

01076010 เครื่องหมายคอมพิวเตอร์ : 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 คือเป็นช่องทางสำหรับรับส่งคำสั่ง 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\AMHARC>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)): ^C
C:\Users\AMHARC>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:demo
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 32.67Kbytes/sec.
ftp> bye
221 Goodbye.
```

row	packet	row	packet
2	4	-	28
-	5	16	29
3	6		
4	8		
5	9		
6	11		
7	12		
-	14		
9	15		
-	16		
10	19		
13	20		

ftp	No.	Time	Source	Destination	Protocol	Length	DNS DELTA	Info
4 0.404615			195.144.107.198	10.66.4.20	FTP	81		Response: 220 Microsoft FTP Service
5 0.407642			10.66.4.20	195.144.107.198	FTP	68		Request: OPTS UTF8 ON
6 0.601602			195.144.107.198	10.66.4.20	FTP	112		Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
8 4.729441			10.66.4.20	195.144.107.198	FTP	65		Request: USER demo
9 4.919860			195.144.107.198	10.66.4.20	FTP	87		Response: 331 Password required for demo.
11 7.630564			10.66.4.20	195.144.107.198	FTP	69		Request: PASS password
12 7.826674			195.144.107.198	10.66.4.20	FTP	75		Response: 230 User logged in.
14 10.929332			10.66.4.20	195.144.107.198	FTP	78		Request: PORT 10,66,4,20,198,26
15 11.138156			195.144.107.198	10.66.4.20	FTP	84		Response: 200 PORT command successful.
16 11.131981			10.66.4.20	195.144.107.198	FTP	60		Request: LIST
19 11.325974			195.144.107.198	10.66.4.20	FTP	95		Response: 150 Opening ASCII mode data connection.
20 11.345688			195.144.107.198	10.66.4.20	FTP	78		Response: 226 Transfer complete.
28 14.561826			10.66.4.20	195.144.107.198	FTP	60		Request: QUIT
29 14.752472			195.144.107.198	10.66.4.20	FTP	68		Response: 221 Goodbye.

ଓঁ পূজা প্রেসার্ব 63010871 SEC 03
(ৰাম লাব : ম. ১৩.০০-১৬.০০)

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

source port 21 (delen għabbar port 21) : paġġek 20

Flow

1. St connection port
 2. Request Dir
 3. Client : flag send (SYN)
 4. Server : flag send (SYN+ACK)
 5. Request And Response Period.
 6. End Connection (FIN)

No.	Time	Source	Destination	Protocol	Length	DNS DELTA	Info
4	0.4804615	195.144.187.198	10.66.4.20	FTP	81		Response: 220 Microsoft FTP Service
5	0.487642	195.144.187.198	10.66.4.20	FTP	68		Request: USER UTF8 ON
6	0.500	195.144.187.198	10.66.4.20	FTP	112		Response: 200 The UTF8 command successful - UTF8 encoding now ON.
8	0.729441	195.144.187.198	10.66.4.20	FTP	65		Request: USER demo
9	0.919368	195.144.187.198	10.66.4.20	FTP	87		Response: 331 Password required for demo.
11	7.639864	195.144.187.198	10.66.4.20	FTP	69		Request: PASS password
12	7.640074	195.144.187.198	10.66.4.20	FTP	79		Response: 230 User logged in.
14	18.929332	195.144.187.198	10.66.4.20	FTP	78		Request: PORT 10.66.4.20,198,26
15	11.381056	195.144.187.198	10.66.4.20	FTP	84		Response: 200 PORT command successful.
15	11.313081	195.144.187.198	10.66.4.20	FTP	60		Request: LIST
15	11.313105	195.144.187.198	10.66.4.20	FTP	95		Response: 150 Opening ASCII mode data connection.
28	11.345688	195.144.187.198	10.66.4.20	FTP	78		Response: 226 Transfer complete.
28	14.561826	195.144.187.198	10.66.4.20	FTP	68		Request: QUIT
29	14.752472	195.144.187.198	10.66.4.20	FTP	68		Response: 221 Goodbye.

> Framerate: 0.000000 bytes on wire (0 Bits), 78 bytes captured (0 Bits) on Interface 'bpf@nic[MPD]_0x0000000f-000f-000f-0e10-000fb03402', id 0

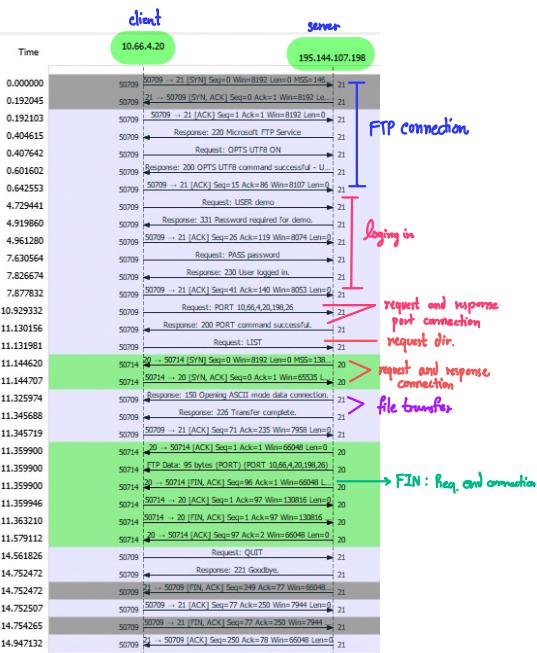
Ethernet II, Src: Huawei_Board[00:00:00:00:00:00], Dst: IntelPro_1_GbE [08:00:00:00:00:00] (8:18:00:00:00:00)

> Internet Protocol Version 4, Src: 195.144.187.198, Dst: 10.66.4.20

> Internet Control Message Protocol, Src Port: 21, Dst Port: 507099, Seq: 211, Ack: 71, Len: 24

Source Port: 507099
 Destination Port: 21
 [String index: 0]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Length: 24]
 Sequence Number (raw): 105314727
 Sequence Number (rel.): (relative sequence number)
 Sequence Number (raw): 105314727
 [Next Sequence Number: 235 (relative sequence number)]
 Acknowledgment Number (raw): 2083282320
 Acknowledgment Number (rel.): (relative acknowledgement number)
 Acknowledgment Number (raw): 2083282320
 0101 - Header Length: 20 bytes (5)
 <-- Flags: PSH, ACK
 0000.... - Reset: Not set
 0.... Nonce: Not set
 0.... Congestion Window Reduced (CWR): Not set
 0.... ECN-Echo: Not set
 0.... Urgent: Not set
 1.... Window Scale: Set
 1.... Push: Set
 0.... .R..: Reset: Not set
 0.... .S..: Syn: Not set
 0.... .A..: Ack: Not set
 [TCP Flags:AP....]
 Header: 258
 [Minimum window size: 66488]
 [Minimum size scaling factor: 256]
 Checksum: 0x2120 [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 > [Timeline: 14.752472000]
 > [SEQ/ACK analysis]
 TCP payload (24 bytes)
 > Framerate: 0.000000 bytes on wire (0 Bits), 78 bytes captured (0 Bits)
 > 226 Transfer complete.\r\n

[Current working directory:]



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

```
amharc@DESKTOP-PK3GHP3:~$ cat readme.txt
```

You are connected to an FTP or SFTP server used for testing purposes by Rebex FTP/SSL or Rebex SFTP sample code. 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, please visit our website at <https://www.rebex.net/>

For feedback and support, contact support@rebex.net

Thanks!

amharc@DESKTOP-PK3GHP3:~\$

Time	Source	Destination	Protocol	Length	DNS.DELTA	Info
10:43:06.095	195.144.168.198	195.168.1.21	FTP	81		Request: 220 Microsoft FTP Service
10:43:09.587	195.168.1.21	195.144.168.198	FTP	55		Response: 221 User does not exist.
11:21:29.144	195.144.168.198	195.168.1.21	FTP	87		Request: 331 Password required for demo.
9:46:05.949	192.168.1.21	195.144.168.198	FTP	69		Request: PASS password
11:21:30.000	195.144.168.198	195.168.1.21	FTP	75		Request: 230 User Logged In.
11:21:30.000	192.168.1.21	195.144.168.198	FTP	68		Request: SYST
12:10:29.232	195.144.168.198	195.168.1.21	FTP	78		Response: 215 Windows NT
12:10:29.232	192.168.1.21	195.144.168.198	FTP	88		Request: 200 PORT command successful.
12:10:29.232	195.144.168.198	195.168.1.21	FTP	54		Response: 200 PORT command successful
10:44:18.575	195.144.168.198	195.168.1.21	FTP	68		Request: LIST
10:44:18.575	192.168.1.21	195.144.168.198	FTP	108		Response: 125 Data connection already open; Transfer starting.
10:44:18.575	195.144.168.198	195.168.1.21	FTP	78		Response: 126 Transfer complete.
17:27:44.607	192.168.1.21	195.144.168.198	FTP	88		Request: PORT 192.168.1.21,21,21,57
17:27:44.607	195.144.168.198	195.168.1.21	FTP	84		Response: 200 PORT command successful.
17:27:44.607	192.168.1.21	195.144.168.198	FTP	96		Request: PWD
17:27:44.607	195.144.168.198	195.168.1.21	FTP	108		Response: 125 Data connection already open; Transfer starting.
17:27:44.607	192.168.1.21	195.144.168.198	FTP	108		Response: 126 Transfer complete.
17:27:44.607	195.144.168.198	195.168.1.21	FTP	78		Request: 226 Transfer complete.
17:27:44.607	192.168.1.21	195.144.168.198	FTP	68		Request: QUIT
18:39:06.018	195.144.168.198	195.168.1.21	FTP	68		Response: 221 Goodbye.
22:27:59.099	195.144.168.198	195.168.1.21	FTP	68		Request: 222 Goodbye.

Frame 32: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{D0789461-BC09-4438-8390-85AC6C40588C}, id 8
Ethernet II, Src: LCF\HeFe_79:5c:d4 (00:2b:67:79:5c:d4), Dst: HuaweiLe_bca:a:e2 (3c:e8:24:bc:a0:e2)

Internet Protocol Version 4, Src: 192.168.1.21, Dst: 195.144.107.198
Transmission Control Protocol, Src Port: 55093, Dst Port: 21, Seq: 91, Ack: 236, Len: 17
File Transfer Protocol (FTP)

Request command: RETR

```
Request arg: README.txt  
Current working directory: ]
```

```

amharc@DESKTOP-PK3GHP3:~$ ftp test.rebex.net
Connected to test.rebex.net.
220 Microsoft FTP Service
Name (test.rebex.net:amharc): demo
331 Password required for demo.
Password:
230 User logged in.
Remote system type is Windows_NT.
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> get readme.txt
local: readme.txt remote: readme.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
405 bytes received in 0.23 secs (1.7379 kB/s)
ftp> bye
221 Goodbye.

```

ວິຊາ ດະນີຍຸດ 63010871 SEC 03
(ຝາກ LAB : ຮ. 13.00-16.00)

```

220 Microsoft FTP Service
USER demo
331 Password required for demo.
PASS password
230 User logged in.
SYST
215 Windows_NT
PORT 192,168,1,21,215,57
200 PORT command successful.
LIST
125 Data connection already open; Transfer starting.
226 Transfer complete.
PORT 192,168,1,21,215,61
200 PORT command successful.
RETR readme.txt
125 Data connection already open; Transfer starting.
226 Transfer complete.
QUIT
221 Goodbye.

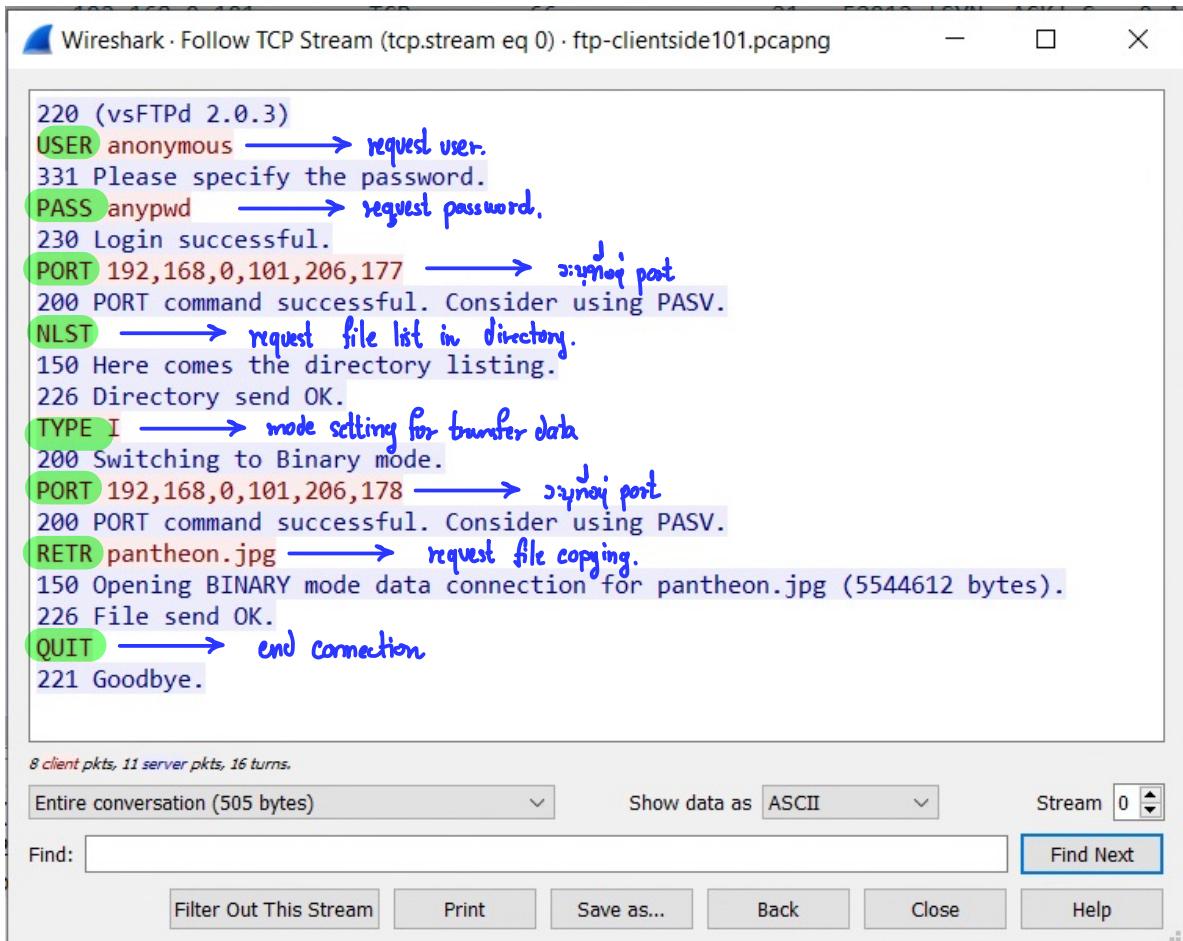
```

6. ໃຫ້ຄລິກຂວາທີ່ packet ທີ່ເປັນຂໍ້ມູນຂອງ readme.txt ແລະເລືອກ Follow TCP Stream ແລະ Save as... ເປັນໄຟລ໌ ໃຫ້ຕັ້ງຊື່ອະໄຣກີໄດ້ ຈາກນັ້ນເປີດໄຟລ໌ດ້ວຍ notepad ແລ້ວເປົ້າຍເຖິງກັບໄຟລ໌ readme.txt ວ່າມີອະໄຣແດກຕາງກັນຫຼືອຳນວຍ

ວິນຍາທີ່ TCP Command ມີ Capture ມານວິທີກຳນົດ

7. ໃຫ້ເປີດໄຟລ໌ ftp-clientside101.pcapng ຄລິກຂວາທີ່ Packet 6 (USER anonymous) ແລະເລືອກ Follow TCP Stream ໃຫ້ Capture ມານວິທີກຳນົດຂອງ Follow TCP Stream ທີ່ແສດງການໂຕຕອບຂອງ FTP ໃຫ້ອືບາຍວ່າມີຄຳສັ່ງຂອງ FTP Protocol ອະໄຮບ້າງ (ຄຳສັ່ງຂອງ Protocol ໡ີໃຊ້ຄຳສັ່ງຂອງໂປຣແກຣມ)

FTP commands : USER, PASS, PORT, NLST, TYPE, 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  `!(tcp.stream eq 0) and !(tcp.stream eq 1)`

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

ဂိမ္မရ Pantheon.



10. ให้คุณนายความร่วมทำงานในข้อ 8 ทำเพื่อรักษา

នរណាគារពីក្នុង tcp.stream ជាមួយ និង tcp.stream ជាមួយ

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

Questa pagina download nel 1.328 sec.
Pagine

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

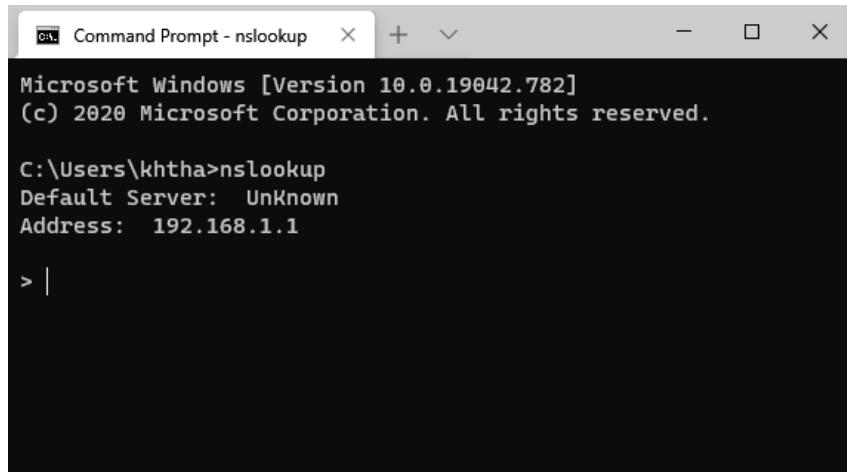
3. obtain packet origin from set/time reference (for time with *BEF*)
(current packet timestamp = 0 sec.)

3. en packet ស្រើរក្សា នៃអាមេរិកចាប់ពី 1.924230 sec.

667 1.261162	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
668 1.265256	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
670 1.266485	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
672 1.270128	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
673 1.274872	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
675 1.276897	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
677 1.279822	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
678 1.286568	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
680 1.287794	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
682 1.291458	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
683 1.296565	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
685 1.297794	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
687 1.301002	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
688 1.302230	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
690 1.304530	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
691 1.308490	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
693 1.309722	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
695 1.313384	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
696 1.318251	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
698 1.319480	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
700 1.322874	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
701 1.327756	128.121.136.217	67.180.72.76	FTP-DA-	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
703 1.328233	128.121.136.217	67.180.72.76	FTP-DA-	288	FTP Data: 234 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)

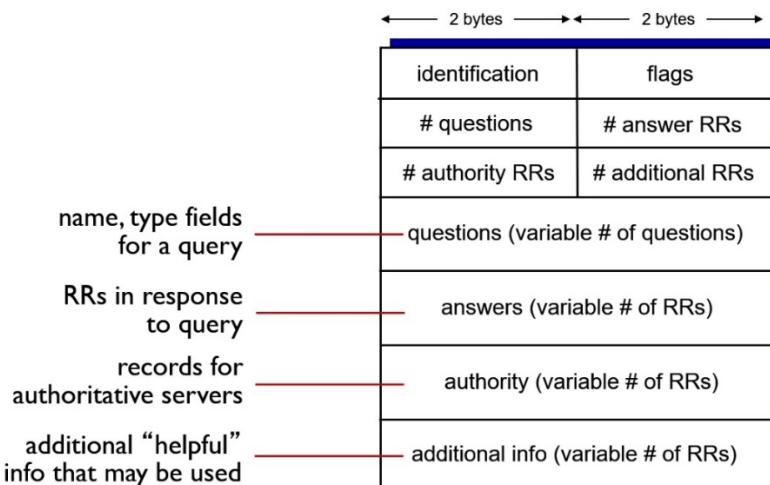
DNS (Domain Name System)

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



- filter: port 53

12. ให้เปิดโปรแกรม Wireshark กำหนดเงื่อนไขให้ Capture เฉพาะโปรโตคอล DNS พิมพ์ server 161.246.52.21 ลงไป (เป็นการกำหนดให้เชื่อมต่อ กับ DNS Server ที่มี IP Address 161.246.52.21 แทน Default Server) ให้ตอบว่า 161.246.52.21 มีชื่อ Domain Name อะไร ns1.lamth.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

2) question 1 : type A

- ```
 < 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)
```

| No.             | Time         | Source       | Destination | Protocol | Length                                                                                                                                  | Info |
|-----------------|--------------|--------------|-------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------|------|
| 3490 1.991568   | 10.66.4.20   | 10.252.99.21 | DNS         | 70       | Standard query 0x2fab A dns.google                                                                                                      |      |
| 3491 2.004635   | 10.252.99.21 | 10.66.4.20   | DNS         | 345      | Standard query response 0x2fab A dns.google A 8.8.8.8 A 8.8.4.4 NS j.root-servers.net NS h.root-servers.net NS a.root-servers.net NS... |      |
| 28315 26.050089 | 10.66.4.20   | 10.252.99.21 | DNS         | 86       | Standard query 0xf95e PTR 21.52.246.161.in-addr.arpa                                                                                    |      |
| 28316 26.066402 | 10.252.99.21 | 10.66.4.20   | DNS         | 258      | Standard query response 0xf95e PTR 21.52.246.161.in-addr.arpa PTR ns1.kmitl.ac.th NS diamond.ce.kmitl.ac.th NS clarinet.asianet.co.t... |      |
| 62585 53.538245 | 10.66.4.20   | 10.252.99.21 | DNS         | 78       | Standard query 0x7cd1 A www.ce.kmitl.ac.th                                                                                              |      |
| 62657 53.567303 | 10.252.99.21 | 10.66.4.20   | DNS         | 224      | Standard query response 0x7cd1 A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th A 161.246.4.119 NS clarinet.asianet.co.th NS ns1...  |      |
| 62661 53.571804 | 10.66.4.20   | 10.252.99.21 | DNS         | 84       | Standard query 0xb8a1 AAAA jeweler19.ce.kmitl.ac.th                                                                                     |      |
| 62662 53.578769 | 10.252.99.21 | 10.66.4.20   | DNS         | 133      | Standard query response 0xb8a1 AAAA jeweler19.ce.kmitl.ac.th SOA diamond.ce.kmitl.ac.th                                                 |      |

Transaction ID: 0x7cd1  
 > Flags: 0x0100 Standard query  
 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: 62657]

ថ្លែង ចិត្តក្រឡាយ 13010871 SEC 03  
 (This LAB : ន. 18.00-16.00)

- នៃ DNS Response មី # answer ពេញវា និងមានព័ត៌មាននៃ answer គឺជាដឹងទៀត នៅ Capture សំណង់ Packet

### Details Pane ព្រមករបគរយ

នៅ Answer 2 : នៅ

| Answers                                                                                                                                                                              |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| ✓ www.ce.kmitl.ac.th: type CNAME, class IN, cname jeweler19.ce.kmitl.ac.th                                                                                                           |  |
| Name: www.ce.kmitl.ac.th<br>Type: CNAME (Canonical NAME for an alias) (5)<br>Class: IN (0x0001)<br>Time to live: 3600 (1 hour)<br>Data length: 12<br>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<br>Type: A (Host Address) (1)<br>Class: IN (0x0001)<br>Time to live: 3600 (1 hour)<br>Data length: 4<br>Address: 161.246.4.119                        |  |

| No.             | Time         | Source       | Destination | Protocol | Length                                                                                                                                  | Info |
|-----------------|--------------|--------------|-------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------|------|
| 3490 1.991568   | 10.66.4.20   | 10.252.99.21 | DNS         | 70       | Standard query 0x2fab A dns.google                                                                                                      |      |
| 3491 2.004635   | 10.252.99.21 | 10.66.4.20   | DNS         | 345      | Standard query response 0x2fab A dns.google A 8.8.8.8 A 8.8.4.4 NS j.root-servers.net NS h.root-servers.net NS a.root-servers.net NS... |      |
| 28315 26.050089 | 10.66.4.20   | 10.252.99.21 | DNS         | 86       | Standard query 0xf95e PTR 21.52.246.161.in-addr.arpa                                                                                    |      |
| 28316 26.066402 | 10.252.99.21 | 10.66.4.20   | DNS         | 258      | Standard query response 0xf95e PTR 21.52.246.161.in-addr.arpa PTR ns1.kmitl.ac.th NS diamond.ce.kmitl.ac.th NS clarinet.asianet.co.t... |      |
| 62585 53.538245 | 10.66.4.20   | 10.252.99.21 | DNS         | 78       | Standard query 0x7cd1 A www.ce.kmitl.ac.th                                                                                              |      |
| 62657 53.567303 | 10.252.99.21 | 10.66.4.20   | DNS         | 224      | Standard query response 0x7cd1 A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th A 161.246.4.119 NS clarinet.asianet.co.th NS ns1...  |      |
| 62661 53.571804 | 10.66.4.20   | 10.252.99.21 | DNS         | 84       | Standard query 0xb8a1 AAAA jeweler19.ce.kmitl.ac.th                                                                                     |      |
| 62662 53.578769 | 10.252.99.21 | 10.66.4.20   | DNS         | 133      | Standard query response 0xb8a1 AAAA jeweler19.ce.kmitl.ac.th SOA diamond.ce.kmitl.ac.th                                                 |      |

- មី query និង response នៃ packet នៅ Capture សំណង់ Packet Details Pane គរយ

2 query packet

2 response packet

IPV4 (32 bits) } type A: IP Address request  
 IPV6 (128 bits) }

| No.             | Time         | Source       | Destination | Protocol | Length                                                                                                                                 | Info |
|-----------------|--------------|--------------|-------------|----------|----------------------------------------------------------------------------------------------------------------------------------------|------|
| 62585 53.538245 | 10.66.4.20   | 10.252.99.21 | DNS         | 78       | Standard query 0x7cd1 A www.ce.kmitl.ac.th                                                                                             |      |
| 62657 53.567303 | 10.252.99.21 | 10.66.4.20   | DNS         | 224      | Standard query response 0x7cd1 A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th A 161.246.4.119 NS clarinet.asianet.co.th NS ns1... |      |
| 62661 53.571804 | 10.66.4.20   | 10.252.99.21 | DNS         | 84       | Standard query 0xb8a1 AAAA jeweler19.ce.kmitl.ac.th                                                                                    |      |
| 62662 53.578769 | 10.252.99.21 | 10.66.4.20   | DNS         | 133      | Standard query response 0xb8a1 AAAA jeweler19.ce.kmitl.ac.th SOA diamond.ce.kmitl.ac.th                                                |      |

- មីខ័ម្ពលសាន authority និង additional info ទីនេះ បែនិច្ឆ័ត្តម្ពលនៃវា

authority នឹង authoritative name ស្ថិតនៅ domain name នៅរដ្ឋ និង SV.

additional info នឹង response IP Address និង domainname និង 2 domain name

#### ▼ Authoritative nameservers

- > 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
- > ce.kmitl.ac.th: type NS, class IN, ns diamond.ce.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. ទាកោមខែ 13 មិករា នៅថ្ងៃ 161.246.4.119 នៅទីតាំង [www.ce.kmitl.ac.th](http://www.ce.kmitl.ac.th)

- នៃ DNS Query មី # questions ហេតវា និងខ័ម្ពលនៃ questions គឺនេះ តួអេត្របានជាប្រភពទៅ

ស្ថាននៃ Packet Details Pane ប្រភពបាបគាយ  
នៅ 1 Question : 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)

| No. | Time     | Source       | Destination  | Protocol | Length | Info                                                                                                                                    |
|-----|----------|--------------|--------------|----------|--------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 1   | 0.000000 | 10.66.4.20   | 10.252.99.21 | DNS      | 86     | Standard query 0xe5e3 PTR 119.4.246.161.in-addr.arpa                                                                                    |
| 2   | 0.035333 | 10.252.99.21 | 10.66.4.20   | DNS      | 196    | Standard query response 0xe5e3 PTR 119.4.246.161.in-addr.arpa PTR jeweler19.ce.kmitl.ac.th NS ns1.kmitl.ac.th NS diamond.ce.kmitl.ac.th |

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 ns1.kmitl.ac.th  
 4.246.161.in-addr.arpa: type NS, class IN, ns diamond.ce.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:]  
 [Time: 0.035333000 seconds]

- នៃ DNS Response មី # answer ហេតវា និងខ័ម្ពលនៃ answer គឺនេះ តួអេត្របានជាប្រភព

Details Pane ប្រភពបាបគាយ

នៅ 1 Answer

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

| No. | Time     | Source       | Destination  | Protocol | Length | Info                                                                                                                                    |
|-----|----------|--------------|--------------|----------|--------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 1   | 0.000000 | 10.66.4.20   | 10.252.99.21 | DNS      | 86     | Standard query 0xe5e3 PTR 119.4.246.161.in-addr.arpa                                                                                    |
| 2   | 0.035333 | 10.252.99.21 | 10.66.4.20   | DNS      | 196    | Standard query response 0xe5e3 PTR 119.4.246.161.in-addr.arpa PTR jeweler19.ce.kmitl.ac.th NS ns1.kmitl.ac.th NS diamond.ce.kmitl.ac.th |

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 ns1.kmitl.ac.th
- 4.246.161.in-addr.arpa: type NS, class IN, ns diamond.ce.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: 11]  
[Time: 0.035333000 seconds]

ວິທີສະຫຼຸບ ດົກເຈົ້າ 63010871 SEC 03  
(Tham LAB : ນ. 13.00 - 16.00)

- ມີ query ແລະ response ອີ່ packet ໃຫ້ Capture ສ່ວນຂອງ Packet Details Pane ດ້ວຍ

| Query Packet

| Response Packet

| No. | Time     | Source       | Destination  | Protocol | Length | Info                                                                                                                                    |
|-----|----------|--------------|--------------|----------|--------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 1   | 0.000000 | 10.66.4.20   | 10.252.99.21 | DNS      | 86     | Standard query 0xe5e3 PTR 119.4.246.161.in-addr.arpa                                                                                    |
| 2   | 0.035333 | 10.252.99.21 | 10.66.4.20   | DNS      | 196    | Standard query response 0xe5e3 PTR 119.4.246.161.in-addr.arpa PTR jeweler19.ce.kmitl.ac.th NS ns1.kmitl.ac.th NS diamond.ce.kmitl.ac.th |

|                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Queries                                                                                                                                                                                                                                                                                                                                            |
| 119.4.246.161.in-addr.arpa: type PTR, class IN <ul style="list-style-type: none"> <li>Name: 119.4.246.161.in-addr.arpa</li> <li>[Name Length: 26]</li> <li>[Label Count: 6]</li> <li>Type: PTR (domain name PoinTeR) (12)</li> <li>Class: IN (0x0001)</li> </ul>                                                                                   |
| Answers                                                                                                                                                                                                                                                                                                                                            |
| 119.4.246.161.in-addr.arpa: type PTR, class IN, jeweler19.ce.kmitl.ac.th <ul style="list-style-type: none"> <li>Name: 119.4.246.161.in-addr.arpa</li> <li>Type: PTR (domain name PoinTeR) (12)</li> <li>Class: IN (0x0001)</li> <li>Time to live: 3600 (1 hour)</li> <li>Data length: 26</li> <li>Domain Name: jeweler19.ce.kmitl.ac.th</li> </ul> |
| Authoritative nameservers                                                                                                                                                                                                                                                                                                                          |

- ມີຂໍອມລສວນ authority ແລະ additional info ທີ່ຈະໄດ້ເປັນຂໍອມລວະໄຮ

authority ຊີ່ວິທີ authoritative name ສະໜັບສິນ domain name ຂອງ ຂະໜາງ

additional info ສະໜັບສິນ response IP Address ມີ domainname ດີ່ຈຳ ຂະໜາງ

|                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authoritative nameservers                                                                                                                                                                                                                                                                                                                    |
| 4.246.161.in-addr.arpa: type NS, class IN, ns ns1.kmitl.ac.th <ul style="list-style-type: none"> <li>Name: 4.246.161.in-addr.arpa</li> <li>Type: NS (authoritative Name Server) (2)</li> <li>Class: IN (0x0001)</li> <li>Time to live: 3600 (1 hour)</li> <li>Data length: 6</li> <li>Name Server: ns1.kmitl.ac.th</li> </ul>                |
| 4.246.161.in-addr.arpa: type NS, class IN, ns diamond.ce.kmitl.ac.th <ul style="list-style-type: none"> <li>Name: 4.246.161.in-addr.arpa</li> <li>Type: NS (authoritative Name Server) (2)</li> <li>Class: IN (0x0001)</li> <li>Time to live: 3600 (1 hour)</li> <li>Data length: 10</li> <li>Name Server: diamond.ce.kmitl.ac.th</li> </ul> |
| Additional records                                                                                                                                                                                                                                                                                                                           |
| ns1.kmitl.ac.th: type A, class IN, addr 161.246.52.21 <ul style="list-style-type: none"> <li>Name: ns1.kmitl.ac.th</li> <li>Type: A (Host Address) (1)</li> <li>Class: IN (0x0001)</li> <li>Time to live: 3600 (1 hour)</li> <li>Data length: 4</li> <li>Address: 161.246.52.21</li> </ul>                                                   |
| diamond.ce.kmitl.ac.th: type A, class IN, addr 161.246.4.3 <ul style="list-style-type: none"> <li>Name: diamond.ce.kmitl.ac.th</li> <li>Type: A (Host Address) (1)</li> <li>Class: IN (0x0001)</li> <li>Time to live: 3600 (1 hour)</li> <li>Data length: 4</li> <li>Address: 161.246.4.3</li> </ul>                                         |

15. ໃຫ້ໃຊ້ព្រограм nslookup ឡាតាំង server เป็น 199.7.91.13 ຈាន់នៅໃន້ ប៉ុន 199.7.91.13 ព្រogram  
 แสดงផលខ្លួនបាន ໃຫ້ capture មាសេច នៃកីកម្មាគិតវា 199.7.91.13 បែន server នេះ  
 199.7.91.13 នឹង Root Server

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

16. ໃຫ້បូន query www.ce.kmitl.ac.th ផលខ្លួនបាន ໃຫ້ capture មាសេច ជាន់នៅໃន້ ដើម្បី IP Address  
 ខ្លួន ns.thnic.net បែន server ជាន់នៅໃហ៊ូន ac.th, kmitl.ac.th និង ce.kmitl.ac.th តាមលំដាប ໃຫ້  
 capture មាសេច និងនៃកីកម្មាគាត់រូបភាពា name resolution ខ្លួន www.ce.kmitl.ac.th ទូយសមមនុ  
 ឲ្យគឺទី request បែនគីឡូវិញទៀតូច្ចារម្មាត់

```
> 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 ns.thnic.net
*** Can't find address for server ns.thnic.net: Non-authoritative answer
> 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 = 196.216.169.19
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: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

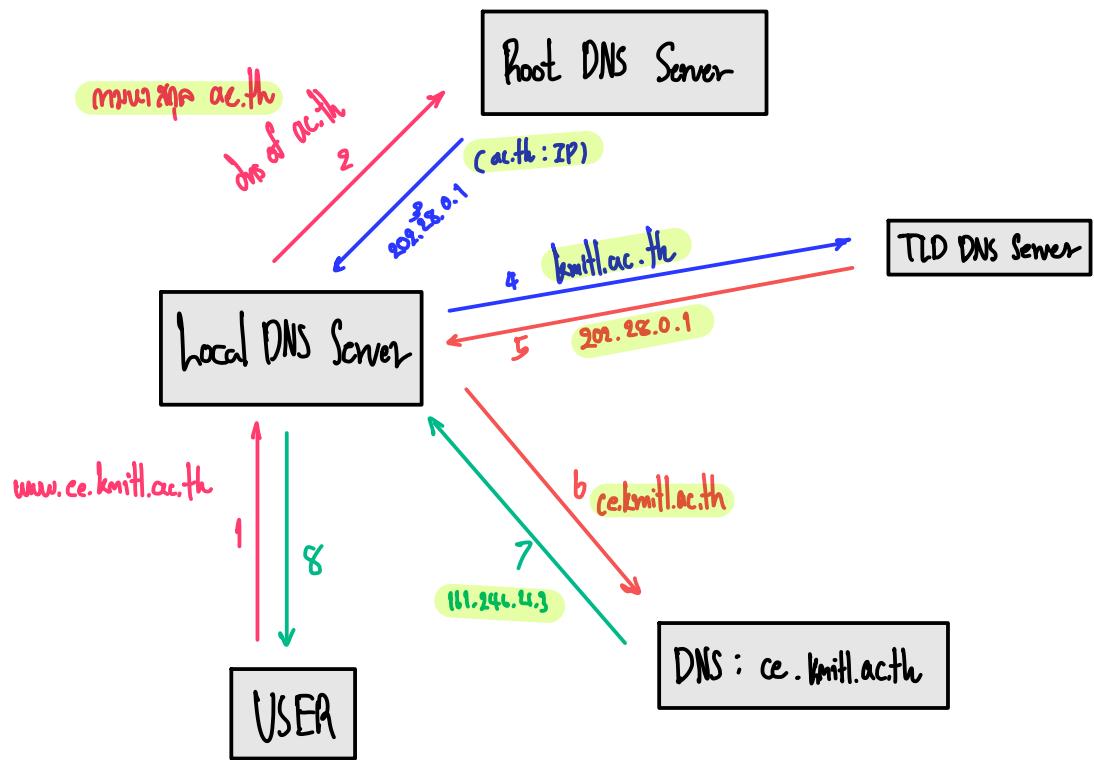
Name: ac.th

> 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 และดูว่ามี DNS Query/Response ใด ที่ใช้เวลาเกิน 1 วินาที ให้ capture ผลการค้นหากماแสดง
- packet ที่ 11 : 1.99292 sec.

| dns.flags.response == 1 |                |              |             |                                                                                                                                            |        |           |      |
|-------------------------|----------------|--------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------|-----------|------|
| No.                     | Time           | Source       | Destination | Protocol                                                                                                                                   | Length | 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 CNAME us.missingkids.com.edgesuite.net CNAME a1403.g.akamai.net A 205.161.7 |        |           |      |
| 107 2. 329101           | 216.148.227.68 | 24.6.126.218 | DNS         | 511 0.207250000 Standard query response 0x002a A www.missingkids.com CNAME us.missingkids.com.edgesuite.net CNAME a1403.g.akamai.net A 216 |        |           |      |
| 3 1. 107703             | 204.127.202.4  | 24.6.126.218 | DNS         | 499 0.107083000 Standard query response 0x0029 A www.ncmec.org CNAME us.missingkids.com.edgesuite.net CNAME a1403.g.akamai.net A 146.82.21 |        |           |      |

19. ให้รีเมค capture ใหม่เฉพาะข้อมูล DNS จากนั้นให้ใช้โปรแกรม nslookup และกำหนด server เป็น 161.246.4.3 งานนี้ให้ 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
- ce.kmitl.ac.th      diamond.ce.kmitl.ac.th      google public DNS*  
*161.246.52.21 < 161.246.4.3 < 8.8.8.8 : (8.8.8.8 : google dns (USA) delayed time ??)*

| ip.src == 161.246.4.3 |             |            |             |                                                                                                                                             |        |           |      |
|-----------------------|-------------|------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------|--------|-----------|------|
| No.                   | Time        | Source     | Destination | Protocol                                                                                                                                    | Length | DNS DELTA | Info |
| 4 6. 653651           | 161.246.4.3 | 10.66.4.20 | DNS         | 240 0.122008000 Standard query response 0x0008 A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th A 161.246.4.119 NS ns1.kmitl.ac.th NS    |        |           |      |
| 6 6. 676894           | 161.246.4.3 | 10.66.4.20 | DNS         | 151 0.023006000 Standard query response 0x0009 AAAA www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th SOA diamond.ce.kmitl.ac.th            |        |           |      |
| 12 16. 842328         | 161.246.4.3 | 10.66.4.20 | DNS         | 274 0.019441000 Standard query response 0x000a PTR 21.52.246.161.in-addr.arpa PTR ns1.kmitl.ac.th NS sun.net.kmitl.ac.th NS ns1.kmitl.ac.th |        |           |      |

| ip.src == 161.246.52.21 |               |            |             |                                                                                                                                              |        |           |      |
|-------------------------|---------------|------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------|--------|-----------|------|
| No.                     | Time          | Source     | Destination | Protocol                                                                                                                                     | Length | DNS DELTA | Info |
| 14 21. 982240           | 161.246.52.21 | 10.66.4.20 | DNS         | 224 0.005375000 Standard query response 0x000b A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th A 161.246.4.119 NS diamond.ce.kmitl.ac.th |        |           |      |
| 16 21. 925173           | 161.246.52.21 | 10.66.4.20 | DNS         | 151 0.022754000 Standard query response 0x000c AAAA www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th SOA diamond.ce.kmitl.ac.th             |        |           |      |
| 18 26. 863364           | 161.246.52.21 | 10.66.4.20 | DNS         | 460 0.024349000 Standard query response 0x000d PTR 8.8.8.in-addr.arpa PTR dns.google NS z.arin.net NS u.arin.net NS arin.net NS arin.a       |        |           |      |

| ip.src == 8.8.8.8 |         |            |             |                                                                                                                                  |        |           |      |
|-------------------|---------|------------|-------------|----------------------------------------------------------------------------------------------------------------------------------|--------|-----------|------|
| No.               | Time    | Source     | Destination | Protocol                                                                                                                         | Length | DNS DELTA | Info |
| 2 0.134223        | 8.8.8.8 | 10.66.4.20 | DNS         | 120 0.134223000 Standard query response 0x0007 PTR 3.4.246.161.in-addr.arpa PTR diamond.ce.kmitl.ac.th                           |        |           |      |
| 20 33. 153950     | 8.8.8.8 | 10.66.4.20 | DNS         | 118 0.086132000 Standard query response 0x000e A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th A 161.246.4.119               |        |           |      |
| 22 33. 334817     | 8.8.8.8 | 10.66.4.20 | DNS         | 151 0.177907000 Standard query response 0x000f AAAA www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th SOA diamond.ce.kmitl.ac.th |        |           |      |

## งานครั้งที่ 5

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

ผู้เรียน วิจิตร 63010871 SEC 03  
 ( เวลา LAB : 9. 13.00 - 16.00 )