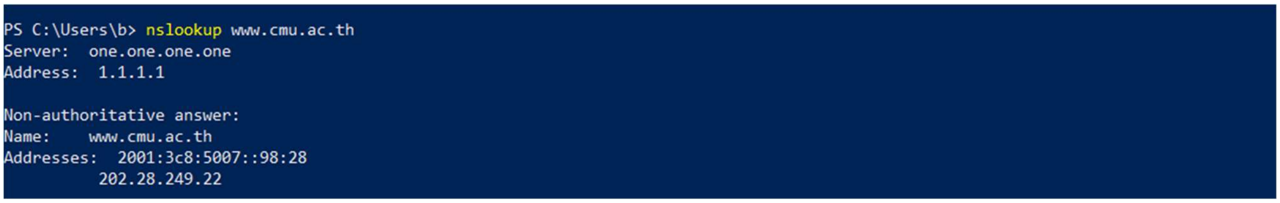
นาย เสฏฐวุฒิ ทิพย์กรรภิรมย์

61011433

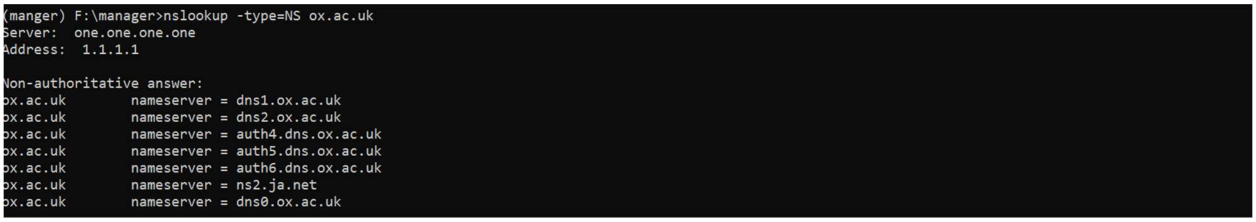
Lab3 DNS

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?



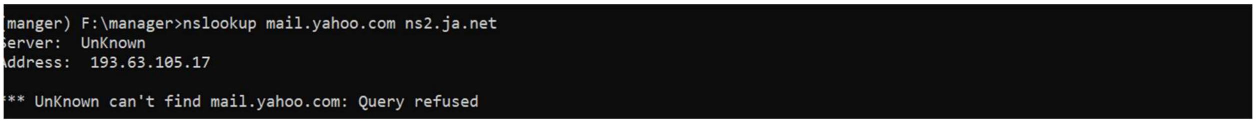
```
PS C:\Users\b> nslookup www.cmu.ac.th
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    www.cmu.ac.th
Addresses:  2001:3c8:5007::98:28
          202.28.249.22
```

2. Run nslookup to determine the authoritative DNS servers for a university in Europe.



```
(manger) F:\manager>nslookup -type=NS ox.ac.uk
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
ox.ac.uk        nameserver = dns1.ox.ac.uk
ox.ac.uk        nameserver = dns2.ox.ac.uk
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk
ox.ac.uk        nameserver = ns2.ja.net
ox.ac.uk        nameserver = dns0.ox.ac.uk
```

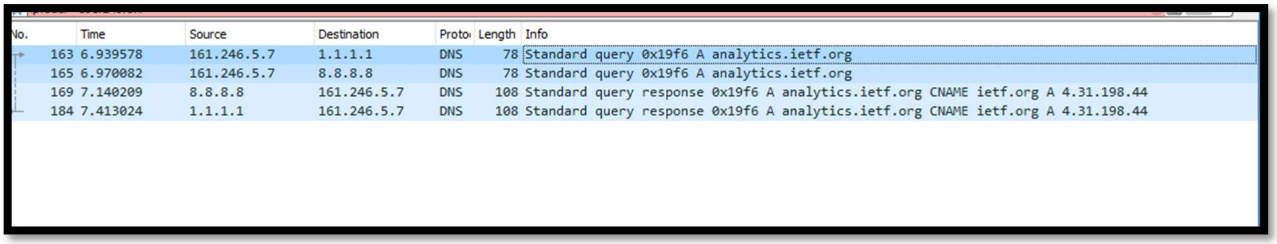
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?



```
(manger) F:\manager>nslookup mail.yahoo.com ns2.ja.net
Server:  UnKnown
Address:  193.63.105.17

*** UnKnown can't find mail.yahoo.com: Query refused
```

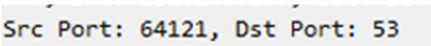
4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

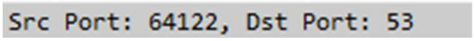
โปรโตคอล UDP มักใช้กับข้อมูลที่ต้องการความรวดเร็วและสามารถผิดพลาดได้บ้าง เช่น การรับ-ส่งข้อมูลวีดีโอสตรีมมิ่ง การรับ-ส่งข้อมูลภายในเกมออนไลน์ โปรโตคอลประยุกต์ที่นำไปใช้งาน เช่น DNS



No.	Time	Source	Destination	Proto	Length	Info
163	6.939578	161.246.5.7	1.1.1.1	DNS	78	Standard query 0x19f6 A analytics.ietf.org
165	6.970082	161.246.5.7	8.8.8.8	DNS	78	Standard query 0x19f6 A analytics.ietf.org
169	7.140209	8.8.8.8	161.246.5.7	DNS	108	Standard query response 0x19f6 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
184	7.413024	1.1.1.1	161.246.5.7	DNS	108	Standard query response 0x19f6 A analytics.ietf.org CNAME ietf.org A 4.31.198.44

5. What is the destination port for the DNS query message? What is the source port of DNS response message?

ตอนเราเป็นคนส่ง request ไป  Src Port: 64121, Dst Port: 53

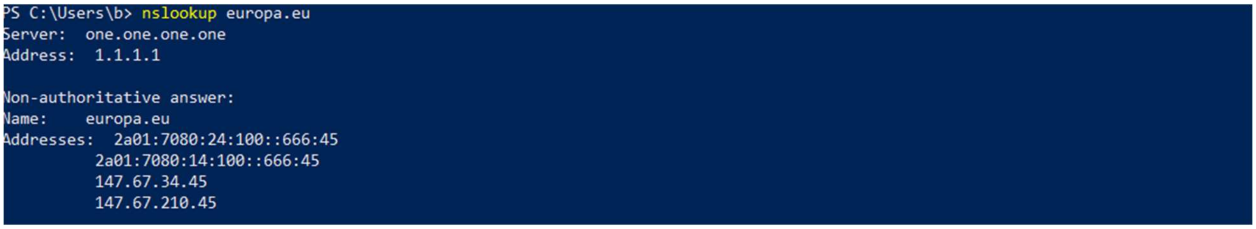
ตอนรับ response กลับมา  Src Port: 64122, Dst Port: 53

6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

นาย เสฎฐวุฒิ ทิพย์กรรภิรมย์

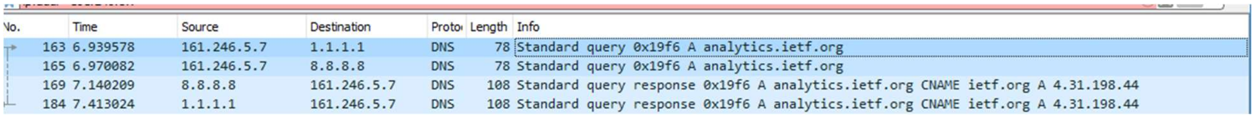
61011433

รูปด้านบนผมใช้ DNS ns1.bt.net ถ้ากลับมาใช้ของตัวเอง



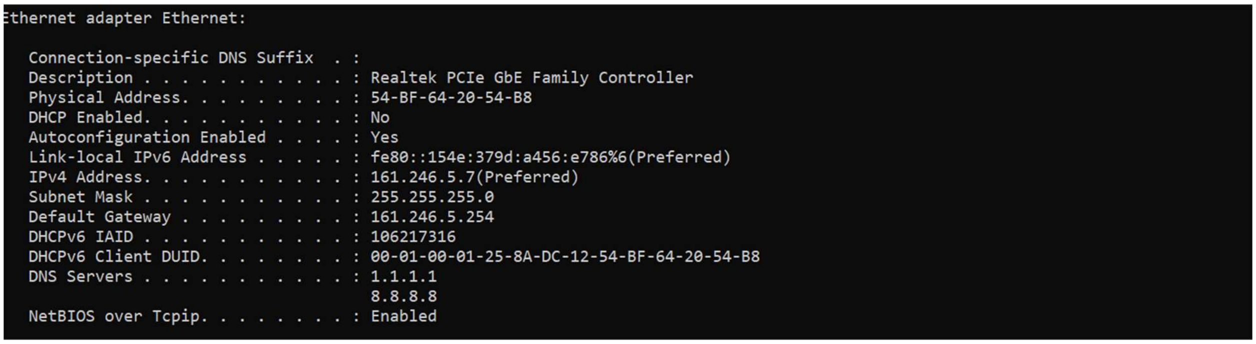
```
PS C:\Users\b> nslookup europa.eu
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    europa.eu
Addresses:  2a01:7080:24:100::666:45
          2a01:7080:14:100::666:45
          147.67.34.45
          147.67.210.45
```

ภาพใน wireshark



```
No.   Time         Source        Destination   Proto Length Info
  163 6.939578     161.246.5.7   1.1.1.1       DNS      78 Standard query 0x19f6 A analytics.ietf.org
  165 6.970082     161.246.5.7   8.8.8.8       DNS      78 Standard query 0x19f6 A analytics.ietf.org
  169 7.140209     8.8.8.8       161.246.5.7   DNS     108 Standard query response 0x19f6 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
  184 7.413024     1.1.1.1       161.246.5.7   DNS     108 Standard query response 0x19f6 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
```

ipconfig /all

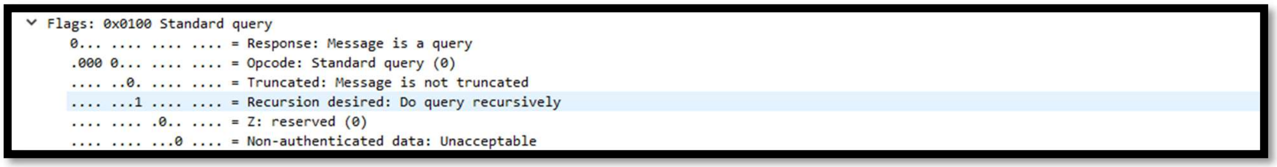


```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 54-BF-64-20-54-B8
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::154e:379d:a456:e786%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 161.246.5.7(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 161.246.5.254
   DHCPv6 IAID . . . . . . . . . . . : 106217316
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-8A-DC-12-54-BF-64-20-54-B8
   DNS Servers . . . . . . . . . . . : 1.1.1.1
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

ตรงกัน

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

type A เนื่องจาก header เป็นแบบนี้

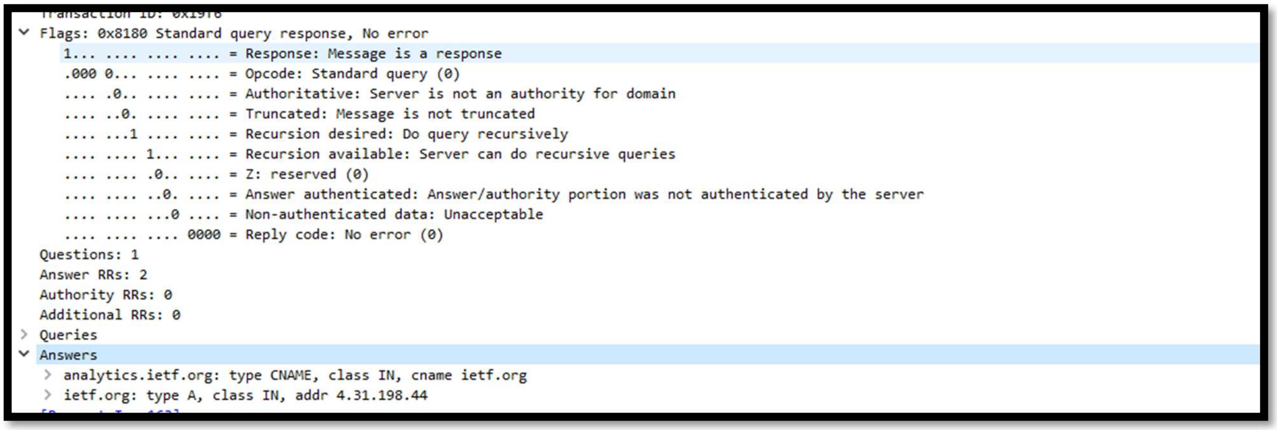


```
v Flags: 0x0100 Standard query
    0... .... .... .... = Response: Message is a query
    .000 0... .... .... = Opcode: Standard query (0)
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... .0.. .... = Z: reserved (0)
    .... .... ...0 .... = Non-authenticated data: Unacceptable
```

ไม่มี answer ใน packet นี้

8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

: ตอบกลับมา 2 เพราะ Answer RRs = 2



```
    Transaction ID: 0x1916
  ˅ 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: 2
    Authority RRs: 0
    Additional RRs: 0
  › Queries
  ˅ Answers
    › analytics.ietf.org: type CNAME, class IN, cname ietf.org
    › ietf.org: type A, class IN, addr 4.31.198.44
```

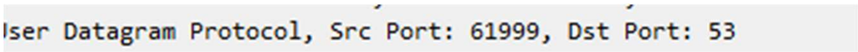
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

ตรงกันครับ

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

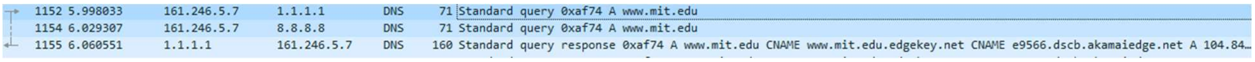
ไม่เพราะเราโหลดรูปจาก web site ไม่ใช่ DNS, และเรามี ip address ของเว็ปนี้เก็บไว้ใน cache เรียบร้อยแล้ว

11. What is the destination port for the DNS query message? What is the source port of DNS response message?



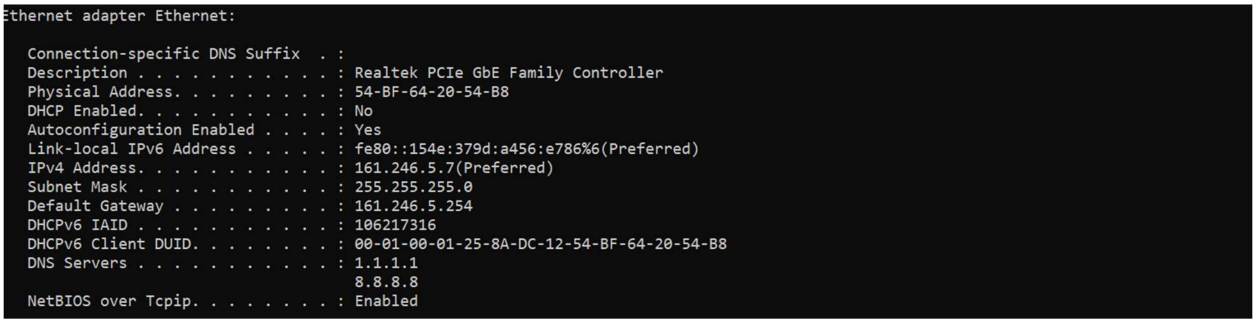
```
User Datagram Protocol, Src Port: 61999, Dst Port: 53
```

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



```
1152 5.998033   161.246.5.7   1.1.1.1       DNS    71 Standard query 0xaf74 A www.mit.edu
1154 6.029307   161.246.5.7   8.8.8.8       DNS    71 Standard query 0xaf74 A www.mit.edu
1155 6.060551   1.1.1.1       161.246.5.7   DNS   160 Standard query response 0xaf74 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.84…
```

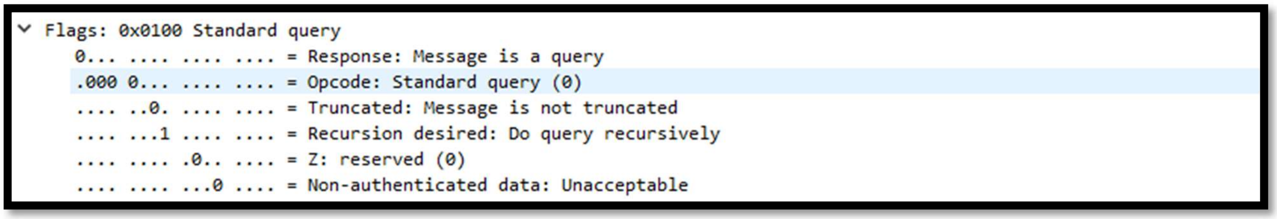
ตรงกันกับใน DNS ที่ผมเซ็ตใน network adapter



```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 54-BF-64-20-54-B8
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::154e:379d:a456:e786%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 161.246.5.7(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 161.246.5.254
   DHCPv6 IAID . . . . . . . . . . . : 106217316
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-8A-DC-12-54-BF-64-20-54-B8
   DNS Servers . . . . . . . . . . . : 1.1.1.1
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

เป็น type A

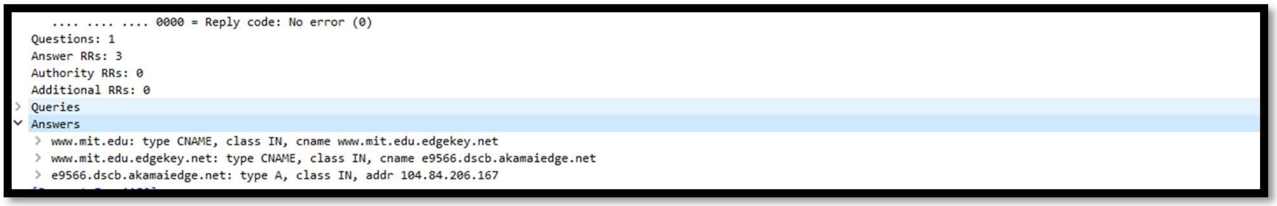


```
∨ Flags: 0x0100 Standard query
    0... .... .... .... = Response: Message is a query
    .000 0... .... .... = Opcode: Standard query (0)
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... .0.. .... = Z: reserved (0)
    .... .... ...0 .... = Non-authenticated data: Unacceptable
```

ไม่มีคำตอบ

14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

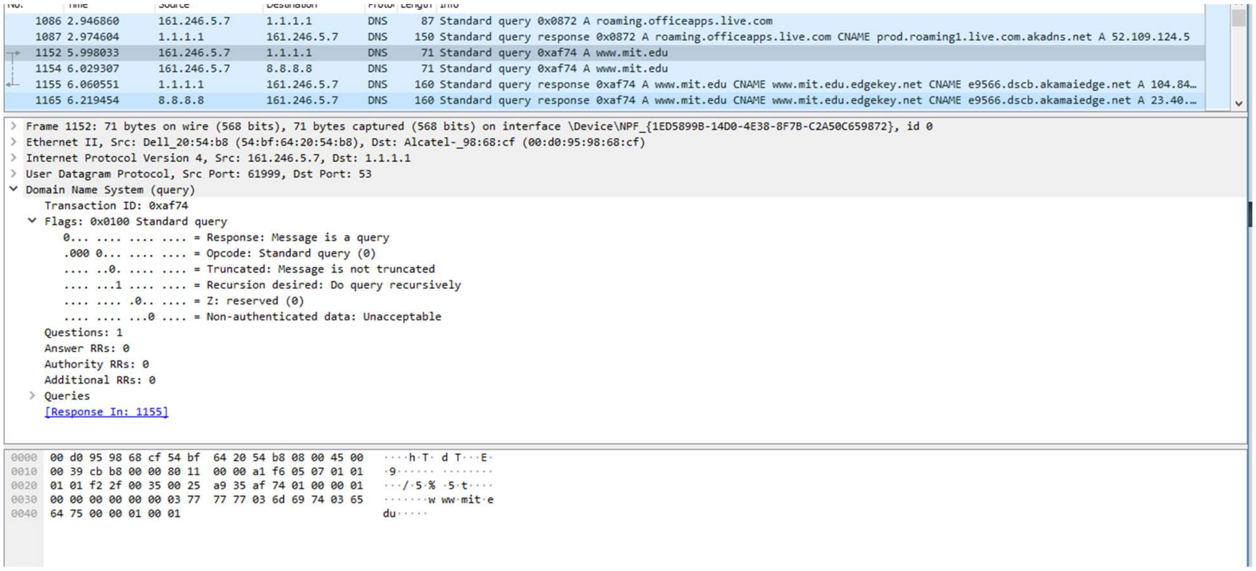
ได้กลับมาทั้งหมด 3 คำตอบ



```
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
> Queries
∨ Answers
  > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  > e9566.dscb.akamaiedge.net: type A, class IN, addr 104.84.206.167
```

15. Provide a screenshot.

ของตอนส่ง

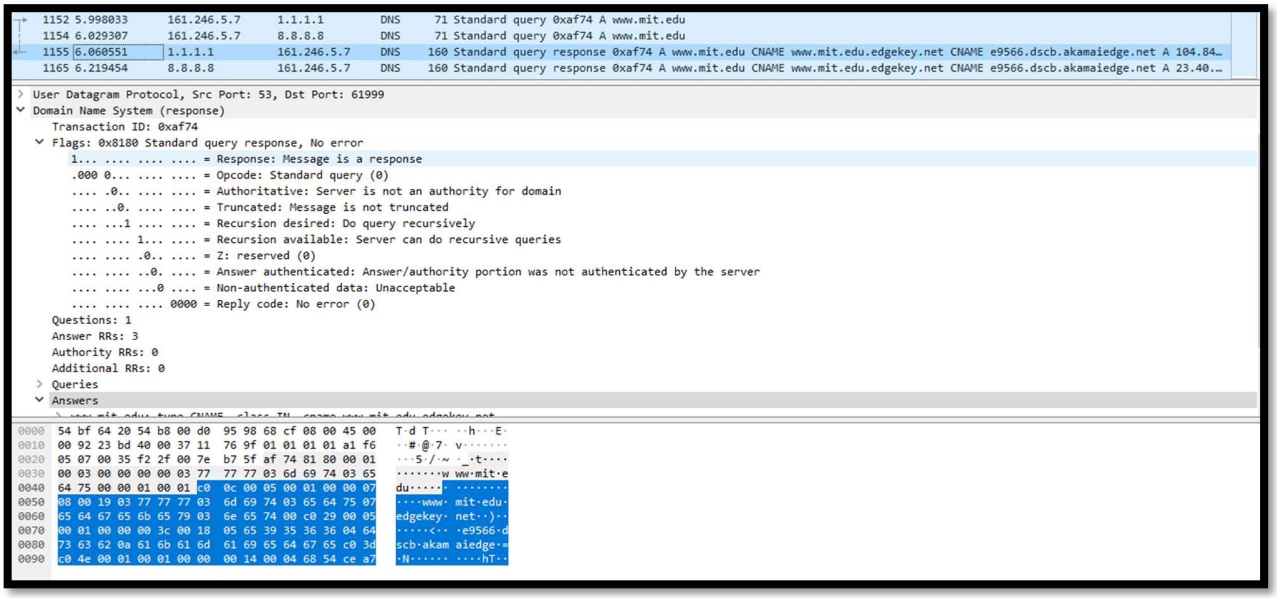


```
   1086 2.946860   161.246.5.7   1.1.1.1       DNS    87 Standard query 0x0872 A roaming.officeapps.live.com
   1087 2.974604   1.1.1.1       161.246.5.7   DNS   150 Standard query response 0x0872 A roaming.officeapps.live.com CNAME prod.roaming1.live.com.akadns.net A 52.109.124.5
   1152 5.998033   161.246.5.7   1.1.1.1       DNS    71 Standard query 0xaf74 A www.mit.edu
   1154 6.029307   161.246.5.7   8.8.8.8       DNS    71 Standard query 0xaf74 A www.mit.edu
   1155 6.060551   1.1.1.1       161.246.5.7   DNS   160 Standard query response 0xaf74 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.84…
   1165 6.219454   8.8.8.8       161.246.5.7   DNS   160 Standard query response 0xaf74 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.40.…

> Frame 1152: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{1ED5899B-14D0-4E38-8F7B-C2A50C659872}, id 0
> Ethernet II, Src: Dell_20:54:b8 (54:bf:64:20:54:b8), Dst: Alcatel-_98:68:cf (00:d0:95:98:68:cf)
> Internet Protocol Version 4, Src: 161.246.5.7, Dst: 1.1.1.1
> User Datagram Protocol, Src Port: 61999, Dst Port: 53
∨ Domain Name System (query)
    Transaction ID: 0xaf74
  ∨ 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
    [Response In: 1155]

0000  00 d0 95 98 68 cf 54 bf  64 20 54 b8 08 00 45 00   ····h·T· d T···E·
0010  00 39 cb b8 00 00 80 11  00 00 a1 f6 05 07 01 01   ·9······ ········
0020  01 01 f2 2f 00 35 00 25  a9 35 af 74 01 00 00 01   ···/·5·% ·5·t····
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 01 00 01                               du·····
```

ของตอนรับกลับ

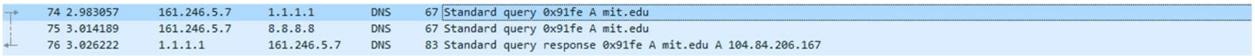
นาย เสฏฐวุฒิ ทิพย์กรรภิรมย์

61011433



```
 1152 5.998033    161.246.5.7   1.1.1.1       DNS    71 Standard query 0xaf74 A www.mit.edu
 1154 6.029307    161.246.5.7   8.8.8.8       DNS    71 Standard query 0xaf74 A www.mit.edu
 1155 6.060551    1.1.1.1       161.246.5.7   DNS   160 Standard query response 0xaf74 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.84…
 1165 6.219454    8.8.8.8       161.246.5.7   DNS   160 Standard query response 0xaf74 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.40.…

> User Datagram Protocol, Src Port: 53, Dst Port: 61999
v Domain Name System (response)
    Transaction ID: 0xaf74
  v 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: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net

0000  54 bf 64 20 54 b8 00 d0  95 98 68 cf 08 00 45 00   T·d T··· ··h···E·
0010  00 92 23 bd 40 00 37 11  76 9f 01 01 01 01 a1 f6   ··#·@·7· v·······
0020  05 07 00 35 f2 2f 00 7e  b7 5f af 74 81 80 00 01   ···5·/·~ ·_·t····
0030  00 03 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 01 00 01 c0  0c 00 05 00 01 00 00 07   du······ ········
0050  08 00 19 03 77 77 77 03  6d 69 74 03 65 64 75 07   ····www· mit·edu·
0060  65 64 67 65 6b 65 79 03  6e 65 74 00 c0 29 00 05   edgekey· net··)··
0070  00 01 00 00 00 3c 00 18  05 65 39 35 36 36 04 64   ·····<·· ·e9566·d
0080  73 63 62 0a 61 6b 61 6d  61 69 65 64 67 65 c0 3d   scb·akam aiedge·=
0090  c0 4e 00 01 00 01 00 00  00 14 00 04 68 54 ce a7   ·N······ ····hT··
```

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

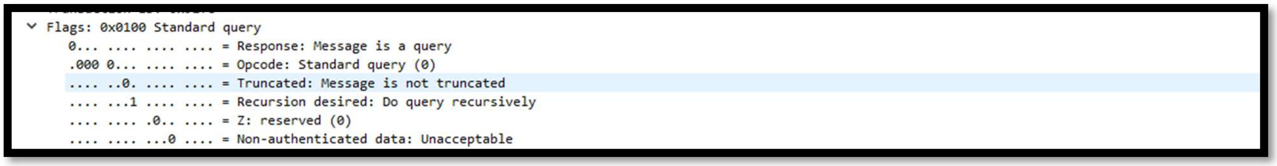


```
 74 2.983057    161.246.5.7   1.1.1.1       DNS    67 Standard query 0x91fe A mit.edu
 75 3.014189    161.246.5.7   8.8.8.8       DNS    67 Standard query 0x91fe A mit.edu
 76 3.026222    1.1.1.1       161.246.5.7   DNS    83 Standard query response 0x91fe A mit.edu A 104.84.206.167
```

ตรงกับ DNS ที่ผมได้ตั้งค่า

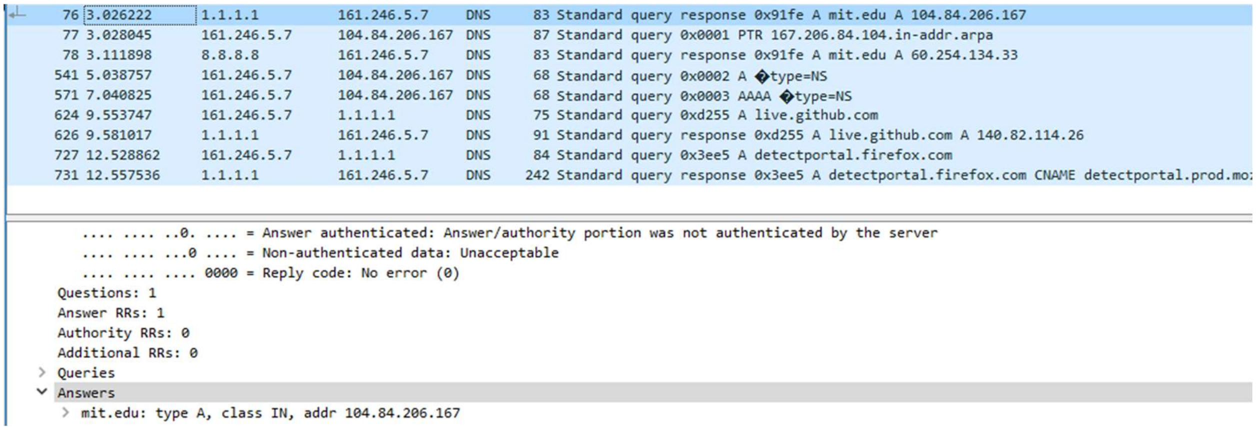
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

เป็น type A ไม่มีคำตอบอยู่ด้านใน



```
v 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
```

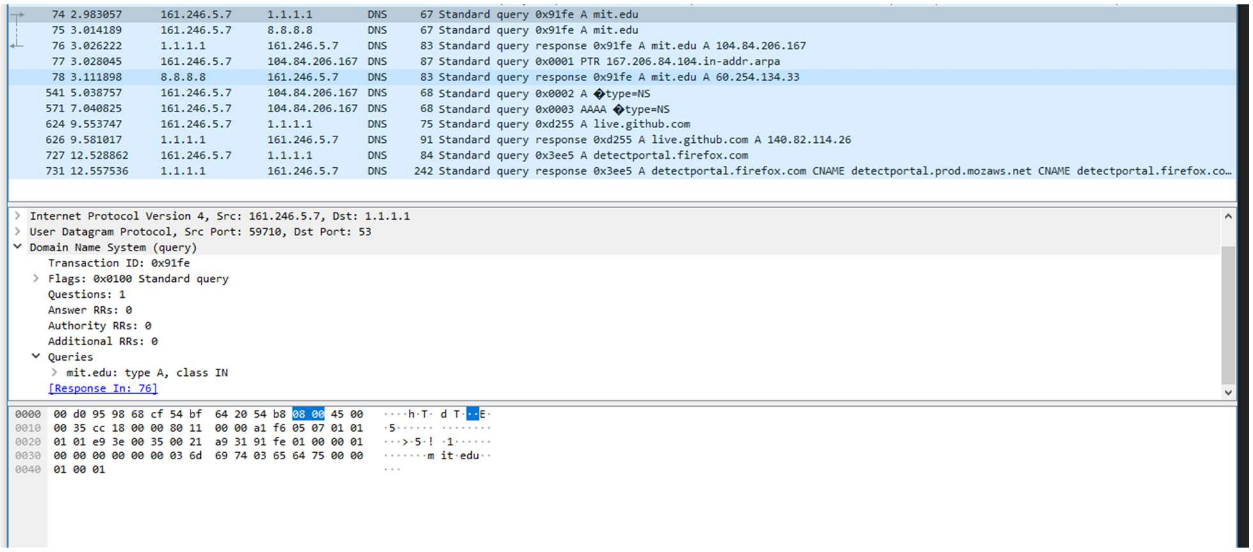
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameserver



```
 76 3.026222    1.1.1.1        161.246.5.7      DNS    83 Standard query response 0x91fe A mit.edu A 104.84.206.167
 77 3.028045    161.246.5.7    104.84.206.167   DNS    87 Standard query 0x0001 PTR 167.206.84.104.in-addr.arpa
 78 3.111898    8.8.8.8        161.246.5.7      DNS    83 Standard query response 0x91fe A mit.edu A 60.254.134.33
541 5.038757    161.246.5.7    104.84.206.167   DNS    68 Standard query 0x0002 A �type=NS
571 7.040825    161.246.5.7    104.84.206.167   DNS    68 Standard query 0x0003 AAAA �type=NS
624 9.553747    161.246.5.7    1.1.1.1          DNS    75 Standard query 0xd255 A live.github.com
626 9.581017    1.1.1.1        161.246.5.7      DNS    91 Standard query response 0xd255 A live.github.com A 140.82.114.26
727 12.528862   161.246.5.7    1.1.1.1          DNS    84 Standard query 0x3ee5 A detectportal.firefox.com
731 12.557536   1.1.1.1        161.246.5.7      DNS   242 Standard query response 0x3ee5 A detectportal.firefox.com CNAME detectportal.prod.mo:

      .... .... ..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
  ˅ Answers
    > mit.edu: type A, class IN, addr 104.84.206.167
```

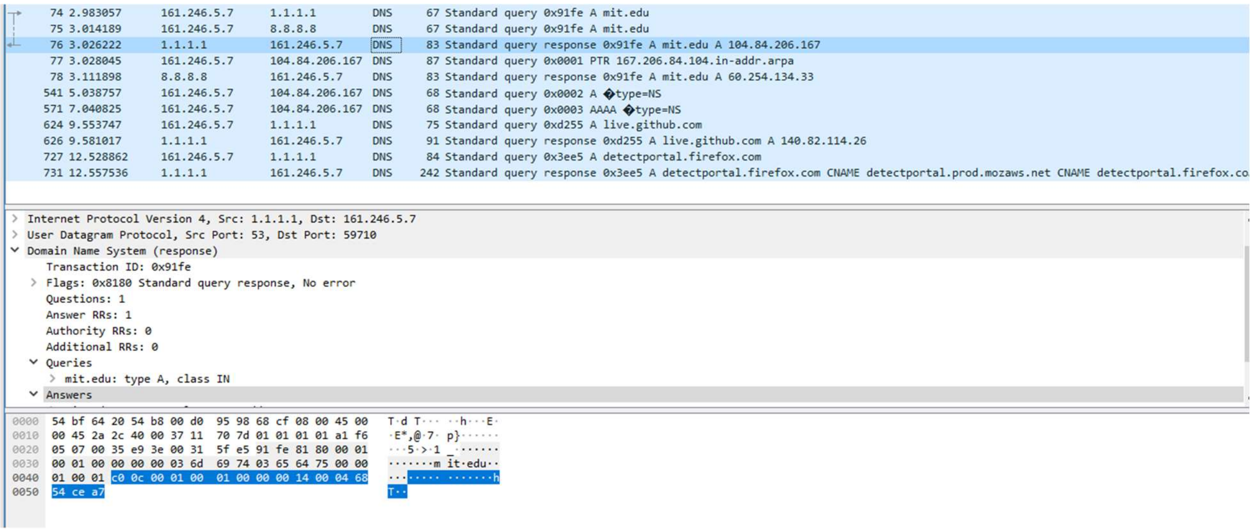
19. Provide a screenshot.

ของตอนส่ง



```
 74 2.983057    161.246.5.7    1.1.1.1          DNS    67 Standard query 0x91fe A mit.edu
 75 3.014189    161.246.5.7    8.8.8.8          DNS    67 Standard query 0x91fe A mit.edu
 76 3.026222    1.1.1.1        161.246.5.7      DNS    83 Standard query response 0x91fe A mit.edu A 104.84.206.167
 77 3.028045    161.246.5.7    104.84.206.167   DNS    87 Standard query 0x0001 PTR 167.206.84.104.in-addr.arpa
 78 3.111898    8.8.8.8        161.246.5.7      DNS    83 Standard query response 0x91fe A mit.edu A 60.254.134.33
541 5.038757    161.246.5.7    104.84.206.167   DNS    68 Standard query 0x0002 A �type=NS
571 7.040825    161.246.5.7    104.84.206.167   DNS    68 Standard query 0x0003 AAAA �type=NS
624 9.553747    161.246.5.7    1.1.1.1          DNS    75 Standard query 0xd255 A live.github.com
626 9.581017    1.1.1.1        161.246.5.7      DNS    91 Standard query response 0xd255 A live.github.com A 140.82.114.26
727 12.528862   161.246.5.7    1.1.1.1          DNS    84 Standard query 0x3ee5 A detectportal.firefox.com
731 12.557536   1.1.1.1        161.246.5.7      DNS   242 Standard query response 0x3ee5 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME detectportal.firefox.co…

> Internet Protocol Version 4, Src: 161.246.5.7, Dst: 1.1.1.1
> User Datagram Protocol, Src Port: 59710, Dst Port: 53
˅ Domain Name System (query)
    Transaction ID: 0x91fe
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ˅ Queries
    > mit.edu: type A, class IN
    [Response In: 76]

0000  00 d0 95 98 68 cf 54 bf  64 20 54 b8 08 00 45 00   ····h·T· d T···E·
0010  00 35 cc 18 00 00 80 11  00 00 a1 f6 05 07 01 01   ·5······ ········
0020  01 01 e9 3e 00 35 00 21  a9 31 91 fe 01 00 00 01   ···>·5·! ·1······
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  01 00 01                                           ···
```

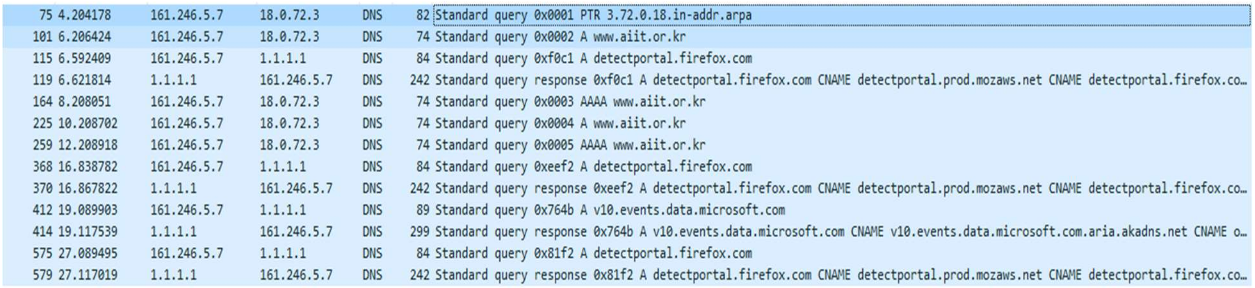
ของตอนรับ



```
 74 2.983057    161.246.5.7    1.1.1.1          DNS    67 Standard query 0x91fe A mit.edu
 75 3.014189    161.246.5.7    8.8.8.8          DNS    67 Standard query 0x91fe A mit.edu
 76 3.026222    1.1.1.1        161.246.5.7      DNS    83 Standard query response 0x91fe A mit.edu A 104.84.206.167
 77 3.028045    161.246.5.7    104.84.206.167   DNS    87 Standard query 0x0001 PTR 167.206.84.104.in-addr.arpa
 78 3.111898    8.8.8.8        161.246.5.7      DNS    83 Standard query response 0x91fe A mit.edu A 60.254.134.33
541 5.038757    161.246.5.7    104.84.206.167   DNS    68 Standard query 0x0002 A �type=NS
571 7.040825    161.246.5.7    104.84.206.167   DNS    68 Standard query 0x0003 AAAA �type=NS
624 9.553747    161.246.5.7    1.1.1.1          DNS    75 Standard query 0xd255 A live.github.com
626 9.581017    1.1.1.1        161.246.5.7      DNS    91 Standard query response 0xd255 A live.github.com A 140.82.114.26
727 12.528862   161.246.5.7    1.1.1.1          DNS    84 Standard query 0x3ee5 A detectportal.firefox.com
731 12.557536   1.1.1.1        161.246.5.7      DNS   242 Standard query response 0x3ee5 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME detectportal.firefox.co

> Internet Protocol Version 4, Src: 1.1.1.1, Dst: 161.246.5.7
> User Datagram Protocol, Src Port: 53, Dst Port: 59710
˅ Domain Name System (response)
    Transaction ID: 0x91fe
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ˅ Queries
    > mit.edu: type A, class IN
  ˅ Answers

0000  54 bf 64 20 54 b8 00 d0  95 98 68 cf 08 00 45 00   T·d T··· ··h···E·
0010  00 45 2a 2c 40 00 37 11  70 7d 01 01 01 01 a1 f6   ·E*,@·7· p}······
0020  05 07 00 35 e9 3e 00 31  5f e5 91 fe 81 80 00 01   ···5·>·1 _·······
0030  00 01 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  01 00 01 c0 0c 00 01 00  01 00 00 00 14 00 04 68   ········ ·······h
0050  54 ce a7                                           T··
```

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

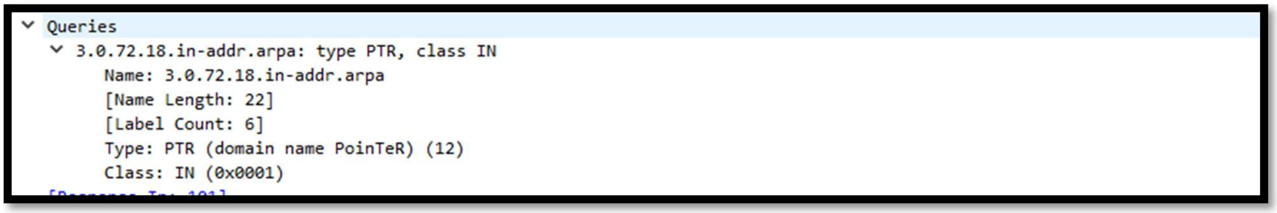
packet แรกๆ ไม่ตรงกับที่เราทำการ setting ไว้เพราะเนื่องจากระบุ dns ของ bitsy.mit.edu



```
 75 4.204178    161.246.5.7   18.0.72.3     DNS   82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
101 6.206424    161.246.5.7   18.0.72.3     DNS   74 Standard query 0x0002 A www.aiit.or.kr
115 6.592409    161.246.5.7   1.1.1.1       DNS   84 Standard query 0xf0c1 A detectportal.firefox.com
119 6.621814    1.1.1.1       161.246.5.7   DNS  242 Standard query response 0xf0c1 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME detectportal.firefox.co…
164 8.208051    161.246.5.7   18.0.72.3     DNS   74 Standard query 0x0003 AAAA www.aiit.or.kr
225 10.208702   161.246.5.7   18.0.72.3     DNS   74 Standard query 0x0004 A www.aiit.or.kr
259 12.208918   161.246.5.7   18.0.72.3     DNS   74 Standard query 0x0005 AAAA www.aiit.or.kr
368 16.838782   161.246.5.7   1.1.1.1       DNS   84 Standard query 0xeef2 A detectportal.firefox.com
370 16.867822   1.1.1.1       161.246.5.7   DNS  242 Standard query response 0xeef2 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME detectportal.firefox.co…
412 19.089903   161.246.5.7   1.1.1.1       DNS   89 Standard query 0x764b A v10.events.data.microsoft.com
414 19.117539   1.1.1.1       161.246.5.7   DNS  299 Standard query response 0x764b A v10.events.data.microsoft.com CNAME v10.events.data.microsoft.com.aria.akadns.net CNAME o…
575 27.089495   161.246.5.7   1.1.1.1       DNS   84 Standard query 0x81f2 A detectportal.firefox.com
579 27.117019   1.1.1.1       161.246.5.7   DNS  242 Standard query response 0x81f2 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME detectportal.firefox.co…
```

21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

PTR type

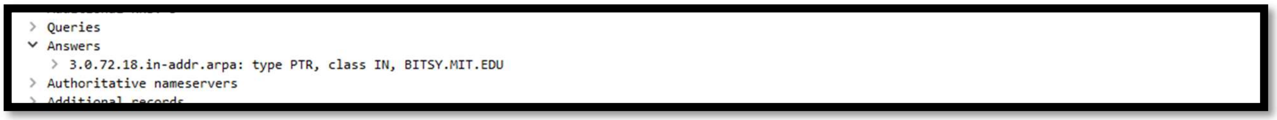


```
˅ Queries
  ˅ 3.0.72.18.in-addr.arpa: type PTR, class IN
       Name: 3.0.72.18.in-addr.arpa
       [Name Length: 22]
       [Label Count: 6]
       Type: PTR (domain name PoinTeR) (12)
       Class: IN (0x0001)
  [Response In: 101]
```

ไม่มีคำตอบอยู่

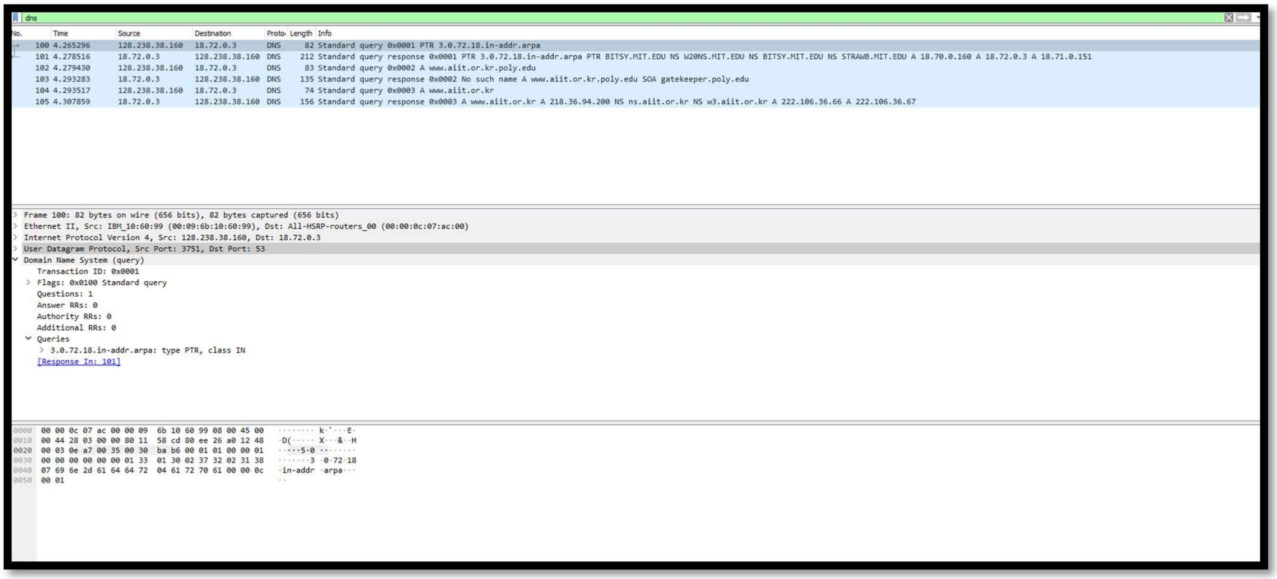
22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

มี 1 answer, ด้านใน



```
> Queries
˅ Answers
   > 3.0.72.18.in-addr.arpa: type PTR, class IN, BITSY.MIT.EDU
> Authoritative nameservers
> Additional records
```

23. Provide a screenshot.



dns

```
No.  Time      Source          Destination     Proto Length Info
 100 4.265296  128.238.38.160  18.72.0.3       DNS      82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
 101 4.278516  18.72.0.3       128.238.38.160  DNS     212 Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY.MIT.EDU NS W20NS.MIT.EDU NS BITSY.MIT.EDU NS STRAWB.MIT.EDU A 18.70.0.160 A 18.72.0.3 A 18.71.0.151
 102 4.279430  128.238.38.160  18.72.0.3       DNS      83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
 103 4.293283  18.72.0.3       128.238.38.160  DNS     135 Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.poly.edu
 104 4.293517  128.238.38.160  18.72.0.3       DNS      74 Standard query 0x0003 A www.aiit.or.kr
 105 4.307859  18.72.0.3       128.238.38.160  DNS     156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.106.36.66 A 222.106.36.67
```

```
> Frame 100: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 3751, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > 3.0.72.18.in-addr.arpa: type PTR, class IN
    [Response In: 101]
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········ k·`···E·
0010  00 44 28 03 00 00 80 11  58 cd 80 ee 26 a0 12 48   ·D(····· X···&··H
0020  00 03 0e a7 00 35 00 30  ba b6 00 01 01 00 00 01   ·····5·0 ········
0030  00 00 00 00 00 00 01 33  01 30 02 37 32 02 31 38   ·······3 ·0·72·18
0040  07 69 6e 2d 61 64 64 72  04 61 72 70 61 00 00 0c   ·in-addr ·arpa···
0050  00 01                                              ··
```