

นายภากรณ์ ธนประชาพันธ์ 62010694

3. ใช้คำสั่ง `dir` ในโปรแกรม `ftp` และ capture ภาพการทำงานของคำสั่ง `dir` จากนั้นกลับมาที่ Wireshark แล้วใช้ display filter เป็น `ftp` ให้เปรียบเทียบระหว่างคำสั่งของ `ftp` ที่ใช้กับ packet ของ Wireshark ที่ดักจับได้ ให้ capture ภาพของ packet list pane ที่แสดงคำสั่งมาแสดงด้วย

The screenshot displays two windows side-by-side. The left window is a Command Prompt titled "Command Prompt - ftp test.rebex.net" showing the output of an FTP session. The right window is Wireshark titled "Wi-Fi (host test.rebex.net)" showing a packet capture of the same session.

Command Prompt Output:

```
c:\Users\Tree>ftp test.rebex.net
Microsoft Windows [Version 10.0.18363.1316]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Tree>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 03:10PM      <DIR>          pub
04-08-14 03:09PM      403 readme.txt
226 Transfer complete.
ftp>
ftp> 98 bytes received in 0.01Seconds 19.60Kbytes/sec.
ftp>
```

Wireshark Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
4	0.482434	195.144.107.198	192.168.1.3	FTP	81	Response: 220 Microsoft FTP Service
5	0.486371	192.168.1.3	195.144.107.198	FTP	68	Request: OPTS UTF8 ON
6	0.721747	195.144.107.198	192.168.1.3	FTP	112	Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
8	5.900516	192.168.1.3	195.144.107.198	FTP	65	Request: USER demo
9	6.132293	195.144.107.198	192.168.1.3	FTP	87	Response: 331 Password required for demo.
11	10.343727	192.168.1.3	195.144.107.198	FTP	69	Request: PASS password
12	10.585376	195.144.107.198	192.168.1.3	FTP	75	Response: 230 User logged in.
14	21.205884	192.168.1.3	195.144.107.198	FTP	79	Request: PORT 192,168,1,3,198,56
15	21.435068	195.144.107.198	192.168.1.3	FTP	84	Response: 200 PORT command successful.
18	21.439189	192.168.1.3	195.144.107.198	FTP	60	Request: LIST
20	21.672273	195.144.107.198	192.168.1.3	FTP	108	Response: 125 Data connection already open; Transfer starting.
21	21.672273	195.144.107.198	192.168.1.3	FTP	78	Response: 226 Transfer complete.

Wireshark Packet Details (Frame 4):

- > Frame 4: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_{82238ED6-8438-475C-8B40-A5A21C8D6827}, id 0
- > Ethernet II, Src: HuaweiTe_8e:0a:29 (c8:0c:c8:8e:0a:29), Dst: Microsof_60:ee:63 (28:16:a8:60:ee:63)
- > Internet Protocol Version 4, Src: 195.144.107.198, Dst: 192.168.1.3
- > Transmission Control Protocol, Src Port: 21, Dst Port: 50727, Seq: 1, Ack: 1, Len: 27
- > File Transfer Protocol (FTP)
- [Current working directory:]

Wireshark Packet Bytes:

```
0000  28 16 a8 60 ee 63 c8 0c c8 8e 0a 29 08 00 45 00  (...).c...).E-
0010  00 43 6f 6f 40 00 6a 06 b0 43 c3 90 6b c6 c0 a8  -Coo@j-.C-.k...
0020  01 03 00 15 c6 27 38 21 51 72 37 fe 6c a7 50 18  -....8!Qn7.l.P.
0030  fd b8 31 97 00 00 32 32 30 20 4d 69 63 72 6f 73  -1...22 0 Micros
0040  6f 66 74 20 46 54 50 20 53 65 72 76 69 63 65 0d  -ft FTP Service-
0050  0a
```

4. ให้นำ packet ที่ได้ดักจับไว้ ที่มีชื่อไฟล์ readme.txt (ซึ่งเป็นข้อมูลที่ ftp server ส่งมา) ว่าส่งมาทาง port ใด และอยู่ใน packet ใด จากนั้นให้วาดภาพแสดงการทำงานของ ftp สำหรับคำสั่ง dir ข้างต้น ว่ามีการส่งข้อมูลอย่างไร

*Wi-Fi (host test.rebex.net)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
35	29.589318	195.144.107.198	192.168.1.3	TCP	54	20 → 58877 [ACK] Seq=1 Ack=1 Win=64952 Len=0
36	29.589318	195.144.107.198	192.168.1.3	FTP-DATA	457	FTP Data: 403 bytes (PORT) (RETR readme.txt)
37	29.630455	192.168.1.3	195.144.107.198	TCP	54	58877 → 20 [ACK] Seq=1 Ack=404 Win=64952 Len=0

> Internet Protocol Version 4, Src: 195.144.107.198, Dst: 192.168.1.3

▼ Transmission Control Protocol, Src Port: 20, Dst Port: 58877, Seq: 1, Ack: 1, Len: 403

Source Port: 20

Destination Port: 58877

[Stream index: 2]

[TCP Segment Len: 403]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 3475457636

[Next Sequence Number: 404 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 3661702443

0101 = Header Length: 20 bytes (5)

▼ Flags: 0x018 (PSH, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

....1... = Push: Set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

[TCP Flags:AP...]

Window: 64952

[Calculated window size: 64952]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0xa4e0 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

▼ [SEQ/ACK analysis]

[iRTT: 0.241952000 seconds]

[Bytes in flight: 403]

[Bytes sent since last PSH flag: 403]

▼ [Timestamps]

[Time since first frame in this TCP stream: 0.241952000 seconds]

[Time since previous frame in this TCP stream: 0.000000000 seconds]

TCP payload (403 bytes)

FTP Data (403 bytes data)

[Setup frame: 28]

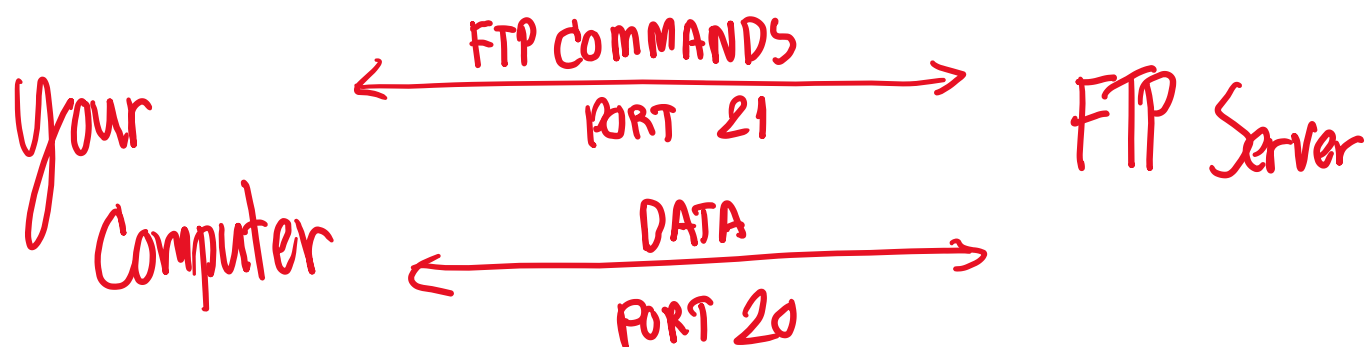
[Setup method: PORT]

[Command: RETR readme.txt]

Command frame: 30

```
0020 01 03 00 14 e5 fd c5 27 46 64 da 41 25 2b 50 18 .....Fd.A%+P.
0030 fd b8 a4 e0 00 00 57 65 6c 63 6f 6d 65 2c 0d 0a .....We lcome,.
0040 0d 0a 79 6f 75 20 61 72 65 20 63 6f 6e 6e 65 63 ..you ar e connec
0050 74 65 64 20 74 6f 20 61 6e 20 46 54 50 20 6f 72 ted to a n FTP or
```

มี Source Port เป็น 20 Destination Port เป็น 58877 อยู่ใน Packet ที่ 36 ซึ่งเป็น
การ RETR readme.txt จาก 195.144.107.198 มาที่ 192.168.1.3 โดย Protocol FTP-DATA



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

The image shows a network capture in Wireshark and the corresponding file content in Notepad. The Wireshark packet list shows a packet of 149 bytes (FTP-DATA) from 192.168.1.3 to 192.168.1.3. The packet details pane shows the FTP structure, including the command 'RETR readme.txt' and the file data. The Notepad window displays the text content of the file, which is a welcome message for the Rebox FTP/SSL server.

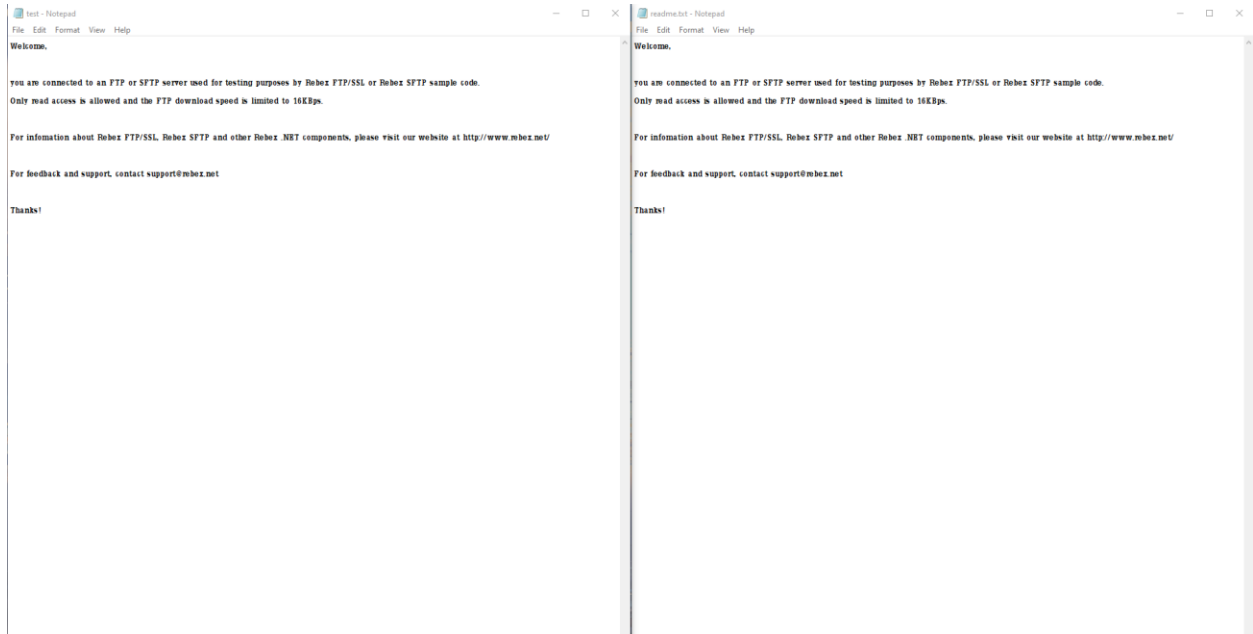
Wireshark Packet Details:

- No. 21: 15.256700 192.168.1.3 → 192.168.1.3 TCP 54 58871 → 58871 [ACK] Seq=1 Ack=1 Win=0
- No. 22: 15.256708 192.168.1.3 → 192.168.1.3 TCP 54 58871 → 58871 [FIN, ACK] Seq=96 Ack=1
- No. 23: 15.278479 192.168.1.3 → 192.168.1.3 FTP 149 FTP Data: 95 bytes (PORT) (LIST)
- No. 24: 15.280479 192.168.1.3 → 192.168.1.3 FTP 108 Response: 125 Data connection already open; may transfer files

Notepad Content:

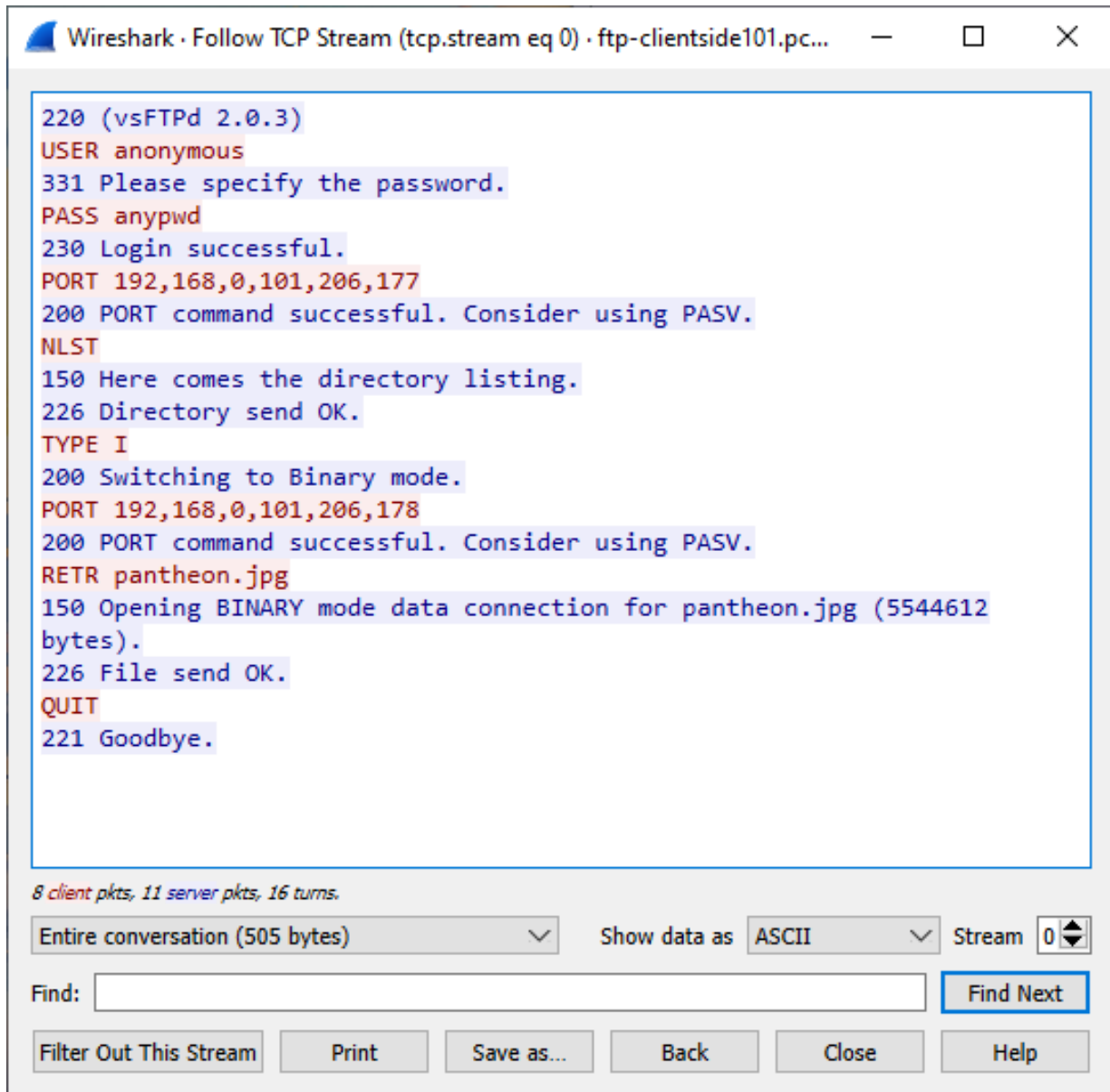
```
Welcome,\n\nYou are connected to an FTP or SFTP server used for testing purposes by Rebox FTP/SSL or Rebox SFTP sample code.\nOnly read access is allowed and the FTP download speed is limited to 16KBps.\n\nFor information about Rebox FTP/SSL, Rebox SFTP and other Rebox .NET components, please visit our website at http://www.rebox.net\n\nFor feedback and support, contact support@rebox.net\n\nThanks!\n
```

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



เหมือนกัน

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



-USER ทำการส่ง User Identification ไปให้ Server (ชื่อผู้ใช้ anonymous)

-PASS ทำการส่ง User Password ไปให้ Server (รหัส anypwd)

-PORT สร้างการเชื่อมต่อกับผู้ใช้งานเพื่อส่งไฟล์ผ่าน Port 20

-NLST ส่ง List Directory ให้กับผู้ใช้

-TYPE บอกชนิดบอกไฟล์ที่ต้องการ

-RETR ทำการร้องขอไฟล์จาก FTP Server (pantheon.jpg)

-QUIT ออกจากการใช้งาน FTP พร้อมปิดการเชื่อมต่อ

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



10. ให้อธิบายว่าการทำงานในข้อ 8 ทำเพื่ออะไร

เพื่อกรอง Packet TCP Stream ที่ไม่ต้องการเห็นออกด้วยเงื่อนไข `!(tcp.stream eq 0)` and `!(tcp.stream eq 1)` หลังจากนั้นจะได้ TCP Stream ที่เราทำการ Follow เอาไว้

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

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	Protocol	Length	Info
16	*REF*	128.121.136.217	67.180.72.76	FTP-DATA	1078	FTP Data: 1024 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
17	0.001203	128.121.136.217	67.180.72.76	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
19	0.014867	128.121.136.217	67.180.72.76	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
20	0.016068	128.121.136.217	67.180.72.76	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
22	0.017303	128.121.136.217	67.180.72.76	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
691	1.308490	128.121.136.217	67.180.72.76	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
693	1.309722	128.121.136.217	67.180.72.76	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
695	1.313384	128.121.136.217	67.180.72.76	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
696	1.318251	128.121.136.217	67.180.72.76	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
698	1.319480	128.121.136.217	67.180.72.76	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
700	1.322874	128.121.136.217	67.180.72.76	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
701	1.327756	128.121.136.217	67.180.72.76	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)
703	1.328233	128.121.136.217	67.180.72.76	FTP-DATA	288	FTP Data: 234 bytes (PASV) (SIZE OS Fingerprinting with ICMP.zip)

Display Filter ใช้ “ftp-data.command == "SIZE OS Fingerprinting with ICMP.zip"”

Ctrl-T ที่ Packet แรกที่เริ่มโหลดMark เป็น Ref เวลา

หา Packet สุดท้ายที่โหลด และอ่านค่าเวลา ซึ่งอ่านได้ 1.328233 วินาที

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

```
C:\Users\Tree>nslookup
Default Server:  UnKnown
Address:  192.168.1.1

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

ns1.kmitl.ac.th

```
<
.... .... 0 .... = Non-authenticated data: Unacceptable
.... .... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
v Queries
  v 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)
v Answers
  v www.ce.kmitl.ac.th: type CNAME, class IN, cname jeweler19.ce.kmitl.ac.th
    Name: www.ce.kmitl.ac.th
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 2452 (40 minutes, 52 seconds)
    Data length: 26
    CNAME: jeweler19.ce.kmitl.ac.th
  v jeweler19.ce.kmitl.ac.th: type A, class IN, addr 161.246.4.119
    Name: jeweler19.ce.kmitl.ac.th
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 3187 (53 minutes, 7 seconds)
    Data length: 4
    Address: 161.246.4.119
```

13. ให้พิมพ์ `www.ce.kmitl.ac.th` และหยุด Capture ให้ตอบคำถามดังนี้
- ใน DNS Query มี # questions เท่าไร และข้อมูลใน questions คืออะไร type เป็นค่าอะไร ให้ Capture ส่วนของ Packet Details Pane ประกอบด้วย

1 Question ซึ่งมีข้อมูลเป็น `www.ce.kmitl.ac.th`, type A Class IN เป็น Type A

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

- มี query และ response ที่ packet ให้ Capture ส่วนของ Packet Details Pane ด้วย
- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

มี 2 Answer เป็น www.ce.kmitl.ac.th : type CNAME , class IN , cname
 jeweler19.ce.kmitl.ac.th และ jeweler19.ce.kmitl.ac.th : type A , class IN , addr
 161.246.4.119

No.	Time	Source	Destination	Protocol	Length	Questions	Answer RRs	Authority RRs	Additional RRs	Info
1	0.000000	192.168.1.3	192.168.1.1	DNS	83	1	0	0	0	@ Standard query 0x000d A www.ce.kmitl.ac.th.home
2	0.009981	192.168.1.1	192.168.1.3	DNS	158	1	0	1	0	@ Standard query response 0x000d No such name A www.ce.kmitl.ac.th.home SOA a.root-servers.net
3	0.040219	192.168.1.3	192.168.1.1	DNS	83	1	0	0	0	@ Standard query 0x000e AAAA www.ce.kmitl.ac.th.home
4	0.081222	192.168.1.1	192.168.1.3	DNS	158	1	0	1	0	@ Standard query response 0x000e No such name AAAA www.ce.kmitl.ac.th.home SOA a.root-servers.net
5	0.081449	192.168.1.3	192.168.1.1	DNS	78	1	0	0	0	@ Standard query 0x000f A www.ce.kmitl.ac.th
6	0.087182	192.168.1.1	192.168.1.3	DNS	132	1	2	0	0	@ Standard query response 0x000f A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th A 161.246.4.119
7	0.087813	192.168.1.3	192.168.1.1	DNS	78	1	0	0	0	@ Standard query 0x0010 AAAA www.ce.kmitl.ac.th
8	0.109340	192.168.1.1	192.168.1.3	DNS	151	1	1	1	1	@ Standard query response 0x0010 AAAA www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th SOA diamond.ce.kmitl.ac.th

มี 8 packet

```

▼ Authoritative nameservers
> ce.kmitl.ac.th: type NS, class IN, ns diamond.ce.kmitl.ac.th
> ce.kmitl.ac.th: type NS, class IN, ns clarinet.asianet.co.th
> ce.kmitl.ac.th: type NS, class IN, ns ns1.kmitl.ac.th
▼ Additional records
> ns1.kmitl.ac.th: type A, class IN, addr 161.246.52.21
> diamond.ce.kmitl.ac.th: type A, class IN, addr 161.246.4.3

```

มี เป็นข้อมูลตามในภาพซึ่งเป็น ชื่อของ server ทั้งหมด และ ip ทั้งหมดของ server ตามลำดับ

14. ทำตามข้อ 2 อีกครั้ง แต่ใช้ 161.246.4.119 แทนที่จะใช้ www.ce.kmitl.ac.th

No.	Time	Source	Destination	Protocol	Length	Questions	Answer RRs	Authority RRs	Additional RRs	Info
1	0.000000	192.168.1.3	192.168.1.1	DNS	86	1	0	0	0	Standard query 0x0011 PTR 119.4.246.161.in-addr.arpa
2	0.002614	192.168.1.1	192.168.1.3	DNS	124	1	1	0	0	Standard query response 0x0011 PTR 119.4.246.161.in-addr.arpa PTR jeweler19.ce.kmitl.ac.th

```
> Ethernet II, Src: HuaweiTe_8e:0a:29 (c8:0c:c8:8e:0a:29), Dst: Microsof_60:ee:63 (28:16:a8:60:ee:63)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3
> User Datagram Protocol, Src Port: 53, Dst Port: 57526
▼ Domain Name System (response)
  Transaction ID: 0x000c
  ▼ Flags: 0x8180 Standard query response, No error
    1... .... = Response: Message is a response
    .000 0... = Opcode: Standard query (0)
    .... 0.. = Authoritative: Server is not an authority for domain
    .... ..0. = Truncated: Message is not truncated
    .... ...1 = Recursion desired: Do query recursively
    .... .... 1... = Recursion available: Server can do recursive queries
    .... .... .0.. = Z: reserved (0)
    .... .... ..0. = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... .... ...0 = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 1
  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)
  ▼ 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: 3350 (55 minutes, 50 seconds)
      Data length: 26
      Domain Name: jeweler19.ce.kmitl.ac.th
```

มี 1 Question เป็น 119.4.246.161 ,type PTR ,class IN

มี 1 Answer เป็น 119.4.246.161 type PTR, class IN, jeweler19.ce.kmitl.ac.th

มี 2 Packet

ไม่มี Authority , Additional Info

15. ให้ใช้โปรแกรม nslookup แล้วตั้ง server เป็น 199.7.91.13 จากนั้นให้ ป้อน 199.7.91.13 โปรแกรมแสดงผลลัพธ์อะไรบ้าง ให้ capture มาแสดง นักศึกษาคิดว่า 199.7.91.13 เป็น server อะไร

```
> 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
>
```

คือว่าเป็น **d.root-servers.net**

16. ให้ป้อน query `www.ce.kmitl.ac.th` แสดงผลอะไรมาบ้าง 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 และให้นักศึกษาวาดรูปการทำ 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
    2001:c00:4618:3000::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
Default Server: ns.thnic.net
Address: 202.28.0.1

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

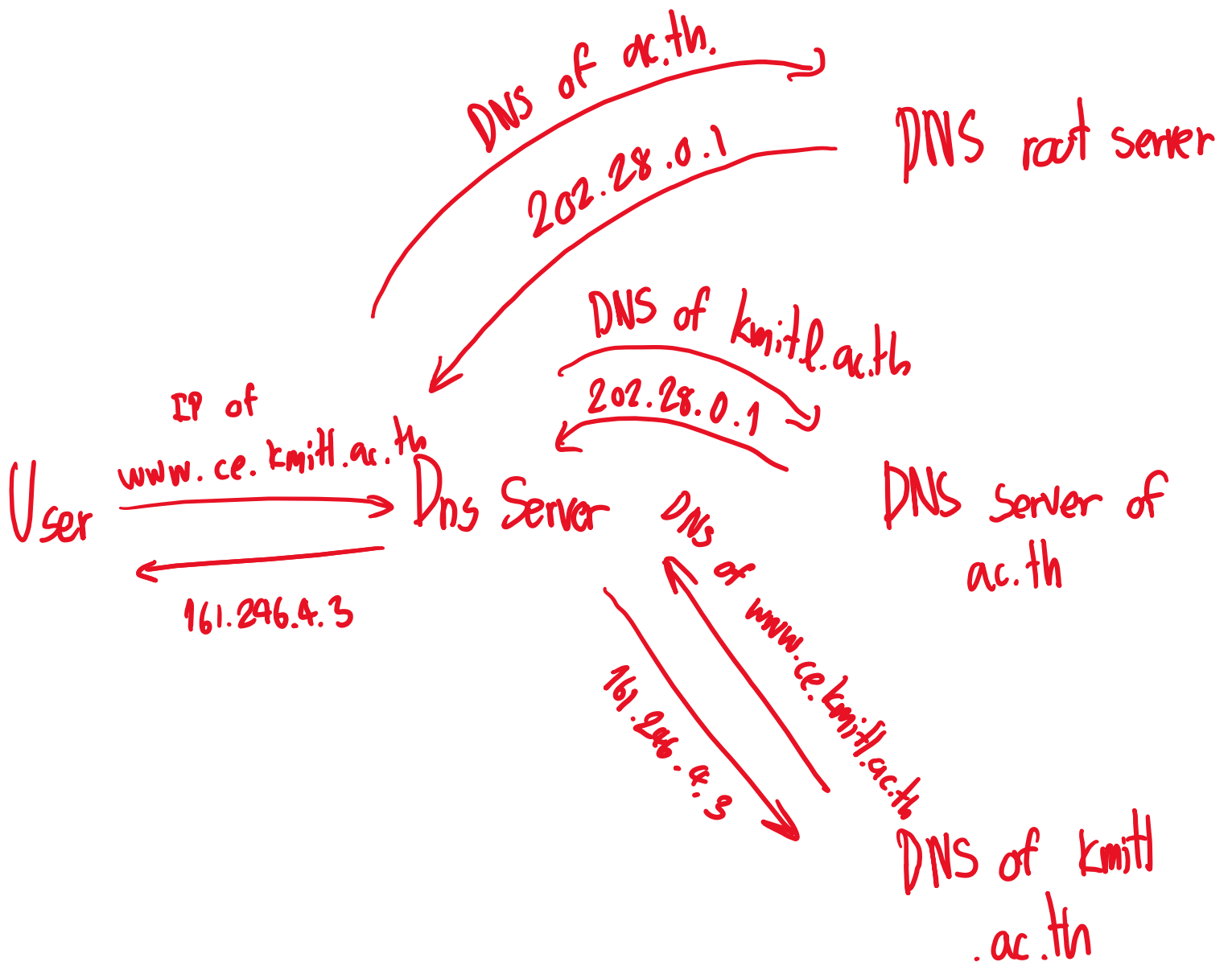
Name: ac.th

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

Name: kmitl.ac.th
Address: 161.246.34.11

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

18. ให้ Sort แล้วดูว่ามี DNS Query/Response ไດ ที่ใช้เวลาเกิน 1 วินาที

No.	Time	Source	Destination	Protocol	Length	Questions	Answer RRs	Authority RRs	Additional RRs	DNS Data	Info
11	1.292192	216.148.227.68	24.6.126.218	DNS	499	1	4	9	9	1.292192000	Standard query response 0x0029 A www.ncmec.org CNAME us.missingkids.com.edgesuite.net CNAME a1403.g.akamai.net A 205.161.7.14
107	2.329101	216.148.227.68	24.6.126.218	DNS	511	1	4	9	9	0.207250000	Standard query response 0x002a A www.missingkids.com CNAME us.missingkids.com.edgesuite.net CNAME a1403.g.akamai.net A 216.14
5	1.107705	204.127.202.4	24.6.126.218	DNS	499	1	4	9	9	0.107083000	Standard query response 0x0029 A www.ncmec.org CNAME us.missingkids.com.edgesuite.net CNAME a1403.g.akamai.net A 146.82.218.1
200	3.381529	24.6.126.218	146.82.218.136	TCP	54						[TCP Window Update] 3619 → 80 [ACK] Seq=4279 Ack=34820 Win=64512 Len=0
199	3.381431	24.6.126.218	146.82.218.136	TCP	54						3619 → 80 [ACK] Seq=4279 Ack=34820 Win=62633 Len=0
100	3.381345	146.82.218.136	24.6.126.218	TCP	1514						[TCP Out-Of-Order] 80 → 3619 [ACK] Seq=32039 Ack=4279 Win=16800 Len=1460
101	3.380805	24.6.126.218	146.82.218.136	TCP	44						[TCP Window Update] 3619 → 80 [ACK] Seq=4279 Ack=34820 Win=64512 Len=0

Frame 11: 499 bytes on wire (3992 bits), 499 bytes captured (3992 bits) on interface unknown, id 0

Ethernet II, Src: Cadent_22:89:c2 (00:01:5c:22:89:c2), Dst: AmbitNet_aai:af:80 (00:00:50:aaf:80)

Internet Protocol Version 4, Src: 216.148.227.68, Dst: 24.6.126.218

User Datagram Protocol, Src Port: 53, Dst Port: 3617

Domain Name System (response)

Transaction ID: 0x0029

Flags: 0x100 Standard query response, No error

1... .. = Response: Message is a response

...000 0... .. = Opcode: Standard query (0)

... ..0... .. = Authoritative: Server is not an authority for domain

... ..0... .. = Truncated: Message is not truncated

... ..1... .. = Recursion desired: Do query recursively

... ..1... .. = Recursion available: Server can do recursive queries

... ..0... .. = 2: reserved (0)

... ..0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server

... ..0... .. = Non-authenticated data: Unacceptable

... ..0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 4

Authority RRs: 9

Additional RRs: 9

Queries

www.ncmec.org: type A, class IN

Name: www.ncmec.org

[Name Length: 13]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

Answers

www.ncmec.org: type CNAME, class IN, cname us.missingkids.com.edgesuite.net

us.missingkids.com.edgesuite.net: type CNAME, class IN, cname a1403.g.akamai.net

a1403.g.akamai.net: type A, class IN, addr 205.161.7.142

a1403.g.akamai.net: type A, class IN, addr 205.161.7.144

Authoritative nameservers

Additional records

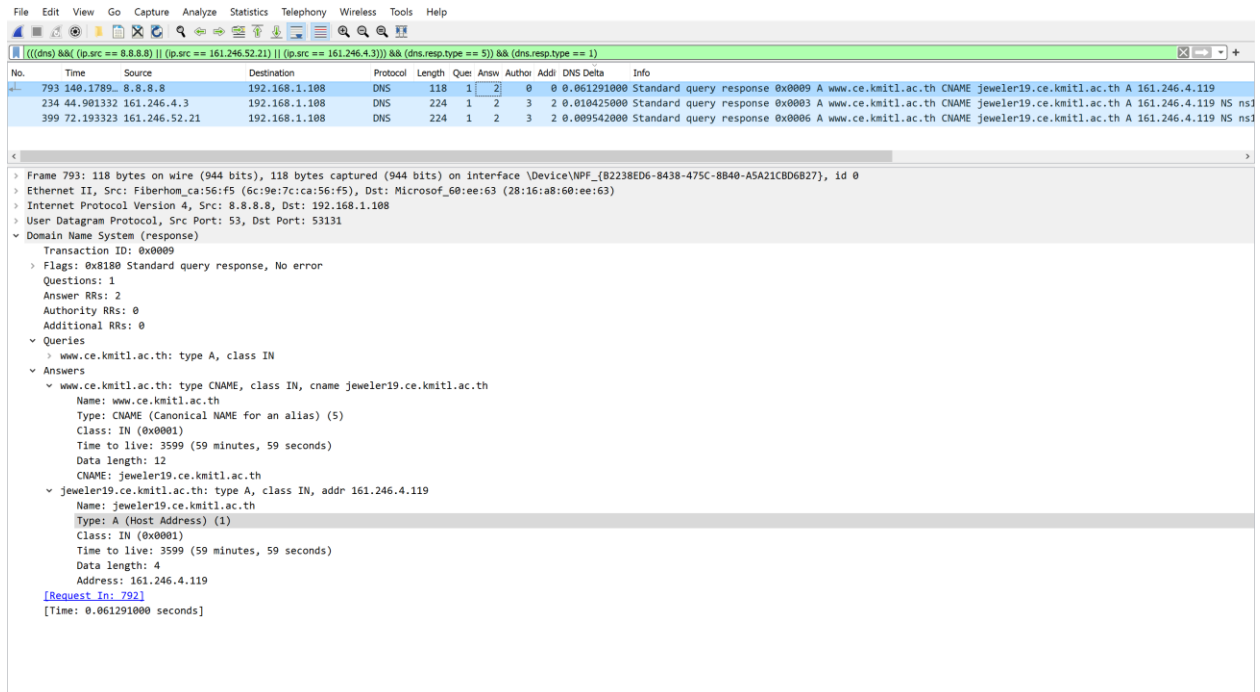
[Request In: 1]

[Time: 1.292192000 seconds]

Packet ที่ 11 ใช้เวลาไป 1.292192 วินาที

19. ให้เริ่ม 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 ให้เปรียบเทียบ DNS Delta ที่ได้จากแต่ละ Server (แสดงตัวเลขที่ได้) จากนั้นให้วิเคราะห์ผล

File Edit View Go Capture Analyze Statistics Telephony Wireless Help



No.	Time	Source	Destination	Protocol	Length	Que	Ans	Auth	Addi	DNS Delta	Info
793	140.1789.	8.8.8.8	192.168.1.108	DNS	118	1	2	0	0.061291000	Standard query response 0x0009 A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th A 161.246.4.119	
234	44.901332	161.246.4.3	192.168.1.108	DNS	224	1	2	3	2.0.010425000	Standard query response 0x0003 A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th A 161.246.4.119 NS ns1	
399	72.193323	161.246.52.21	192.168.1.108	DNS	224	1	2	3	2.0.009542000	Standard query response 0x0006 A www.ce.kmitl.ac.th CNAME jeweler19.ce.kmitl.ac.th A 161.246.4.119 NS ns1	

< >

> Frame 793: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface \Device\NPF_{B2238ED6-8438-475C-8B40-ASA21CB06827}, id 0
> Ethernet II, Src: Fiberhom_ca:56:f5 (6c:9e:7c:ca:56:f5), Dst: Microsof_60:ee:63 (28:16:a8:60:ee:63)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.108
> User Datagram Protocol, Src Port: 53, Dst Port: 53131
v Domain Name System (response)
Transaction ID: 0x0009
> Flags: 0x180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
v Queries
> www.ce.kmitl.ac.th: type A, class IN
v Answers
v www.ce.kmitl.ac.th: type CNAME, class IN, cname jeweler19.ce.kmitl.ac.th
Name: www.ce.kmitl.ac.th
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 3599 (59 minutes, 59 seconds)
Data length: 12
CNAME: jeweler19.ce.kmitl.ac.th
v jeweler19.ce.kmitl.ac.th: type A, class IN, addr 161.246.4.119
Name: jeweler19.ce.kmitl.ac.th
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 3599 (59 minutes, 59 seconds)
Data length: 4
Address: 161.246.4.119
[Request In: 792]
[Time: 0.061291000 seconds]

จาก Column DNS Delta จะพบว่า 8.8.8.8 มีเวลาเท่ากับ 0.061291 วินาที ซึ่งจะต่างจาก 161.246.4.3 และ 162.246.52.21 อย่างมากซึ่งมีเวลาเท่ากับ 0.010425 กับ 0.009542 เนื่องจากสอง DNS อยู่ใกล้ๆ 8.8.8.8 ซึ่งเป็น Public DNS ของ Google ,round trip time เลยมีค่าน้อยกว่านั่นเอง