

01076117 ปฏิบัติการเครือข่ายคอมพิวเตอร์ 2/2565
 ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
 สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

กิจกรรมที่ 5 : FTP และ DNS

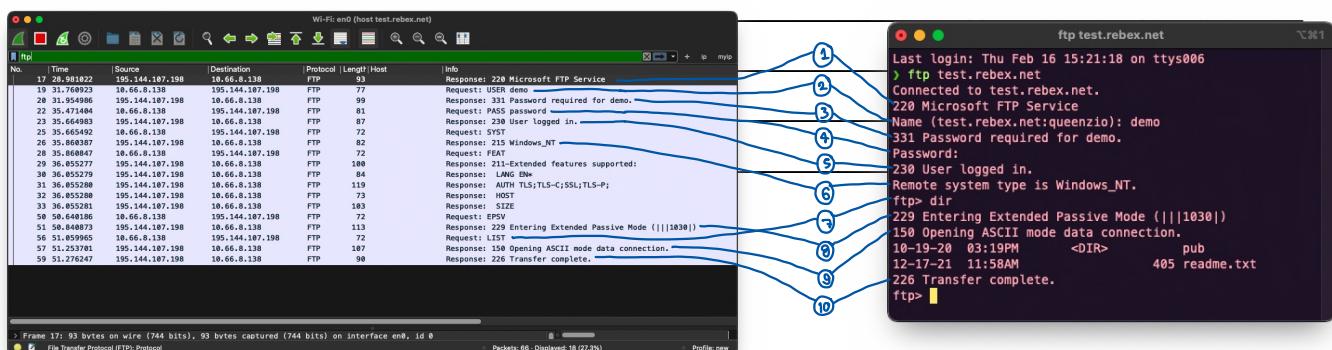
กิจกรรมครั้งนี้จะเป็นการทำความเข้าใจกับโปรโตคอล FTP (File Transfer Protocol) และ DNS (Domain Name System) เพื่อเสริมสร้างความเข้าใจในการทำงานของโปรโตคอลทั้ง 2 ตัว

↑ นั่นก็คือ passive mode กะ random port กะ เป็น port ไหน กะ เป็น port ไหนๆ

FTP (File Transfer Protocol)

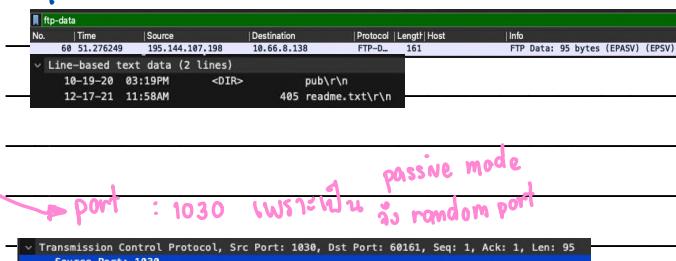
↑ นั่นก็คือ active mode โปรโตคอล FTP จะใช้ 2 พอร์ต คือ พอร์ต 21 ใช้เป็น control channel คือเป็นช่องทางสำหรับรับส่งคำสั่ง และ พอร์ต 20 ใช้เป็น data channel ซึ่งใช้ในการรับส่งไฟล์

1. เปิดโปรแกรม Wireshark ให้กำหนดให้ capture เฉพาะ host test.rebex.net
2. เรียก Command Prompt แล้วป้อนคำสั่ง **ftp test.rebex.net** โดยให้ใส่ user เป็น demo และใส่ password เป็น password
3. ใช้คำสั่ง **dir** ในโปรแกรม ftp และบันทึก screenshot ภาพการทำงานของคำสั่ง dir จากนั้นกลับมาที่ Wireshark และใช้ display filter เป็น **ftp** ให้เบรยนเทียบแต่ละคำสั่งของ ftp ว่าตรงกับ packet ใดที่ Wireshark ดักจับได้ ให้บันทึก screenshot ภาพของ Packet List Pane ที่แสดงคำสั่งมาแสดงด้วย



4. จาก packet ที่ได้ดักจับไว้ ให้ค้นหา packet ที่มีเนื้อหาระบุชื่อไฟล์ **readme.txt** (ซึ่งเป็นข้อมูลที่ ftp server ส่งมา) ว่าอยู่ใน packet ใด และส่งมาทางหมายเลข port ใด จากที่ระบุไว้ใน header ของ Transport Layer Protocol จากนั้นให้ปิดคู่ที่ Statistics -> Flow graph และนำมาอธิบายขั้นตอนการทำงานของคำสั่ง **dir** โดยละเอียด โดยอ้างอิงจาก Flow graph

→ packet ที่ 60 น้ากๆก filter **ftp-data**



→ port : 1030 เพราะเป็น passive mode
 และ random port

น้ำก๊กๆก

ນີ້ແລ້ວ ດຳເນັ້ນ dir ຫຼື client ຂຶ້ນ

request ຫຼືຈູ້ server ຕ້ອງ source port 60139
destination port 21

client ໂມນກັນ
ໃຈບົນຊີແລ້ວ
ດໍາເນັດກາ ສຳເນົາ
source port 60139
destination port 21

60139	Request: LIST	21
60139	Response: 150 Opening ASCII mode data connecti...	21
60139	60139 → 21 [ACK] Seq=51 Ack=335 Win=131024 ..	21
60139	Response: 226 Transfer complete.	21
60161	FTP Data: 95 bytes (EPASV) (EPSV)	1030
60161	1030 → 60161 [FIN, ACK] Seq=96 Ack=1 Win=655...	1030

server ໂມນກັນວ່າ
ກໍ່ມີເປົ້າ ASCII mode
ໃຈ source port 21
destination port 60139

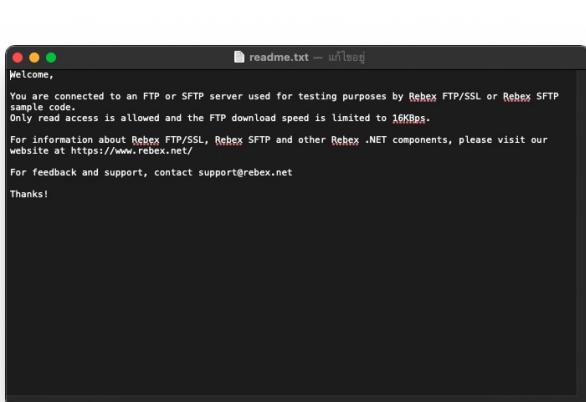
server ສຳເນົາ
FIN, ACK ໂມນຮັດໂນ
source port 1030
destination port 60161

Transfer complete
source port 21
destination port 60139

do data ຫຼັງຈູ້ client
ກຸ່ມື້ນດີ read me.txt
source port 1030
destination port 60161 if active
mode port 20

ftp> dir
229 Entering Extended Passive Mode (|||1030||)
150 Opening ASCII mode data connection.

- ใช้คำสั่ง **get readme.txt** เพื่อดownloadไฟล์ readme.txt จาก ftp server เมื่อดownloadเสร็จสิ้นให้เปิดไฟล์ดังกล่าวด้วยโปรแกรม notepad และบันทึกภาพ screenshot นำมาแสดง (หากไม่รู้ว่า path ของไฟล์ที่ดาวน์โหลดมาแล้วว่าอยู่ที่ path ใดบนเครื่อง ให้พิมพ์คำสั่ง **lcd** เพื่อแสดง current directory ของผู้client) พร้อมทั้งนำภาพ screenshot จากหน้าโปรแกรม Wireshark ส่วนที่แสดงข้อมูลในการส่งไฟล์ readme.txt มาบุรีบเทียบด้วย



	Request: RETR readme.txt	21
61238	[TCP Retransmission] 61238 → 21 [PSH, ACK] Seq=1 Ack=21	21
61238	Response: 150 Opening ASCII mode data connect...	21
61238	61238 → 21 [ACK] Seq=91 Ack=456 Win=131024	21
61285	61285 → 1027 [FIN, ACK] Seq=1 Ack=1 Win=1313...	1027
61238	[TCP Spurious Retransmission] Response: 150 Op...	21
61238	[TCP Window Update] 61238 → 21 [ACK] Seq=91	21
61285	1027 → 61285 [ACK] Seq=1 Ack=2 Win=65536 Le...	1027
61285	FTP Data: 405 bytes (EPASV) (RETR readme.txt)	1027

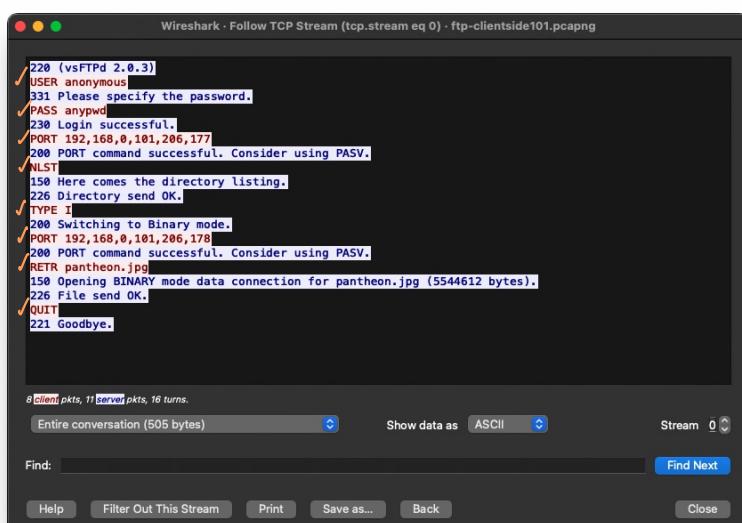
port data channel
ມຳນັກ ໂນດອງຈາກ ຕິດຕະຫຼາດ ທຸລາ
ມີນັກ ດ້ວຍກົມພົມ
ເຊື່ອງກົມພົມ

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

ໄຊ່ເຕັກຕ່າງກົນ

- พิมพ์คำสั่ง disconnect เพื่อให้โปรแกรม ftp client ตัดการเชื่อมต่อกับ ftp server
 - พิมพ์คำสั่ง bye หรือ quit ก็ได้ เพื่อจบการทำงานของโปรแกรม ftp client
 - ให้เปิดไฟล์ ftp-clientside101.pcapng คลิกขวาที่ packet ที่ 6 (USER anonymous) และเลือก Follow TCP Stream ให้บันทึก screenshot หน้าต่าง Follow TCP Stream ที่แสดงการโต้ตอบของ FTP ให้อธิบายว่ามีคำสั่งของ FTP Protocol อะไรบ้าง (ระบบชื่อ FTP Commands ไม่ใช่คำสั่งของโปรแกรม)

USER PASS PORT NLST TYPE PORT RETR QUIT



10. จากนั้นที่หน้าต่างของ Follow TCP Stream ให้เลือก Filter Out this Stream และให้ดูที่ display filter ว่า แสดงว่าอะไร จากนั้นคลิกขวาที่ packet 16 และเลือก Follow TCP Stream อีกรอบและเลือก Filter Out this Stream อีกรอบ
11. จากนั้นคลิกที่ packet ใดก็ได้และเลือก Follow TCP Stream คลิก Save as ให้ตั้งชื่อ pantheon.jpg โดย เลือกชนิดเป็น raw และให้เปิดภาพขึ้นมาดูว่าเป็นภาพอะไร
-
12. ให้อธิบายว่าการทำงานในข้อ 10. ทำเพื่ออะไร
- คือ ! หน้า filter เดิม เนื่องจากเรา filter อยู่ packet ที่ 16 ที่นอกเหนือจากบันเดิม
-
13. ให้เปิดไฟล์ ftp-download-good2.pcapng ให้หาคำตอบว่าเวลาที่ใช้ในการโหลดไฟล์ “SIZE OS Fingerprinting with ICMP.zip” เท่ากับเท่าไร อธิบายวิธีการ

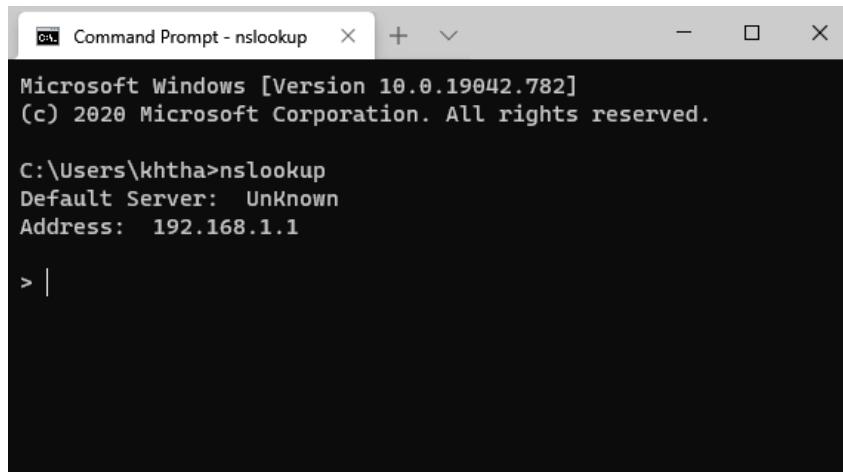


- เริ่มจากการนัด packet ที่ 16 download (คำสั่ง RETR) packet ที่ 14
 - นำตัวที่ “เริ่ม download” ถือ FTP-data ตัวแรก แล้วทำการ follow
 - ถ้า timestamps ก็ต้องๆ แล้ว apply column
 - สังเกตุว่า FTP-data ตัวแรก เวลาที่ 0.054643000
 - เลื่อนลงไปถึงสุด ณ FTP-data ตัวสุดท้าย แล้วนา Ack ที่ต่อไป packet FTP-data ข้างต่อ
 ถือ packet ที่ download เสร็จสิ้น เวลาที่ 1.382987000

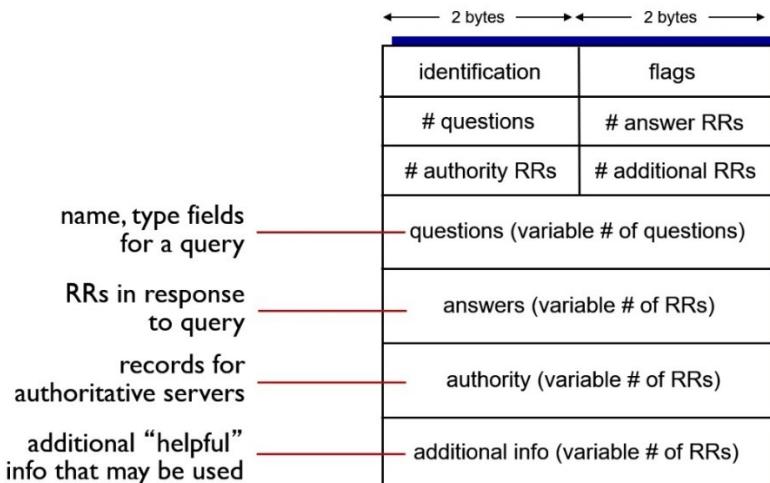
∴ เวลา download ทั้งหมด คือ 1.328344000 seconds

DNS (Domain Name System)

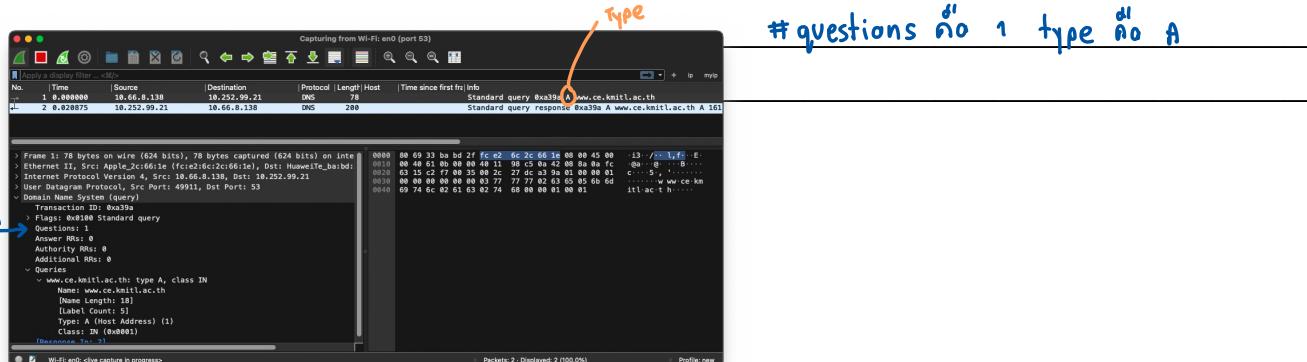
โปรโตคอล DNS จะใช้พอร์ต 53 โดยระบบปฏิบัติการส่วนใหญ่จะมีโปรแกรมชื่อว่า nslookup ซึ่งสามารถใช้ติดต่อกับ DNS Server ได้ ในการนี้ของ Windows ให้เรียก Command Prompt จากนั้นให้เรียกโปรแกรม nslookup (หากใช้ระบบปฏิบัติการอื่นก็ทำคล้ายกัน) จะปรากฏหน้าจอดังรูป



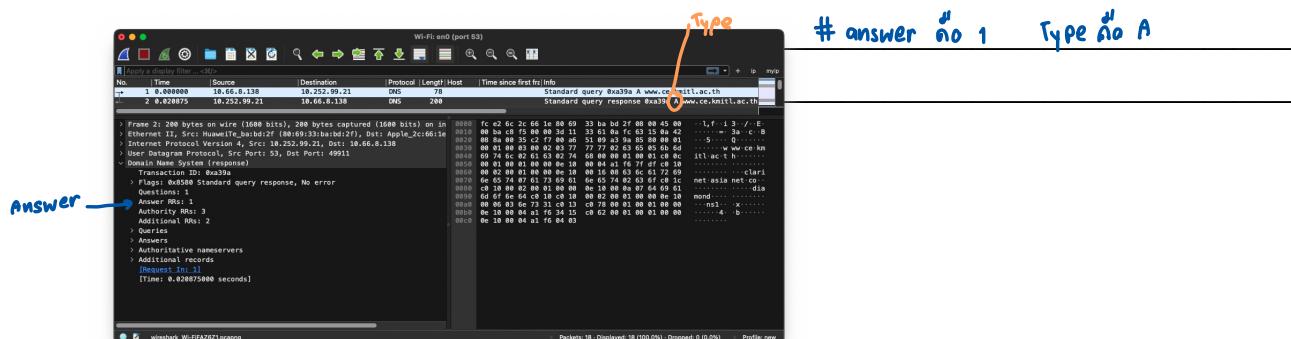
- ให้เปิดโปรแกรม Wireshark เพื่อ capture โดยกำหนดเงื่อนไขให้ capture เนพาะโปรโตคอล DNS จากนั้นในหน้าที่เรียก nslookup ไว้แล้ว ให้พิมพ์ **server 161.246.52.21** ลงไป (เป็นการกำหนดให้เชื่อมต่อกับ DNS Server ที่มี IP Address 161.246.52.21 แทน Default Server) ให้ตอบว่า 161.246.52.21 มีชื่อ Domain Name อะไร ns1.kmitl.ac.th



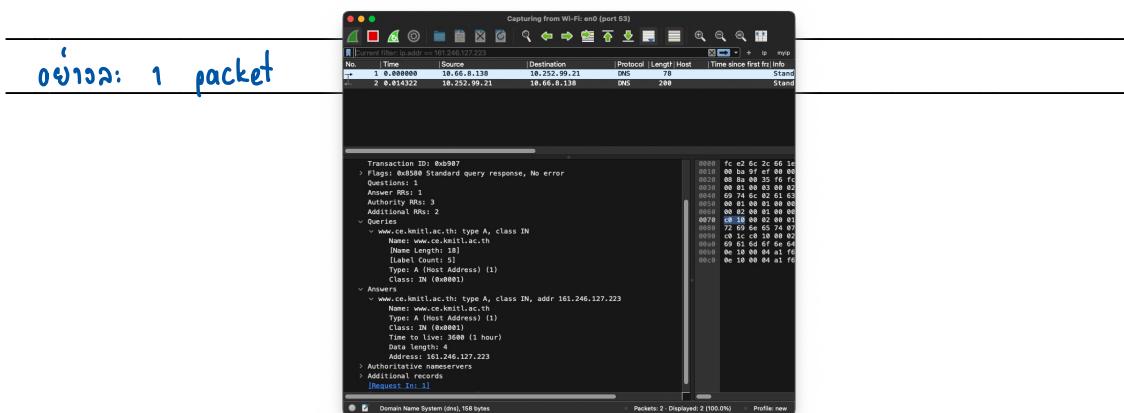
- ให้พิมพ์ www.ce.kmitl.ac.th ป้อนให้กับโปรแกรม nslookup จากนั้นหยุด capture และตอบคำถามดังนี้
 - ใน DNS query มี # questions เท่าไร และข้อมูลใน questions คืออะไร type เป็นค่าอะไร ให้บันทึก screenshot ส่วนของ Packet Details Pane นำมาแสดงประกอบด้วย



- ใน DNS response มี # answer เท่าไร และข้อมูลใน answer คืออะไร ให้บันทึก screenshot ส่วนของ Packet Details Pane ประกอบด้วย



- มี query และ response กี่ packet ให้บันทึก screenshot ส่วนของ Packet Details Pane ด้วย



- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

query กี่ packet response กี่

Authority : 2 - แบบ Name Server

additional : 3 - แบบ IP Address ของ Name Server

- ใน DNS query มี # questions เท่าไร และข้อมูลใน questions คืออะไร type เป็นค่าอะไร ให้บันทึก screenshot ส่วนของ Packet Details Pane นำมาแสดงประกอบด้วย

#questions ถ้า 1

Type PTR

```

Capturing from Wi-Fi: en0 (port 63)
No. Time Source Destination Protocol Length Host Time since first tx: Info
1 0.000000 10.66.8.138 18.252.99.21 DNS 88 Standard query 0x0f18 PTR 223.127.246.161.in-addr.arpa
2 0.004276 10.252.99.21 10.66.8.138 DNS 278 Standard query response 0x0f18 PTR 223.127.246.161.in-addr.arpa PTR ce.kmilt.ac.th

> Frame 1: 88 bytes on wire (696 bits), 88 bytes captured (696 bits) on interface en0, interface 1, source Apple_2c:66:1c (fc:ee:02:c2:66:1c), destination Huawei_8c:43:31 (00:0c:29:43:31:0f)
> Internet Protocol Version 4, Src: 10.66.8.138, Dst: 10.252.99.21
> User Datagram Protocol, Src Port: 53, Dst Port: 53
> Domain Name System, Transaction ID: 0x0f18
> Flags: 0x0000 Standard query
> Questions: 1
> Flags: 0x0000 Standard query
> Authority RRs: 0
> Additional RRs: 0
> Queries: 1
> Response: 1

Number of queries in packet (dns.count.queries), 2 bytes
Packets: 2 - Displayed: 2 (100.0%)
Profile: new
  
```

- ใน DNS response มี # answer เท่าไร และข้อมูลใน answer คืออะไร ให้บันทึก screenshot ส่วนของ Packet Details Pane ประกอบด้วย

Answer ถ้า 2

Type PTR

```

Capturing from Wi-Fi: en0 (port 63)
No. Time Source Destination Protocol Length Host Time since first tx: Info
1 0.000000 10.66.8.138 18.252.99.21 DNS 88 Standard query 0x0f18 PTR 223.127.246.161.in-addr.arpa
2 0.004276 10.252.99.21 10.66.8.138 DNS 278 Standard query response 0x0f18 PTR 223.127.246.161.in-addr.arpa PTR ce.kmilt.ac.th

> Frame 2: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits) on interface en0, interface 1, source Apple_2c:66:1c (fc:ee:02:c2:66:1c), destination Huawei_8c:43:31 (00:0c:29:43:31:0f)
> Internet Protocol Version 4, Src: 10.252.99.21, Dst: 10.66.8.138
> User Datagram Protocol, Src Port: 53, Dst Port: 53
> Domain Name System, Transaction ID: 0x0f18
> Flags: 0x0000 Standard query response, No error
> Questions: 1
> Answers: 2
> Authority RRs: 4
> Additional RRs: 3
> Queries: 1
> Answers: 2
> Authoritative nameservers
> Additional records
> Request In: 1
> Time: 0.004276000 seconds

Number of answers in packet (dns.count.answers), 2 bytes
Packets: 2 - Displayed: 2 (100.0%)
Profile: new
  
```

- มี query และ response กี่ packet ให้บันทึก screenshot ส่วนของ Packet Details Pane ด้วย

อย่างน้อย 1 packet

Type PTR

```

Capturing from Wi-Fi: en0 (port 63)
No. Time Source Destination Protocol Length Host Time since first tx: Info
1 0.000000 10.66.8.138 18.252.99.21 DNS 88 Standard query 0x0f18 PTR 223.127.246.161.in-addr.arpa
2 0.004276 10.252.99.21 10.66.8.138 DNS 278 Standard query response 0x0f18 PTR 223.127.246.161.in-addr.arpa PTR ce.kmilt.ac.th

> Frame 2: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits) on interface en0, interface 1, source Apple_2c:66:1c (fc:ee:02:c2:66:1c), destination Huawei_8c:43:31 (00:0c:29:43:31:0f)
> Internet Protocol Version 4, Src: 10.252.99.21, Dst: 10.66.8.138
> User Datagram Protocol, Src Port: 53, Dst Port: 53
> Domain Name System, Transaction ID: 0x0f18
> Flags: 0x0000 Standard query response, No error
> Questions: 1
> Answers: 2
> Authority RRs: 4
> Additional RRs: 3
> Queries: 1
> Answers: 2
> Authoritative nameservers
> Additional records
> Request In: 1
> Time: 0.004276000 seconds

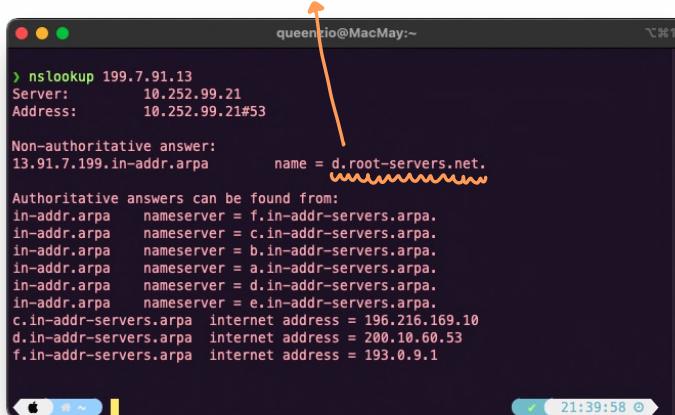
Number of answers in packet (dns.count.answers), 2 bytes
Packets: 2 - Displayed: 2 (100.0%)
Profile: new
  
```

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

query กี่ กี่ response กี่ Authority : 4 - แบบ Name Server

additional : 3 - แบบ IP Address ของ Name Server

17. ให้ใช้โปรแกรม nslookup และตั้ง server เป็น 199.7.91.13 จากนั้นให้ป้อน 199.7.91.13 โปรแกรมแสดงผลอะไรมาบ้าง ให้บันทึก screenshot มาแสดง นักศึกษาติดว่า 199.7.91.13 เป็น server อะไร
- d.root-servers.net คือ เป็น root server



```

> nslookup 199.7.91.13
Server:      10.252.99.21
Address:     10.252.99.21#53

Non-authoritative answer:
13.91.7.199.in-addr.arpa      name = d.root-servers.net.

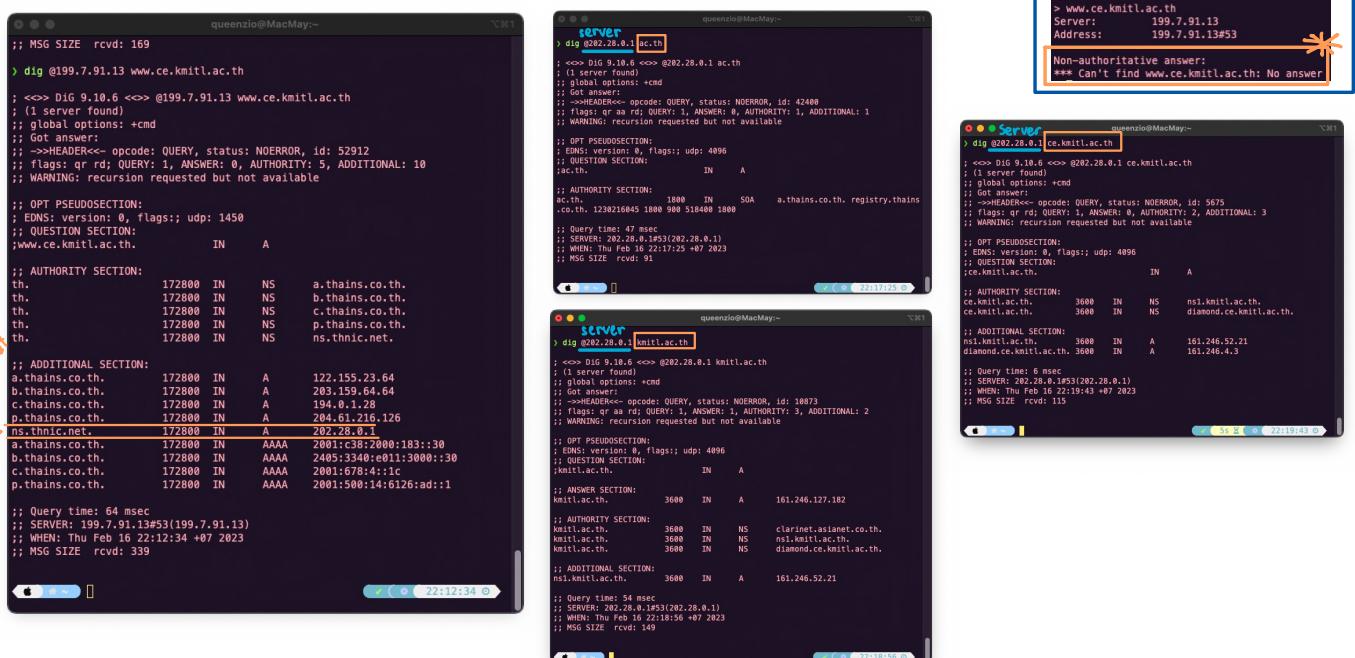
Authoritative answers can be found from:
in-addr.arpa      nameserver = f.in-addr-servers.arpa.
in-addr.arpa      nameserver = c.in-addr-servers.arpa.
in-addr.arpa      nameserver = b.in-addr-servers.arpa.
in-addr.arpa      nameserver = a.in-addr-servers.arpa.
in-addr.arpa      nameserver = d.in-addr-servers.arpa.
in-addr.arpa      nameserver = e.in-addr-servers.arpa.
c.in-addr-servers.arpa  internet address = 196.216.169.10
d.in-addr-servers.arpa  internet address = 200.10.60.53
f.in-addr-servers.arpa  internet address = 193.0.9.1

```

18. ให้ป้อน query เป็น www.ce.kmitl.ac.th แสดงผลอะไรมาบ้าง ให้บันทึก screenshot มาแสดง จากนั้นให้ใช้ IP Address ของ ns.thnic.net เป็น server และป้อน query เป็น ac.th, kmitl.ac.th และ ce.kmitl.ac.th ตามลำดับ ให้บันทึก screenshot มาแสดง และให้นักศึกษาตรวจสอบการทำการ name resolution ของ www.ce.kmitl.ac.th โดยสมมติให้เครื่องที่ request เป็นเครื่องที่อยู่ต่างประเทศ

* 98 dig 98: mac 98 nslookup ไม่สามารถ query ได้ จังแบบนี้ด้วย →

Tip ns.thnic.net



```

;; MSG SIZE rcvd: 169
> dig @199.7.91.13 www.ce.kmitl.ac.th
; (1 server found)
; global options: +cmd
; Got answer:
;-->HEADER<-- opcode: QUERY, status: NOERROR, id: 52912
; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 10
; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1450
;; SECTION: QUESTION
;www.ce.kmitl.ac.th. IN A
;; AUTHORITY SECTION:
th.          172800 IN  NS   a.thains.co.th.
th.          172800 IN  NS   b.thains.co.th.
th.          172800 IN  NS   c.thains.co.th.
th.          172800 IN  NS   p.thains.co.th.
th.          172800 IN  NS   ns.thnic.net.

;; ADDITIONAL SECTION:
a.thains.co.th. 172800 IN  A   122.155.23.64
b.thains.co.th. 172800 IN  A   203.159.64.64
c.thains.co.th. 172800 IN  A   194.11.1.28
p.thains.co.th. 172800 IN  A   204.51.216.126
ns.thnic.net.   172800 IN  A   202.28.0.1

;; Query time: 64 msec
;; SERVER: 199.7.91.13#53(199.7.91.13)
;; WHEN: Thu Feb 16 22:12:34 +07 2023
;; MSG SIZE rcvd: 339


```



```

server
> dig @202.28.0.1 ac.th
; (1 server found)
; global options: +cmd
; Got answer:
;-->HEADER<-- opcode: QUERY, status: NOERROR, id: 42488
; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 4096
;; SECTION: QUESTION
;ac.th.           IN  A
;; AUTHORITY SECTION:
ac.th.          1800  IN  SOA  a.thains.co.th. registry.thains
.co.th.         1230210645 1800 900 518400 1800

;; Query time: 47 msec
;; SERVER: 202.28.0.1#53(202.28.0.1)
;; WHEN: Thu Feb 16 22:17:25 +07 2023
;; MSG SIZE rcvd: 91


```



```

server
> dig @202.28.0.1 kmitl.ac.th
; (1 server found)
; global options: +cmd
; Got answer:
;-->HEADER<-- opcode: QUERY, status: NOERROR, id: 5675
; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 3
; WARNING: recursion requested but not available

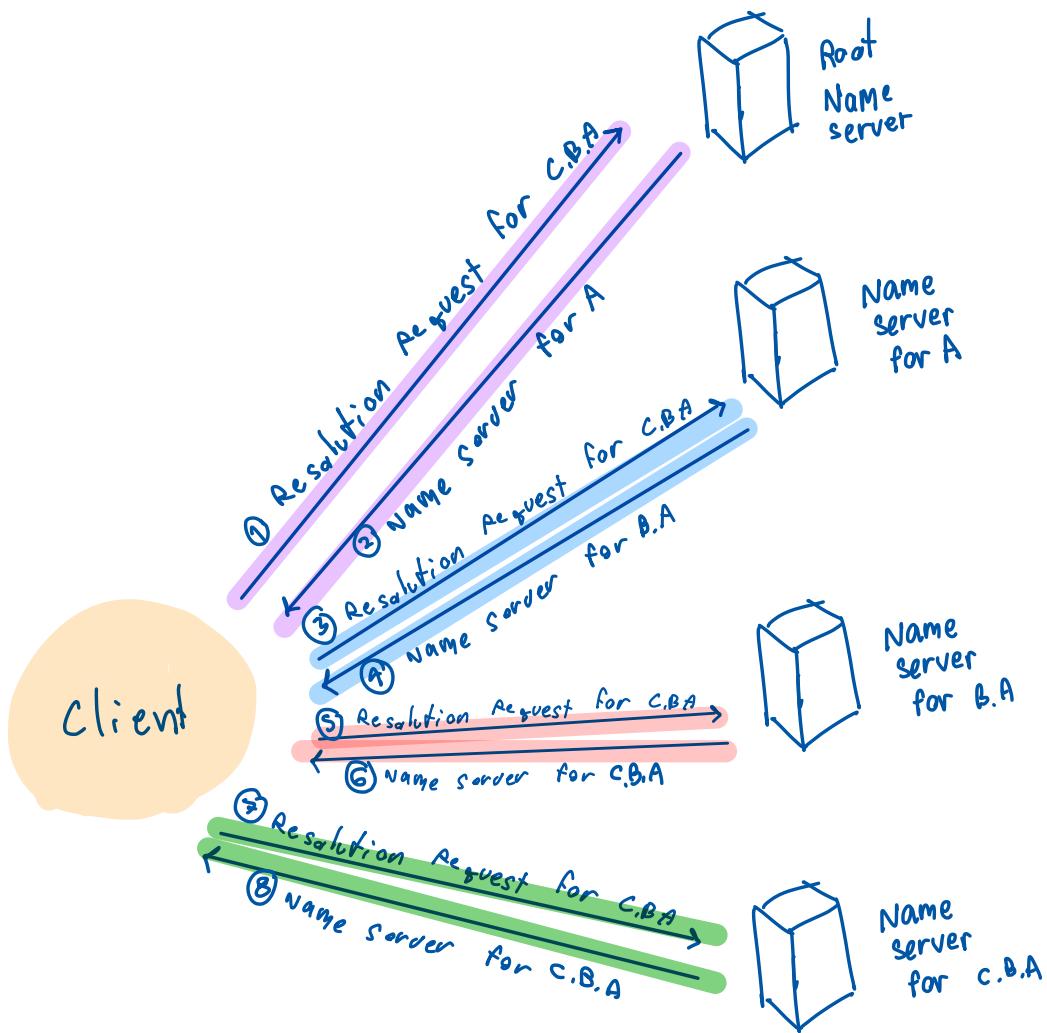
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 4096
;; SECTION: QUESTION
;ce.kmitl.ac.th. IN  A
;ce.kmitl.ac.th. 3600  IN  NS   ns1.kmitl.ac.th.
;ce.kmitl.ac.th. 3600  IN  NS   diamond.ce.kmitl.ac.th.

;; AUTHORITY SECTION:
ce.kmitl.ac.th. 3600  IN  NS   ns1.kmitl.ac.th.
ce.kmitl.ac.th. 3600  IN  NS   diamond.ce.kmitl.ac.th.

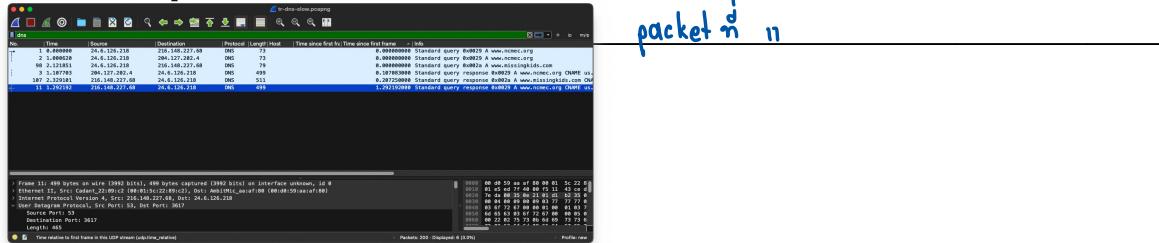
;; ADDITIONAL SECTION:
ns1.kmitl.ac.th. 3600  IN  A   161.246.52.21
diamond.ce.kmitl.ac.th. 3600  IN  A   161.246.4.3

;; Query time: 6 msec
;; SERVER: 202.28.0.1#53(202.28.0.1)
;; WHEN: Thu Feb 16 22:19:43 +07 2023
;; MSG SIZE rcvd: 113


```



19. ให้เปิดไฟล์ tr-dns-slow.pcapng และหา packet response ของ DNS แล้วขยายส่วนที่เป็น DNS หาข้อมูลเวลา จากนั้นให้สร้างเป็นคอลัมน์ ตั้งชื่อเป็น DNS Delta
20. ให้ sort แล้วดูว่ามี DNS query/response ใด ที่ใช้เวลาเกิน 1 วินาที ให้บันทึก screenshot มาแสดง



21. ให้เปิด Wireshark เพื่อ capture ใหม่ โดยให้ดักจับเฉพาะข้อมูล DNS จากนั้นให้ใช้โปรแกรม nslookup โดยให้กำหนด 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 ให้เบริรยบเทียบ DNS Delta ที่ได้จากแต่ละ server (แสดงตัวเลขที่ได้) จากนั้นให้วิเคราะห์ผล

1 15.10.46.98	161.246.4.3	DNS	85	0.00000000 Standard query 0xfa48 A ce.kmitl.ac.th OPT
2 161.246.4.3	15.10.46.98	DNS	207	0.00000000 Standard query response 0xfa48 A ce.kmitl.ac.th A 161.246.127.223 NS clarinet.a
3 15.10.46.98	161.246.52.21	DNS	85	0.00000000 Standard query 0x275c A ce.kmitl.ac.th OPT
4 161.246.52.21	15.10.46.98	DNS	207	0.0213550000 Standard query response 0x275c A ce.kmitl.ac.th A 161.246.127.223 NS diamond.ce
5 15.10.46.98	8.8.8.8	DNS	85	0.00000000 Standard query 0x7469 A ce.kmitl.ac.th OPT
6 8.8.8.8	15.10.46.98	DNS	101	0.0003160000 Standard query response 0x7469 A ce.kmitl.ac.th A 161.246.127.223 OPT

161.246.4.3 < 161.246.52.21 < 8.8.8.8

งานครั้งที่ 5

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา ตามด้วย section และ _lab05 ตามตัวอย่างต่อไปนี้
64019999_sec20_lab05.pdf
- กำหนดส่ง ภายในวันที่ 17 กุมภาพันธ์ 2566 โดยให้ส่งใน Microsoft Teams ของรายวิชา