	1	0 Standard query 0x0003 PTR 119.4.246.161
18967	99.165323	161.246.52.21	192.168.1.105	DNS	196	1	1 Standard query response 0x0003 PTR 119.

```

> Frame 18961: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{7F53127C-AA18-4753-8E87-1134BC4DCABE}, id 0
> Ethernet II, Src: IntelCor_52:98:72 (4c:1d:96:52:98:72), Dst: zte_04:6b:40 (c0:b1:01:04:6b:40)
> Internet Protocol Version 4, Src: 192.168.1.105, Dst: 161.246.52.21
> User Datagram Protocol, Src Port: 56238, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x0003
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    ▼ 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: 18967]

```

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

มี ใจที่อยู่ในงานนี้ เป็น ns server ไม่ ip

```

Questions: 1
Answer RRs: 1
Authority RRs: 2
Additional RRs: 2
> Queries
> Answers
▼ Authoritative nameservers
  ▶ 4.246.161.in-addr.arpa: type NS, class IN, ns diamond.ce.kmitl.ac.th
  ▶ 4.246.161.in-addr.arpa: 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
[Request In: 18961]
[Time: 0.017057000 seconds]

```

15. ให้ใช้โปรแกรม nslookup และตั้ง server เป็น 199.7.91.13 จากนั้นให้ป้อน 199.7.91.13 โปรแกรม

แสดงผลอะไรมาบ้าง ให้ capture มาแสดง นักศึกษาคิดว่า 199.7.91.13 เป็น server อะไร

d.root-servers.net (Root Server) ลักษณะ 13 บิต 0 8-m.root-servers

```
Windows Command Prompt - nslookup
Microsoft Windows [Version 10.0.19044.1503]
(c) Microsoft Corporation. All rights reserved.

C:\Users\P>nslookup
Default Server: nsc02.awn.co.th
Address: 2405:9800:a::2:26

> 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 = 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 จากนั้นให้ป้อน ac.th, kmitl.ac.th และ ce.kmitl.ac.th ตามลำดับ ให้

capture มาแสดง และให้นักศึกษาคาดคะเนว่าการที่ name resolution ของ www.ce.kmitl.ac.th โดยสมมติ ให้เครื่องที่ 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
```

```
> server 202.28.0.1
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
Default Server: [202.28.0.1]
Address: 202.28.0.1

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

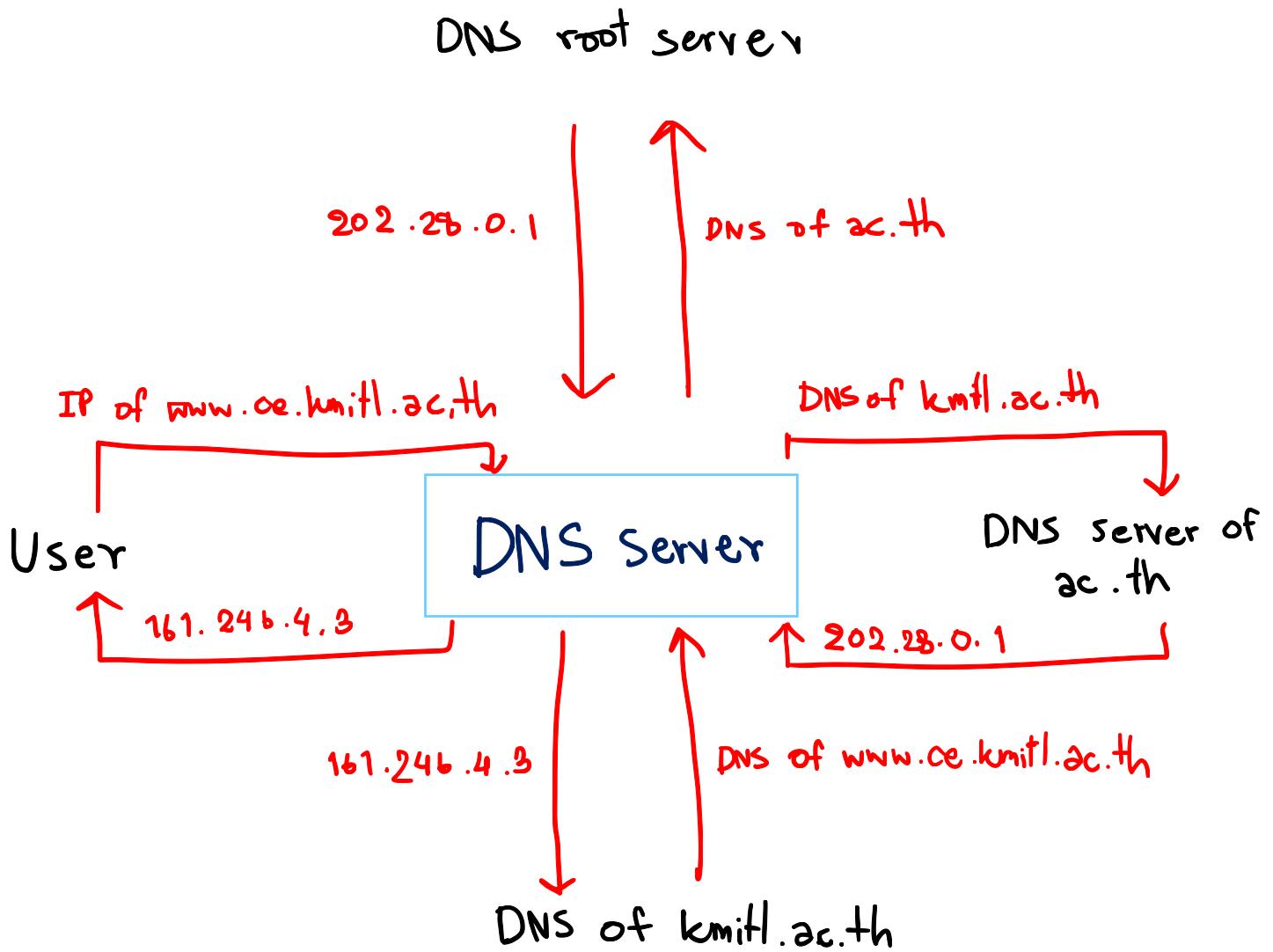
Name: ac.th

> 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
```



17. ให้เปิดไฟล์ tr-dns-slow.pcapng และหา packet response ของ DNS และขยายส่วนที่เป็น DNS หาข้อมูลเวลา งานนี้ให้สร้างเป็นคอลัมน์ ตั้งชื่อเป็น DNS Delta
18. ให้ Sort แล้วดูว่ามี DNS Query/Response ใด ที่ใช้เวลาเกิน 1 วินาที ให้ capture ผลการค้นหากماแสดง

packet # 11 เวลา 1.29219200

3 1.107703	204.127.202.4	24.6.126.218	DNS	499	1	4 0.107083000 Standard query response 0x0029 A
107 2.329101	216.148.227.68	24.6.126.218	DNS	511	1	4 0.207250000 Standard query response 0x002a A
11 1.292192	216.148.227.68	24.6.126.218	DNS	499	1	4 1.292192000 Standard query response 0x0029 A

19. ให้รีบ 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 ให้比べยับเทียบ DNS Delta ที่ได้จากแต่ละ Server (แสดงตัวเลขที่โดด) จากนั้นให้วิเคราะห์ผล

สเกตไกด์ค่า DNS Delta นะ

161.246.4.3 กับ 161.246.52.21 มีต่างกันเท่าไร

แต่ 8.8.8.8 ต่างหากกว่าค่าบนมาก เพราะ-

2 ต่อไปนี้คือ public DNS หาก 8.8.8.8

Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
> www.ce.kmitl.ac.th: type A, class IN
> Answers
[Request In: 16997]
[Time: 0.073017000 seconds]

No.	Time	Source	Destination	Protocol	Length	HTTP Delta	Questions	Answer RRs	DNS Delta	Info
7463	36.005160	161.246.4.3	192.168.1.105	DNS	224		1	2	0.016724000	Standard query response 0x0
13516	58.887690	161.246.52.21	192.168.1.105	DNS	224		1	2	0.016839000	Standard query response 0x0
17008	72.221267	8.8.8.8	192.168.1.105	DNS	118		1	2	0.073017000	Standard query response 0x0

งานครั้งที่ 5

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งโดยเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา และ _Lab5 เช่น 63010789_Lab5.pdf
- กำหนดส่ง ภายในวันที่ 16 กุมภาพันธ์ 2565