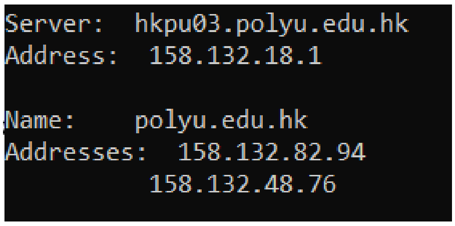
Lab Report

Lab 3 DNS

ZHOU Siyu

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



```
Server:  hkpu03.polyu.edu.hk
Address:  158.132.18.1

Name:    polyu.edu.hk
Addresses:  158.132.82.94
          158.132.48.76
```

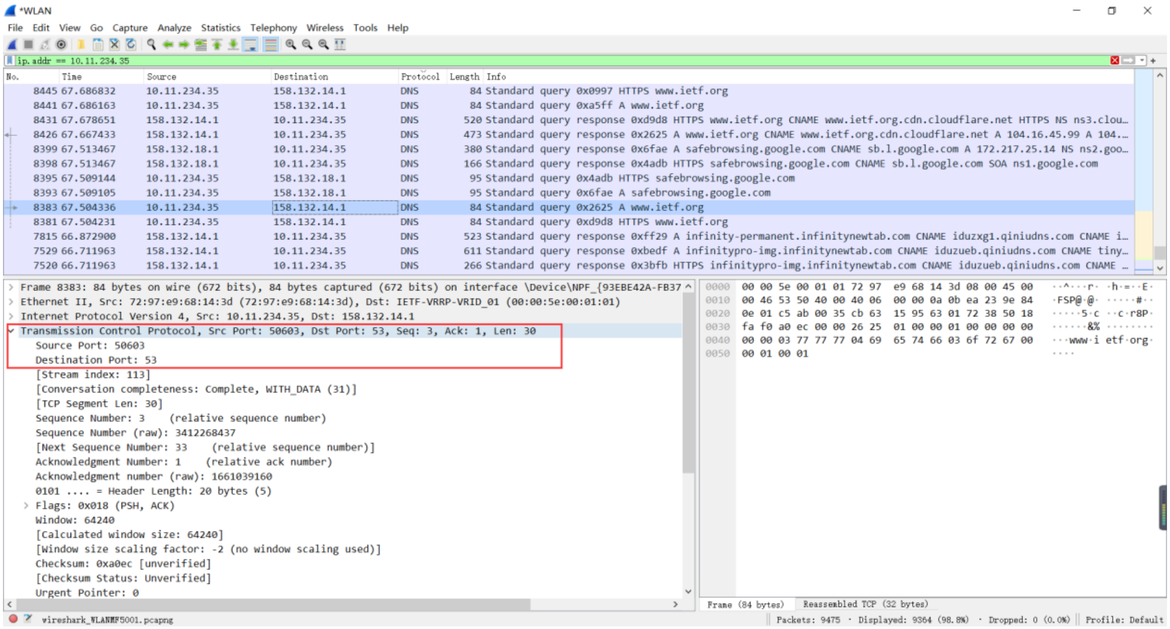
I use webpage http://polyu.edu.hk

IP addresses of that server is 158.132.83.94 and 158.132.48.76

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

Destination port for DNS query message: 53

Source port of DNS response message: 53



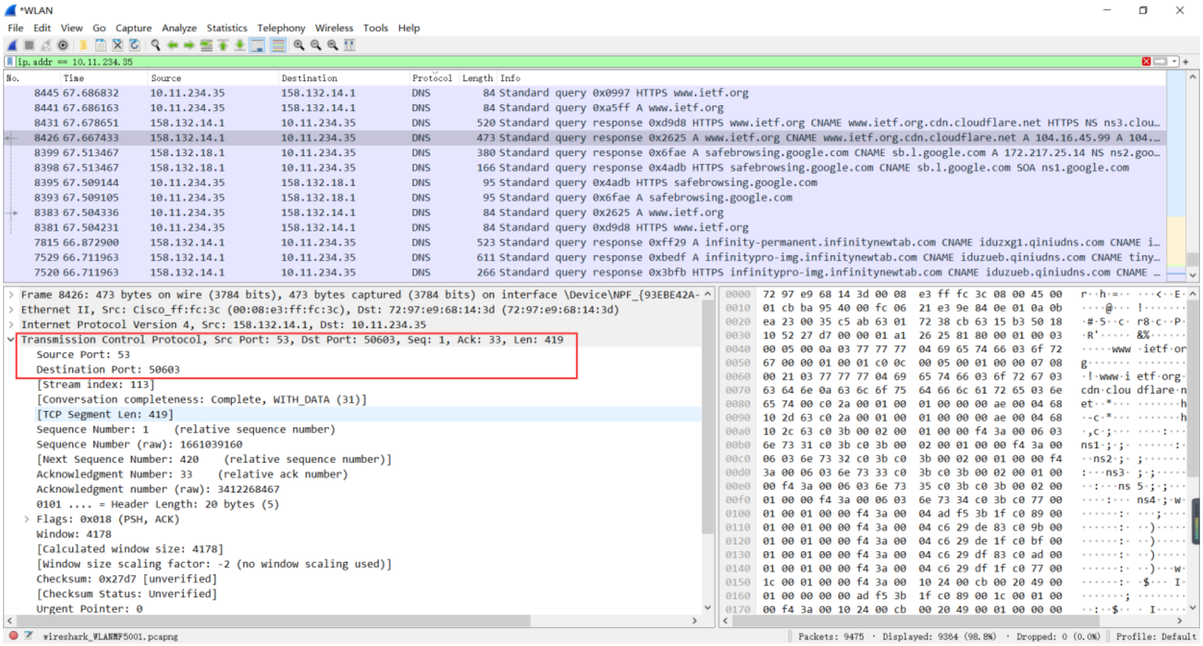
```
ip.addr == 10.11.234.35
```

```
No.   Time       Source          Destination     Protocol Length Info
 8445 67.686832  10.11.234.35    158.132.14.1    DNS        84 Standard query 0x0997 HTTPS www.ietf.org
 8441 67.686163  10.11.234.35    158.132.14.1    DNS        84 Standard query 0xa5ff A www.ietf.org
 8431 67.678651  158.132.14.1    10.11.234.35    DNS       520 Standard query response 0xd9d8 HTTPS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net HTTPS NS ns3.clou…
 8426 67.667433  158.132.14.1    10.11.234.35    DNS       473 Standard query response 0x2625 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.…
 8399 67.513467  158.132.18.1    10.11.234.35    DNS       380 Standard query response 0x6fae A safebrowsing.google.com CNAME sb.l.google.com A 172.217.25.14 NS ns2.goo…
 8398 67.513467  158.132.18.1    10.11.234.35    DNS       166 Standard query response 0x4adb HTTPS safebrowsing.google.com CNAME sb.l.google.com SOA ns1.google.com
 8395 67.509144  10.11.234.35    158.132.18.1    DNS        95 Standard query 0x4adb HTTPS safebrowsing.google.com
 8393 67.509105  10.11.234.35    158.132.18.1    DNS        95 Standard query 0x6fae A safebrowsing.google.com
 8383 67.504336  10.11.234.35    158.132.14.1    DNS        84 Standard query 0x2625 A www.ietf.org
 8381 67.504231  10.11.234.35    158.132.14.1    DNS        84 Standard query 0xd9d8 HTTPS www.ietf.org
 7815 66.872900  158.132.14.1    10.11.234.35    DNS       523 Standard query response 0xff29 A infinity-permanent.infinitynewtab.com CNAME iduzxg1.qiniudns.com CNAME i…
 7529 66.711963  158.132.14.1    10.11.234.35    DNS       611 Standard query response 0xbedf A infinitypro-img.infinitynewtab.com CNAME iduzueb.qiniudns.com CNAME tiny…
 7520 66.711963  158.132.14.1    10.11.234.35    DNS       266 Standard query response 0x3bfb HTTPS infinitypro-img.infinitynewtab.com CNAME iduzueb.qiniudns.com CNAME …
```

```
> Frame 8383: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{93EBE42A-FB37
> Ethernet II, Src: 72:97:e9:68:14:3d (72:97:e9:68:14:3d), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.11.234.35, Dst: 158.132.14.1
v Transmission Control Protocol, Src Port: 50603, Dst Port: 53, Seq: 3, Ack: 1, Len: 30
    Source Port: 50603
    Destination Port: 53
    [Stream index: 113]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 30]
    Sequence Number: 3    (relative sequence number)
    Sequence Number (raw): 3412268437
    [Next Sequence Number: 33    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1661039160
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xa0ec [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

```
0000  00 00 5e 00 01 01 72 97  e9 68 14 3d 08 00 45 00   ··^···r· ·h·=··E·
0010  00 46 53 50 40 00 40 06  00 00 0a 0b ea 23 9e 84   ·FSP@·@· ·····#··
0020  0e 01 c5 ab 00 35 cb 63  15 95 63 01 72 38 50 18   ·····5·c ··c·r8P·
0030  fa f0 a0 ec 00 00 26 25  01 00 00 01 00 00 00 00   ······&% ········
0040  00 00 03 77 77 77 04 69  65 74 66 03 6f 72 67 00   ···www·i etf·org·
0050  00 01 00 01                                        ····
```

```
Frame (84 bytes)   Reassembled TCP (32 bytes)
wireshark_WLANMF5001.pcapng     Packets: 9475 · Displayed: 9364 (98.8%) · Dropped: 0 (0.0%)   Profile: Default
```



```
ip.addr == 10.11.234.35
```

```
No.   Time       Source          Destination     Protocol Length Info
 8445 67.686832  10.11.234.35    158.132.14.1    DNS        84 Standard query 0x0997 HTTPS www.ietf.org
 8441 67.686163  10.11.234.35    158.132.14.1    DNS        84 Standard query 0xa5ff A www.ietf.org
 8431 67.678651  158.132.14.1    10.11.234.35    DNS       520 Standard query response 0xd9d8 HTTPS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net HTTPS NS ns3.clou…
 8426 67.667433  158.132.14.1    10.11.234.35    DNS       473 Standard query response 0x2625 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.…
 8399 67.513467  158.132.18.1    10.11.234.35    DNS       380 Standard query response 0x6fae A safebrowsing.google.com CNAME sb.l.google.com A 172.217.25.14 NS ns2.goo…
 8398 67.513467  158.132.18.1    10.11.234.35    DNS       166 Standard query response 0x4adb HTTPS safebrowsing.google.com CNAME sb.l.google.com SOA ns1.google.com
 8395 67.509144  10.11.234.35    158.132.18.1    DNS        95 Standard query 0x4adb HTTPS safebrowsing.google.com
 8393 67.509105  10.11.234.35    158.132.18.1    DNS        95 Standard query 0x6fae A safebrowsing.google.com
 8383 67.504336  10.11.234.35    158.132.14.1    DNS        84 Standard query 0x2625 A www.ietf.org
 8381 67.504231  10.11.234.35    158.132.14.1    DNS        84 Standard query 0xd9d8 HTTPS www.ietf.org
 7815 66.872900  158.132.14.1    10.11.234.35    DNS       523 Standard query response 0xff29 A infinity-permanent.infinitynewtab.com CNAME iduzxg1.qiniudns.com CNAME i…
 7529 66.711963  158.132.14.1    10.11.234.35    DNS       611 Standard query response 0xbedf A infinitypro-img.infinitynewtab.com CNAME iduzueb.qiniudns.com CNAME tiny…
 7520 66.711963  158.132.14.1    10.11.234.35    DNS       266 Standard query response 0x3bfb HTTPS infinitypro-img.infinitynewtab.com CNAME iduzueb.qiniudns.com CNAME …
```

```
> Frame 8426: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface \Device\NPF_{93EBE42A-
> Ethernet II, Src: Cisco_ff:fc:3c (00:08:e3:ff:fc:3c), Dst: 72:97:e9:68:14:3d (72:97:e9:68:14:3d)
> Internet Protocol Version 4, Src: 158.132.14.1, Dst: 10.11.234.35
v Transmission Control Protocol, Src Port: 53, Dst Port: 50603, Seq: 1, Ack: 33, Len: 419
    Source Port: 53
    Destination Port: 50603
    [Stream index: 113]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 419]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1661039160
    [Next Sequence Number: 420    (relative sequence number)]
    Acknowledgment Number: 33    (relative ack number)
    Acknowledgment number (raw): 3412268467
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 4178
    [Calculated window size: 4178]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x27d7 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

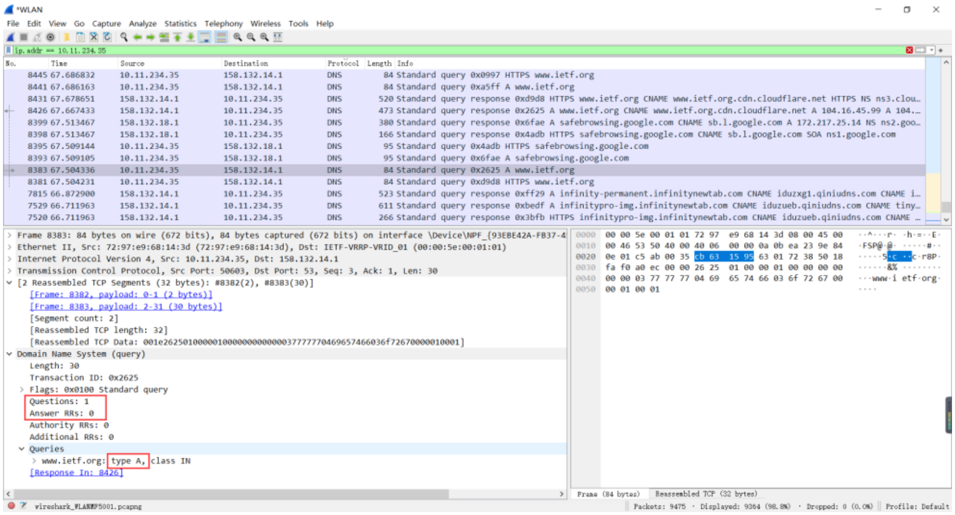
```
0000  72 97 e9 68 14 3d 00 08  e3 ff fc 3c 08 00 45 00   r··h·=·· ···<··E·
0010  01 cb ba 95 40 00 fc 06  21 e3 9e 84 0e 01 0a 0b   ····@··· !·······
0020  ea 23 00 35 c5 ab 63 01  72 38 cb 63 15 b3 50 18   ·#·5··c· r8·c··P·
0030  10 52 27 d7 00 00 01 a1  26 25 81 80 00 01 00 03   ·R'····· &%······
0040  00 05 00 0a 03 77 77 77  04 69 65 74 66 03 6f 72   ·····www ·ietf·or
0050  67 00 00 01 00 01 c0 0c  00 05 00 01 00 00 07 08   g······· ········
0060  00 21 03 77 77 77 04 69  65 74 66 03 6f 72 67 03   ·!·www·i etf·org·
0070  63 64 6e 0a 63 6c 6f 75  64 66 6c 61 72 65 03 6e   cdn·clou dflare·n
0080  65 74 00 c0 2a 00 01 00  01 00 00 00 ae 00 04 68   et··*··· ·······h
0090  10 2d 63 c0 2a 00 01 00  01 00 00 00 ae 00 04 68   ·-c·*··· ·······h
00a0  10 2c 63 c0 3b 00 02 00  01 00 00 f4 3a 00 06 03   ·,c·;··· ····:···
00b0  6e 73 31 c0 3b c0 3b 00  02 00 01 00 00 f4 3a 00   ns1·;·;· ······:·
00c0  06 03 6e 73 32 c0 3b c0  3b 00 02 00 01 00 00 f4   ··ns2·;· ;·······
00d0  3a 00 06 03 6e 73 33 c0  3b c0 3b 00 02 00 01 00   :···ns3· ;·;·····
00e0  00 f4 3a 00 06 03 6e 73  35 c0 3b c0 3b 00 02 00   ··:···ns 5·;·;···
00f0  01 00 00 f4 3a 00 06 03  6e 73 34 c0 3b c0 77 00   ····:··· ns4·;·w·
0100  01 00 01 00 00 f4 3a 00  04 ad f5 3b 1f c0 89 00   ······:· ···;····
0110  01 00 01 00 00 f4 3a 00  04 c6 29 de 83 c0 9b 00   ······:· ··)·····
0120  01 00 01 00 00 f4 3a 00  04 c6 29 de 1f c0 bf 00   ······:· ··)·····
0130  01 00 01 00 00 f4 3a 00  04 c6 29 df 83 c0 ad 00   ······:· ··)·····
0140  01 00 01 00 00 f4 3a 00  04 c6 29 df 1f c0 77 00   ······:· ··)···w·
0150  1c 00 01 00 00 f4 3a 00  10 24 00 cb 00 20 49 00   ······:· ·$··· I·
0160  01 00 00 00 00 ad f5 3b  1f c0 89 00 1c 00 01 00   ·······; ········
0170  00 f4 3a 00 10 24 00 cb  00 20 49 00 01 00 00 00   ··:··$·· · I·····
```

```
wireshark_WLANMF5001.pcapng     Packets: 9475 · Displayed: 9364 (98.8%) · Dropped: 0 (0.0%)   Profile: Default
```

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

DNS query is Type A.

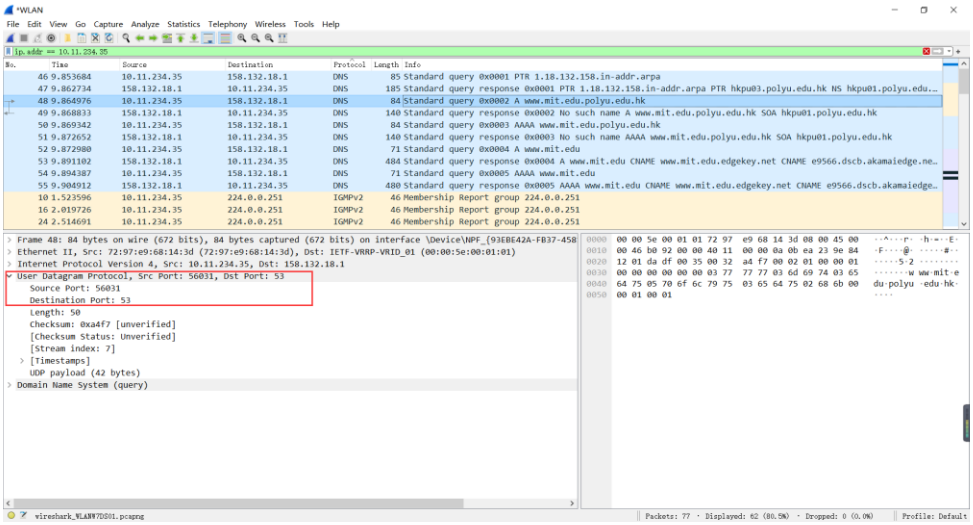
It does not contain any “answers”.


*WLAN
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.11.234.35

No.   Time       Source         Destination    Protocol Length Info
 8445 67.686832  10.11.234.35   158.132.14.1   DNS       84 Standard query 0x0997 HTTPS www.ietf.org
 8441 67.686163  10.11.234.35   158.132.14.1   DNS       84 Standard query 0xa5ff A www.ietf.org
 8431 67.678651  158.132.14.1   10.11.234.35   DNS      520 Standard query response 0xd9d8 HTTPS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net HTTPS NS ns3.clou…
 8426 67.667433  158.132.14.1   10.11.234.35   DNS      473 Standard query response 0x2625 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.…
 8399 67.513467  158.132.18.1   10.11.234.35   DNS      380 Standard query response 0x6fae A safebrowsing.google.com CNAME sb.l.google.com A 172.217.25.14 NS ns2.goo…
 8398 67.513467  158.132.18.1   10.11.234.35   DNS      166 Standard query response 0x4adb HTTPS safebrowsing.google.com CNAME sb.l.google.com SOA ns1.google.com
 8395 67.509144  10.11.234.35   158.132.18.1   DNS       95 Standard query 0x4adb HTTPS safebrowsing.google.com
 8393 67.509105  10.11.234.35   158.132.18.1   DNS       95 Standard query 0x6fae A safebrowsing.google.com
 8383 67.504336  10.11.234.35   158.132.14.1   DNS       84 Standard query 0x2625 A www.ietf.org
 8381 67.504231  10.11.234.35   158.132.14.1   DNS       84 Standard query 0xd9d8 HTTPS www.ietf.org
 7815 66.872900  158.132.14.1   10.11.234.35   DNS      523 Standard query response 0xff29 A infinity-permanent.infinitynewtab.com CNAME iduzxg1.qiniudns.com CNAME i…
 7529 66.711963  158.132.14.1   10.11.234.35   DNS      611 Standard query response 0xbedf A infinitypro-img.infinitynewtab.com CNAME iduzueb.qiniudns.com CNAME tiny…
 7520 66.711963  158.132.14.1   10.11.234.35   DNS      266 Standard query response 0x3bfb HTTPS infinitypro-img.infinitynewtab.com CNAME iduzueb.qiniudns.com CNAME …

> Frame 8383: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{93EBE42A-FB37-4
> Ethernet II, Src: 72:97:e9:68:14:3d (72:97:e9:68:14:3d), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.11.234.35, Dst: 158.132.14.1
> Transmission Control Protocol, Src Port: 50603, Dst Port: 53, Seq: 3, Ack: 1, Len: 30
v [2 Reassembled TCP Segments (32 bytes): #8382(2), #8383(30)]
    [Frame: 8382, payload: 0-1 (2 bytes)]
    [Frame: 8383, payload: 2-31 (30 bytes)]
    [Segment count: 2]
    [Reassembled TCP length: 32]
    [Reassembled TCP Data: 001e262501000001000000000000037777770469657466036f72670000010001]
v Domain Name System (query)
    Length: 30
    Transaction ID: 0x2625
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
    [Response In: 8426]

0000  00 00 5e 00 01 01 72 97  e9 68 14 3d 08 00 45 00   ··^···r· ·h·=··E·
0010  00 46 53 50 40 00 40 06  00 00 0a 0b ea 23 9e 84   ·FSP@·@· ·····#··
0020  0e 01 c5 ab 00 35 cb 63  15 95 63 01 72 38 50 18   ·····5·c ··c·r8P·
0030  fa f0 a0 ec 00 00 26 25  01 00 00 01 00 00 00 00   ······&% ········
0040  00 00 03 77 77 77 04 69  65 74 66 03 6f 72 67 00   ···www·i etf·org·
0050  00 01 00 01                                        ····

Frame (84 bytes)   Reassembled TCP (32 bytes)

wireshark_WLANMF5001.pcapng     Packets: 9475 · Displayed: 9364 (98.8%) · Dropped: 0 (0.0%)     Profile: Default
```

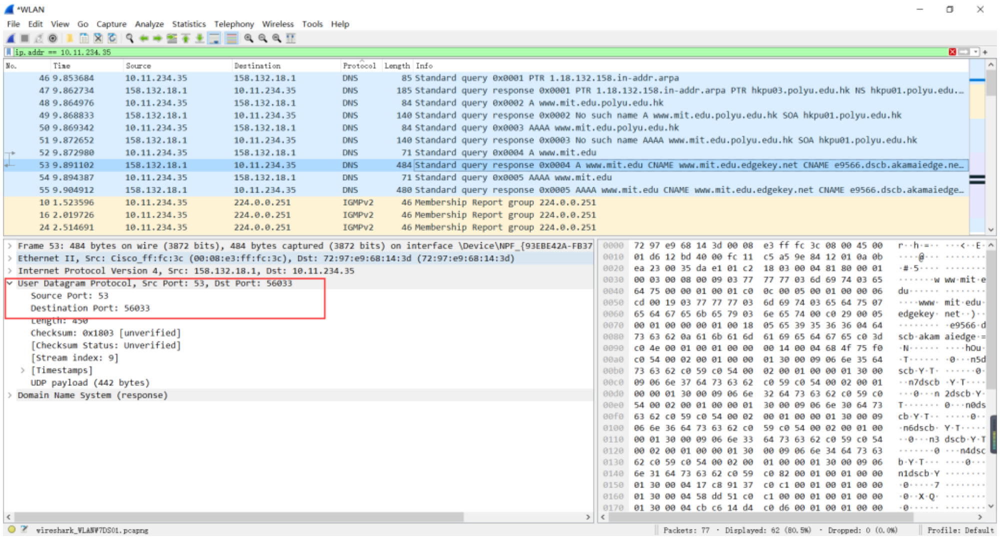
11. What is the destination port for the DNS query message? What is the source port of DNS response message?

Destination port for DNS query message: 53


*WLAN
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.11.234.35

No.   Time      Source         Destination    Protocol Length Info
   46 9.853684  10.11.234.35   158.132.18.1   DNS       85 Standard query 0x0001 PTR 1.18.132.158.in-addr.arpa
   47 9.862734  158.132.18.1   10.11.234.35   DNS      185 Standard query response 0x0001 PTR 1.18.132.158.in-addr.arpa PTR hkpu03.polyu.edu.hk NS hkpu01.polyu.edu.…
   48 9.864976  10.11.234.35   158.132.18.1   DNS       84 Standard query 0x0002 A www.mit.edu.polyu.edu.hk
   49 9.868833  158.132.18.1   10.11.234.35   DNS      140 Standard query response 0x0002 No such name A www.mit.edu.polyu.edu.hk SOA hkpu01.polyu.edu.hk
   50 9.869342  10.11.234.35   158.132.18.1   DNS       84 Standard query 0x0003 AAAA www.mit.edu.polyu.edu.hk
   51 9.872652  158.132.18.1   10.11.234.35   DNS      140 Standard query response 0x0003 No such name AAAA www.mit.edu.polyu.edu.hk SOA hkpu01.polyu.edu.hk
   52 9.872980  10.11.234.35   158.132.18.1   DNS       71 Standard query 0x0004 A www.mit.edu
   53 9.891102  158.132.18.1   10.11.234.35   DNS      484 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.ne…
   54 9.894387  10.11.234.35   158.132.18.1   DNS       71 Standard query 0x0005 AAAA www.mit.edu
   55 9.904912  158.132.18.1   10.11.234.35   DNS      480 Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge…
   10 1.523596  10.11.234.35   224.0.0.251    IGMPv2    46 Membership Report group 224.0.0.251
   16 2.019726  10.11.234.35   224.0.0.251    IGMPv2    46 Membership Report group 224.0.0.251
   24 2.514691  10.11.234.35   224.0.0.251    IGMPv2    46 Membership Report group 224.0.0.251

> Frame 48: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{93EBE42A-FB37-458
> Ethernet II, Src: 72:97:e9:68:14:3d (72:97:e9:68:14:3d), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.11.234.35, Dst: 158.132.18.1
v User Datagram Protocol, Src Port: 56031, Dst Port: 53
    Source Port: 56031
    Destination Port: 53
    Length: 50
    Checksum: 0xa4f7 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
  > [Timestamps]
    UDP payload (42 bytes)
> Domain Name System (query)

0000  00 00 5e 00 01 01 72 97  e9 68 14 3d 08 00 45 00   ··^···r· ·h·=··E·
0010  00 46 b0 92 00 00 40 11  00 00 0a 0b ea 23 9e 84   ·F····@· ·····#··
0020  12 01 da df 00 35 00 32  a4 f7 00 02 01 00 00 01   ·····5·2 ········
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 05 70 6f 6c 79 75  03 65 64 75 02 68 6b 00   du·polyu ·edu·hk·
0050  00 01 00 01                                        ····

wireshark_WLANW7DS01.pcapng     Packets: 77 · Displayed: 62 (80.5%) · Dropped: 0 (0.0%)     Profile: Default
```

Source port of DNS response message: 53

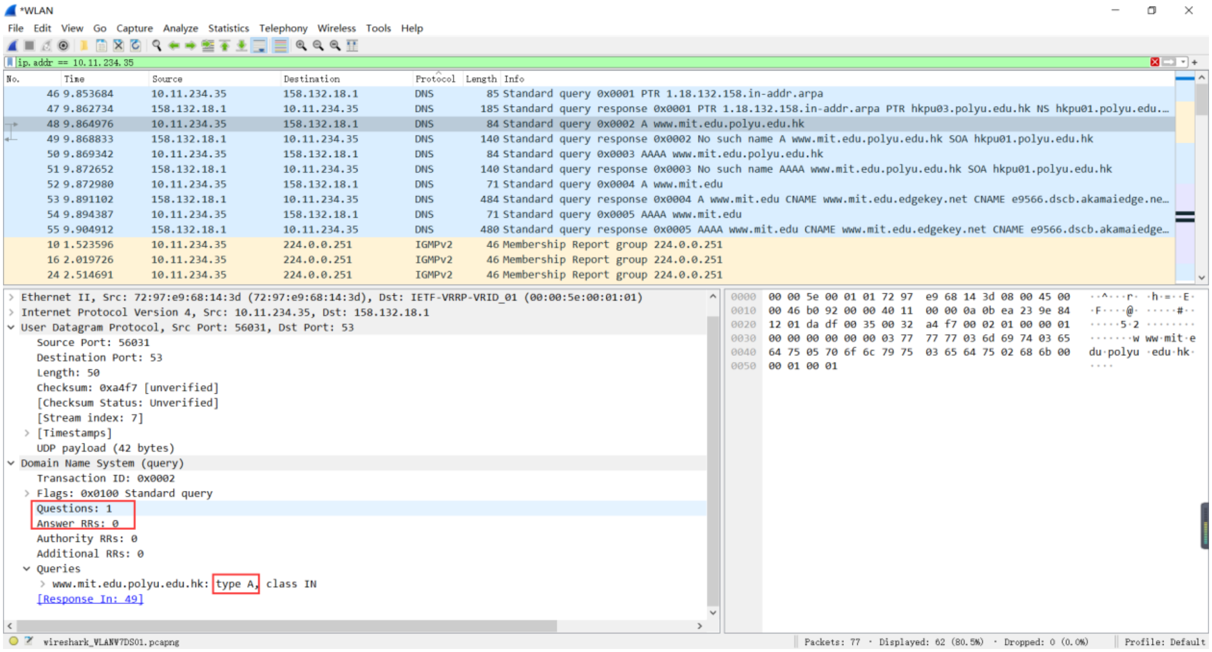

*WLAN
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.11.234.35

No.   Time      Source         Destination    Protocol Length Info
   46 9.853684  10.11.234.35   158.132.18.1   DNS       85 Standard query 0x0001 PTR 1.18.132.158.in-addr.arpa
   47 9.862734  158.132.18.1   10.11.234.35   DNS      185 Standard query response 0x0001 PTR 1.18.132.158.in-addr.arpa PTR hkpu03.polyu.edu.hk NS hkpu01.polyu.edu.…
   48 9.864976  10.11.234.35   158.132.18.1   DNS       84 Standard query 0x0002 A www.mit.edu.polyu.edu.hk
   49 9.868833  158.132.18.1   10.11.234.35   DNS      140 Standard query response 0x0002 No such name A www.mit.edu.polyu.edu.hk SOA hkpu01.polyu.edu.hk
   50 9.869342  10.11.234.35   158.132.18.1   DNS       84 Standard query 0x0003 AAAA www.mit.edu.polyu.edu.hk
   51 9.872652  158.132.18.1   10.11.234.35   DNS      140 Standard query response 0x0003 No such name AAAA www.mit.edu.polyu.edu.hk SOA hkpu01.polyu.edu.hk
   52 9.872980  10.11.234.35   158.132.18.1   DNS       71 Standard query 0x0004 A www.mit.edu
   53 9.891102  158.132.18.1   10.11.234.35   DNS      484 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.ne…
   54 9.894387  10.11.234.35   158.132.18.1   DNS       71 Standard query 0x0005 AAAA www.mit.edu
   55 9.904912  158.132.18.1   10.11.234.35   DNS      480 Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge…
   10 1.523596  10.11.234.35   224.0.0.251    IGMPv2    46 Membership Report group 224.0.0.251
   16 2.019726  10.11.234.35   224.0.0.251    IGMPv2    46 Membership Report group 224.0.0.251
   24 2.514691  10.11.234.35   224.0.0.251    IGMPv2    46 Membership Report group 224.0.0.251

> Frame 53: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits) on interface \Device\NPF_{93EBE42A-FB37
> Ethernet II, Src: Cisco_ff:fc:3c (00:08:e3:ff:fc:3c), Dst: 72:97:e9:68:14:3d (72:97:e9:68:14:3d)
> Internet Protocol Version 4, Src: 158.132.18.1, Dst: 10.11.234.35
v User Datagram Protocol, Src Port: 53, Dst Port: 56033
    Source Port: 53
    Destination Port: 56033
    Length: 450
    Checksum: 0x1803 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 9]
  > [Timestamps]
    UDP payload (442 bytes)
> Domain Name System (response)

0000  72 97 e9 68 14 3d 00 08  e3 ff fc 3c 08 00 45 00   r··h·=·· ···<··E·
0010  01 d6 12 bd 40 00 fc 11  c5 a5 9e 84 12 01 0a 0b   ····@··· ········
0020  ea 23 00 35 da e1 01 c2  18 03 00 04 81 80 00 01   ·#·5···· ········
0030  00 03 00 08 00 09 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 06   du······ ········
0050  cd 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 01 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 4f 75 f0   ·N······ ····hOu·
00a0  c0 54 00 02 00 01 00 00  01 30 00 09 06 6e 35 64   ·T······ ·0···n5d
00b0  73 63 62 c0 59 c0 54 00  02 00 01 00 00 01 30 00   scb·Y·T· ······0·
00c0  09 06 6e 37 64 73 63 62  c0 59 c0 54 00 02 00 01   ··n7dscb ·Y·T····
00d0  00 00 01 30 00 09 06 6e  32 64 73 63 62 c0 59 c0   ···0···n 2dscb·Y·
00e0  54 00 02 00 01 00 00 01  30 00 09 06 6e 30 64 73   T······· 0···n0ds
00f0  63 62 c0 59 c0 54 00 02  00 01 00 00 01 30 00 09   cb·Y·T·· ·····0··
0100  06 6e 36 64 73 63 62 c0  59 c0 54 00 02 00 01 00   ·n6dscb· Y·T·····
0110  00 01 30 00 09 06 6e 33  64 73 63 62 c0 59 c0 54   ··0···n3 dscb·Y·T
0120  00 02 00 01 00 00 01 30  00 09 06 6e 34 64 73 63   ·······0 ···n4dsc
0130  62 c0 59 c0 54 00 02 00  01 00 00 01 30 00 09 06   b·Y·T··· ····0···
0140  6e 31 64 73 63 62 c0 59  c0 82 00 01 00 01 00 00   n1dscb·Y ········
0150  01 30 00 04 17 c8 91 37  c0 c1 00 01 00 01 00 00   ·0·····7 ········
0160  01 30 00 04 58 dd 51 c0  c1 00 00 01 00 01 00 00   ·0··X·Q· ········
0170  01 30 00 04 cb c6 14 d4  c0 d6 00 01 00 01 00 00   ·0······ ········

wireshark_WLANW7DS01.pcapng     Packets: 77 · Displayed: 62 (80.5%) · Dropped: 0 (0.0%)     Profile: Default
```

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

DNS query is Type A.

This message does not contain any answer.


*WLAN
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.11.234.35
No.   Time       Source          Destination     Protocol Length Info
   46 9.853684   10.11.234.35    158.132.18.1    DNS       85 Standard query 0x0001 PTR 1.18.132.158.in-addr.arpa
   47 9.862734   158.132.18.1    10.11.234.35    DNS      185 Standard query response 0x0001 PTR 1.18.132.158.in-addr.arpa PTR hkpu03.polyu.edu.hk NS hkpu01.polyu.edu.…
   48 9.864976   10.11.234.35    158.132.18.1    DNS       84 Standard query 0x0002 A www.mit.edu.polyu.edu.hk
   49 9.868833   158.132.18.1    10.11.234.35    DNS      140 Standard query response 0x0002 No such name A www.mit.edu.polyu.edu.hk SOA hkpu01.polyu.edu.hk
   50 9.869342   10.11.234.35    158.132.18.1    DNS       84 Standard query 0x0003 AAAA www.mit.edu.polyu.edu.hk
   51 9.872652   158.132.18.1    10.11.234.35    DNS      140 Standard query response 0x0003 No such name AAAA www.mit.edu.polyu.edu.hk SOA hkpu01.polyu.edu.hk
   52 9.872980   10.11.234.35    158.132.18.1    DNS       71 Standard query 0x0004 A www.mit.edu
   53 9.891102   158.132.18.1    10.11.234.35    DNS      484 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.ne…
   54 9.894387   10.11.234.35    158.132.18.1    DNS       71 Standard query 0x0005 AAAA www.mit.edu
   55 9.904912   158.132.18.1    10.11.234.35    DNS      480 Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge…
   10 1.523596   10.11.234.35    224.0.0.251     IGMPv2    46 Membership Report group 224.0.0.251
   16 2.019726   10.11.234.35    224.0.0.251     IGMPv2    46 Membership Report group 224.0.0.251
   24 2.514691   10.11.234.35    224.0.0.251     IGMPv2    46 Membership Report group 224.0.0.251
```

```
> Ethernet II, Src: 72:97:e9:68:14:3d (72:97:e9:68:14:3d), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.11.234.35, Dst: 158.132.18.1
v User Datagram Protocol, Src Port: 56031, Dst Port: 53
    Source Port: 56031
    Destination Port: 53
    Length: 50
    Checksum: 0xa4f7 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
  > [Timestamps]
    UDP payload (42 bytes)
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.mit.edu.polyu.edu.hk: type A, class IN
    [Response In: 49]
```

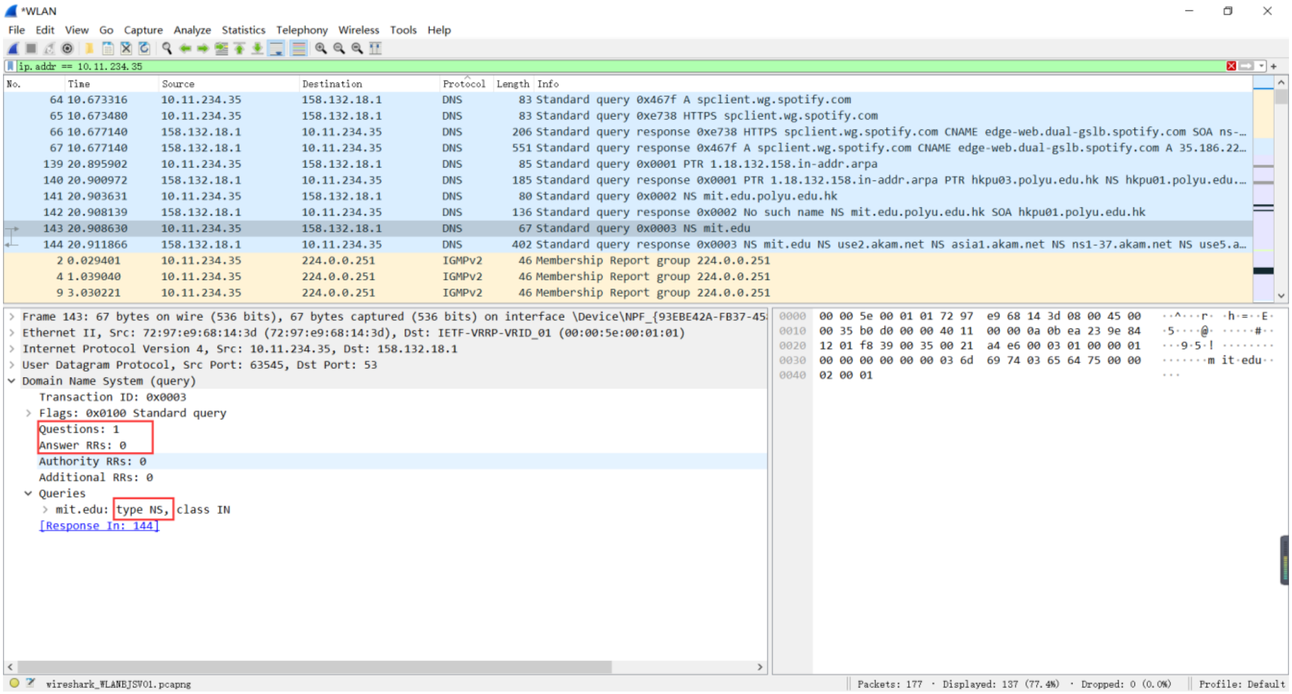
```
0000  00 00 5e 00 01 01 72 97  e9 68 14 3d 08 00 45 00   ··^···r· ·h·=··E·
0010  00 46 b0 92 00 00 40 11  00 00 0a 0b ea 23 9e 84   ·F····@· ·····#··
0020  12 01 da df 00 35 00 32  a4 f7 00 02 01 00 00 01   ·····5·2 ········
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 05 70 6f 6c 79 75  03 65 64 75 02 68 6b 00   du·polyu ·edu·hk·
0050  00 01 00 01                                        ····
```

```
wireshark_WLANW7DS01.pcapng    Packets: 77 · Displayed: 62 (80.5%) · Dropped: 0 (0.0%)    Profile: Default
```

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

DNS query is type NS.

Query message does not contain any answers.


*WLAN
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.11.234.35
No.   Time        Source          Destination     Protocol Length Info
   64 10.673316   10.11.234.35    158.132.18.1    DNS       83 Standard query 0x467f A spclient.wg.spotify.com
   65 10.673480   10.11.234.35    158.132.18.1    DNS       83 Standard query 0xe738 HTTPS spclient.wg.spotify.com
   66 10.677140   158.132.18.1    10.11.234.35    DNS      206 Standard query response 0xe738 HTTPS spclient.wg.spotify.com CNAME edge-web.dual-gslb.spotify.com SOA ns-…
   67 10.677140   158.132.18.1    10.11.234.35    DNS      551 Standard query response 0x467f A spclient.wg.spotify.com CNAME edge-web.dual-gslb.spotify.com A 35.186.22…
  139 20.895902   10.11.234.35    158.132.18.1    DNS       85 Standard query 0x0001 PTR 1.18.132.158.in-addr.arpa
  140 20.900972   158.132.18.1    10.11.234.35    DNS      185 Standard query response 0x0001 PTR 1.18.132.158.in-addr.arpa PTR hkpu03.polyu.edu.hk NS hkpu01.polyu.edu.…
  141 20.903631   10.11.234.35    158.132.18.1    DNS       80 Standard query 0x0002 NS mit.edu.polyu.edu.hk
  142 20.908139   158.132.18.1    10.11.234.35    DNS      136 Standard query response 0x0002 No such name NS mit.edu.polyu.edu.hk SOA hkpu01.polyu.edu.hk
  143 20.908630   10.11.234.35    158.132.18.1    DNS       67 Standard query 0x0003 NS mit.edu
  144 20.911866   158.132.18.1    10.11.234.35    DNS      402 Standard query response 0x0003 NS mit.edu NS use2.akam.net NS asia1.akam.net NS ns1-37.akam.net NS use5.a…
    2 0.029401    10.11.234.35    224.0.0.251     IGMPv2    46 Membership Report group 224.0.0.251
    4 1.039040    10.11.234.35    224.0.0.251     IGMPv2    46 Membership Report group 224.0.0.251
    9 3.030221    10.11.234.35    224.0.0.251     IGMPv2    46 Membership Report group 224.0.0.251
```

```
> Frame 143: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{93EBE42A-FB37-45
> Ethernet II, Src: 72:97:e9:68:14:3d (72:97:e9:68:14:3d), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.11.234.35, Dst: 158.132.18.1
> User Datagram Protocol, Src Port: 63545, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > mit.edu: type NS, class IN
    [Response In: 144]
```

```
0000  00 00 5e 00 01 01 72 97  e9 68 14 3d 08 00 45 00   ··^···r· ·h·=··E·
0010  00 35 b0 d0 00 00 40 11  00 00 0a 0b ea 23 9e 84   ·5····@· ·····#··
0020  12 01 f8 39 00 35 00 21  a4 e6 00 03 01 00 00 01   ···9·5·! ········
0030  00 00 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  02 00 01                                           ···
```

```
wireshark_WLANBJSV01.pcapng    Packets: 177 · Displayed: 137 (77.4%) · Dropped: 0 (0.0%)    Profile: Default
```