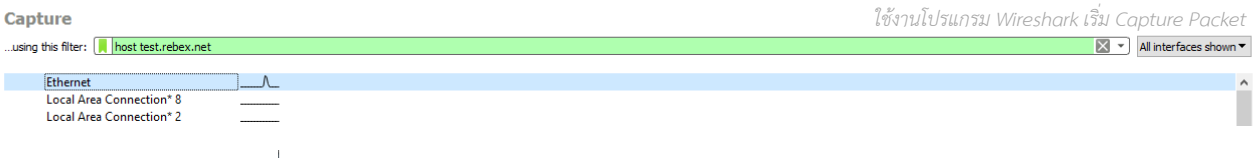
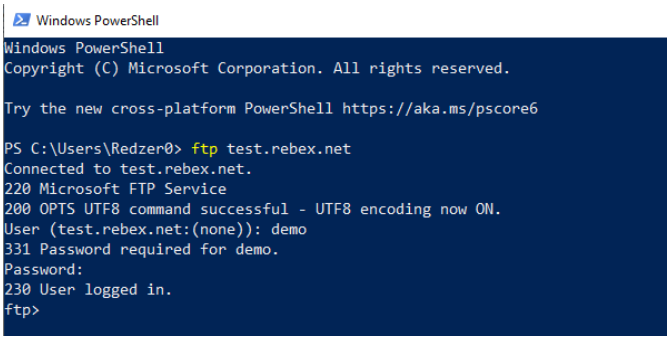
ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

กิจกรรมที่ 5 : FTP และ DNS

เปิดโปรแกรม wireshark ให้กำหนดให้ capture เฉพาะ host test.rebex.net และใช้เรียก Command Prompt แล้วป้อนคำสั่ง ftp test.rebex.net โดยให้ใส่ user เป็น demo และใช้ passwordเป็น password



ใช้งานโปรแกรม Wireshark เริ่ม Capture Packet

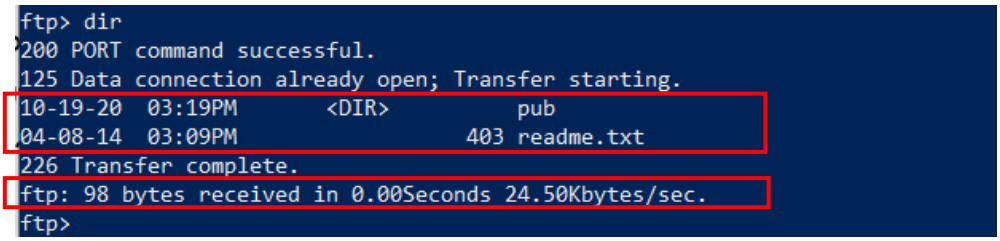


ใช้งานโปรแกรม Windows PowerShell และเรียกใช้งาน FTP service

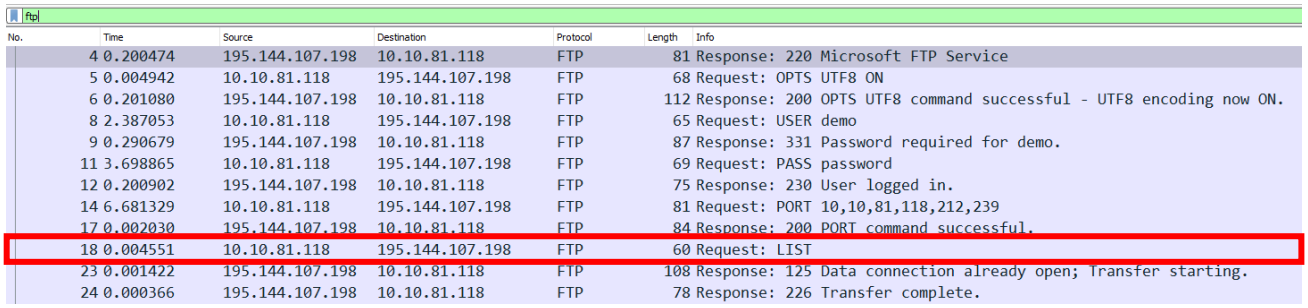
Q(3) : ใช้คำสั่ง dir ในโปรแกรม ftp และ capture ภาพการทำงานของคำสั่ง dir จากนั้นกลับมาที่ Wireshark แล้วใช้ display filter เป็น ftp ให้เปรียบเทียบระหว่างคำสั่งของ ftp ที่ใช้กับ packet ของ Wireshark ที่ดักจับได้ ให้ capture ภาพของ packet list pane ที่แสดงคำสั่งมาแสดงด้วย

A(3) : เมื่อใช้คำสั่ง dir หรือเป็นการ list directory ของ directory นั้น เมื่อเปรียบเทียบระหว่างการแสดงผลของ PowerShell และใน Packet list Plane แล้วพบว่าหลังใช้ คำสั่ง dir บนตัว PowerShell จะแสดงรายละเอียดการเชื่อมต่อและแสดงไฟล์ที่มีอยู่ใน directory นั้นในที่นี้คือไฟล์ readme.txt แสดงขนาดไฟล์ เวลาที่ใช้งานในการรับไฟล์ ความเร็วในการถ่ายโอนไฟล์ แต่ในส่วนของ Packet List Plane จะแสดงเฉพาะสถานการณ์เชื่อมต่อและสถานการณ์ทำงาน เท่านั้น

การใช้งานคำสั่ง dir บน PowerShell



Packet ที่ใช้จากการ Capture และใช้ Display Filter : ftp หลังจากเริ่มใช้งาน ftp บน PowerShell



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

A(4) : ส่งมาจาก port ต้นทางคือ 20 และ port ปลายทางคือ 24511 ใน packet ที่ 20

ใช้ Display Filter : ftp-data ใน Packet List Plane จะปรากฏ packet ที่มีชื่อไฟล์ readme.txt

ftp-data

No.	Time	Source	Destination	Protocol	Length	Info
20	0.001690	195.144.107.198	10.10.81.118	FTP-DATA	149	FTP Data: 95 bytes (PORT) (LIST)

รายละเอียดใน packet ที่ 20 ที่ดักจับได้

```
Transmission Control Protocol, Src Port: 20, Dst Port: 54511, Seq: 1, Ack: 1, Len: 
    Source Port: 20
    Destination Port: 54511
    [Stream index: 1]
    [TCP Segment Len: 95]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 536320082
    [Next Sequence Number: 96    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2753851866
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 260
    [Calculated window size: 66560]
    [Window size scaling factor: 256]
    Checksum: 0xf306 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (95 bytes)
FTP Data (95 bytes data)
[Setup frame: 14]
[Setup method: PORT]
[Command: LIST]
Command frame: 18
[Current working directory: ]
Line-based text data (2 lines)
    10-19-20  03:19PM       <DIR>          pub\r\n
    04-08-14  03:09PM                  403 readme.txt\r\n
```

แสดงรายละเอียด Port ต้นทางและปลายทาง

แสดงชื่อไฟล์ readme.txt

การใช้งาน port ของ client ในการรับ-ส่งไฟล์ โดย client จะสุ่ม port การใช้งานขึ้นโดยเป็นไปตามนี้คือ

```
    14 6.681329     10.10.81.118     195.144.107.198  FTP      81 Request: PORT 10,10,81,118,212,239
    17 0.002030     195.144.107.198  10.10.81.118     FTP      84 Response: 200 PORT command successful.
    18 0.004551     10.10.81.118     195.144.107.198  FTP      60 Request: LIST
File Transfer Protocol (FTP)
  PORT 10,10,81,118,212,239\r\n
    Request command: PORT
    Request arg: 10,10,81,118,212,239
    Active IP address: 10.10.81.118
    Active port: 54511
```

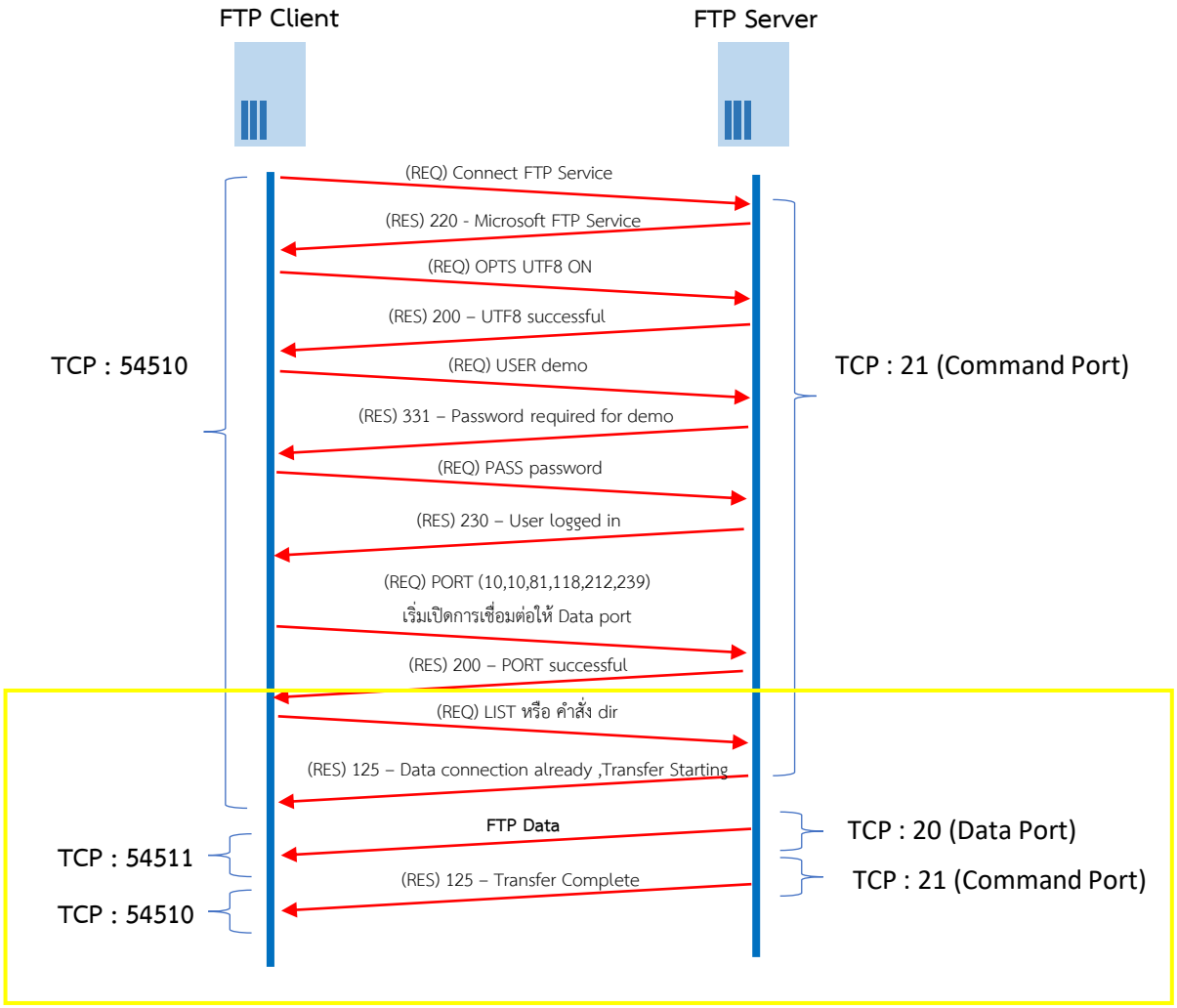
แสดง Argument ทั้ง 6 ค่าที่ Client request ไป

แสดง Data Port

Client จะส่งคำสั่ง PORT ตามด้วย Argument จำนวน 6 ค่า request ไปยัง FTP Server ซึ่ง FTP server จะนำค่าไปคำนวณต่อเพื่อส่งข้อมูลมายัง Port นี้โดยมีรูปแบบการคำนวณดังนี้ PORT (h1,h2,h3,h4,p1,p2) การคำนวณ Data Port = (p1 * 256) + p2 เช่น ในที่นี้ p1 = 212 และ p2 = 239 จะได้ว่า (212 * 256) + 239 = 54511 ซึ่ง port 54511 จะถูกนำไปใช้เป็น Data Port ในการรับ-ส่งข้อมูลของการเชื่อมต่อครั้งนี้ ส่วน h1-h4 คือ IP Address ของ Client ในที่นี้คือ 10.10.81.118

หมายเหตุ : โดยปกติแล้ว Data Port ของ FTP คือ port 20 แต่ด้วยข้อกำหนดของ IANA ที่ควรใช้ port ที่อยู่ในช่วง 49152 ถึง 65535 ในการใช้งาน ดังนั้น Client Port จะถูกคำนวณใหม่เป็นแบบ Dynamic port ขึ้นอยู่กับ Argument ที่สุ่มขึ้นมาได้ซึ่งจะแตกต่างกันออกไปของการเชื่อมต่อกับ Client

แผนภาพการทำงาน คำสั่ง dir ของ FTP



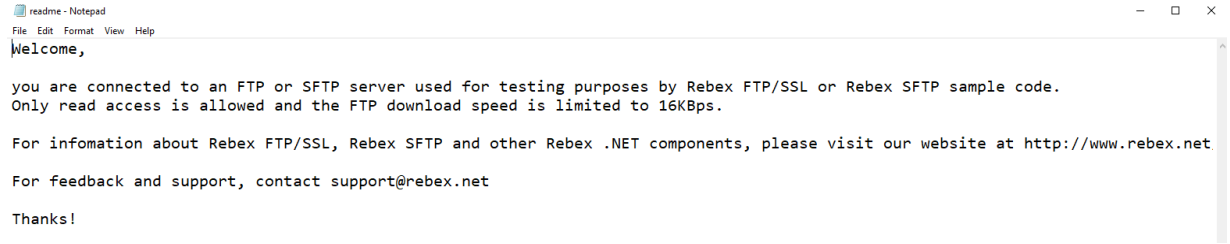
Q(5) : ใช้คำสั่ง get readme.txt เพื่อรับไฟล์ readme.txt จาก ftp server จากนั้นให้เปิดไฟล์ใน notepad และ capture มาแสดง และ capture ข้อมูลใน Wireshark ที่เป็นการส่งไฟล์ readme.txt มาเปรียบเทียบ

A(5) :

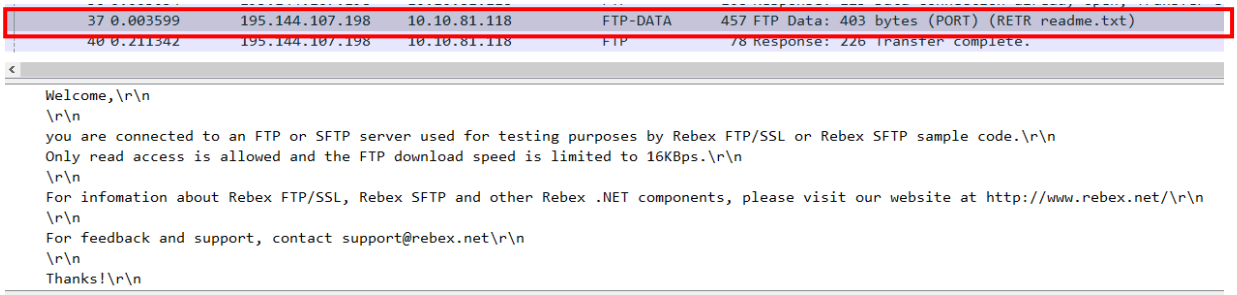
การใช้งานคำสั่ง get readme.txt บน PowerShell

```
ftp> get readme.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp: 403 bytes received in 0.26Seconds 1.53Kbytes/sec.
ftp>
```

ไฟล์ readme.txt ที่ถูกเปิดด้วยโปรแกรม Notepad



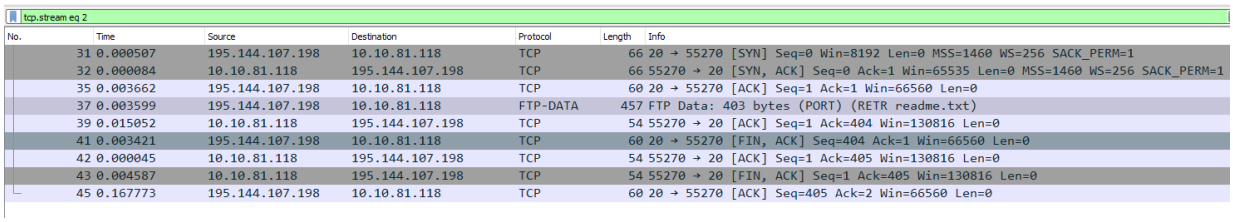
ไฟล์ readme.txt ที่ได้จากการ Capture packet บน Wireshark ใน packet ที่ 37



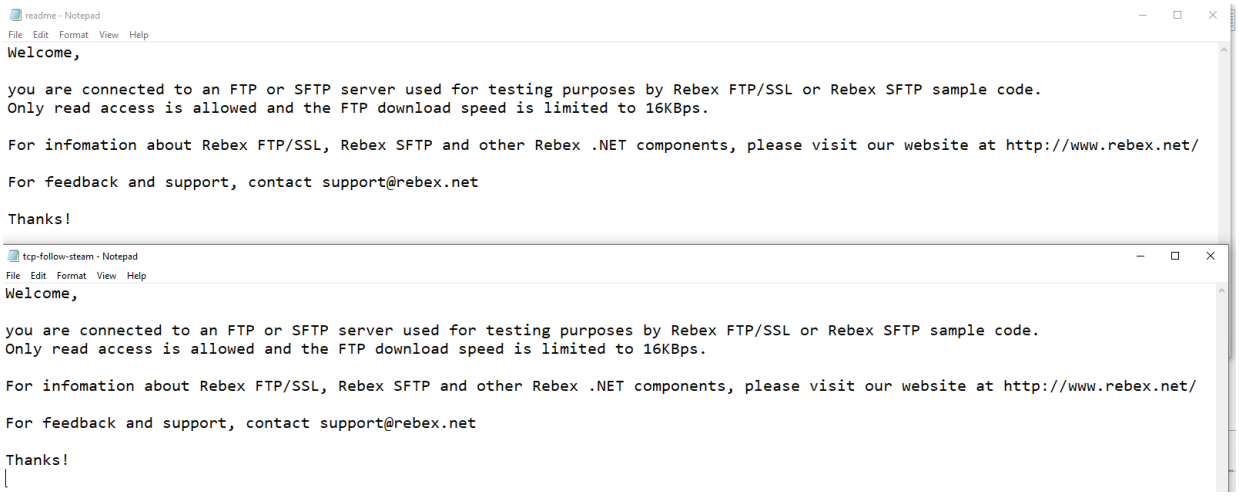
Q(6) : ให้คลิกขวาที่ packet ที่เป็นข้อมูลของ readme.txt และเลือก Follow TCP Stream และ Save as... เป็นไฟล์ ให้ตั้งชื่ออะไรก็ได้ จากนั้นเปิดไฟล์ด้วย notepad แล้วเปรียบเทียบกับไฟล์ readme.txt ว่ามีอะไรแตกต่างกันหรือไม่

A(6) :

Packet ใน Packet List Plane หลังจากเลือก Follow TCP Stream ของ FTP-DATA ไฟล์ readme.txt



ไฟล์ที่ได้ จาก save as... และไฟล์ readme.txt ที่ได้มาจากคำสั่ง get ทั้งสองไฟล์มีข้อความข้อมูลข้างในเหมือนกัน



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

A(7) :

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

```
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.
```

คำสั่ง	คำอธิบาย (Client ส่ง request ไป FTP server)
USER anonymous	ต้องการใช้งาน user ชื่อ anonymous
PASS anypwd	รหัสผ่านของ user anonymous คือ anypwd
PORT 192,168,0,101,206,177	FTP Command Port ของ Client คือ (206 * 256) + 177 = 52913 192.168.0.101:52913
NLST	แสดง List ของไฟล์ใน directory นั้น
TYPE I	ชนิดของข้อมูลที่ต้องการ transfer โดย Type : I หมายถึงไฟล์รูปภาพ
PORT 192,168,0,101,206,178	FTP Data Port ของ Client คือ (206 * 256) + 178 = 52913 192.168.0.101:52914
RETP pantheon.jpg	ดึงสำเนาของไฟล์ชื่อ pantheon.jpg
QUIT	สิ้นสุดการเชื่อมต่อ

ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

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

A(9) :

Q(10) : ให้อธิบายว่าการทำงานในข้อ 8 ทำเพื่ออะไร

A(10) : ข้อ 8 เป็นการ filter conversation ของ FTP และ ERROR ออกไป ให้เหลือแต่ตัว steam ของข้อมูลที่สมบูรณ์

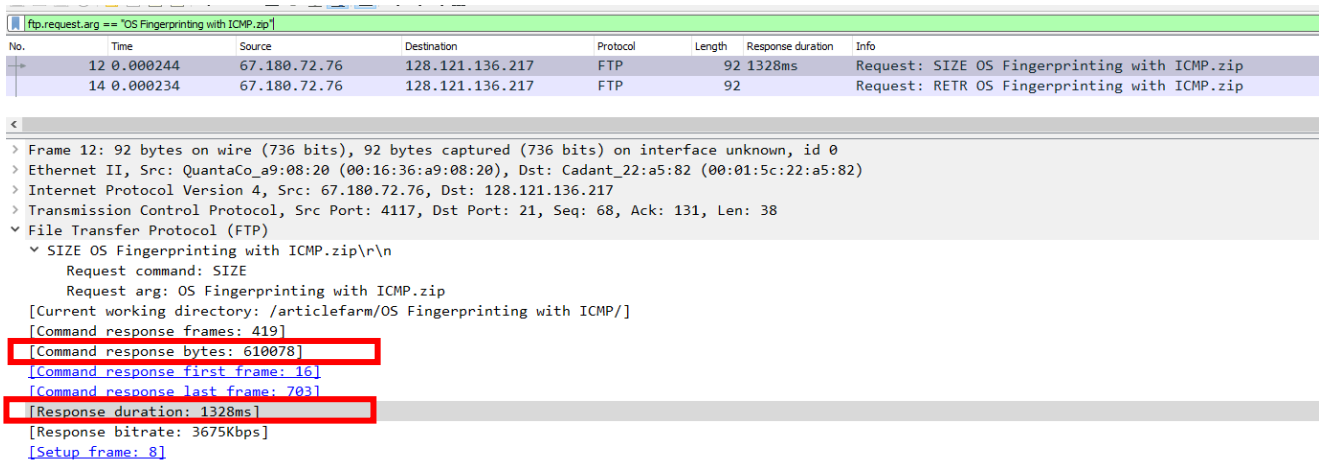
ภาพ pantheon.jpg ไม่สมบูรณ์เมื่อไม่ทำตามข้อ 8

ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

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

A(11) : ใช้เวลาในการโหลดไฟล์ 1328 ms และขนาดไฟล์ของ SIZE OS Fingerprinting with ICMP.zip เท่ากับ 610078 byte

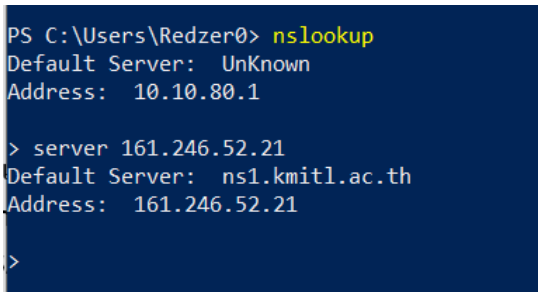
1. ใช้ Display filter คือ ftp.request.arg == "OS Fingerprinting with ICMP.zip"



2. สังเกตค่าจาก Response duration = 1328 ms คือ เวลาที่ใช้ในการดาวน์โหลดไฟล์ และ
Command response bytes = 610078 byte คือ ขนาดของไฟล์

Q(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 _____

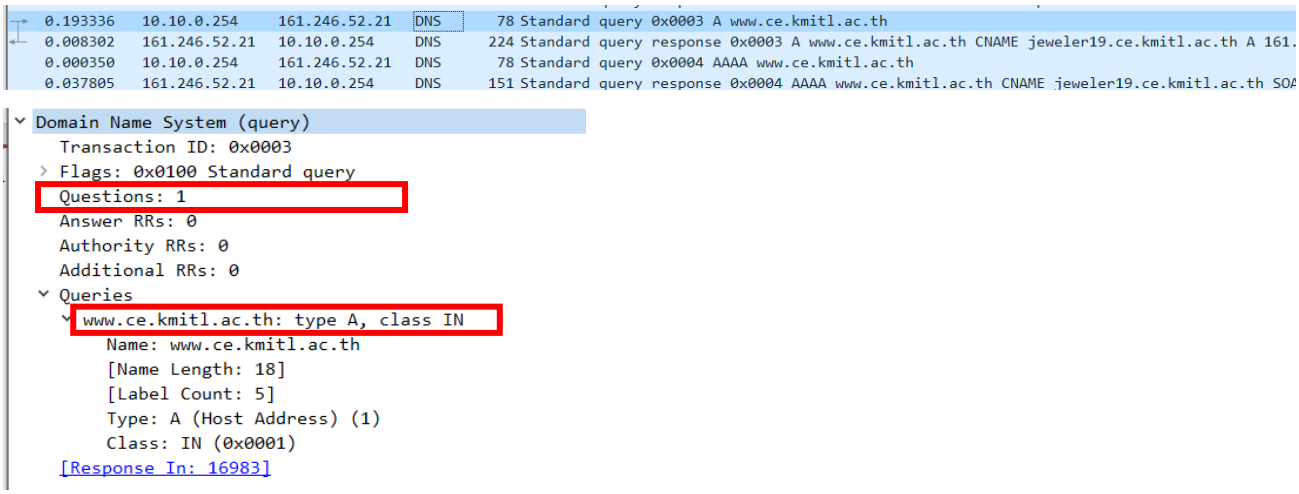
A(12) : มีชื่อว่า ns1.kmitl.ac.th



Q(13) : ให้พิมพ์ www.ce.kmitl.ac.th และหยุด Capture ให้ตอบคำถามดังนี้

Q(13.1) : ใน DNS Query มี # questions เท่าไร และข้อมูลใน questions คืออะไร type เป็นค่าอะไร ให้ Capture ส่วนของ Packet Details Pane ประกอบด้วย

A(13.1) : มี 1 Questions คือ www.ce.kmitl.ac.th เป็น Type A และ class IN (Internet)

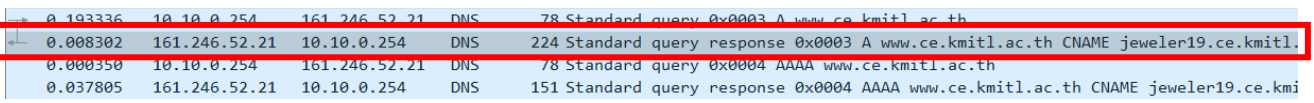


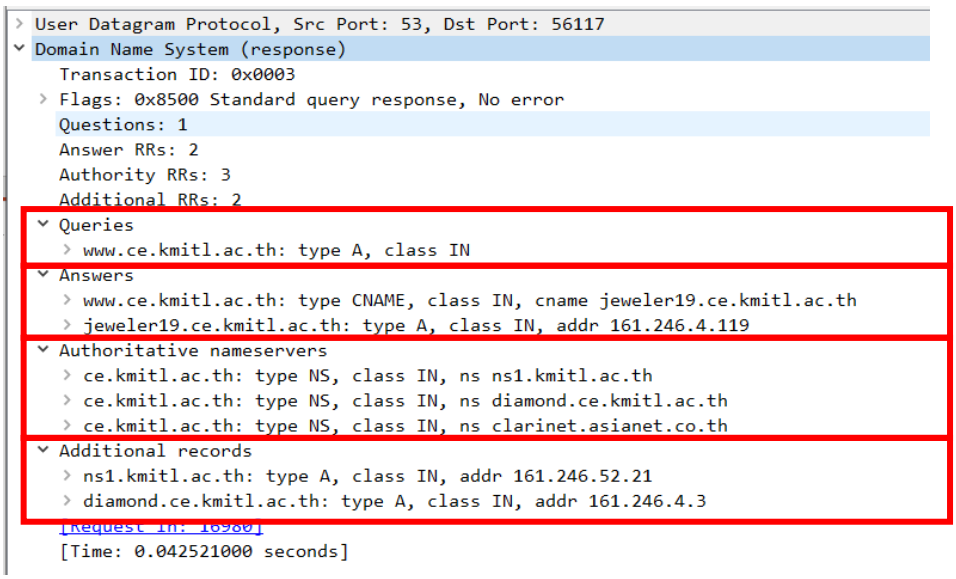
Q(13.2) : ใน DNS Response มี # answer เท่าไร และข้อมูลใน answer คืออะไร ให้ Capture ส่วนของ Packet Details Pane ประกอบด้วย มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

A(13.2) : มี 1 Questions (query) คือ www.ce.kmitl.ac.th เป็น Type A และ class IN (Internet) และมี Answer RRs ตอบกลับมา 2 คือ

1. www.ce.kmitl.ac.th , Type CNAME , cname คือ jeweler16.ce.kmitl.ac.th
2. jeweler19.ce.kmitl.ac.th , Type A , Address คือ 161.246.4.119

มีข้อมูลส่วนของ Authority คือ 3 RRs และ Additional คือ 2 RRs ดังนี้





แสดง Query

แสดง Response

แสดง Authority

แสดง Additional info

ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

Q(14) : ทำตามข้อ 2 อีกครั้ง แต่ใช้ 161.246.4.119 แทนที่จะใช้ www.ce.kmitl.ac.th

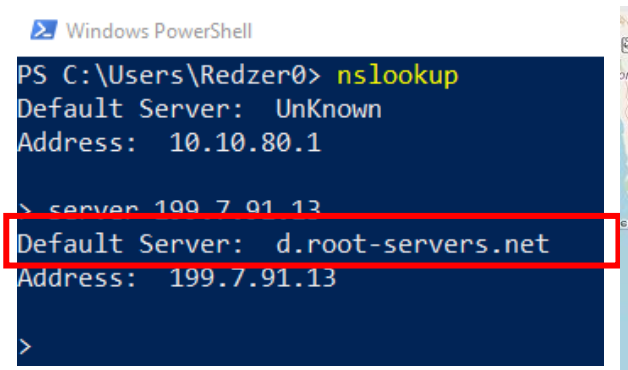
A(14) : มี 1 Questions คือ 119.4.246.161.in-addr.arpa มี Type PTR (domain name PoinTeR) หรือเป็นการค้นว่า IP Address นี้ถูกชี้ไปยังที่ใดภายใต้ .in-addr.arpa ซึ่งเป็นการแปลง ip กลับไปเป็นชื่อ ในที่นี้คือ jaweler19.ce.kmitl.ac.th

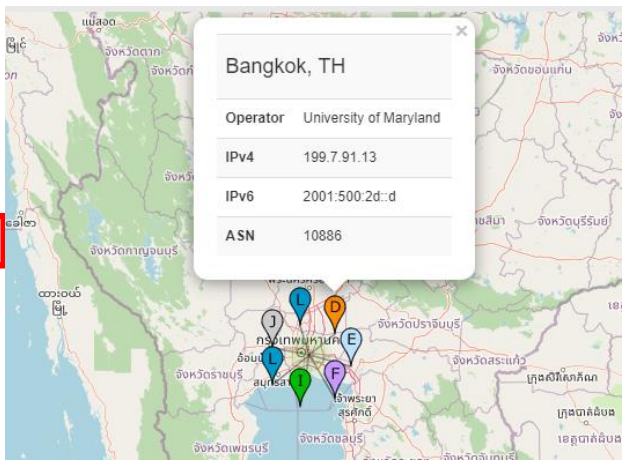
```
1 0.000000   10.10.0.218    161.246.52.21  DNS      86 Standard query 0x0004 PTR 119.4.246.161.in-addr.arpa
2 0.151764   161.246.52.21  10.10.0.218    DNS     196 Standard query response 0x0004 PTR 119.4.246.161.in-addr.arpa PTR jeweler19.ce.kmitl.ac.th
```

```
Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8500 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  v Queries
    v 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)
  v Answers
    > 119.4.246.161.in-addr.arpa: type PTR, class IN, jeweler19.ce.kmitl.ac.th
  v Authoritative nameservers
    > 4.246.161.in-addr.arpa: type NS, class IN, ns diamond.ce.kmitl.ac.th
    > 4.246.161.in-addr.arpa: type NS, class IN, ns ns1.kmitl.ac.th
  v 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: 1]
    [Time: 0.151764000 seconds]
```

Q(15) : ให้ใช้โปรแกรม nslookup แล้วตั้ง server เป็น 199.7.91.13 จากนั้นให้ ป้อน 199.7.91.13 โปรแกรมแสดงผลอะไรมาบ้าง ให้ capture มาแสดง นักศึกษาคิดว่า 199.7.91.13 เป็น server อะไร

A(15) : แสดงผลเป็น d.root-server.net ซึ่งเป็น 1 ใน 13 root server ซึ่งจะเก็บทุก name space เอาไว้เป็นจุดแรกสุดในการค้นหา . (root)





ชื่อ นาย รวีโรจน์ ทองดี **รหัสนักศึกษา** 62010763

Q(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.kmit.ac.th ตามลำดับ ให้ capture มาแสดง และให้นักศึกษาวาดรูปการทำ name resolution ของ www.ce.kmitl.ac.th โดยสมมติให้เครื่องที่ request เป็นเครื่องที่อยู่ต่างประเทศ

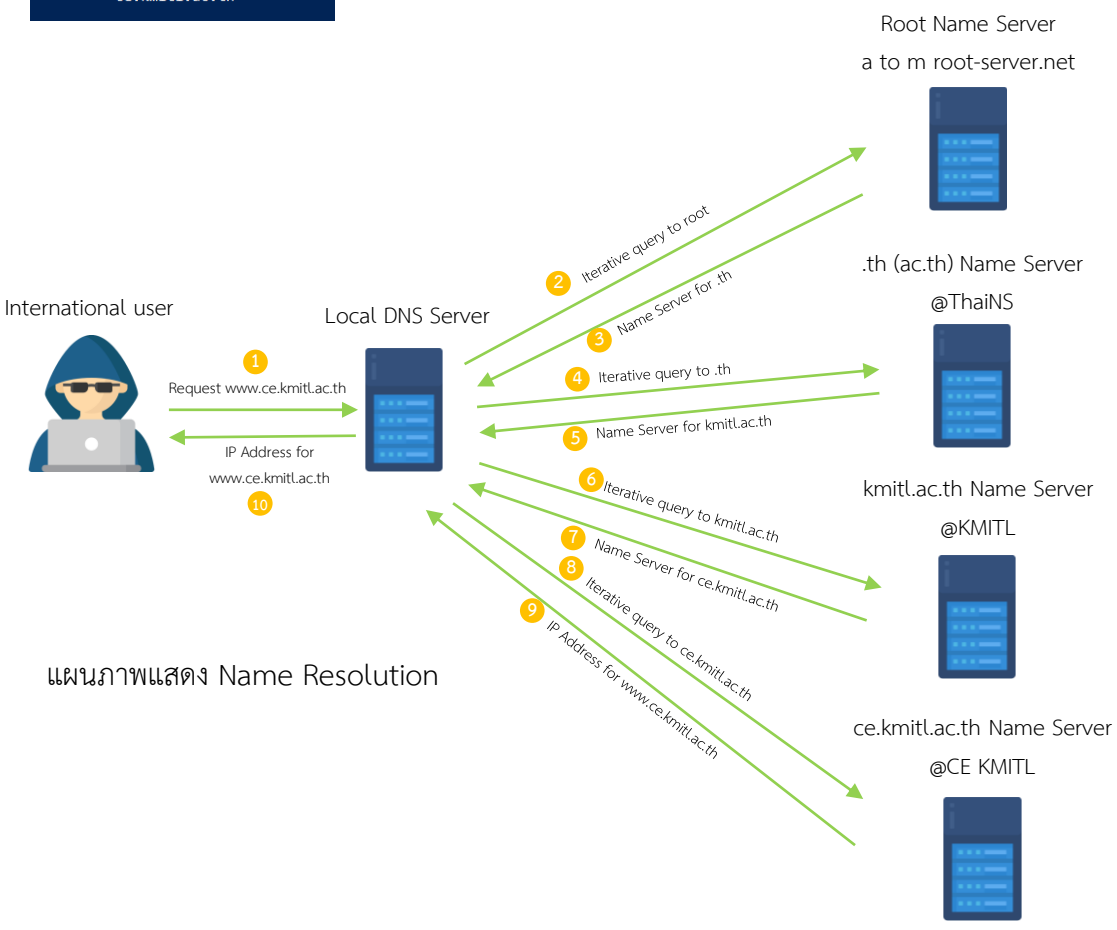
A(16) :

แสดงการใช้ nslookup

```
PS C:\Users\Redzer0> nslookup
Default Server:  UnKnown
Address:  10.10.0.1

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

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

Name:    ac.th

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

Name:    kmitl.ac.th
Address:  161.246.34.11

> 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
```

แสดงการ query www.ce.kmitl.ac.th

```
PS C:\Users\Redzer0> nslookup
Default Server:  UnKnown
Address:  10.10.80.1

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

> query www.ce.kmitl.ac.th
Server:  jeweler19.ce.kmitl.ac.th
Address:  161.246.4.119
Aliases:  www.ce.kmitl.ac.th
```



แผนภาพแสดง Name Resolution

Q(18) : ให้ Sort แล้วดูว่ามี DNS Query/Response ใด ที่ใช้เวลาเกิน 1 วินาที

A(18) : packet ที่ 11 ของ DNS = 1.292192000 วินาที

dns

No.	Time	Source	Destination	Protocol	Length	DNS Delta	Info
11	0.000056	216.148.227.68	24.6.126.218	DNS	499	1.292192000	Standard query response 0x0029 A www.ncmec.org
107	0.057464	216.148.227.68	24.6.126.218	DNS	511	0.207250000	Standard query response 0x002a A www.missingk
3	0.107083	204.127.202.4	24.6.126.218	DNS	499	0.107083000	Standard query response 0x0029 A www.ncmec.org
98	0.002127	24.6.126.218	216.148.227.68	DNS	79		Standard query 0x002a A www.missingkids.com
2	1.000620	24.6.126.218	204.127.202.4	DNS	73		Standard query 0x0029 A www.ncmec.org
1	0.000000	24.6.126.218	216.148.227.68	DNS	73		Standard query 0x0029 A www.ncmec.org

Q(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

A(19) : จากการใช้งาน nslookup และใช้ query ไปหา www.ce.kmitl.ac.th พบว่า DNS server 161.246.4.3 ทำเวลาในการตอบสนองได้เร็วที่สุด คือ 0.03461000 วินาที รองลงมา คือ Server 161.246.52.21 ที่เวลา 0.068272000 วินาที ส่วน Server 8.8.8.8 นั้นใช้เวลามากที่สุด คือ 0.08489800 วินาที ซึ่งอาจวิเคราะห์ได้ว่า Server 161.246.4.3 หรือ diamond.ce.kmitl.ac.th นั้นเป็น Name Server ที่เป็น Forward zone หรือใกล้กับ www.ce.kmitl.ac.th เลยทำให้เวลาให้การ query น้อยที่สุด ส่วน Server 8.8.8.8 ซึ่งเป็น Public DNS Server ซึ่งการใช้งานอาจมี traffic ไปหา server ของ Google ที่อยู่ต่างประเทศได้ ดังนั้นเลยทำให้เวลาที่ใช้ในการตอบกลับช้าสุด เมื่อเทียบกับ ns1.kmitl.ac.th และ diamond.ce.kmitl.ac.th แล้ว

dns.response_to

No.	Time	Source	Destination	Protocol	Length	DNS Delta
6	0.034610	161.246.4.3	10.10.0.218	DNS	224	0.034610000
	0.068272	161.246.52.21	10.10.0.218	DNS	224	0.068272000
	0.084898	8.8.8.8	10.10.0.218	DNS	118	0.084898000

```
> server 161.246.4.3
Default Server:  diamond.ce.kmitl.ac.th
Address:  161.246.4.3

> query www.ce.kmitl.ac.th
Server:  jeweler19.ce.kmitl.ac.th
Address:  161.246.4.119
Aliases:  www.ce.kmitl.ac.th

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to www.ce.kmitl.ac.th timed-out
```

ใช้ server 161.246.4.3

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

> query www.ce.kmitl.ac.th
Server:  jeweler19.ce.kmitl.ac.th
Address:  161.246.4.119
Aliases:  www.ce.kmitl.ac.th

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to www.ce.kmitl.ac.th timed-out
```

ใช้ server 161.246.52.21

```
> server 8.8.8.8
Default Server:  [8.8.8.8]
Address:  8.8.8.8

> query www.ce.kmitl.ac.th
Server:  jeweler19.ce.kmitl.ac.th
Address:  161.246.4.119
Aliases:  www.ce.kmitl.ac.th

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to www.ce.kmitl.ac.th timed-out
```

ใช้ server 161.246.52.21

No.	Time	Source	Destination	Protocol	Length	DNS Delta
4	0.389866	1.1.1.1	10.10.0.218	DNS	118	0.389866000

```
> server 1.1.1.1
Default Server:  one.one.one.one
Address:  1.1.1.1

> query www.ce.kmitl.ac.th
Server:  jeweler19.ce.kmitl.ac.th
Address:  161.246.4.119
Aliases:  www.ce.kmitl.ac.th
```

ใช้ server 1.1.1.1 (Cloudflare Public DNS and CDN)