

01076010 เครื่องข่ายคอมพิวเตอร์ : 2/2564

ภาควิชาศึกษาและนวัตกรรมคอมพิวเตอร์ คณะศึกษาและนวัตกรรมศาสตร์  
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 โดยให้ 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 ที่ตัดกับ โดยให้ capture ภาพของ packet list pane ที่แสดงคำสั่งมาแสดงด้วย
- packet ที่ 4,5,6 คือ คำสั่ง ftp test.rebex.net
- packet ที่ 8 คือ user = demo , packet ที่ 11 คือ รหัส password
- packet ที่ 14 คือ คำสั่ง dir

Capturing from Ethernet (host test.rebex.net)								
No.	Time	Source	Destination	Protocol	Length	Time since previous frame in this TCP stream	HTTP Delta	Info
4	0.000000	195.144.107.198	192.168.1.103	FTP	81	0.219947000		Response: 220 Microsoft FTP Service
5	0.003056	192.168.1.103	195.144.107.198	FTP	68	0.003085000		Request: OPTS UTF8 ON
6	0.219956	195.144.107.198	192.168.1.103	FTP	112	0.219955000		Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
8	2.509534	192.168.1.103	195.144.107.198	FTP	65	2.466002000		Request: USER demo
9	0.220504	195.144.107.198	192.168.1.103	FTP	87	0.220504000		Response: 331 Password required for demo.
11	3.225925	192.168.1.103	195.144.107.198	FTP	69	3.171813000		Request: PASS password
12	0.220711	195.144.107.198	192.168.1.103	FTP	75	0.220711000		Response: 230 User logged in.
14	2.426094	192.168.1.103	195.144.107.198	FTP	82	2.372330000		Request: PORT 192,168,1,103,204,206
17	0.226129	195.144.107.198	192.168.1.103	FTP	84	0.226129000		Response: 200 PORT command successful.
18	0.003261	192.168.1.103	195.144.107.198	FTP	60	0.003261000		Request: LIST
20	0.220164	195.144.107.198	192.168.1.103	FTP	108	0.220164000		Response: 125 Data connection already open; Transfer starting.
21	0.001255	195.144.107.198	192.168.1.103	FTP	78	0.001255000		Response: 226 Transfer complete.

```
> Frame 4: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_{7D7C3302-37B7-41BA-B015-0DEBF93EBFA5}, id 0
> Ethernet II, Src: zte_bb:32:74 (44:fb:5a:bb:32:74), Dst: HewlettP_92:eb:ce (c4:65:16:92:eb:ce)
> Internet Protocol Version 4, Src: 195.144.107.198, Dst: 192.168.1.103
> Transmission Control Protocol, Src Port: 21, Dst Port: 52429, Seq: 1, Ack: 1, Len: 27
> File Transfer Protocol (FTP)
[Current working directory: ]
```

```
Command Prompt - ftp test.rebex.net
Microsoft Windows [Version 10.0.19044.1503]
(c) Microsoft Corporation. All rights reserved.

C:\Users\phanc>ftp test.rebex.net
Connected to test.rebex.net.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (test.rebex.net:(none)): demo
331 Password required for demo.
Password:
230 User logged in.
Ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
10-19-20 03:19PM <DIR> pub
12-17-21 11:58AM 405 readme.txt
226 Transfer complete.
Ftp> 98 bytes received in 0.00Seconds 49.00Kbytes/sec.
Ftp>
```

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

packet ที่ 35

Source port ที่ 20

Destination port ที่ 55350

① ผู้คนค้น, get readme.txt

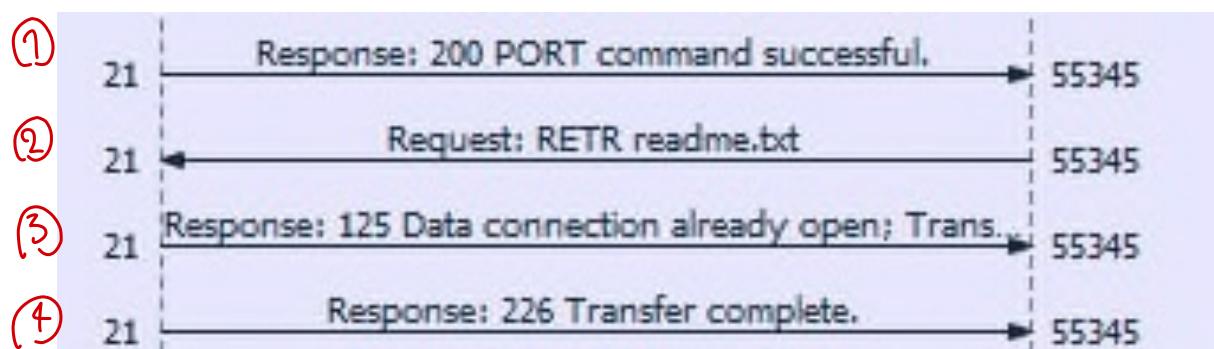
② รับ request จาก 192.168.1.103 ไป 195.144.107.198

③ ตอบกลับ รับทราบเรียบร้อยแล้ว ไป Transfer

④ ตอบกลับ Transfer สำเร็จ

195.144.107.198

192.168.1.103



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

dir (list)

ben get readme.txt

No.	Time	Source	Destination	Protocol	Length	Time since previous frame in this TCP stream	Info
23	0.000000	195.144.107.198	192.168.1.103	FTP-DATA	149	0.005847000	FTP Data: 95 bytes (PORT) (LIST)
35	103.854246	195.144.107.198	192.168.1.103	FTP-DATA	459	0.006988000	FTP Data: 405 bytes (PORT) (PORT 192.168.1.103,216,54)

```

> Frame 35: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface \Device\NPF_{7D7C3302-3787-41BA-B015-0DEBF93EBFA5}, id 0
> Ethernet II, Src: zte_bb:32:74 (44:fb:5a:bb:32:74), Dst: HewlettP_92:eb:ce (c4:65:16:92:eb:ce)
> Internet Protocol Version 4, Src: 195.144.107.198, Dst: 192.168.1.103
> Transmission Control Protocol, Src Port: 20, Dst Port: 55350, Seq: 1, Ack: 1, Len: 405
    Source Port: 20
    Destination Port: 55350
    [Stream index: 2]
    [Conversation completeness: Incomplete (30)]
    [TCP Segment Len: 405]
    Sequence Number: 1 (relative sequence number)
    Sequence Number (raw): 648817221
    [Next Sequence Number: 406 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment number (raw): 1202054145
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x0108 (PSH, ACK)
    Window: 260
    [Calculated window size: 66560]
    [Window size scaling factor: 256]
    CharCount: 0x0000000000000000
  
```

readme.txt - Notepad

File Edit Format View Help

Welcome,

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!

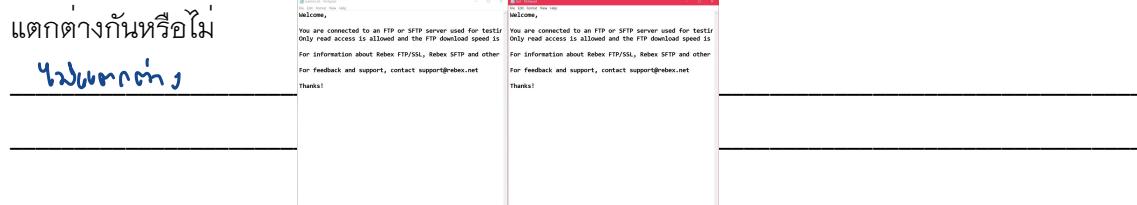
readme.txt

Command Prompt - ftp test.rebex.net

Microsoft Windows [Version 10.0.19044.1503]  
(c) Microsoft Corporation. All rights reserved.

```
C:\Users\phanc>ftp test.rebex.net
Connected to test.rebex.net.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (test.rebex.net:(none)): demo
331 Password required for demo.
Password:
230 User logged in.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
10-19-20 03:19PM <DIR> pub
12-17-21 11:58AM 405 readme.txt
226 Transfer complete.
ftp: 98 bytes received in 0.00Seconds 32.67Kbytes/sec.
ftp> get readme.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp: 405 bytes received in 0.25Seconds 1.61Kbytes/sec.
ftp>
```

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



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 ⇒ username login ถือ anonymous

PASS ⇒ password ถือ anypwd

PORT ⇒ กระบวนการเรื่องต่อไปนี้จะเป็นส่วนหนึ่งของ PORT 20

NLST ⇒ คำสั่ง List Directory คือลิสต์

TYPE ⇒ ชนิดไฟล์ที่ต้องการ (I = Image)

RETR ⇒ request ข้อมูลจาก FTP Server (pantheon.jpg)

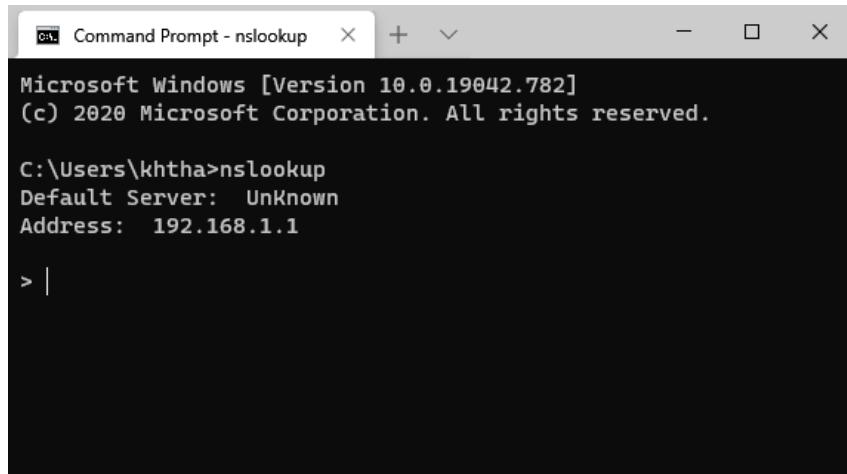
QUIT ⇒ ออกจาก FTP Server

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  
รูปภาพ Pantheon
10. ให้อธิบายว่าการทำงานในข้อ 8 ทำเพื่ออะไร  
กรอง Packet TCP Stream กรณี !(tcp.stream eq 0) and !(tcp.stream eq 1)  
คุณกำลังกรอง แล้ว TCP Stream ที่หายไป
11. ให้เปิดไฟล์ ftp-download-good2.pcapng ให้หาคำตอบว่าเราที่ใช้ในการโหลดไฟล์ “SIZE OS Fingerprinting with ICMP.zip” เท่ากับเท่าไร อธิบายวิธีการ  
ถ้า Display Filter พิมพ์ ftp.data.command == "SIZE OS Fingerprinting with ICMP.zip"  
เลือกที่ packet 16 ทำ msr Mark (Ctrl+T) ทันที \*REF\*  
สักครู่ packet จะต่อเวลา 0.000477 วินาที



## DNS (Domain Name System)

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

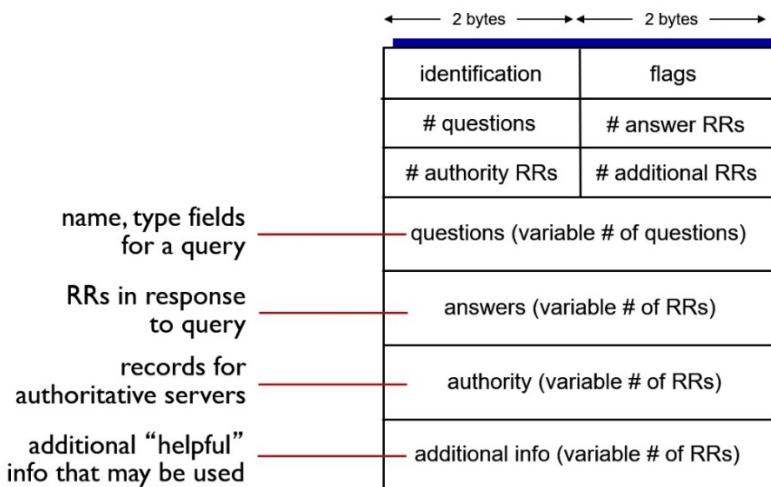


```
Microsoft Windows [Version 10.0.19042.782]
(c) 2020 Microsoft Corporation. All rights reserved.

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 (ເປັນການກຳນົດໃຫ້ເຂື້ອມຕ້ອກນ DNS Server ທີ່ມີ IP Address 161.246.52.21 ແລ້ວ Default Server) ໃຫ້ອີບວ່າ 161.246.52.21 ມີສື່ອ Domain Name ອະໄຮ ns1.kmitl.ac.th



13. ໃຫ້ພິມພໍ www.ce.kmitl.ac.th ແລະໜູ້ດ Capture ໃຫ້ອີບຄໍາຖາມຕັ້ງນີ້
- ໃນ DNS Query ມີ # questions ເທົ່າໄວ ແລະຂໍ້ອມນູລໃນ questions ດີອະໄວ type ເປັນຄ່າອະໄວ ໃຫ້ Capture ສ່ວນຂອງ Packet Details Pane ປະກອບດວຍ

1 questions ນັ້ນຈະ www.ce.kmitl.ac.th : type A, class IN

45214 0.000214	192.168.1.103	213.179.201.60	UDP	1073	64584 → 50015 Len=1031
45215 0.000031	192.168.1.103	213.179.201.60	UDP	1101	64584 → 50015 Len=1059
45216 0.005828	192.168.1.103	161.246.52.21	DNS	78	Standard query 0x0003 A www.ce.kmitl.ac.th
45217 0.000142	192.168.1.103	213.179.201.60	UDP	1102	64584 → 50015 Len=1060
45218 0.019809	213.179.200.209	192.168.1.103	UDP	85	50003 → 62862 Len=43
45219 0.000682	161.246.52.21	192.168.1.103	DNS	224	Standard query response 0x0003 A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th A 161.2
45220 0.000304	192.168.1.103	161.246.52.21	DNS	78	Standard query 0x0004 AAAA www.ce.kmitl.ac.th
45221 0.003156	192.168.1.103	213.179.201.60	UDP	1075	64584 → 50015 Len=1033
45222 0.000014	192.168.1.103	213.179.201.60	UDP	1076	64584 → 50015 Len=1034
45223 0.014834	213.179.200.209	192.168.1.103	UDP	85	50003 → 62862 Len=43
45224 0.001470	161.246.52.21	192.168.1.103	DNS	151	Standard query response 0x0004 AAAA www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th SOA
45225 0.013639	213.179.201.60	192.168.1.103	UDP	94	50015 → 64584 Len=52
45226 0.000725	213.179.200.209	192.168.1.103	UDP	85	50003 → 62862 Len=43

Source Port: 50322  
 Destination Port: 53  
 Length: 44  
 Checksum: 0xb29a [unverified]  
 [Checksum Status: Unverified]  
 [Stream index: 9]  
 > [Timestamps]  
 UDP payload (36 bytes)  
 ✓ Domain Name System (query)  
 Transaction ID: 0x0003  
 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: 45219]

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

#### Details Pane ประกอบด้วย

2 Answer ตอบ 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

No.	Time	Source	Destination	Protocol	Length	Time since previous frame in this TCP stream	Info
45214 0.000214	192.168.1.103	213.179.201.60	UDP	1073	64584 → 50015 Len=1031		
45215 0.000031	192.168.1.103	213.179.201.60	UDP	1101	64584 → 50015 Len=1059		
45216 0.005828	192.168.1.103	161.246.52.21	DNS	78	Standard query 0x0003 A www.ce.kmitl.ac.th		
45217 0.000142	192.168.1.103	213.179.201.60	UDP	1102	64584 → 50015 Len=1060		
45218 0.019809	213.179.200.209	192.168.1.103	UDP	85	50003 → 62862 Len=43		
45219 0.000682	161.246.52.21	192.168.1.103	DNS	224	Standard query response 0x0003 A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th A 161.2		
45220 0.000304	192.168.1.103	161.246.52.21	DNS	78	Standard query 0x0004 AAAA www.ce.kmitl.ac.th		
45221 0.003156	192.168.1.103	213.179.201.60	UDP	1075	64584 → 50015 Len=1033		
45222 0.000014	192.168.1.103	213.179.201.60	UDP	1076	64584 → 50015 Len=1034		
45223 0.014834	213.179.200.209	192.168.1.103	UDP	85	50003 → 62862 Len=43		
45224 0.001470	161.246.52.21	192.168.1.103	DNS	151	Standard query response 0x0004 AAAA www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th SOA		
45225 0.013639	213.179.201.60	192.168.1.103	UDP	94	50015 → 64584 Len=52		
45226 0.000725	213.179.200.209	192.168.1.103	UDP	85	50003 → 62862 Len=43		

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

#### 4 packet

10350 0.000000	192.168.1.103	161.246.52.21	DNS	78	Standard query 0x0003 A www.ce.kmitl.ac.th
10351 0.008377	161.246.52.21	192.168.1.103	DNS	224	Standard query response 0x0003 A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th A 161.246.4.1
10352 0.000597	192.168.1.103	161.246.52.21	DNS	78	Standard query 0x0004 AAAA www.ce.kmitl.ac.th
10353 0.006156	161.246.52.21	192.168.1.103	DNS	151	Standard query response 0x0004 AAAA www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th SOA diamon

[Stream index: 25]	> [Timestamps]
UDP payload (182 bytes)	
✓ Domain Name System (response)	
Transaction ID: 0x0003	
> Flags: 0x8500 Standard query response, No error	
Questions: 1	
Answer RRs: 2	
Authority RRs: 3	
Additional RRs: 2	
✓ Queries	
> www.ce.kmitl.ac.th: type A, class IN	
Name: www.ce.kmitl.ac.th	
[Name Length: 18]	
[Label Count: 5]	
Type: A (Host Address) (1)	
Class: IN (0x0001)	
Answers	
> www.ce.kmitl.ac.th: type CNAME, class IN, cname jeweler19.ce.kmitl.ac.th	
> jeweler19.ce.kmitl.ac.th: type A, class IN, addr 161.246.4.119	
Authoritative nameservers	
> ce.kmitl.ac.th: type NS, class IN, ns clarinet.asianet.co.th	
> ce.kmitl.ac.th: type NS, class IN, ns diamond.ce.kmitl.ac.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: 10350]	
[Time: 0.020633000 seconds]	

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร  
ที่เป็น Server ทั้งหมดแล้ว IP ของ Server ตามลับตืบ
- 

▼ 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 ns1.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 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: 10350]  
[Time: 0.008377000 seconds]

14. ทำการข้อ 13 อีกครั้ง แต่ใช้ 161.246.4.119 แทนที่จะใช้ [www.ce.kmitl.ac.th](http://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 119.4.246.161.in-addr.arpa: type PTR, class IN

---

No.	Time	Source	Destination	Protocol	Length	Time since previous frame in this TCP stream	Info
39386	0.000000	192.168.1.103	161.246.52.21	DNS	86		Standard query 0x0003 PTR 119.4.246.161.in-addr.arpa
39388	0.007170	161.246.52.21	192.168.1.103	DNS	196		Standard query response 0x0003 PTR 119.4.246.161.in-addr.arpa PTR jeweler19.ce.kmitl.ac.th NS ns1.kmitl.ac.th

Details pane:

```

...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0xf98e [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.103
Destination Address: 161.246.52.21
User Datagram Protocol, Src Port: 54845, Dst Port: 53
Source Port: 54845
Destination Port: 53
Length: 52
Checksum: 0xd63f [unverified]
[Checksum Status: Unverified]
[Stream index: 9]
> [Timestamps]
  UDP payload (44 bytes)
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: 39388]

```

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

1 answer 119.4.246.161.in-addr.arpa: type PTR, class IN, jeweler19.ce.kmitl.ac.th

---

No.	Time	Source	Destination	Protocol	Length	Time since previous frame in this TCP stream	Info	Find	Cancel
39386	0.000000	192.168.1.103	161.246.52.21	DNS	86		Standard query 0x0003 PTR 119.4.246.161.in-addr.arpa		
39388	0.007170	161.246.52.21	192.168.1.103	DNS	196		Standard query response 0x0003 PTR 119.4.246.161.in-addr.arpa PTR jeweler19.ce.kmitl.ac.th NS ns		

< >

```

Destination Port: 54845
Length: 162
Checksum: 0xaae2 [unverified]
[Checksum Status: Unverified]
[Stream index: 9]
> [Timestamps]
UDP payload (154 bytes)
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
  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: 39386]
[Time: 0.007170000 seconds]

```

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

2 packet

---



---

No.	Time	Source	Destination	Protocol	Length	Time since previous frame in this TCP stream	Info	Find	Cancel
39386	0.000000	192.168.1.103	161.246.52.21	DNS	86		Standard query 0x0003 PTR 119.4.246.161.in-addr.arpa		
39388	0.007170	161.246.52.21	192.168.1.103	DNS	196		Standard query response 0x0003 PTR 119.4.246.161.in-addr.arpa PTR jeweler19.ce.kmitl.ac.th NS ns		

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

ผู้รับ Server ทั้งหมด และ IP ของ Server ทางลับ

---



---

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
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: 39386]
[Time: 0.007170000 seconds]

15. ໃຫ້ໃຊ້ໂປຣແກຣມ nslookup ແລ້ວຕັ້ງ server ເປັນ 199.7.91.13 ຈາກນັ້ນໃຫ້ ປ້ອນ 199.7.91.13 ໂປຣແກຣມ  
ແສດງຜລອະໄຮມາບ່າງ ໃຫ້ capture ມາແສດງ ນັກຕື່ກົມາຄີດວ່າ 199.7.91.13 ເປັນ server ອະໄຮ  
**d.root-servers.net**

```
0. Command Prompt - nslookup
Address: 115.178.58.26
> 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. ໃຫ້ປອນ query www.ce.kmitl.ac.th ແສດງຜລອະໄຮມາບ່າງ ໃຫ້ capture ມາແສດງ ຈາກນັ້ນໃຫ້ໃຊ້ IP Address  
ຂອງ ns.thnic.net ເປັນ server ຈາກນັ້ນໃຫ້ປ້ອນ ac.th, kmitl.ac.th ແລະ ce.kmitl.ac.th ຕາມລຳດັບ ໃຫ້  
capture ມາແສດງ ແລະ ໄທນັກຕື່ກົມາຈາດຮູ່ປັບປຸງການທຳ name resolution ຂອງ www.ce.kmitl.ac.th ໂດຍສມມຕີ  
ໃຫ້ເຄົ່າງໂທ request ເປັນເຄົ່າງໂທທີ່ຢູ່ຕາງປະເທດ

```
> 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

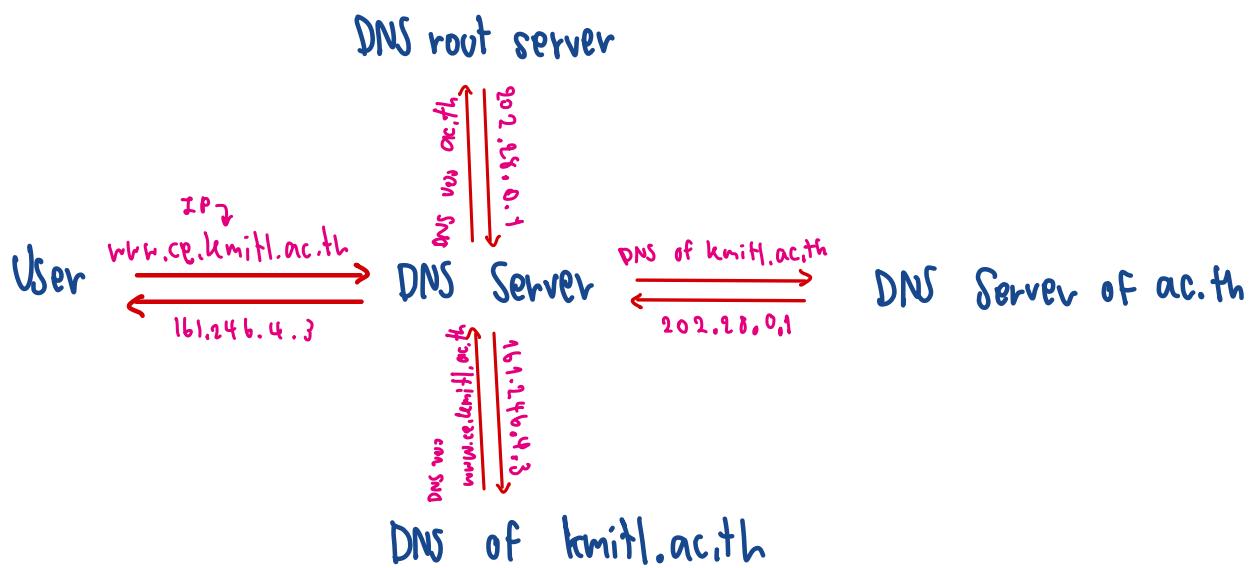
Name: ac.th

> 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:
- diamond.ce.kmitl.ac.th
  161.246.4.3
  ce.kmitl.ac.th
- ns1.kmitl.ac.th
  161.246.52.21
  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 ผลการค้นหาการแสดง packet ที่ 11 ณ เวลา 1.292192000

No.	Time	Source	Destination	Protocol	Length	Time since previous frame in the TCP stream	DNS Delta	Info
7	0.881762	24.0.126.218	146.82.218.136	HTTP	459	0.001045000	GET / HTTP/1.1	88 = 88 [ACK] Seq=1 Ack=88 Win=6432 Len=0
8	0.883053	146.82.218.136	24.0.126.218	TCP	60	0.000310000	*	HTTP/1.1 200 OK (text/html)
9	0.885577	146.82.218.136	24.0.126.218	HTTP	5154	0.003577000	*	HTTP/1.1 200 OK (text/html)
10	0.886139	24.0.126.218	146.82.218.136	TCP	54	0.000053000	3618 + 88 [ACK] Seq=406 Ack=4512 Win=8 Len=0	Standard query response 0x0029 A www.nicenc.org CNAME www.missingkids.com
11	0.886056	216.148.227.68	24.0.126.218	DNS	495	0.000000000	*	Additional records
12	0.886139	216.148.227.68	24.0.126.218	DNS	495	0.000000000	*	Additional records
13	0.886475	146.82.218.136	24.0.126.218	HTTP	2534	0.001550000	Continuation	3618 + 88 [ACK] Seq=406 Ack=4512 Win=4512 Len=0
14	0.890141	24.0.126.218	146.82.218.136	TCP	54	0.000041000	3618 + 88 [ACK] Seq=406 Ack=4512 Win=4512 Len=0	r1g.akamai.net: type A, class IN, addr 216.148.237.141
15	0.891895	146.82.218.136	24.0.126.218	HTTP	1514	0.001049000	Continuation	r1g.akamai.net: type A, class IN, addr 64.239.10.10
16	0.892192	24.0.126.218	146.82.218.136	TCP	54	0.000000000	*	r1g.akamai.net: type A, class IN, addr 216.148.237.23
17	0.892192	146.82.218.136	24.0.126.218	HTTP	1514	0.001049000	*	r1g.akamai.net: type A, class IN, addr 216.148.237.24
18	0.892192	24.0.126.218	146.82.218.136	TCP	54	0.000000000	*	r1g.akamai.net: type A, class IN, addr 216.148.237.25
19	0.892192	146.82.218.136	24.0.126.218	HTTP	1514	0.001049000	*	r1g.akamai.net: type A, class IN, addr 216.148.237.31
20	0.892192	24.0.126.218	146.82.218.136	TCP	54	0.000000000	*	r1g.akamai.net: type A, class IN, addr 63.215.198.5

[Request 10/11]

[Time: 1.292192000 seconds]

19. ให้รีเมิร์ค 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 ให้เบรี่ยงเที่ยบ DNS Delta ที่ได้จากแต่ละ Server (แสดงตัวเลขที่โดด) จากนั้นให้ไวเคราะห์ผล

Column DNS Delta ของ 8.8.8.8 เมนูต่างๆ กัน 2 DNS ที่จ่อ 2 DNS อย่างไร  
Public DNS จะอยู่ 8.8.8.8

(((dns)&&((ip.src == 8.8.8.8))  (ip.src == 161.246.52.21))  (ip.src == 161.246.4.3))&&(dns.resp.type==5)&&(dns.resp.type==1)								
No.	Time	Source	Destination	Protocol	Length	DNS Delta	Info	
44857	0.000000	161.246.4.3	192.168.1.103	DNS	224	0.008554000	Standard query response 0x0003 A www.ce.kmitl.ac.th CNAMES jeweler19.ce.kmitl.ac.th A 161.246.4.119 NS diamond.ce.kmitl.ac.th	
67079	15.919666	161.246.52.21	192.168.1.103	DNS	224	0.018829000	Standard query response 0x0006 A www.ce.kmitl.ac.th CNAMES jeweler19.ce.kmitl.ac.th A 161.246.4.119 NS ns1.kmitl.ac.th	
88565	16.101175	8.8.8.8	192.168.1.103	DNS	118	0.069551000	Standard query response 0x0009 A www.ce.kmitl.ac.th CNAMES jeweler19.ce.kmitl.ac.th A 161.246.4.119	

## งานครั้งที่ 5

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