

Question A :

```
PS C:\Users\HP> nslookup www.iitb.ac.in
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name: www.iitb.ac.in
Address: 103.21.124.10
```

(รูปภาพ A ประกอบคำตอบข้อที่ 1-3)

- 1) จง ใช้ nslookup เพื่อ หาหมายเลข IP ของ web server ของ Indian Institute of Technology in Bombay India ซึ่งมี URL คือ www.iitb.ac.in หมายเลข IP ที่ได้คือหมายเลขใด

Answer www.iitb.ac.in มีaddressเป็น 103.21.124.10

- 2) หมายเลข IP ของ DNS server ที่ส่งคำตอบ มาให้จากการรัน nslookup ตาม 1) คือหมายเลขใด

Answer DNS server มีหมายเลข address คือ 192.168.1.1

- 3) คำตอบที่ได้จากการรัน nslookup ตาม 1) มาจาก authoritative server หรือ non-authoritative server?

Answer คำตอบมาจาก non-authoritative server

```
PS C:\Users\HP> nslookup -type=NS www.iitb.ac.in
Server: UnKnown
Address: 192.168.1.1

iitb.ac.in
primary name server = dns1.iitb.ac.in
responsible mail addr = postmaster.iitb.ac.in
serial = 2013071001
refresh = 16384 (4 hours 33 mins 4 secs)
retry = 2048 (34 mins 8 secs)
expire = 1048576 (12 days 3 hours 16 mins 16 secs)
default TTL = 3960 (1 hour 6 mins)
```

(รูปภาพ B ประกอบคำตอบข้อที่4)

```
PS C:\Users\HP> nslookup www.iitb.ac.in dns1.iitb.ac.in
Server: dns1.iitb.ac.in
Address: 103.21.125.129

Name: www.iitb.ac.in
Address: 103.21.124.10
```

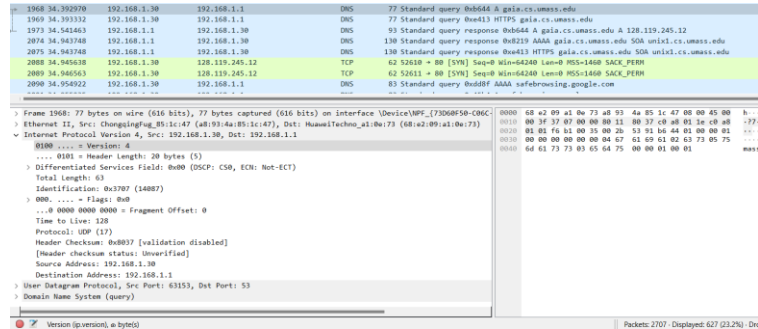
(รูปภาพ C ประกอบคำตอบข้อที่4)

- 4) จง ใช้ nslookup เพื่อหา hostname ของ authoritative name server ของ iitb.ac.in ว่า ชื่ออะไร? หากมีมากกว่าหนึ่ง server ชื่อ name server ไหนเป็นชื่อแรก? และถ้าต้อง หาหมายเลข IP ของ authoritative name server ดังกล่าวจะต้องทำอย่างไร

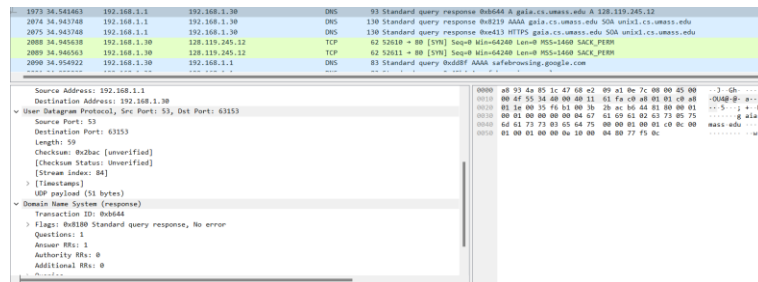
Answer authoritative name server ของ iitb.ac.in มีเพียง server เดียวคือ dns1.iitb.ac.in โดย

หมายเลข ip address สามารถหาได้ดังรูป C

Question C



(รูปภาพ D ใช้ประกอบการตอบคำถามข้อ 5)



(รูปภาพ E ใช้ประกอบการตอบคำถามข้อ 6)

- 5) ค้นหา DNS query ที่ส่งออกไปเพื่อขอแปลงชื่อ gaia.cs.umass.edu จงระบุว่า หมายเลขของ packet ดังกล่าวเป็นเลขอะไร? DNS query ดังกล่าวส่ง ผ่าน Transport Layer Protocol ไດ?

Answer packet ดังกล่าวหมายเลข 1968 และมีการส่งผ่านด้วย User Datagram Protocol (UDP) ดังรูป D

- 6) ค้นหา DNS response ที่ตอบกลับ query ในข้อ 5) จงระบุว่าหมายเลขของ packet ดังกล่าวเป็นเลขอะไร? DNS response ดังกล่าวส่งผ่าน Transport Layer Protocol ไດ?

Answer packet ดังกล่าวหมายเลข 1973 และมีการส่งผ่านด้วย User Datagram Protocol (UDP) ดังรูป E

- 7) หมายเลข port ปลายทาง ของ DNS query message เป็นหมายเลขใด? หมายเลข port ต้นทางของ DNS response message เป็นหมายเลขใด?

Answer จากรูป D ใน packet detail pane ตรง UDP จะเห็นว่า destination port เป็น 53 และจากรูป E จะเห็นว่าใน packet detail pane ตรง UDP จะมี source port เป็น 53 เช่นเดียวกัน

- 8) DNS query ถูกส่งไปที่หมายเลข IP ปลายทางหมายเลขใด?

Answer จะเห็นว่าในรูป D ที่ packet detail pane ตรง internet protocol จะมี destination address เป็น 192.168.1.1

```

Domain Name System (query)
Transaction ID: 0xb644
Flags: 0x0100 Standard query
  0... .. = Response: Message is a query
  .000 0... .. = Opcode: Standard query (0)
  .... 0... .. = Truncated: Message is not truncated
  .... 1... .. = Recursion desired: Do query recursively
  .... 0... .. = Z: reserved (0)
  .... 0... .. = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  > gaia.cs.umass.edu: type A, class IN
  [Response In: 1973]
```

(รูปภาพ F ประกอบการตอบคำถามข้อที่ 9)

```

Domain Name System (response)
Transaction ID: 0xb644
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
  > gaia.cs.umass.edu: type A, class IN
    Name: gaia.cs.umass.edu
    [Name Length: 17]
    [Label Count: 4]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
Answers
  > gaia.cs.umass.edu: type A, class IN, addr 128.119.245.12
```

(รูปภาพ G ประกอบคำตอบข้อที่ 9)

9) ตรวจสอบ DNS query message โดยค้นข้อมูลใน Packet Details Pane จงหาว่า มี จำนวนคำถาม (Questions) กี่คำถาม เป็นคำถามอะไรบ้าง? และมีจำนวน records คำตอบ (Answers) กี่คำตอบ? เป็นคำตอบอะไรบ้าง?

Answer จาก Queries ใน packet detail pane จะที่คำถามเพียงคำถามเดียวคือ ip address ของ domain gaia.cs.umass.edu คืออะไร (จากรูปภาพ F) และ records คำตอบมีจำนวน 1 คำตอบ โดยตอบว่า address ของ domain gaia.cs.umass.edu คือ 128.119.245.12 (จากรูป G)

10) ตรวจสอบ DNS response message โดยค้นข้อมูลใน Packet Details Pane จงหาว่ามีจำนวนคำถาม (Questions) กี่คำถาม? เป็นคำถามอะไรบ้าง? และมีจำนวน records คำตอบ (Answers) กี่คำตอบ? เป็นคำตอบอะไรบ้าง?

11) a. Answer หมายเลข 2155 ดังรูปด้านล่าง

b. Answer หมายเลข 1968 ดังรูป D

c. Answer หมายเลข 1973 ดังรูป E

d. Answer หมายเลข 2212 ดังรูปด้านล่าง

e. Answer หมายถึง 1968 ดังรูป D

นาย พิทักษ์พงษ์ สว่างศ์นาม 65010745 sec 17

Question D

271 44.071279	192.168.1.30	192.168.1.1	DNS	78 Standard query 0xe0bf A www.cics.umass.edu
272 44.071467	192.168.1.30	192.168.1.1	DNS	78 Standard query 0xa2c2 HTTPS www.cics.umass.edu
273 44.090920	192.168.1.1	192.168.1.30	DNS	135 Standard query response 0x81e6 AAAA www.cics.umass.edu SOA unix1.cs.umass.edu
274 44.100008	2403:6200:8832:dc15::...	2404:6800:4001:810::...	QUIC	94 Protected Payload (KP0), DCID=F64549d1bba8bd0a
275 44.100649	2404:6800:4001:800::...	2403:6200:8832:dc15::...	QUIC	163 Protected Payload (KP0)
276 44.100649	2404:6800:4001:800::...	2403:6200:8832:dc15::...	QUIC	83 Protected Payload (KP0)
277 44.101051	2403:6200:8832:dc15::...	2404:6800:4001:800::...	QUIC	97 Protected Payload (KP0), DCID=ff65c0422d614ff5
278 44.126230	2404:6800:4001:810::...	2403:6200:8832:dc15::...	QUIC	86 Protected Payload (KP0)
279 44.126628	2403:6200:8832:dc15::...	2404:6800:4001:800::...	QUIC	94 Protected Payload (KP0), DCID=ff65c0422d614ff5
280 44.156291	2404:6800:4001:800::...	2403:6200:8832:dc15::...	QUIC	86 Protected Payload (KP0)
281 44.260491	192.168.1.1	192.168.1.30	DNS	135 Standard query response 0x4051 AAAA www.cics.umass.edu SOA unix1.cs.umass.edu
282 44.270542	192.168.1.1	192.168.1.30	DNS	94 Standard query response 0x9f0a A www.cics.umass.edu A 128.119.240.84

(รูป H ประกอบการตอบคำถามข้อที่ 12-13)

- 12) หมายเลข port ปลายทาง ของ DNS query message เป็นหมายเลขใด? หมายเลข port ต้นทางของ DNS response message เป็นหมายเลขใด?

Answer หมายเลข port ปลายทาง ของ DNS query message และ DNS response message คือ 53 โดยสังเกตได้จาก transport layer protocol (UDP)

- 13) DNS query ถูกส่งไปที่หมายเลข IP ปลายทางหมายเลขใด? เป็นหมายเลข IP ของ default local DNS server ในเครือข่ายของผู้เรียนหรือไม่?

Answer DNS query ถูกส่งไปที่หมายเลข IP 192.168.1.1 โดยเป็นหมายเลข default local DNS server ในเครือข่าย

- 14) ตรวจสอบ DNS query message ในข้อ 13) จงหาว่าประเภท (Type) ของ DNS query เป็นประเภทใด? ใน query ดังกล่าวมีข้อมูลส่วน records คำตอบ (Answers) ด้วยหรือไม่? หากมี คำตอบดังกล่าวมีข้อมูลใดบ้าง?

Answer DNS query message เป็น Type A (ระบุที่ field Queries ใน UDP protocol) โดย query ดังกล่าวไม่มีข้อมูลส่วน records เลย

The image shows a Wireshark packet capture. The packet list on the left shows a DNS query (282) and a DNS response (283). The packet details pane for the response (283) shows the query type as A and the answer as 128.119.240.84. The packet bytes pane on the right shows the raw data of the response.

(รูป I ประกอบการตอบคำถามข้อที่ 15)

- 15) ตรวจสอบ DNS response message ที่ตอบกลับ query ในข้อ 13) โดยค้นข้อมูลใน Packet Details Pane จงหาว่ามีจำนวนคำถาม (Questions) กี่คำถาม? เป็นคำถามอะไรบ้าง? และมีจำนวน records คำตอบ (Answers) กี่คำตอบ? เป็นคำตอบอะไรบ้าง?

Answer โดยจำนวนคำถามมี 1 คำถาม(จาก field Questions ใน DNS)และเป็นคำถาม Type A หมายความว่าถามถึง address ของ domain และคำตอบมีคำตอบเดียว (จาก field Answer RRs) โดยคำตอบบอก class,address,ttl และ data length (bytes) ของคำถามใน query

Question E

55 27.152283	192.168.1.30	192.168.1.1	DNS	69 Standard query 0x0002 NS umass.edu
56 27.208373	192.168.1.1	192.168.1.30	DNS	123 Standard query response 0x0002 NS umass.edu NS ns1.umass.edu NS ns3.umass.edu NS ns2.umass.edu

Frame 55: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{73D6B5B-08C-0010-8000-000000000000} (08:00:00:00:00:00:00:00) on interface \Device\NPF_{73D6B5B-08C-0010-8000-000000000000} (08:00:00:00:00:00:00:00)	0000 68 e2 09 a1 0e 73 a8 93 4a 85 1c 47 00 00 45 00 h...e...3...G...E...
Ethernet II, Src: ChongqingHu...55:1c:47 (a8:93:4a:85:1c:47), Dst: HuaweiTechno...a1:0e:73 (08:00:00:00:00:00:00:00)	0010 00 37 40 6d 00 00 00 11 76 d9 c8 a8 01 1c c8 a8 78m...c...y...v...r...w...u...mass.edu
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 192.168.1.1	0020 01 01 fa 50 00 35 00 23 2f 8b 00 02 01 00 00 01 ...P.S.#...#...#...#...
.... 0101 = Version: 4	0030 00 00 00 00 00 00 05 75 dd 61 73 73 03 65 64 75
.... 0101 = Header Length: 20 bytes (5)	0040 00 00 02 00 01
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 55	
Identification: 0x0000 (16493)	
> 000... = Flags: 0x0	
...0 0000 0000 0000 = Fragment Offset: 0	
Time to Live: 128	
Protocol: UDP (17)	
Header Checksum: 0x76d9 [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 192.168.1.30	
Destination Address: 192.168.1.1	
> User Datagram Protocol, Src Port: 64888, Dst Port: 53	
Source Port: 64888	
Destination Port: 53	

(รูป J ประกอบการตอบคำถามข้อที่ 16)

16) DNS query ถูกส่งไปที่หมายเลข IP ปลายทางหมายเลขใด? เป็นหมายเลข IP ของ default local DNS server ในเครือข่ายของผู้เรียนหรือไม่?

Answer หมายเลข address 192.168.1.1 (จาก internet protocol ที่ field destination source)เป็นหมายเลข หมายเลข IP ของ default local DNS server

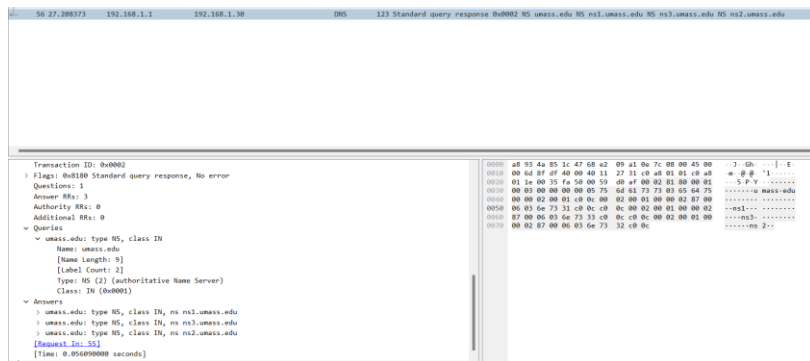
55 27.152283	192.168.1.30	192.168.1.1	DNS	69 Standard query 0x0002 NS umass.edu
56 27.208373	192.168.1.1	192.168.1.30	DNS	123 Standard query response 0x0002 NS umass.edu NS ns1.umass.edu NS ns3.umass.edu NS ns2.umass.edu

Destination Address: 192.168.1.1	0000 68 e2 09 a1 0e 73 a8 93 4a 85 1c 47 00 00 45 00 h...e...3...G...E...
> User Datagram Protocol, Src Port: 64888, Dst Port: 53	0010 00 37 40 6d 00 00 00 11 76 d9 c8 a8 01 1c c8 a8 78m...c...y...v...r...w...u...mass.edu
Source Port: 64888	0020 01 01 fa 50 00 35 00 23 2f 8b 00 02 01 00 00 01 ...P.S.#...#...#...#...
Destination Port: 53	0030 00 00 00 00 00 00 05 75 dd 61 73 73 03 65 64 75
Length: 35	0040 00 00 02 00 01
Checksum: 0x2f8b [unverified]	
[Checksum Status: Unverified]	
[Stream Index: 53]	
> [Timestamp]	
UDP payload (27 bytes)	
> Domain Name System (query)	
Transaction ID: 0x0002	
> Flags: 0x0000 Standard query	
Questions: 1	
Answer RRs: 0	
Authority RRs: 0	
Additional RRs: 0	
> Queries	
[Response In: 56]	

(รูปภาพ K ประกอบการตอบคำถามข้อที่ 17)

17) ตรวจสอบ DNS query message จงหาว่าประเภท (Type) ของ DNS query เป็นประเภทใด? ใน query ดังกล่าวมีข้อมูลส่วน records คำตอบ (Answers) ด้วยหรือไม่? หากมี คำตอบดังกล่าวมีข้อมูลใดบ้าง?

Answer DNS query เป็นประเภท NS (จาก field Queries ใน DNS ที่ packet details pane) โดยไม่มีข้อมูลส่วน records คำตอบเลย



(รูปภาพ L ประกอบการตอบคำถามข้อที่18)

18) ตรวจสอบ DNS response message ที่ตอบกลับ โดยค้นข้อมูลใน Packet Details Pane จงหาว่ามีจำนวน records คำตอบ (Answers) กี่คำตอบ? เป็นคำตอบอะไรบ้าง? มีจำนวน additional resource records มาด้วยเป็นจำนวนกี่ resource records? มีข้อมูลอะไรบ้างใน additional resource records เหล่านั้น? Answer จำนวน records มี 3 คำตอบ (จาก field Answer RRs ใน DNS ที่ packet details pane) โดยแต่ละคำตอบประกอบไปด้วย data length, name Server, ttl, class ซึ่งมีรายละเอียดดังรูปด้านล่าง

▼ Answers

▼ umass.edu: type NS, class IN, ns ns1.umass.edu

Name: umass.edu
Type: NS (2) (authoritative Name Server)
Class: IN (0x0001)
Time to live: 647 (10 minutes, 47 seconds)
Data length: 6

Name Server: ns1.umass.edu

▼ umass.edu: type NS, class IN, ns ns3.umass.edu

Name: umass.edu
Type: NS (2) (authoritative Name Server)
Class: IN (0x0001)
Time to live: 647 (10 minutes, 47 seconds)
Data length: 6

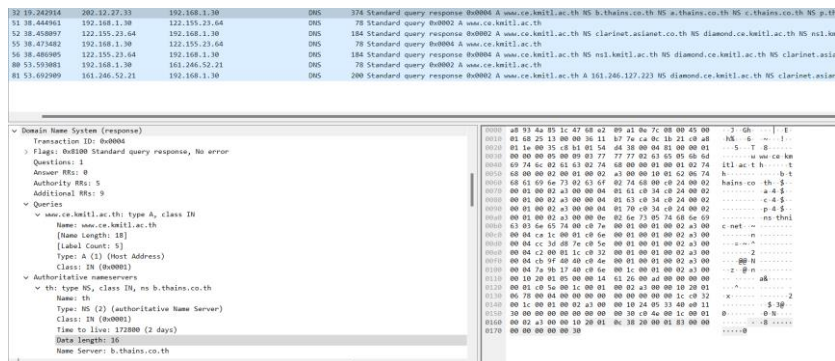
Name Server: ns3.umass.edu

▼ umass.edu: type NS, class IN, ns ns2.umass.edu

Name: umass.edu
Type: NS (2) (authoritative Name Server)
Class: IN (0x0001)
Time to live: 647 (10 minutes, 47 seconds)
Data length: 6

Name Server: ns2.umass.edu

Question F



(รูปภาพ M ประกอบการตอบคำถามข้อที่ 19)

19) จงค้นหา packets ที่ เกิดขึ้นตาม query และ response ใน ขั้นตอนที่ 3 และ 4

a. ใน response มีการระบุจำนวน resource records ในแต่ละส่วนเป็นเท่าไร (จำนวน RRs ใน Question, Answer, Authority, และ Additional resource records)

Answer Question:1, Answer:0, Authority:5, Additional resource records:9 (โดยได้มาจาก packet details pane ที่ dns)

b. ใน response มีข้อมูลหมายเลข IP ที่ ผู้ถามคำถามต้องการหรือไม่? ใน Authority และ Additional resource records name server ของ response ที่ส่งกลับมามีข้อมูลอะไรบ้าง?

Answer ไม่มีหมายเลข ip ที่ต้องการจะถาม , Authority มีข้อมูล Name, Type, Class, TTL, Data length และ name server ของแต่ละ top level domain, Additional records มี Name, Type, Class, TTL, Data length และ Address ของแต่ละ top level domain name server

c. ข้อมูล ส่วน ไใด ใน response ที่ ผู้ถามสามารถนำข้อมูลดังกล่าวไปใช้ประโยชน์ต่อ ได้ และนำไปใช้อย่างไร

Answer ในส่วนของ additional record และ authority โดยจะเอาข้อมูลของ top level domain main name server ไปหา ip ของตัว TLD เอง และสามารถไปหา Authoritative name server ต่อได้

52.38.458997	122.155.23.64	192.168.1.30	DNS	184 Standard query response 0x0002 A www.ce.kmitl.ac.th NS clarinet.asianet.co.th NS diamond.ce.kmitl.ac.th
55.38.473482	192.168.1.30	122.155.23.64	DNS	78 Standard query 0x0004 A www.ce.kmitl.ac.th
56.38.486905	122.155.23.64	192.168.1.30	DNS	184 Standard query response 0x0004 A www.ce.kmitl.ac.th NS ns1.kmitl.ac.th NS diamond.ce.kmitl.ac.th NS
80.53.593081	192.168.1.30	161.246.52.21	DNS	78 Standard query 0x0002 A www.ce.kmitl.ac.th
81.53.692909	161.246.52.21	192.168.1.30	DNS	200 Standard query response 0x0002 A www.ce.kmitl.ac.th A 161.246.127.223 NS diamond.ce.kmitl.ac.th NS

Source Address: 122.155.23.64	0000 a8 93 4a 85 1c 47 68 e2 09 a1 0e 7c 08 00 45 00	3 6h ... E
Destination Address: 192.168.1.30	0010 00 aa 6c e2 00 00 33 11 c6 bf 7a 9b 17 40 c0 a8	...1...3...2...0...
User Datagram Protocol, Src Port: 53, Dst Port: 51383	0020 01 1e 00 35 c8 67 00 96 ca 7d 00 02 01 00 00 01	...5.....}.....
Source Port: 53	0030 00 00 03 00 02 03 77 77 77 02 63 05 05 0a 6dw.....ce.....m
Destination Port: 51383	0040 69 74 6c 02 61 63 02 74 68 00 00 01 00 01 c0 13	iti-act-h.....
Length: 150	0050 00 02 00 01 00 00 1c 20 00 16 08 03 6c 61 72 69-clard
Checksum: 0xca7d [unverified]	0060 6a 65 74 07 61 73 69 61 6a 65 74 02 63 6f c0 1c	net-asia-net-co-
[Checksum Status: Unverified]	0070 c8 13 00 02 00 01 00 00 1c 20 00 0a 07 64 69 61-dia
[Stream Index: 9]	0080 6d 6f 6a 64 c0 10 c0 13 00 02 00 01 00 00 1c 20	end.....
[Timestamps]	0090 00 06 03 6a 73 31 c0 13 c0 68 00 01 00 01 00 00	...ns1...-sh.....
UDP payload (142 bytes)	00a0 1c 20 00 04 a1 f6 34 15 c0 52 00 01 00 01 00 00	...-4...-R.....
Domain Name System (response)	00b0 1c 20 00 04 a1 f6 04 03

Transaction ID: 0x0002	Flags: 0x0100 Standard query response, No error
Questions: 1	Answer RRs: 0
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]

(รูปภาพ N ประกอบการตอบคำถามข้อที่ 20)

20)จงค้นหา packets ที่ เกิดขึ้นตาม query และ response ใน ขั้นตอนที่ 5 และ 6

a.ใน response มีการระบุจำนวน resource records ในแต่ละส่วนเป็นเท่าไร (จำนวน RRs ใน Question , Answer, Authority, และ Additional resource records

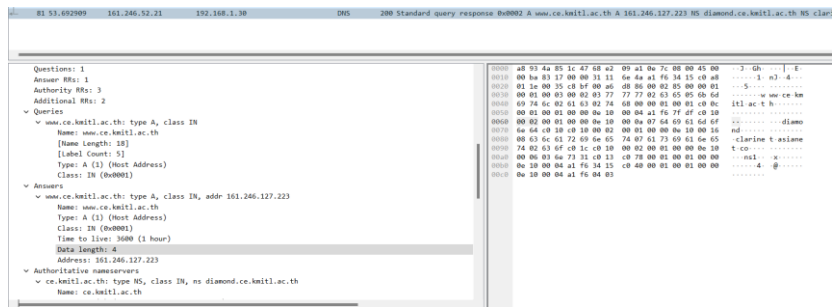
Answer Question:1,Answer:0,Authority:3,Additional resource records:2 (โดยได้มาจาก packet details pane ที่ dns)

b.ใน response มีข้อมูลหมายเลข IP ที่ ผู้ถามคำถามต้องการหรือไม่? ใน Authority และ Additional resource records ของ response ที่ส่งกลับมามีข้อมูลอะไรบ้าง?

Answer ไม่มีหมายเลข ip ที่ต้องการจะถาม ,Authority มีข้อมูล Name,Type,Class,TTL,Data length และ name server ของแต่ละ Authoritative name server, Additional records มี Name,Type,Class,TTL,Data length และ Address ของแต่ละ Authoritative name server

c.ข้อมูล ส่วน ไใด ใน response ที่ ผู้ถามสามารถนำข้อมูลดังกล่าวไปใช้ประโยชน์ต่อ ได้ และนำไปใช้อย่างไร

Answer ในส่วนของ additional record และ authority โดยจะเอาข้อมูลของ Authoritative name server name server สามารถไปหา address ของ domain ที่ต้องการหาตั้งแต่แรกได้



(รูปภาพ O ประกอบการตอบคำถามข้อที่ 21)

21) จงค้นหา packets เกิดขึ้นตาม query และ response ใน ขั้นตอนที่ 7 และ 8

a. ใน response มีการระบุจำนวน resource records ในแต่ละส่วนเป็นเท่าไร (จำนวน RRs ใน Question, Answer, Authority, และ Additional resource records)

Answer Question:1, Answer:1, Authority:3, Additional resource records:2 (โดยได้มาจาก packet details pane ที่ dns)

b. ใน response มีข้อมูลหมายเลข IP ที่ผู้ถามคำถามต้องการหรือไม่? ใน Authority และ Additional resource records ของ response ที่ส่งกลับมามีข้อมูลอะไรบ้าง?

Answer มีหมายเลข IP ที่ต้องการ, Authority มีข้อมูล Name, Type, Class, TTL, Data length และ name server ของแต่ละ Authoritative name server, Additional records มี Name, Type, Class, TTL, Data length และ Address ของแต่ละ Authoritative name server

c. จากข้อมูล query และ response ชื่อ hostname ของ Authoritative Name Server ที่รับผิดชอบ ชื่อ

โดเมน kmitl.ac.th มีชื่อว่าอะไร และมี หมายเลข IP เป็น เลขอะไร

Answer Authoritative Name Server ที่รับผิดชอบ ชื่อโดเมน kmitl.ac.th มีชื่อว่า ns1.kmitl.ac.th และมีหมายเลข ip เป็น 161.246.52.21 (จาก additional records ที่ dns ใน packet details pane)

d. หมายเลข IP ของ www.ce.kmitl.ac.th มี หมายเลข IP เป็นเลขอะไร?

Answer มีหมายเลขเป็น 161.246.127.223 (จาก Answers ที่ dns ใน packet detail pane)