

กิจกรรมที่ 5 : FTP และ DNS

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

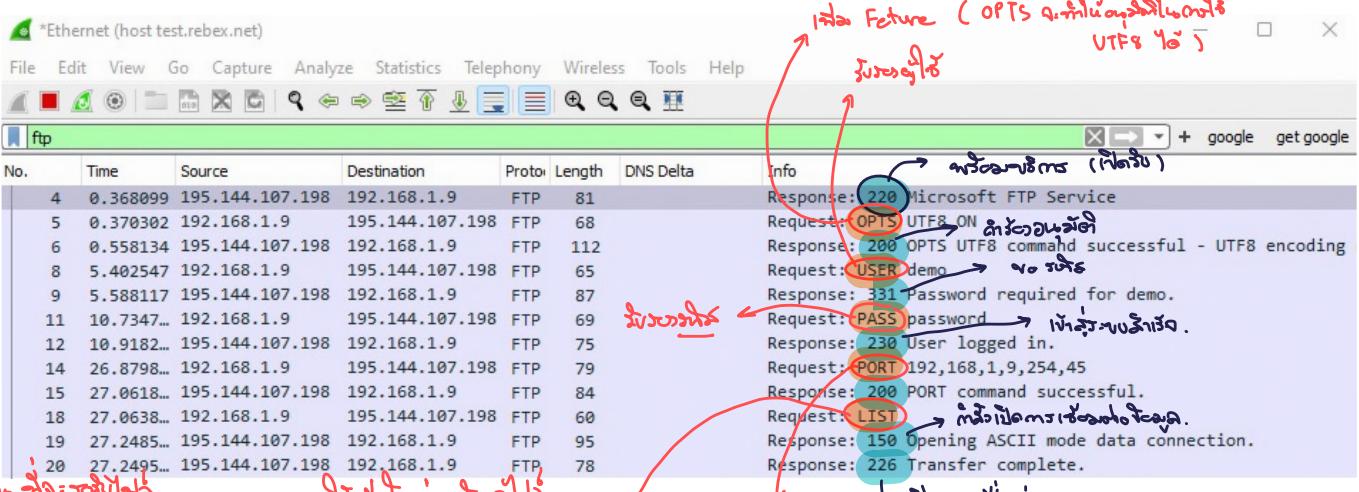
FTP (File Transfer Protocol)

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 ให้เปรียบเทียบระหว่าง แต่ละคำสั่ง ของ ftp ว่าตรงกับ packet ใดของ Wireshark ที่ตักจับ โดยให้ capture ภาพของ packet list pane ที่แสดงคำสั่งมาแสดงด้วย

C:\Users\Pun Punyawat>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.
8 ftp> dir → dir ໄສ່ຕົວຢ່າງດ້ວຍນີ້ເພື່ອ ftp
9 200 PORT command successful.
10 150 Opening ASCII mode data connection.
11 [10-19-20] 03:19PM → ລັບຕົວ
12 [12-17-21] 11:58AM → ລັບຕົວ
13 226 Transfer complete.
14 ftp: 98 bytes received in 0.00Seconds 49.00Kbytes/sec.
ftp> -

අභ්‍යන්තර	මුද්‍රණ පැවති	පිටත
2	මුද්‍රණ පැවති	4
3	මුද්‍රණ පැවති	6
4	මුද්‍රණ පැවති	8
5	මුද්‍රණ පැවති	9
6	මුද්‍රණ පැවති	11
7	මුද්‍රණ පැවති	13
8	මුද්‍රණ පැවති	14
9	මුද්‍රණ පැවති	15
10	මුද්‍රණ පැවති	19
11-12	මුද්‍රණ පැවති	18
13	මුද්‍රණ පැවති	20



20 27.249

၁၇။ မြန်မာ့ဘာတေသနရှုကိပ်ပေါ်။

07.198 192.168.1.9 FTP 78
Informationstechnik
no server in network

$\text{J} = \frac{\pi}{2} \log \text{Port}$
 $\text{J} = 180\text{m}.$

→ សំគាល់រួមចំណាំ
គិតជាក្រសួងការពីរដ្ឋបាល និងក្រសួង
(សំគាល់រួម ដើម្បីការពិន័យបែង)

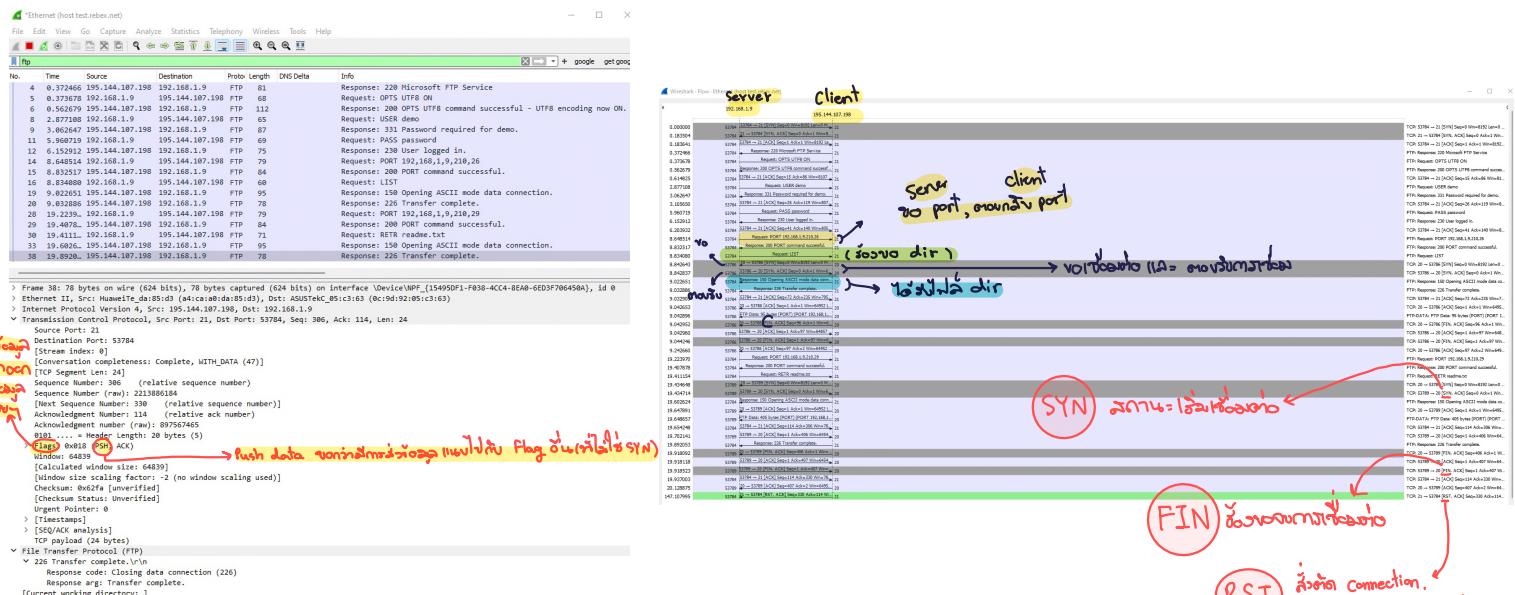
FTP Commands

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

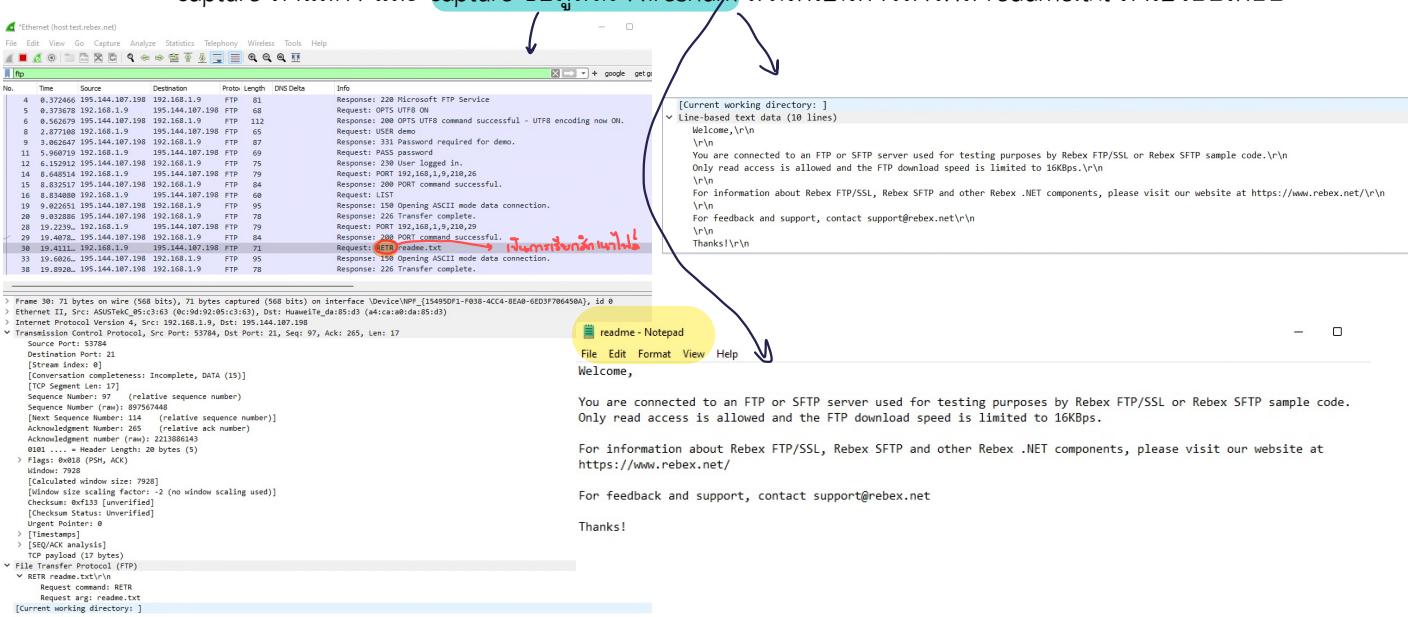
Stream Port 21 (in server) Octet packet # 38

m Flow graph matizas dir (2013)

- ~~First~~ First Port ~~the~~ ~~first~~ ~~available~~ ~~port~~
 - ~~then~~ Request Dir
 - Client $\xrightarrow{\text{}} \text{Flags} = \text{SYN}$ ~~and now we have to~~
 - Server $\xrightarrow{\text{}} \text{Flags} = \text{SYN/ACK}$ ~~and now we have to~~
 - $\xrightarrow{\text{}} \text{Response based on Request.}$
 - ~~responsible for~~ $\xrightarrow{\text{Flags}} \text{FIN}$



5. ใช้คำสั่ง get readme.txt เพื่อรับไฟล์ readme.txt จาก ftp server จากนั้นให้เปิดไฟล์ใน notepad และ capture มาและ แล้ว capture ข้อมูลใน Wireshark ส่วนที่เป็นการส่งไฟล์ readme.txt มาเปลี่ยนเทียบ



```

Command Prompt - ftp test.rebex.net
Microsoft Windows [Version 10.0.22000.434]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Pun Punyawat>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.
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 98.00Kbytes/sec.
ftp> get readme.txt
200 PORT command successful.
150 Opening ASCII mode data connection.
226 Transfer complete.
ftp: 405 bytes received in 0.27Seconds 1.50Kbytes/sec.
ftp>

```

```

Lab6_followTCP - Notepad
File Edit Format View Help
220 Microsoft FTP Service
OPTS UTF8 ON
200 OPTS UTF8 command successful - UTF8 encoding now ON.
USER demo
331 Password required for demo.
PASS password
230 User logged in.
PORT 192,168,1,9,246,254
200 PORT command successful.
LIST
150 Opening ASCII mode data connection.
226 Transfer complete.
PORT 192,168,1,9,247,14
200 PORT command successful.
RETR readme.txt
150 Opening ASCII mode data connection.
226 Transfer complete.

```

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

ສະຫຼຸບຕາມກຳນົດຈີວຫຼັງຕ້ອນນີ້ ຖອນໄສໄປຢູ່ລົດໄໝ

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)

FTP Command ຕະຫີ່ USER, PASS, PORT, NLST, TYPE, RETR
QUIT

Wireshark · Follow TCP Stream (tcp.stream eq 0) · ftp-clientside101.pcapng

```

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

```

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) and !(tcp.stream eq 1)**

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

รูปปั้นวัฒนธรรม

MAG RIPP ALFCOSTERTIVMFECIT



10. ให้อธิบายว่าการทำงานในข้อ 8 ทำเพื่ออะไร

ลดจำนวนข้อมูลที่ไม่ใช่ tcp.stream eq 0 ลง tcp.stream eq 1

27.12.2022

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

ไฟล์จะถูก download ประมาณ 1.328 Second .

วิธีการ

1. กรอก filter ดังนี้ **ftp-data.command == "SIZE OS Fingerprinting with ICMP.zip"**
2. เลือกจาก packet ตามที่ set / Time Reference (จังหวะ *REF*)
3. มอง Packet จะเห็น ระยะเวลาที่นานกว่าเดียว 1.328 seconds คือ 1.328 second

ftp-download-good2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp-data.command == "SIZE OS Fingerprinting with ICMP.zip"

No.	Time	Source	Destination	Proto	Length	DNS Delta	Info
659	1.246263	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
660	1.250956	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
662	1.252182	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
664	1.257468	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
665	1.258697	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
667	1.261162	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
668	1.265256	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
670	1.266485	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
672	1.270129	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
673	1.274872	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
675	1.276097	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
677	1.279822	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
678	1.286568	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
680	1.287794	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
682	1.291458	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
683	1.296565	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
685	1.297794	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
687	1.301002	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
688	1.302230	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
690	1.304530	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
691	1.308490	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
693	1.309722	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
695	1.313384	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
696	1.318251	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
698	1.319480	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
700	1.322874	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
701	1.327756	128.121.136.217	67.180.72.76	FTP..	1514		FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)
703	1.328233	128.121.136.217	67.180.72.76	FTP..	288		FTP Data: 234 bytes (PASV) (SIZE OS Fingerprinting with ICMP.z)

> Frame 16: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits) on interface unknown, id 0
 > Ethernet II, Src: Cadant_22:a5:82 (00:01:5c:22:a5:82), Dst: QuantaCo_a9:08:20 (00:16:36:a9:08:20)
 > Internet Protocol Version 4, Src: 128.121.136.217, Dst: 67.180.72.76
 > Transmission Control Protocol, Src Port: 30189, Dst Port: 4123, Seq: 1, Ack: 1, Len: 1024
 FTP Data (1024 bytes data)
 [Setup frame: 0]
 [Setup method: PASV]

DNS (Domain Name System)

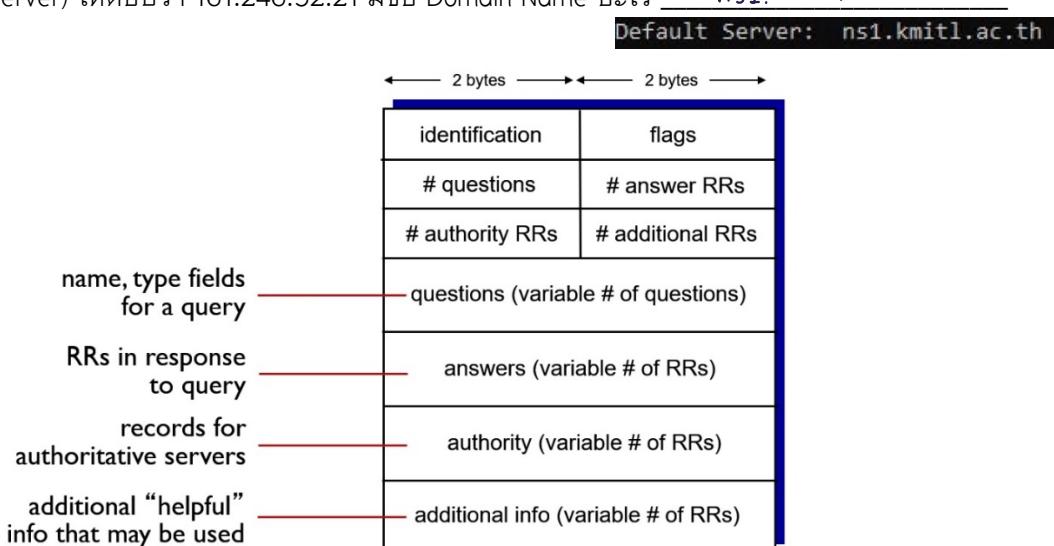
ໂປຣໂຕຄອລ DNS ຈະໃໝ່ພອຣື53 ໂດຍຮະບບປົງບົດກາລົວໃໝ່ຈະມີໂປຣແກຣມທີ່ຕິດຕ້ອກນ DNS ໄດ້ ມີສື່ວ່າ nslookup ກຣນີຂອງ Windows ໃຫ້ເຮັດ Command Prompt ຈາກນັ້ນໃຫ້ເຮັດໂປຣແກຣມ nslookup (ຫັກໃໝ່ຮະບບປົງບົດກາລົວໃໝ່ຈະປ່ຽນເຖິງກຳລັງກັນ) ຈະປ່ຽນກູ້ທີ່ກຳລັງກັນ

```
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

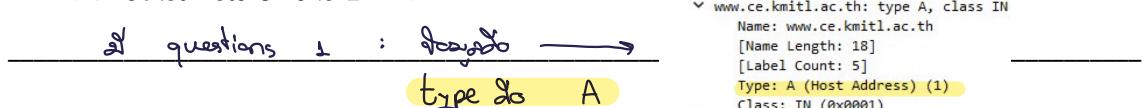
> |
```

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



13. ໃຫ້ພິມພໍ www.ce.kmitl.ac.th ແລະໜູດ Capture ໃຫ້ຕອບຄໍາຕາມຕັ້ງນີ້

- ໃນ DNS Query ມີ # questions ເທົ່າໄວ ແລະຂໍ້ອມນູລໃນ questions ດີວ່າວ່າ type ເປັນຄ່າວ່າໃຫ້ Capture ສ່ວນຂອງ Packet Details Pane ປະກອບດວຍ



1	0.000000	192.168.1.9	161.246.52.21	DNS	78	Standard query 0x0003 A www.ce.kmitl.ac.th
3	0.021626	192.168.1.9	161.246.52.21	DNS	78	Standard query 0x0004 AAAA www.ce.kmitl.ac.th
2	0.021420	161.246.52...	192.168.1.9	DNS	224	Standard query response 0x0003 A www.ce.kmitl.ac.th CNAME jewel
4	0.054870	161.246.52...	192.168.1.9	DNS	151	Standard query response 0x0004 AAAA www.ce.kmitl.ac.th CNAME je

> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPFL_{15495DF1-F038-4CC4-BEA0-6ED3F706450A}, i
> Ethernet II, Src: ASUSTek_05:c3:d3 (0c:9d:92:05:c3:d3), Dst: HuaweiTe_da:85:d3 (a4:ca:a0:d8:85:d3)
> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 161.246.52.21
> User Datagram Protocol, Src Port: 61699, Dst Port: 53
└ Domain Name System (query)
Transaction ID: 0x0003
Flags: 0x0100 Standard query
0... = Response: Message is a query
..000 0... = Opcode: Standard query (0)
....0. = Truncated: Message is not truncated
....1 = Recursion desired: Do query recursively
....0.... = Z: reserved (0)
....0.... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
└ 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)
[Response In: ?]

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

Details Pane ประกอบด้วย

Answer 2 : *Response*

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

1	0.000000	192.168.1.9	161.246.52.21	DNS	78	Standard query 0x0003 A www.ce.kmitl.ac.th
3	0.021626	192.168.1.9	161.246.52.21	DNS	78	Standard query 0x0004 AAAA www.ce.kmitl.ac.th
2	0.021420	161.246.52...	192.168.1.9	DNS	224	Standard query response 0x0003 A www.ce.kmitl.ac.th CNAME jewel
4	0.054870	161.246.52...	192.168.1.9	DNS	151	Standard query response 0x0004 AAAA www.ce.kmitl.ac.th CNAME je

> Frame 2: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface \Device\NPFL_{15495DF1-F038-4CC4-BEA0-6ED3F706450A}
> Ethernet II, Src: ASUSTek_05:c3:d3 (0c:9d:92:05:c3:d3), Dst: HuaweiTe_da:85:d3 (a4:ca:a0:d8:85:d3)
> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 161.246.52.21
> User Datagram Protocol, Src Port: 61699, Dst Port: 53
└ Domain Name System (response)
Transaction ID: 0x0003
Flags: 0x0500 Standard query response, No error
0... = Response: Message is a response
..000 0... = Opcode: Standard query (0)
....1. = Authoritative: Server is an authority for domain
....0. = Truncated: Message is not truncated
....1. = Recursion available: Server can't do recursive queries
....0. = Recursion desired: Do query recursively
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0. = Non-authenticated data: Unacceptable
....0. = Reply code: No error (0)
Questions: 1
Answers: 2
Authority RRs: 3
Additional RRs: 0
└ 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)
└ jeweler19.ce.kmitl.ac.th: type CNAME, class IN, cname jewel
Name: jeweler19.ce.kmitl.ac.th
[Name Length: 18]
[Label Count: 5]
Type: A (Host Address) (1)
Class: IN (0x0001)
└ www.ce.kmitl.ac.th: type A, class IN, addr 161.246.4.119
Name: www.ce.kmitl.ac.th
[Name Length: 18]
[Label Count: 5]
Type: A (Host Address) (1)
Class: IN (0x0001)
└ ce.kmitl.ac.th: type M5, class IN, ns clarinet.asimnet.co.th
Name: ce.kmitl.ac.th
[Name Length: 18]
[Label Count: 5]
Type: M5 (Host Address) (1)
Class: IN (0x0001)
└ ce.kmitl.ac.th: type M5, class IN, ns ns1.kmitl.ac.th
Name: ce.kmitl.ac.th
[Name Length: 18]
[Label Count: 5]
Type: M5 (Host Address) (1)
Class: IN (0x0001)
└ additional records
└ ns1.kmitl.ac.th: type A, class IN, addr 161.246.52.21
Name: ns1.kmitl.ac.th
[Name Length: 18]
[Label Count: 5]
Type: A (Host Address) (1)
Class: IN (0x0001)
└ diamond.ce.kmitl.ac.th: type A, class IN, addr 161.246.4.3
Name: diamond.ce.kmitl.ac.th
[Name Length: 18]
[Label Count: 5]
Type: A (Host Address) (1)
Class: IN (0x0001)

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

query 2 หรือ query response 2 packets

1	0.000000	192.168.1.9	161.246.52.21	DNS	78	Standard query 0x0003 A www.ce.kmitl.ac.th
3	0.021626	192.168.1.9	161.246.52.21	DNS	78	Standard query 0x0004 AAAA www.ce.kmitl.ac.th
2	0.021420	161.246.52...	192.168.1.9	DNS	224	Standard query response 0x0003 A www.ce.kmitl.ac.th CNAME jewel
4	0.054870	161.246.52...	192.168.1.9	DNS	151	Standard query response 0x0004 AAAA www.ce.kmitl.ac.th CNAME je

Type = A คืออะไร ตัวอักษรที่อยู่หลัง IP Address

(IPv4)

(IPv6)

32 bit

128 bit

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

authority : ce.kmitl.ac.th Authoritative nameservers
ce.kmitl.ac.th: type SOA, class IN, mname diamond.ce.kmitl.ac.th

additional : www.ce.kmitl.ac.th

No.	Traffic	TCP Dst	Source	Destination	Proto	Length	Info
1	0.000000		192.168.1.9	161.246.52.21	DNS	86	Standard query 0x0003 A www.ce.kmitl.ac.th
2	0.021139000		192.168.1.9	161.246.52.21	DNS	78	Standard query 0x0004 AAAA www.ce.kmitl.ac.th
3	0.021139000		161.246.52.21	192.168.1.9	DNS	224	Standard query response 0x0003 A www.ce.kmitl.ac.th CNAME Jewel
4	0.021139000		161.246.52.21	192.168.1.9	DNS	311	Standard query response 0x0004 AAAA www.ce.kmitl.ac.th CNAME Jewel

```

> Frame 4: 154 bytes on wire (1236 bits), 154 bytes captured (1236 bits) on interface \Device\NPF_{15495DF1-F038-4CC4-BEA0-6ED3F706450A}
> Ethernet II, Src: HuaweiTe_da85:d3 (04:ca:a0:da:85:d3), Dst: ASUSTeK_05:c3:63 (0c:9d:92:05:c3:63)
> Internet Protocol Version 4, Src: 161.246.52.21, Dst: 192.168.1.9
> User Datagram Protocol, Src Port: 53, Dst Port: 53
> Domain Name System (response)

Transaction ID: 0x0004
Flags: 0x0000 Standard query response, No error
    .000 R.... .... Response: Message is a response
    .000 R.... .... Options: 0x00000000
    .000 R.... .... Authoritative: Server is an authority for domain
    .000 R.... .... Truncated: Message is not truncated
    .000 R.... .... Recursion Desired: Recursion欲求する
    .000 R.... .... Recursion available: Server can't do recursive queries
    .000 R.... .... Zi reserved (0)
    .000 R.... .... Non-authenticated data: Answer/authority portion was not authenticated by the server
    .000 R.... .... Non-authenticated data: Unacceptable
    .000 R.... .... 0000 = Reply code: No error (0)

Questions:
  Address RR(s): 1
  Authoritative RR(s): 1
  Additional RR(s): 0

  Queries
    > www.ce.kmitl.ac.th: type AAAA, class IN
      Name: www.ce.kmitl.ac.th
      [Name Length: 18]
      [Label Count: 6]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)

  Answers
    > www.ce.kmitl.ac.th: type CNAME, class IN, cname Jewel@19.ce.kmitl.ac.th
    > Jewel@19.ce.kmitl.ac.th: type SOA, class IN, mname diamond.ce.kmitl.ac.th
      [Request In: 5]
      [Time: 0.035244000 seconds]
```

14. ทำการข้อ 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

สวนของ Packet Details Pane ประกอบด้วย

questions 1 : ฝ่าย →
type: PTR

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)

```

> Frame 5402: 20 bytes on wire (156 bits), 20 bytes captured (156 bits) on interface \Device\NPF_{15495DF1-F038-4CC4-BEA0-6ED3F706450A}, id 0
> Ethernet II, Src: HuaweiTe_da85:d3 (04:ca:a0:da:85:d3), Dst: ASUSTeK_05:c3:63 (0c:9d:92:05:c3:63)
> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 161.246.52.21
> User Datagram Protocol, Src Port: 53, Dst Port: 53
> Domain Name System (response)

Transaction ID: 0x0003
Flags: 0x0000 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 2
Additional RRs: 2

  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)

  Answers
    > 119.4.246.161.in-addr.arpa: type PTR, class IN, jewel@19.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: jewel@19.ce.kmitl.ac.th

  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: 5]
      [Time: 0.021139000 seconds]
```

- ใน DNS Response มี # answer เท่าไร และข้อมูลใน answer คืออะไร ให้ Capture สวนของ Packet

Details Pane ประกอบด้วย

Answer 1 : ฝ่าย →

Answers
 > 119.4.246.161.in-addr.arpa: type PTR, class IN, jewel@19.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: jewel@19.ce.kmitl.ac.th

```

+ 5402 20.0298.. 192.168.1.9    161.246.52.21   DNS   86      Standard query 0x0003 PTR 119.4.246.161.in-addr.arpa
└ 5406 20.0509.. 161.246.52.21   192.168.1.9    DNS   196   0.021139000 Standard query response 0x0003 PTR 119.4.246.161.in-addr.arpa PTR jeweler19.ce.kmitl.ac.th NS diamond.ce.kmitl.ac.th NS ns1.kmitl.ac.th

> Frame 5406: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits) on interface \Device\NPF_{15495DF1-F038-4CC4-8EA0-6ED3F706450A}, id 0
> Ethernet II, Src: HuaweiTe_da:85:d3 (a4:ca:a0:da:85:d3), Dst: ASUSTek_C_05:c3:63 (0c:9d:92:05:c3:63)
> Internet Protocol Version 4, Src: 161.246.52.21, Dst: 192.168.1.9
> User Datagram Protocol, Src Port: 53, Dst Port: 58689
└ Domain Name System (response)
  Transaction ID: 0x0003
  Flags: 0x8500 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 2
  Additional RRs: 2
  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)
    > 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
    > 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: 5402]
  [Time: 0.021139000 seconds]

```

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

query 1 packet ==> response 1 packet

```

+ 5402 20.0298.. 192.168.1.9    161.246.52.21   DNS   86      Standard query 0x0003 PTR 119.4.246.161.in-addr.arpa
└ 5406 20.0509.. 161.246.52.21   192.168.1.9    DNS   196   0.021139000 Standard query response 0x0003 PTR 119.4.246.161.in-addr.arpa PTR jeweler19.ce.kmitl.ac.th NS diamond.ce.kmitl.ac.th NS ns1.kmitl.ac.th

```

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

authority ถ้า 2 top

additional ถ้า 2 top

```

+ 5402 20.0298.. 192.168.1.9    161.246.52.21   DNS   86      Standard query 0x0003 PTR 119.4.246.161.in-addr.arpa
└ 5406 20.0509.. 161.246.52.21   192.168.1.9    DNS   196   0.021139000 Standard query response 0x0003 PTR 119.4.246.161.in-addr.arpa PTR jeweler19.ce.kmitl.ac.th NS diamond.ce.kmitl.ac.th NS ns1.kmitl.ac.th

> Frame 5406: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits) on interface \Device\NPF_{15495DF1-F038-4CC4-8EA0-6ED3F706450A}, id 0
> Ethernet II, Src: HuaweiTe_da:85:d3 (a4:ca:a0:da:85:d3), Dst: ASUSTek_C_05:c3:63 (0c:9d:92:05:c3:63)
> Internet Protocol Version 4, Src: 161.246.52.21, Dst: 192.168.1.9
> User Datagram Protocol, Src Port: 53, Dst Port: 58689
└ Domain Name System (response)
  Transaction ID: 0x0003
  Flags: 0x8500 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 2
  Additional RRs: 2
  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)
    > 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
    > 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: 5402]
  [Time: 0.021139000 seconds]

```

15. ให้ใช้โปรแกรม nslookup และตั้ง server เป็น 199.7.91.13 จากนั้นให้ป้อน 199.7.91.13 โปรแกรมแสดงผลอะไรมาบ้าง ให้ capture มาแสดง นักศึกษาคิดว่า 199.7.91.13 เป็น server อะไร
- ที่ d.root - servers.net
-

```
C:\Users\Pun Punyawat>nslookup
Default Server: Unknown
Address: 192.168.1.1

> 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 = 199.188.182.53
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 = 200.10.66.53
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 และแสดงผลอะไรมาบ้าง ให้ capture มาแสดง จากนั้นให้ใช้ IP Address ของ ns.thnic.net เป็น server จากนั้นให้ป้อน ac.th, kmitl.ac.th และ ce.kmitl.ac.th ตามลำดับ ให้ capture มาแสดง และให้นักศึกษาหาดูรูปการทำ 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
```

```
Microsoft Windows [Version 10.0.22000.434]
(c) Microsoft Corporation. All rights reserved.

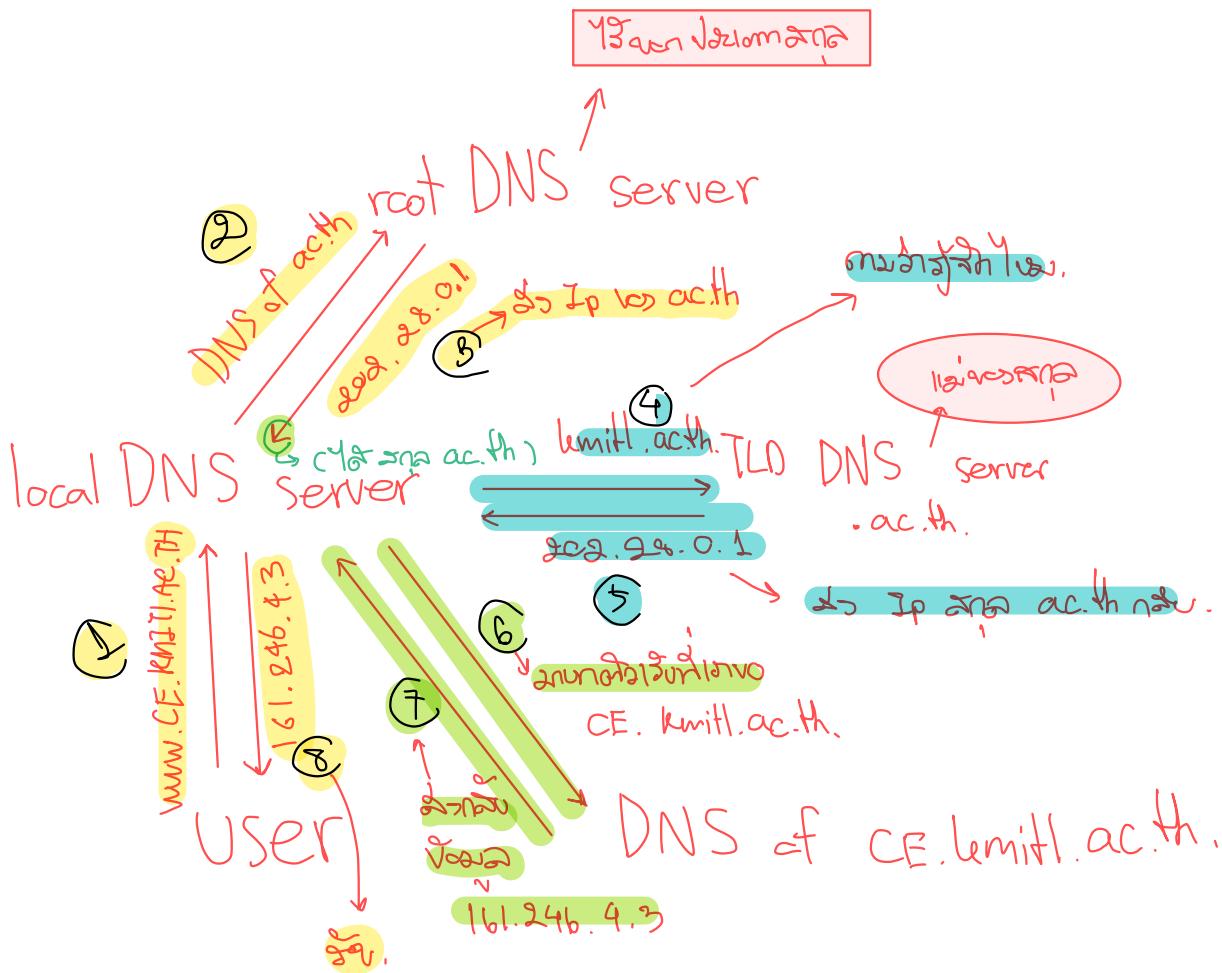
C:\Users\Pun Punyawat>nslookup
Default Server: Unknown
Address: 192.168.1.1

> server ns.thnic.net
Default Server: ns.thnic.net
Address: 202.28.0.1

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

> kmitl.ac.th
Server: ns.thnic.net
Address: 202.28.0.1
Name: kmitl.ac.th
Address: 161.246.127.182

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



161.246.4.19 → jewelers19.ce.km11.ac.th.
 161.246.4.3 → diamond.ce.km11.ac.th. → ce.km11

161.246.52.21 → ns1.km11.ac.th

199.7.91.13 → d.root-servers.net (main)

202.208.0.1 → 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 DNS query response ที่ใช้เวลาเกิน 1 วินาที packets ที่ 11

dns.flags.response==1						
No.	Time	Source	Destination	Proto	Length	DNS Delta
3	1.107703	204.127.202..	24.6.126.218	DNS	499	0.107083000 Standard query response 0x0029 A www.ncmec.org CNAME us.missingkids.com.edgesuite.net CNAME
107	2.329101	216.148.227..	24.6.126.218	DNS	511	0.207250000 Standard query response 0x002a A www.missingkids.com CNAME us.missingkids.com.edgesuite.net CNAME
11	1.292192	216.148.227..	24.6.126.218	DNS	499	1.292192000 Standard query response 0x0029 A www.ncmec.org CNAME us.missingkids.com.edgesuite.net CNAME

19. ให้รีเมิร์ค capture ใหม่เฉพาะข้อมูล DNS จากนั้นให้ใช้โปรแกรม nslookup และกำหนด server เป็น 161.246.4.3 งานนี้ให้ query www.ce.kmitl.ac.th งานนี้เปลี่ยน server เป็น 161.246.52.21 และ 8.8.8.8 ตามลำดับ ให้เปรียบเทียบ DNS Delta ที่ได้จากแต่ละ Server (แสดงตัวเลขที่ได้) งานนี้ให้วิเคราะห์ผล

Server 161.246.4.3 ก็เป็น 161.246.52.21 จึงจะถูก ignore ที่มา

จึงเป็น Server 8.8.8.8 (google to USA) จึงตอบ www.ce.kmitl.ac.th.
จะเห็นว่า
161.246.4.3 > 161.246.52.21 > 8.8.8.8

งานครั้งที่ 5

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

161.246.4.119 → jeweler19.ce.kmitl.ac.th.
161.246.4.3 → diamond.ce.kmitl.ac.th. → ce.kmitl

161.246.52.21 → ns1.kmitl.ac.th

199.7.91.13 → d.root-servers.net (อยู่根)