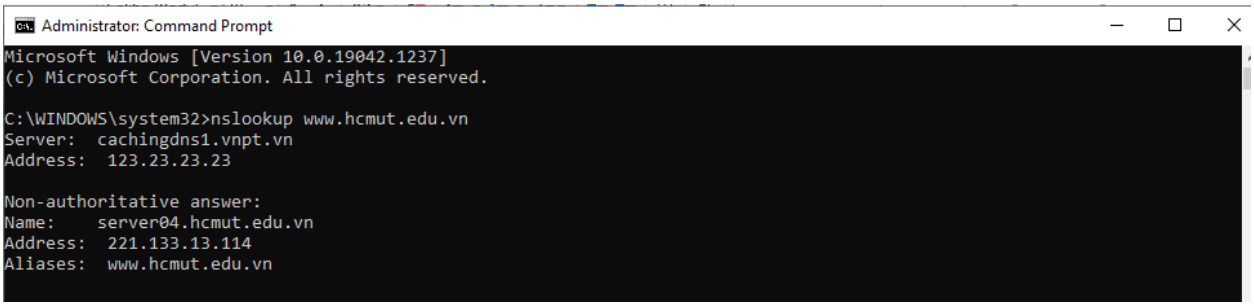
Họ tên : Lê Bảo Khánh
MSSV : 1911363
Lớp : L01

LAB 2b

1. nslookup

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

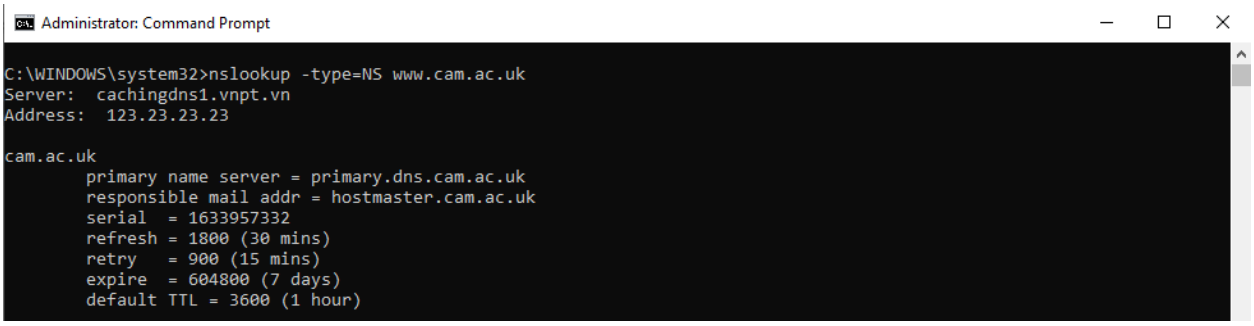
ANSWER:



IP address of server: 221.133.13.114

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

ANSWER:



Authoritative DNS server: primary.dns.cam.ac.uk

Question 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?

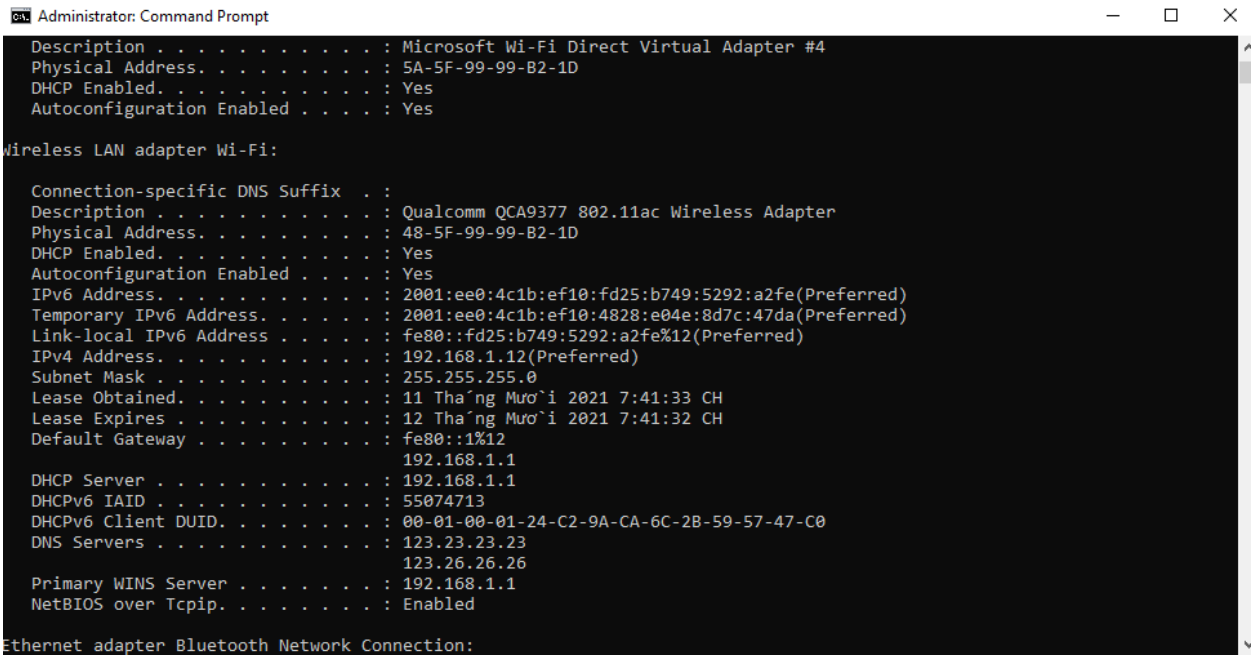
ANSWER:

IP address for Yahoo! mail server: 106.10.236.40

2. ipconfig

3. Tracing DNS with Wireshark

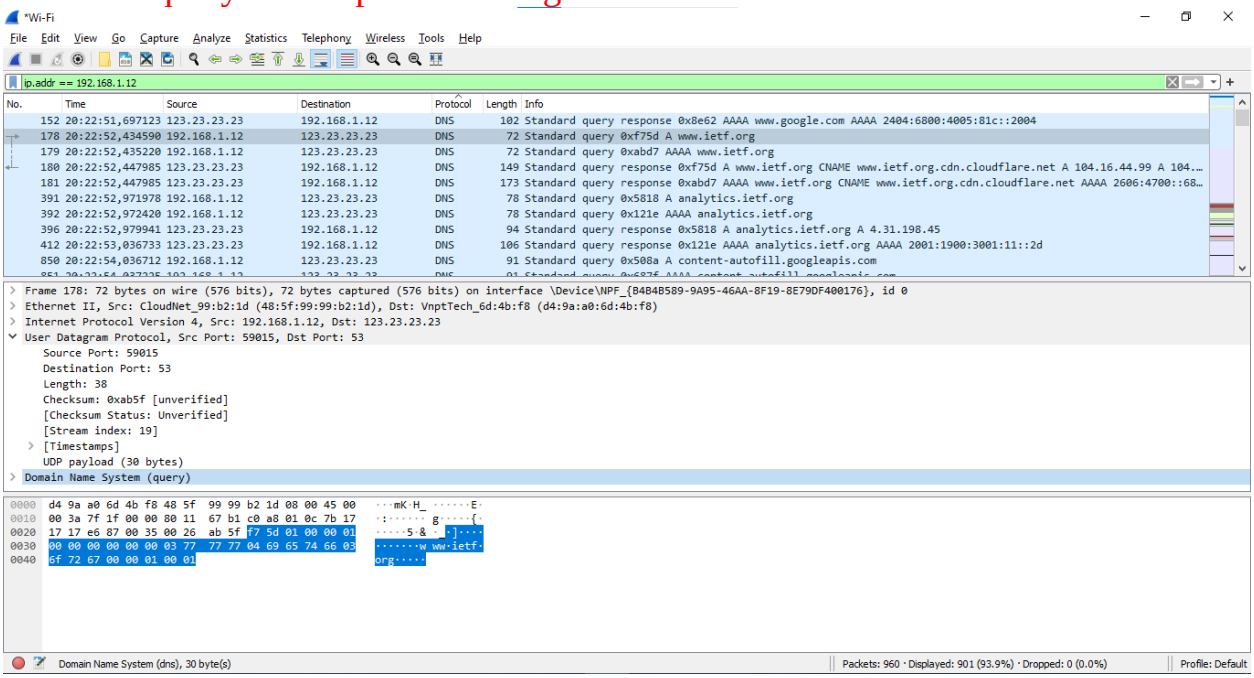
My IP address: 192.168.1.12



<u>Question 4</u>: Locate the DNS query and response messages. Are then sent over UDP or TCP?

ANSWER:

The DNS query and response message are sent over UDP



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

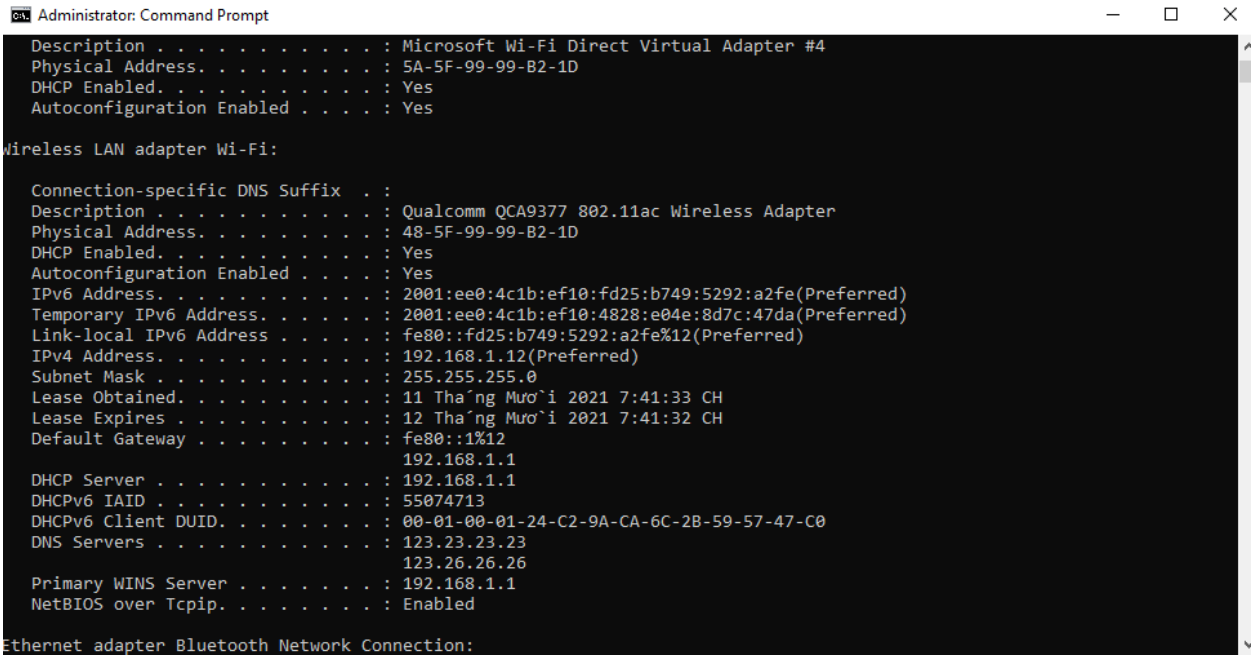
ANSWER:

The destination port: 53
The source port: 59015

Question 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?

ANSWER:

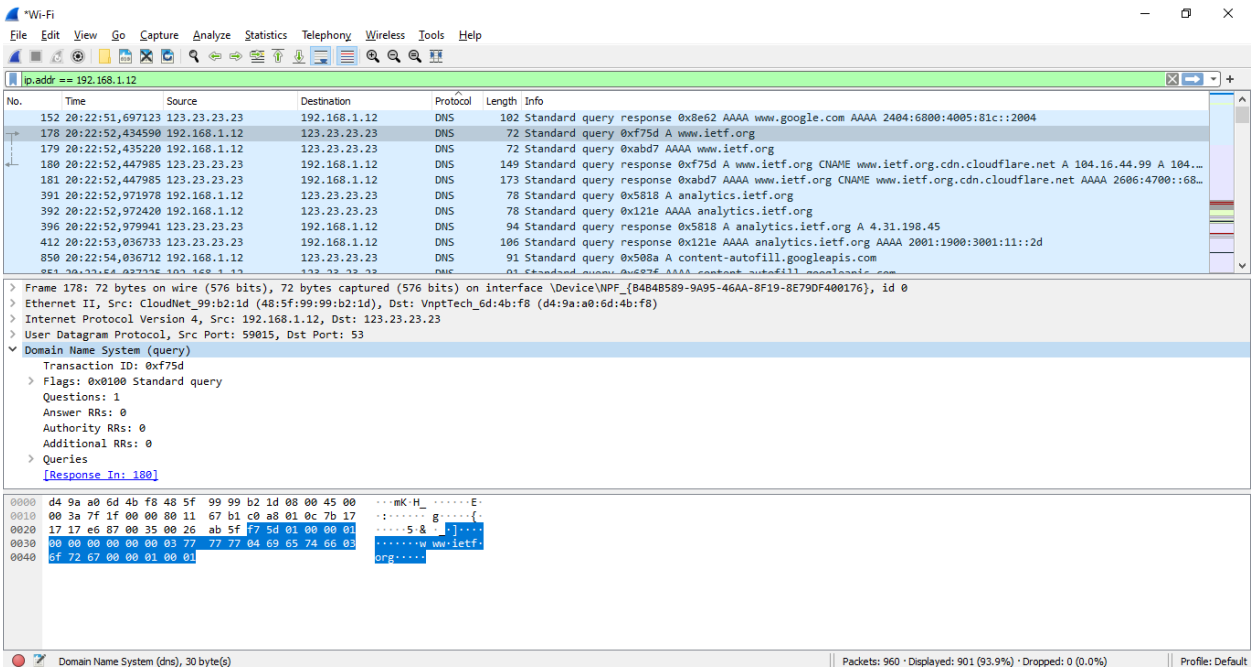
It's sent to 192.168.1.1, which is the IP address of one of my local DNS servers



Question 7: Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

ANSWER:

It's a type A Standard Query and it doesn't contain any answers.



Question 8: Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

ANSWER:

There were 3 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address

```
No.     Time               Source               Destination          Protocol Length Info
    180 20:22:52,447985    123.23.23.23         192.168.1.12         DNS      149    Standard query response 0xf75d A
www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
Frame 180: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface
\Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
Ethernet II, Src: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8), Dst: CloudNet_99:b2:1d (48:5f:99:99:b2:1d)
Internet Protocol Version 4, Src: 123.23.23.23, Dst: 192.168.1.12
User Datagram Protocol, Src Port: 53, Dst Port: 59015
Domain Name System (response)
    Transaction ID: 0xf75d
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.ietf.org: type A, class IN
    Answers
        www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
        www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
        www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
    [Request In: 178]
    [Time: 0.013395000 seconds]
```

Question 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?

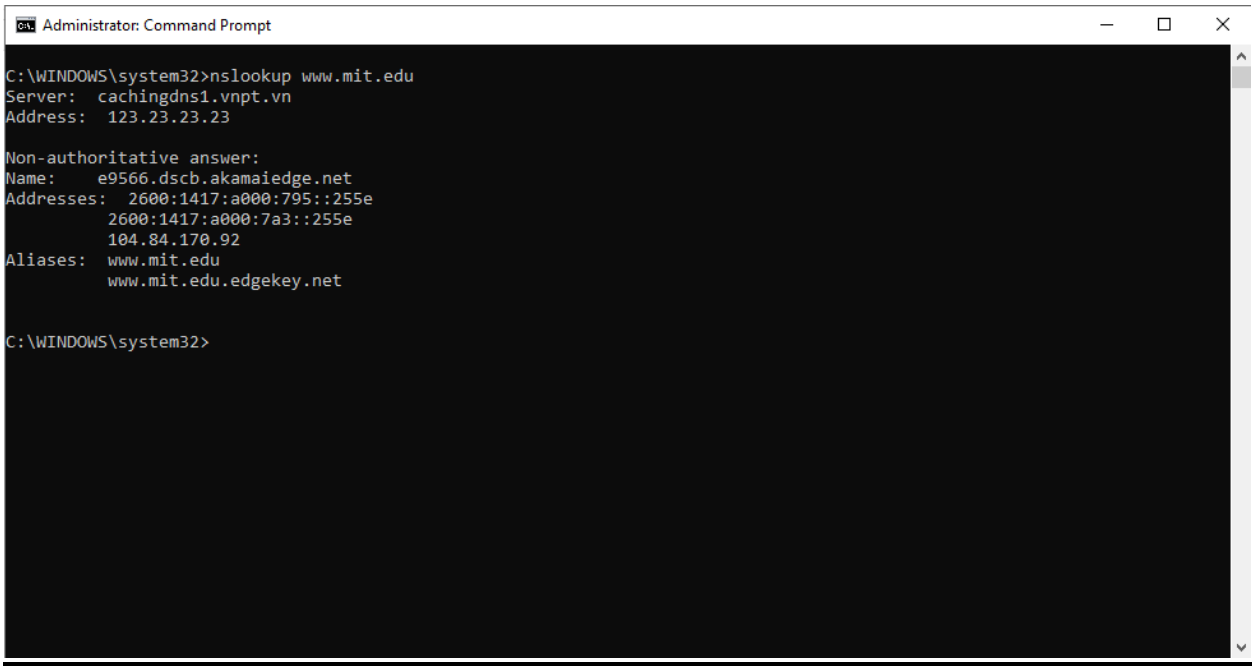
ANSWER:

The first SYN packet was sent to 104.16.44.99 which corresponds to the first IP address provided in the DNS response message.

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

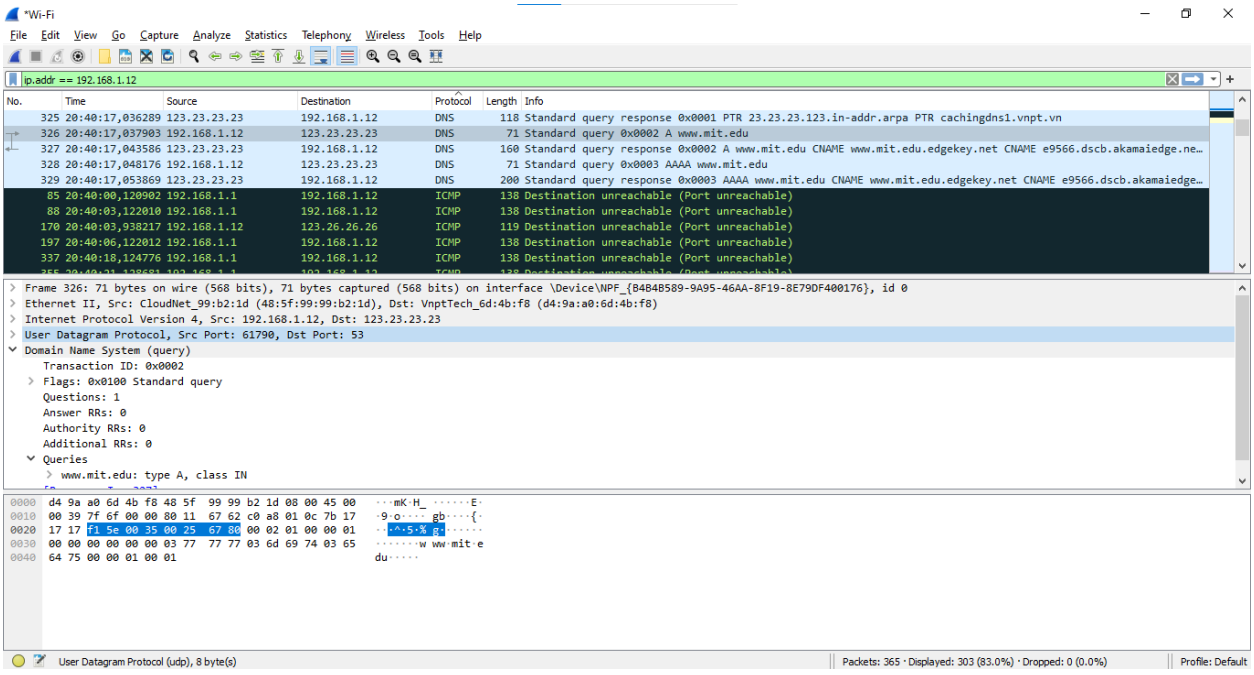
ANSWER:

No



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

ANSWER:



Destination Port: 53
Source Port: 61790

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

ANSWER:

It's sent to 123.23.23.23, which is the IP address of one of my local DNS servers

Question 13: Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

ANSWER:

The query is of type A and it doesn't contain any answers.

Question 14: Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

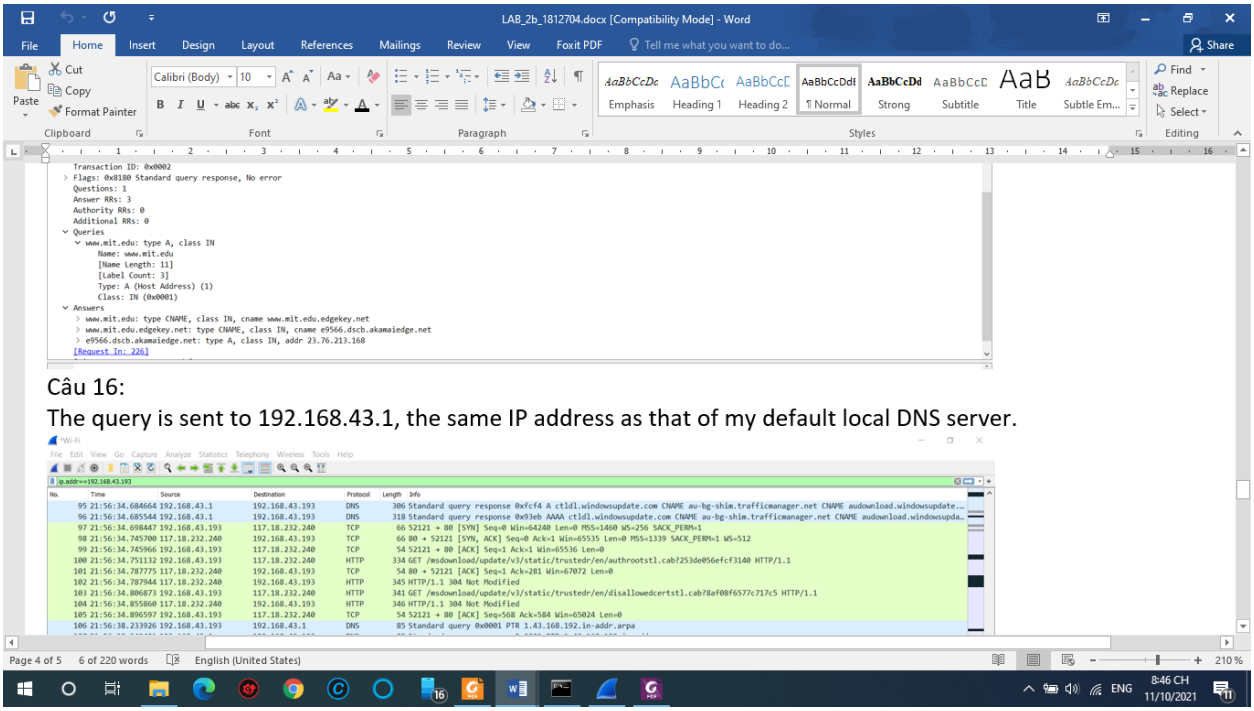
ANSWER:

The response DNS message contains 3 answer containing the name of the host, the type of address, the class, and the IP address.

```
No.     Time              Source                Destination           Protocol Length Info
    327 20:40:17,043586    123.23.23.23          192.168.1.12          DNS      160    Standard query response 0x0002 A www.mit.edu
CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.84.170.92
Frame 327: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface
\Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
Ethernet II, Src: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8), Dst: CloudNet_99:b2:1d (48:5f:99:99:b2:1d)
Internet Protocol Version 4, Src: 123.23.23.23, Dst: 192.168.1.12
User Datagram Protocol, Src Port: 53, Dst Port: 61790
Domain Name System (response)
    Transaction ID: 0x0002
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.mit.edu: type A, class IN
    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 104.84.170.92
    [Request In: 326]
    [Time: 0.005683000 seconds]
```

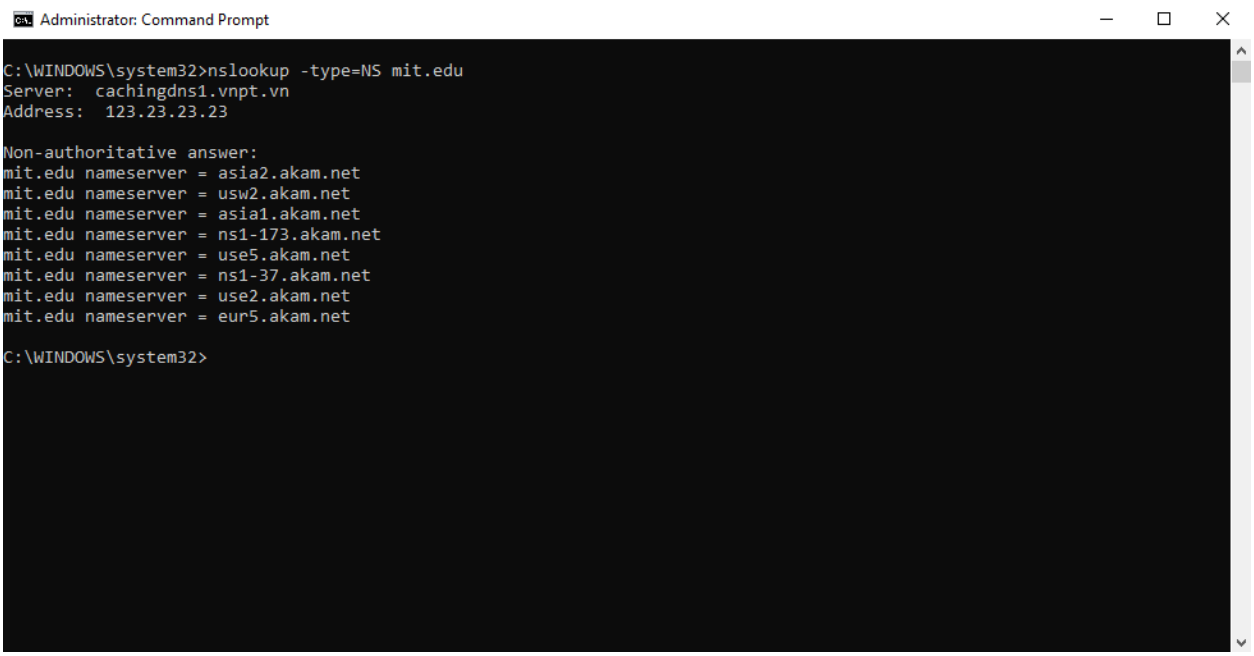
Question 15: Provide a screenshot.

ANSWER:



Câu 16:

The query is sent to 192.168.43.1, the same IP address as that of my default local DNS server.



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

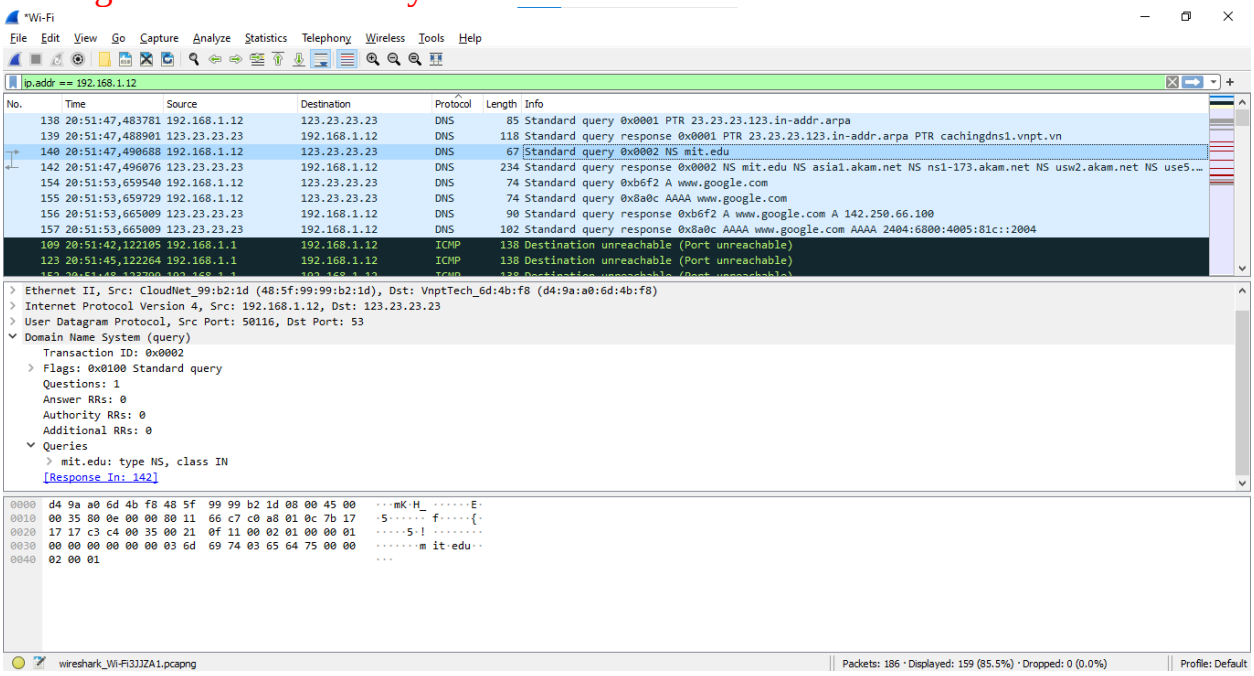
ANSWER:

It was sent to 123.23.23.23 which is my default DNS server.

Question 17: Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

ANSWER:

The DNS query is a type "NS" message including one question. The query message did not contain any answers.



Question 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 namesers?

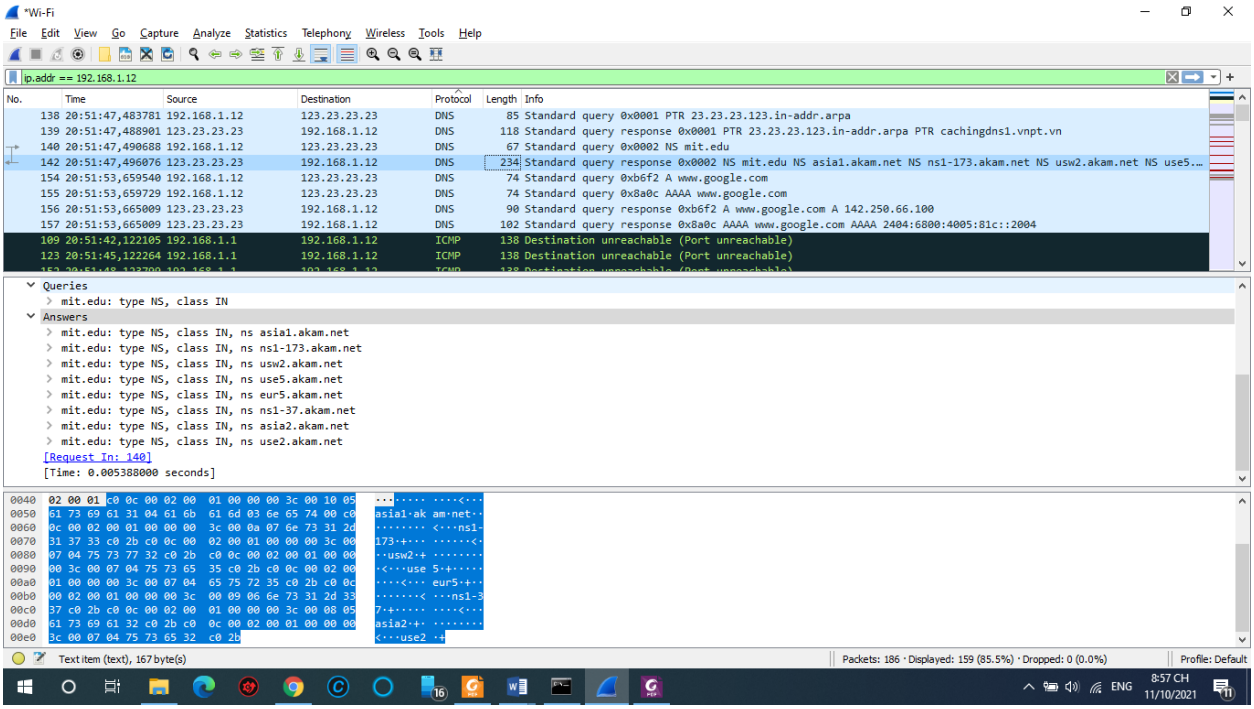
ANSWER:

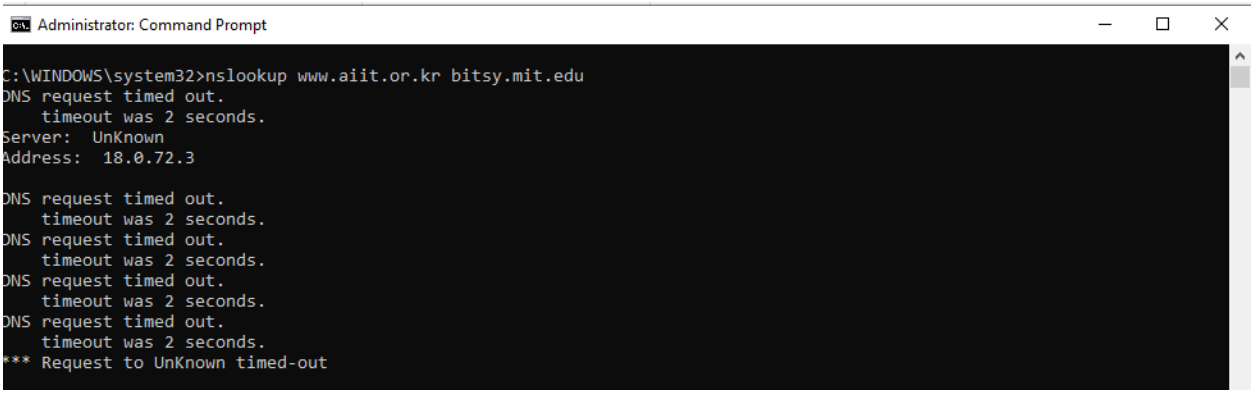
The nameservers are asia1, ns1-173, usw2, use5, eur5, ns1-37, asia2m use2. We can find their IP addresses as seen below.

```
\Device\NPF_{B4B4B589-9A95-46AA-8F19-8E79DF400176}, id 0
Ethernet II, Src: VnptTech_6d:4b:f8 (d4:9a:a0:6d:4b:f8), Dst: CloudNet_99:b2:1d (48:5f:99:99:b2:1d)
Internet Protocol Version 4, Src: 123.23.23.23, Dst: 192.168.1.12
User Datagram Protocol, Src Port: 53, Dst Port: 50116
Domain Name System (response)
    Transaction ID: 0x0002
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
    Queries
        mit.edu: type NS, class IN
    Answers
        mit.edu: type NS, class IN, ns asia1.akam.net
        mit.edu: type NS, class IN, ns ns1-173.akam.net
        mit.edu: type NS, class IN, ns usw2.akam.net
        mit.edu: type NS, class IN, ns use5.akam.net
        mit.edu: type NS, class IN, ns eur5.akam.net
        mit.edu: type NS, class IN, ns ns1-37.akam.net
        mit.edu: type NS, class IN, ns asia2.akam.net
        mit.edu: type NS, class IN, ns use2.akam.net
    [Request In: 140]
    [Time: 0.005388000 seconds]
```

Question 19: Provide a screenshot.

ANSWER:





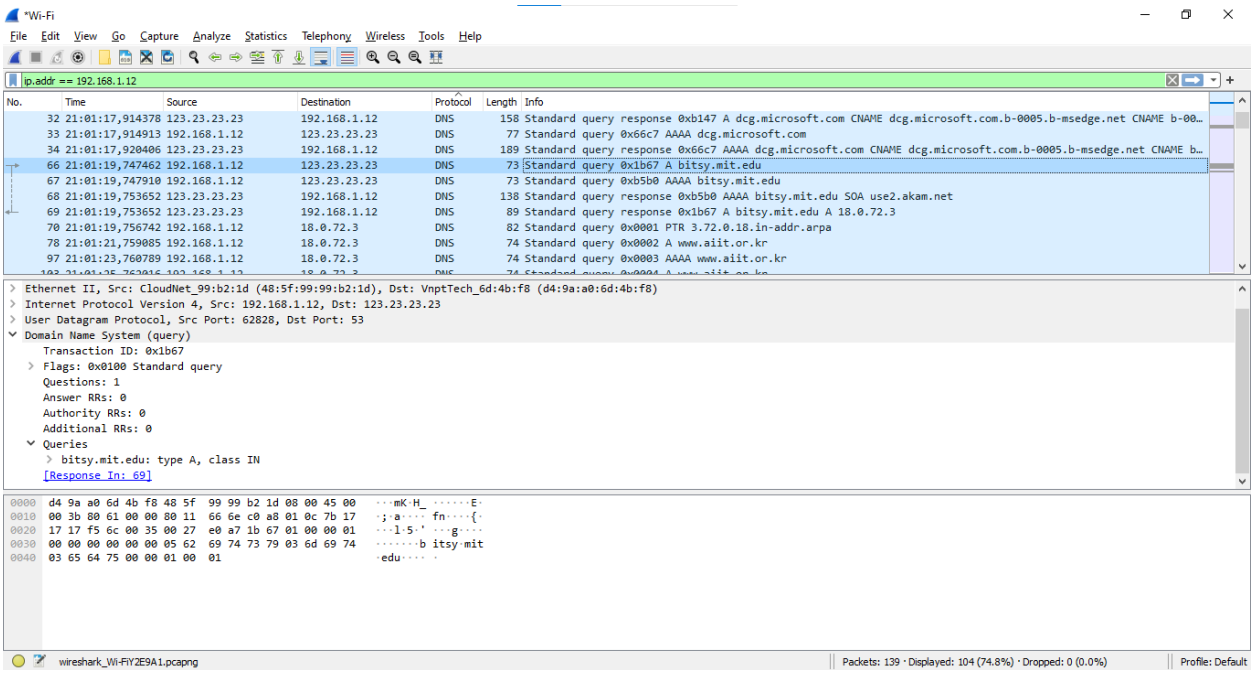
Question 20: To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

ANSWER:

The query is sent to 18.72.0.3 which corresponds to bitsy.mit.edu.

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

ANSWER:



It's a standard type A query that doesn't contain any answers

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

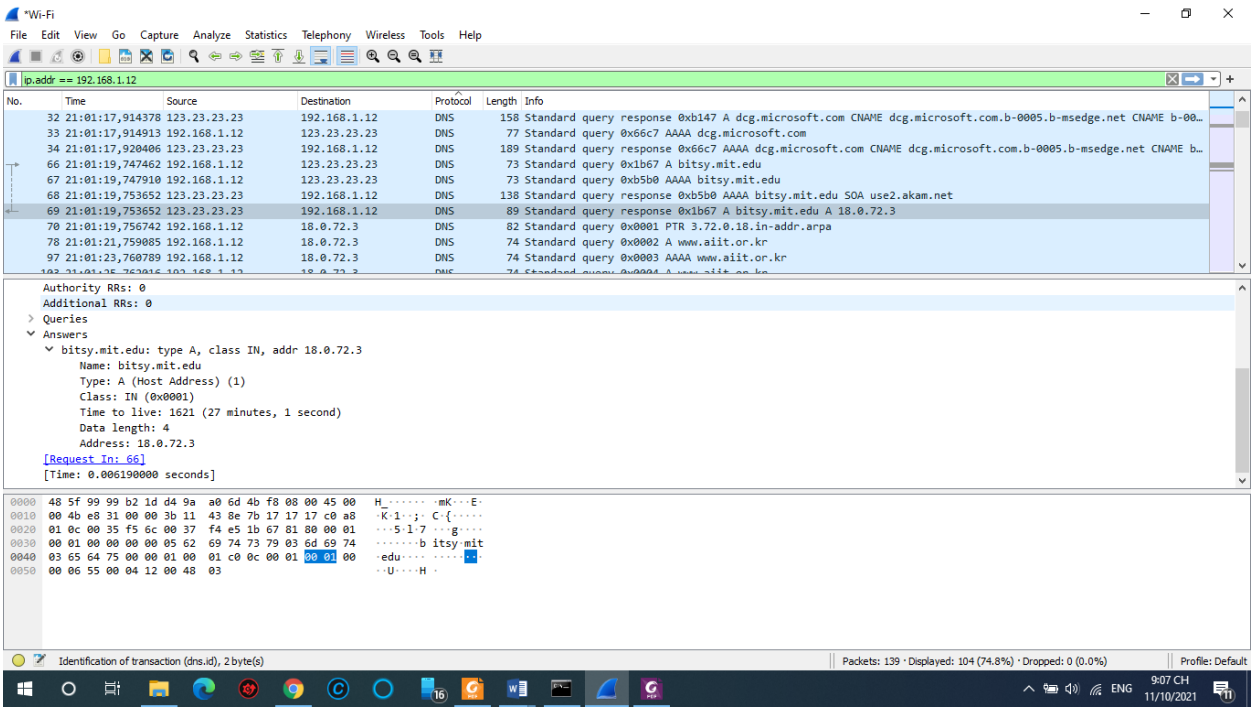
ANSWER:

One answer is provided in the DNS response message

```
Answers
    bitsy.mit.edu: type A, class IN, addr 18.0.72.3
        Name: bitsy.mit.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1621 (27 minutes, 1 second)
        Data length: 4
        Address: 18.0.72.3
[Request In: 66]
[Time: 0.006190000 seconds]
```

Question 23: Provide a screenshot

ANSWER:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.12
No. Time Source Destination Protocol Length Info
32 21:01:17,914378 123.23.23.23 192.168.1.12 DNS 158 Standard query response 0xb147 A dcg.microsoft.com CNAME dcg.microsoft.com.b-0005.b-msedge.net CNAME b-00…
33 21:01:17,914913 192.168.1.12 123.23.23.23 DNS 77 Standard query 0x66c7 AAAA dcg.microsoft.com
34 21:01:17,920406 123.23.23.23 192.168.1.12 DNS 189 Standard query response 0x66c7 AAAA dcg.microsoft.com CNAME dcg.microsoft.com.b-0005.b-msedge.net CNAME b…
66 21:01:19,747462 192.168.1.12 123.23.23.23 DNS 73 Standard query 0x1b67 A bitsy.mit.edu
67 21:01:19,747910 192.168.1.12 123.23.23.23 DNS 73 Standard query 0xb5b0 AAAA bitsy.mit.edu
68 21:01:19,753652 123.23.23.23 192.168.1.12 DNS 138 Standard query response 0xb5b0 AAAA bitsy.mit.edu SOA use2.akam.net
69 21:01:19,753652 123.23.23.23 192.168.1.12 DNS 89 Standard query response 0x1b67 A bitsy.mit.edu A 18.0.72.3
70 21:01:19,756742 192.168.1.12 18.0.72.3 DNS 82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
78 21:01:21,759085 192.168.1.12 18.0.72.3 DNS 74 Standard query 0x0002 A www.aiit.or.kr
97 21:01:23,760789 192.168.1.12 18.0.72.3 DNS 74 Standard query 0x0003 AAAA www.aiit.or.kr
Authority RRs: 0
Additional RRs: 0
Queries
Answers
bitsy.mit.edu: type A, class IN, addr 18.0.72.3
Name: bitsy.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1621 (27 minutes, 1 second)
Data length: 4
Address: 18.0.72.3
[Request In: 66]
[Time: 0.006190000 seconds]
0000 48 5f 99 99 b2 1d d4 9a a0 6d 4b f8 08 00 45 00
0010 00 4b e8 31 00 00 3b 11 43 8e 7b 17 17 17 c0 a8
0020 01 0c 00 35 f5 6c 00 37 f4 e5 1b 67 81 80 00 01
0030 00 01 00 00 00 00 05 62 69 74 73 79 03 6d 69 74
0040 03 65 64 75 00 00 01 00 01 c0 0c 00 01 00 01 00
0050 00 06 55 00 04 12 00 48 03
Identification of transaction (dns.id), 2 byte(s)
Packets: 139 · Displayed: 104 (74.8%) · Dropped: 0 (0.0%)
Profile: Default
ENG
9:07 CH
11/10/2021