UFU 45 ANOS

Prática 3 - Wireshark LAB – DNS

Redes de Comunicações I

Gabriel Resende Soares

11721ECP011

Leonardo Vecchi Meirelles

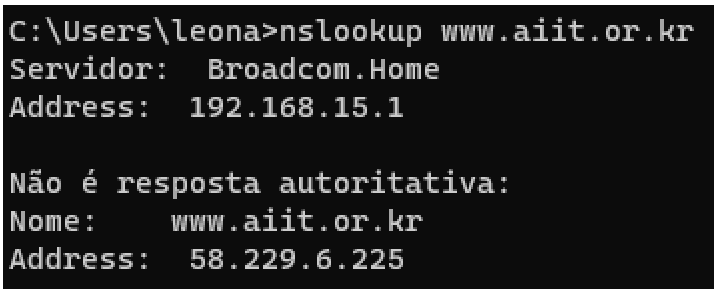
12011ECP002

Setembro 2023

Sumário

Nslookup

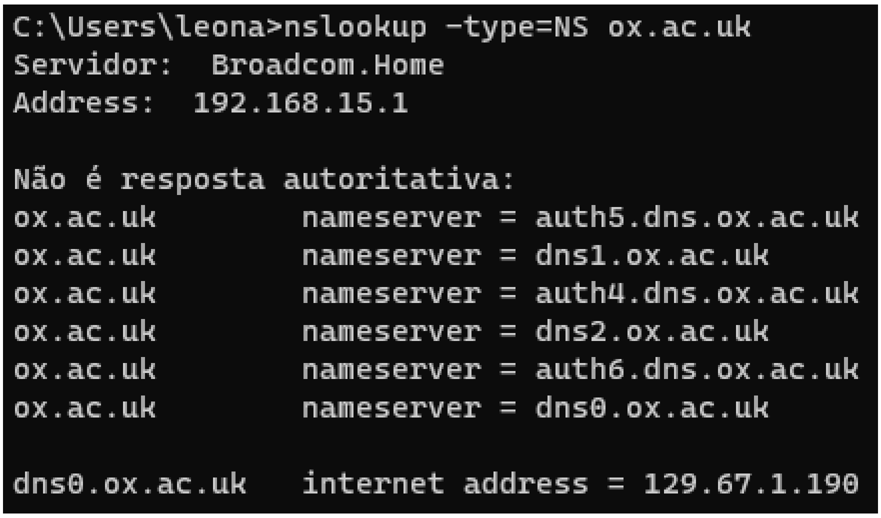
1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?



```
C:\Users\leona>nslookup www.aiit.or.kr
Servidor:  Broadcom.Home
Address:  192.168.15.1

Não é resposta autoritativa:
Nome:    www.aiit.or.kr
Address:  58.229.6.225
```

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

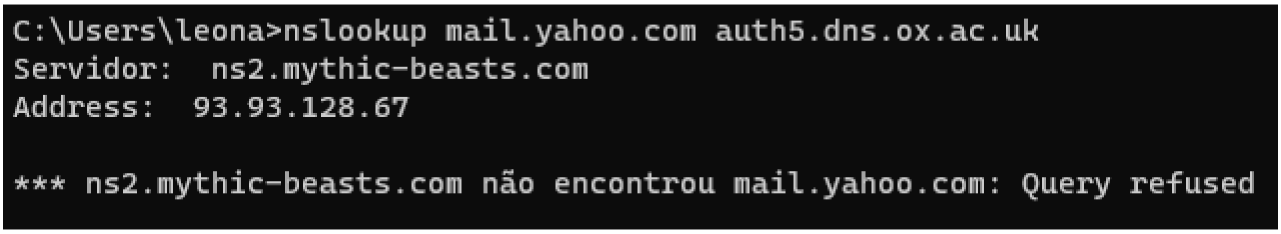


```
C:\Users\leona>nslookup -type=NS ox.ac.uk
Servidor:  Broadcom.Home
Address:  192.168.15.1

Não é resposta autoritativa:
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk
ox.ac.uk        nameserver = dns1.ox.ac.uk
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk
ox.ac.uk        nameserver = dns2.ox.ac.uk
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk
ox.ac.uk        nameserver = dns0.ox.ac.uk

dns0.ox.ac.uk   internet address = 129.67.1.190
```

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?



```
C:\Users\leona>nslookup mail.yahoo.com auth5.dns.ox.ac.uk
Servidor:  ns2.mythic-beasts.com
Address:  93.93.128.67

*** ns2.mythic-beasts.com não encontrou mail.yahoo.com: Query refused
```

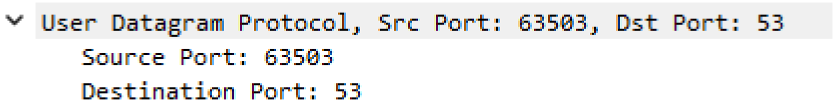
Tracing DNS with Wireshark

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

As respostas foram enviadas por UDP.

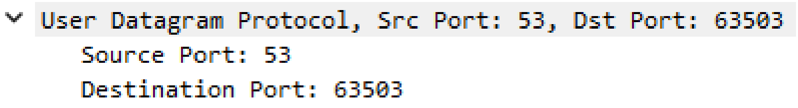
5. What is the destination port for the DNS query message? What is the source port of DNS response message?

Para a mensagem de DNS query, a porta de destino é: 53.



```
⌄ User Datagram Protocol, Src Port: 63503, Dst Port: 53
     Source Port: 63503
     Destination Port: 53
```

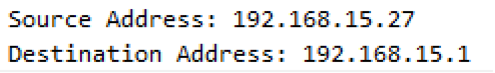
A porta de origem para a mensagem de DNS response é: 53.



```
⌄ User Datagram Protocol, Src Port: 53, Dst Port: 63503
     Source Port: 53
     Destination Port: 63503
```

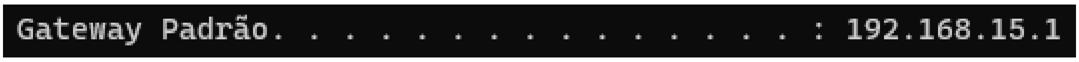
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

A mensagem DNS querry foi mandada para o IP:



```
Source Address: 192.168.15.27
Destination Address: 192.168.15.1
```

E pelo ipconfig:

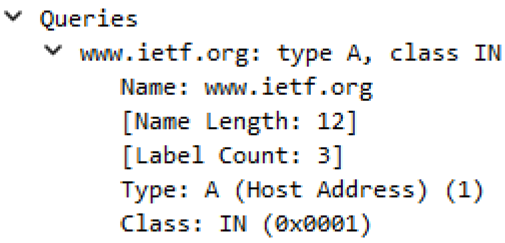


```
Gateway Padrão. . . . . . . . . . . . . . : 192.168.15.1
```

Os endereços são os mesmos.

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

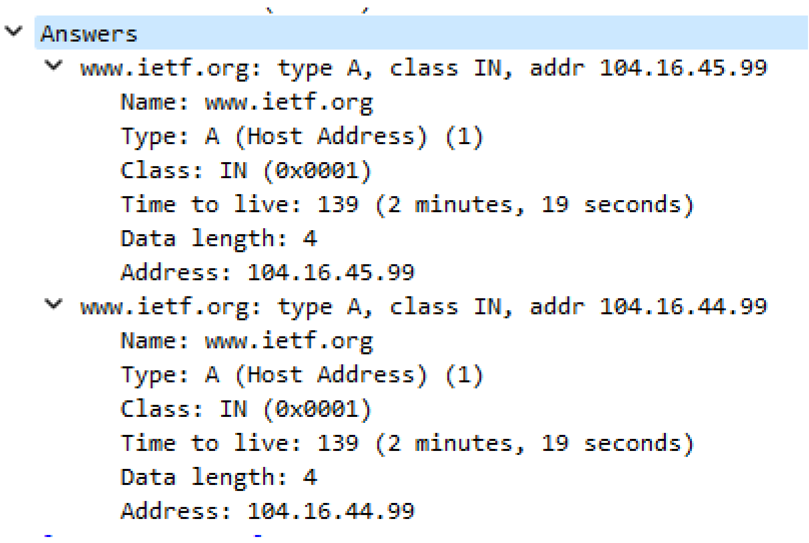
Type A, class IN. Não contém « answers ».



```
⌄ Queries
   ⌄ www.ietf.org: type A, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

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

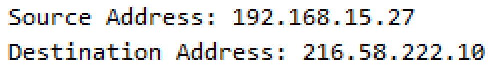
2 « answers » são apresentadas. O conteúdo delas está abaixo:



```
Answers
  www.ietf.org: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 139 (2 minutes, 19 seconds)
      Data length: 4
      Address: 104.16.45.99
  www.ietf.org: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 139 (2 minutes, 19 seconds)
      Data length: 4
      Address: 104.16.44.99
```

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?

O IP de destino é:



```
Source Address: 192.168.15.27
Destination Address: 216.58.222.10
```

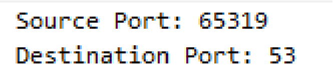
E não corresponde a nenhum IP apresentado na mensagem de resposta DNS.

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

Não.

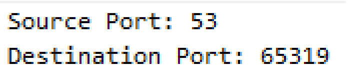
11. What is the destination port for the DNS query message? What is the source port of DNS response message?

A porta de destino da DNS querry message foi:



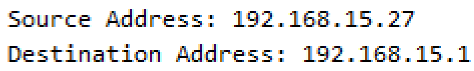
```
Source Port: 65319
Destination Port: 53
```

A porta de origem da DNS response message foi:



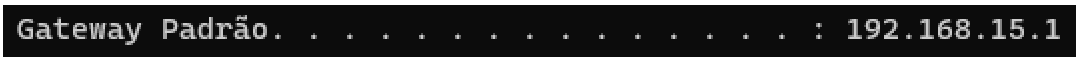
```
Source Port: 53
Destination Port: 65319
```

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



```
Source Address: 192.168.15.27
Destination Address: 192.168.15.1
```

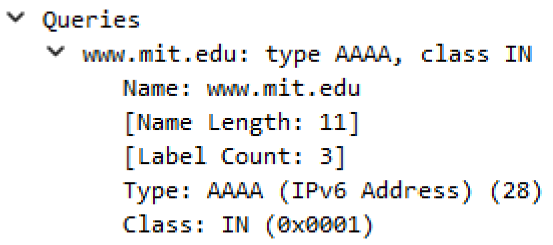
Sim, é meu IP local padrão para servidores DNS.



```
Gateway Padrão. . . . . . . . . . . . . . : 192.168.15.1
```

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

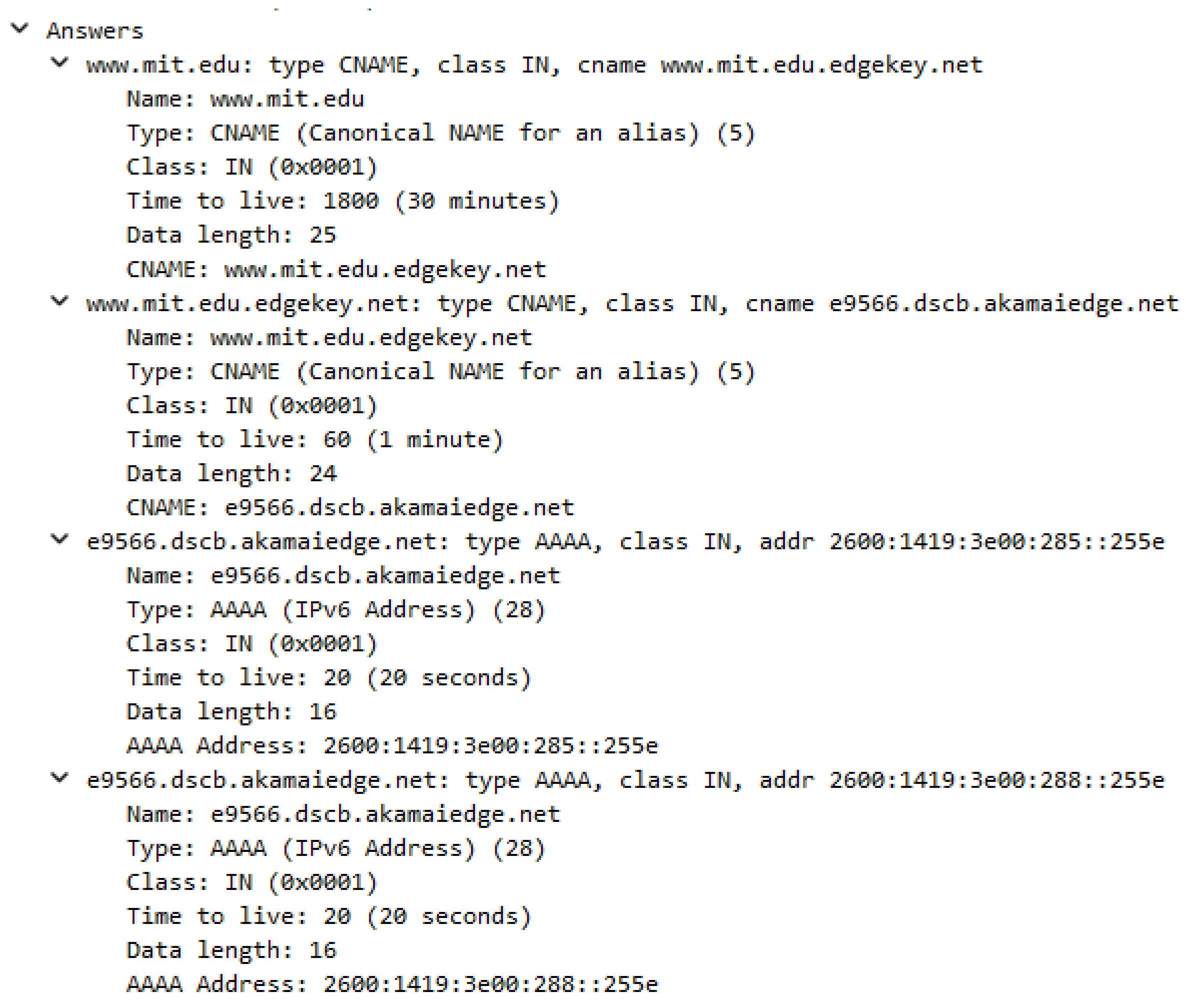
Type « AAAA », class IN. Não contém « answers ».



```
⌄ Queries
  ⌄ www.mit.edu: type AAAA, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
```

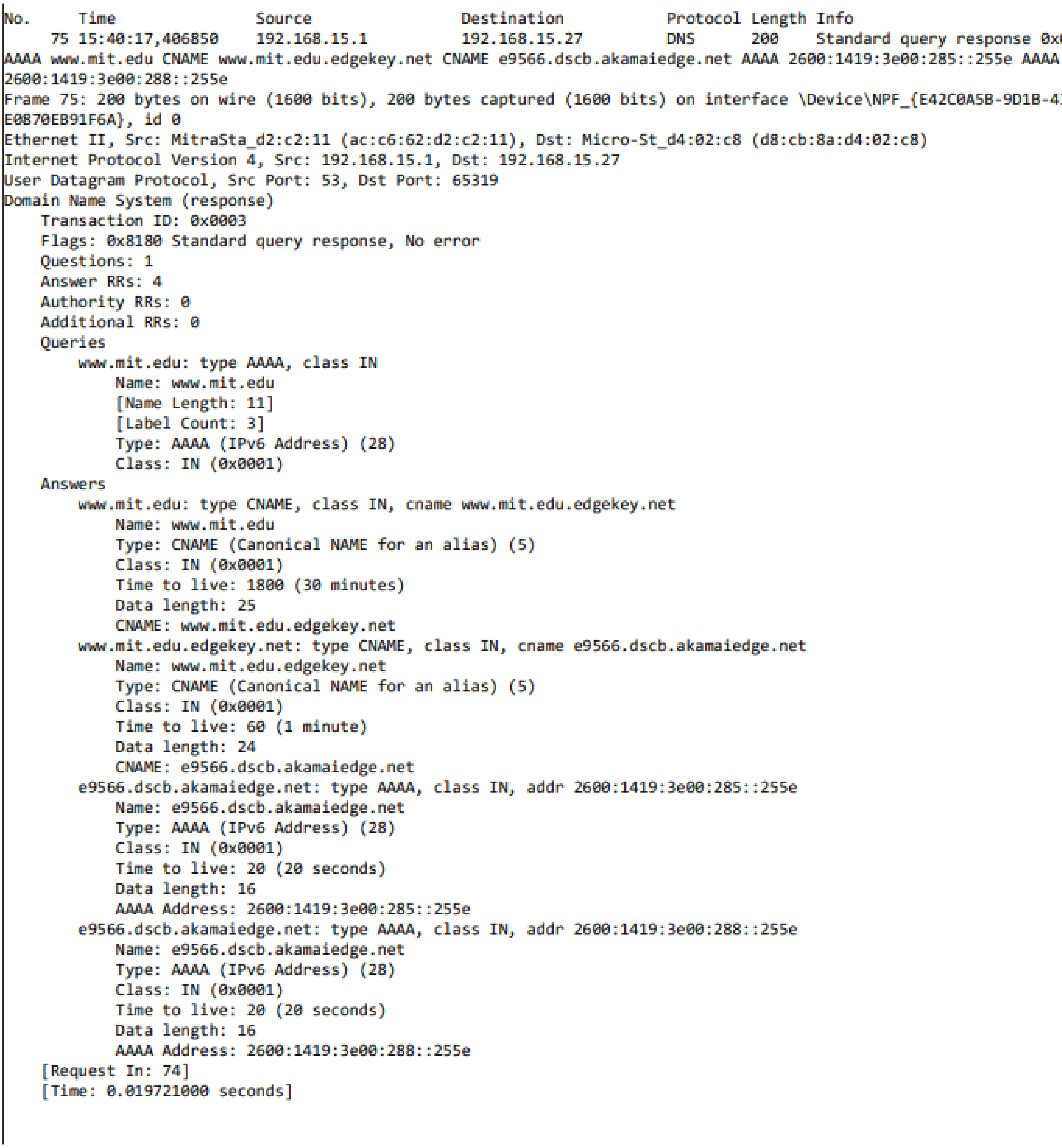
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Contém 4 « answers ». O conteúdo de cada uma é apresentado abaixo:



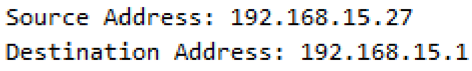
```
⌄ Answers
  ⌄ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  ⌄ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 60 (1 minute)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  ⌄ e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1419:3e00:285::255e
      Name: e9566.dscb.akamaiedge.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 16
      AAAA Address: 2600:1419:3e00:285::255e
  ⌄ e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1419:3e00:288::255e
      Name: e9566.dscb.akamaiedge.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 16
      AAAA Address: 2600:1419:3e00:288::255e
```

15. Provide a screenshot.



```
No.     Time               Source                Destination           Protocol Length Info
     75 15:40:17,406850    192.168.15.1          192.168.15.27         DNS      200    Standard query response 0x0
AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2600:1419:3e00:285::255e AAAA
2600:1419:3e00:288::255e
Frame 75: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4
E0870EB91F6A}, id 0
Ethernet II, Src: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11), Dst: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8)
Internet Protocol Version 4, Src: 192.168.15.1, Dst: 192.168.15.27
User Datagram Protocol, Src Port: 53, Dst Port: 65319
Domain Name System (response)
    Transaction ID: 0x0003
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.mit.edu: type AAAA, class IN
            Name: www.mit.edu
            [Name Length: 11]
            [Label Count: 3]
            Type: AAAA (IPv6 Address) (28)
            Class: IN (0x0001)
    Answers
        www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
            Name: www.mit.edu
            Type: CNAME (Canonical NAME for an alias) (5)
            Class: IN (0x0001)
            Time to live: 1800 (30 minutes)
            Data length: 25
            CNAME: www.mit.edu.edgekey.net
        www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
            Name: www.mit.edu.edgekey.net
            Type: CNAME (Canonical NAME for an alias) (5)
            Class: IN (0x0001)
            Time to live: 60 (1 minute)
            Data length: 24
            CNAME: e9566.dscb.akamaiedge.net
        e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1419:3e00:285::255e
            Name: e9566.dscb.akamaiedge.net
            Type: AAAA (IPv6 Address) (28)
            Class: IN (0x0001)
            Time to live: 20 (20 seconds)
            Data length: 16
            AAAA Address: 2600:1419:3e00:285::255e
        e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1419:3e00:288::255e
            Name: e9566.dscb.akamaiedge.net
            Type: AAAA (IPv6 Address) (28)
            Class: IN (0x0001)
            Time to live: 20 (20 seconds)
            Data length: 16
            AAAA Address: 2600:1419:3e00:288::255e
    [Request In: 74]
    [Time: 0.019721000 seconds]
```

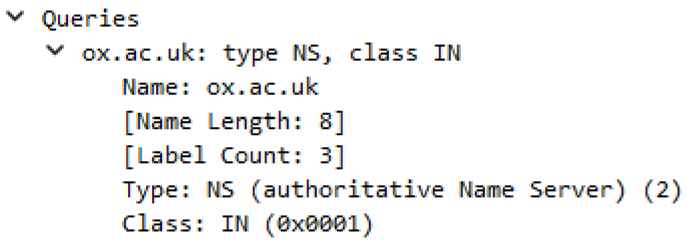
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



```
Source Address: 192.168.15.27
Destination Address: 192.168.15.1
```

Novamente, é meu endereço IP padrão.

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

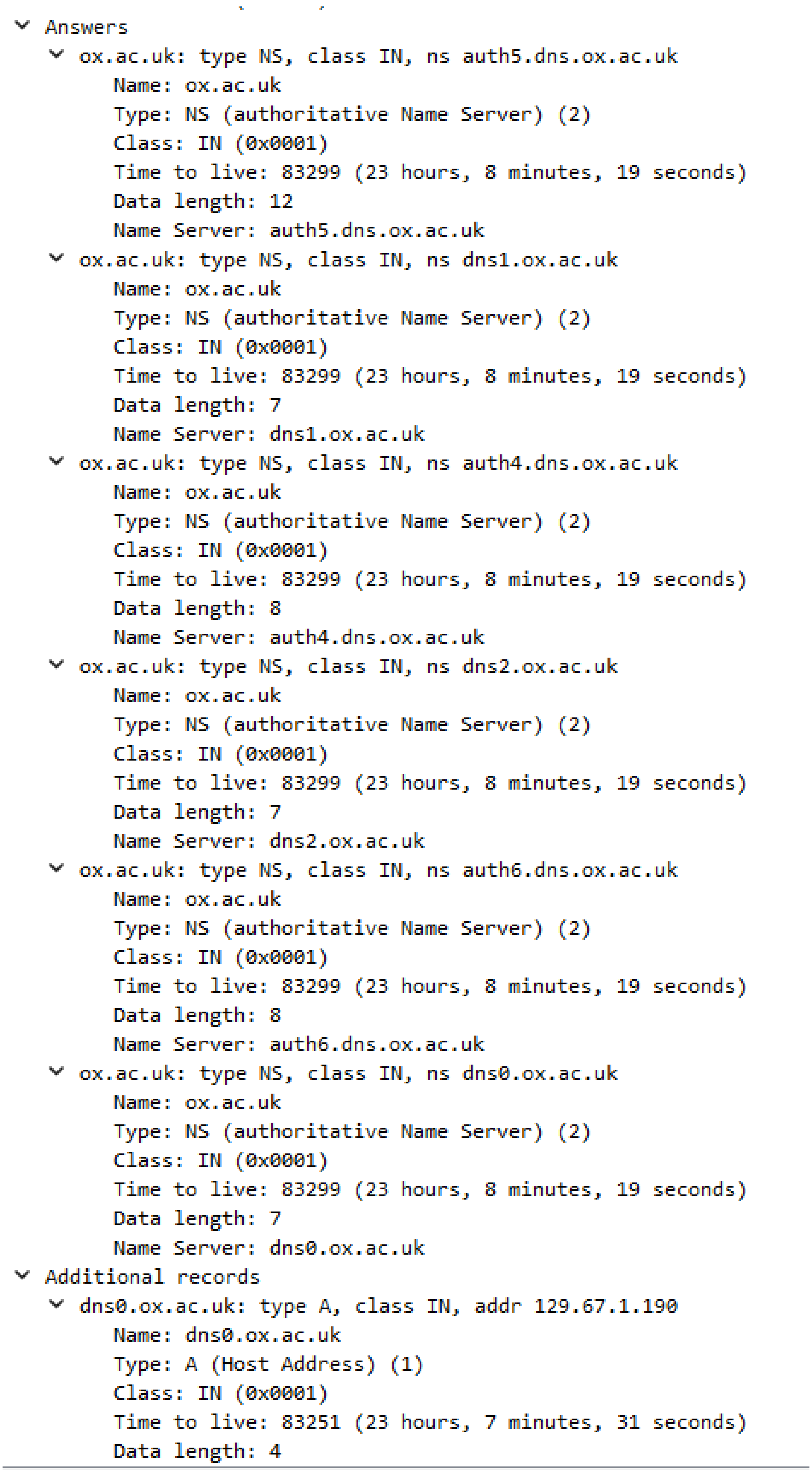


```
⌄ Queries
   ⌄ ox.ac.uk: type NS, class IN
        Name: ox.ac.uk
        [Name Length: 8]
        [Label Count: 3]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
```

Type NS. Não possui “answers”.

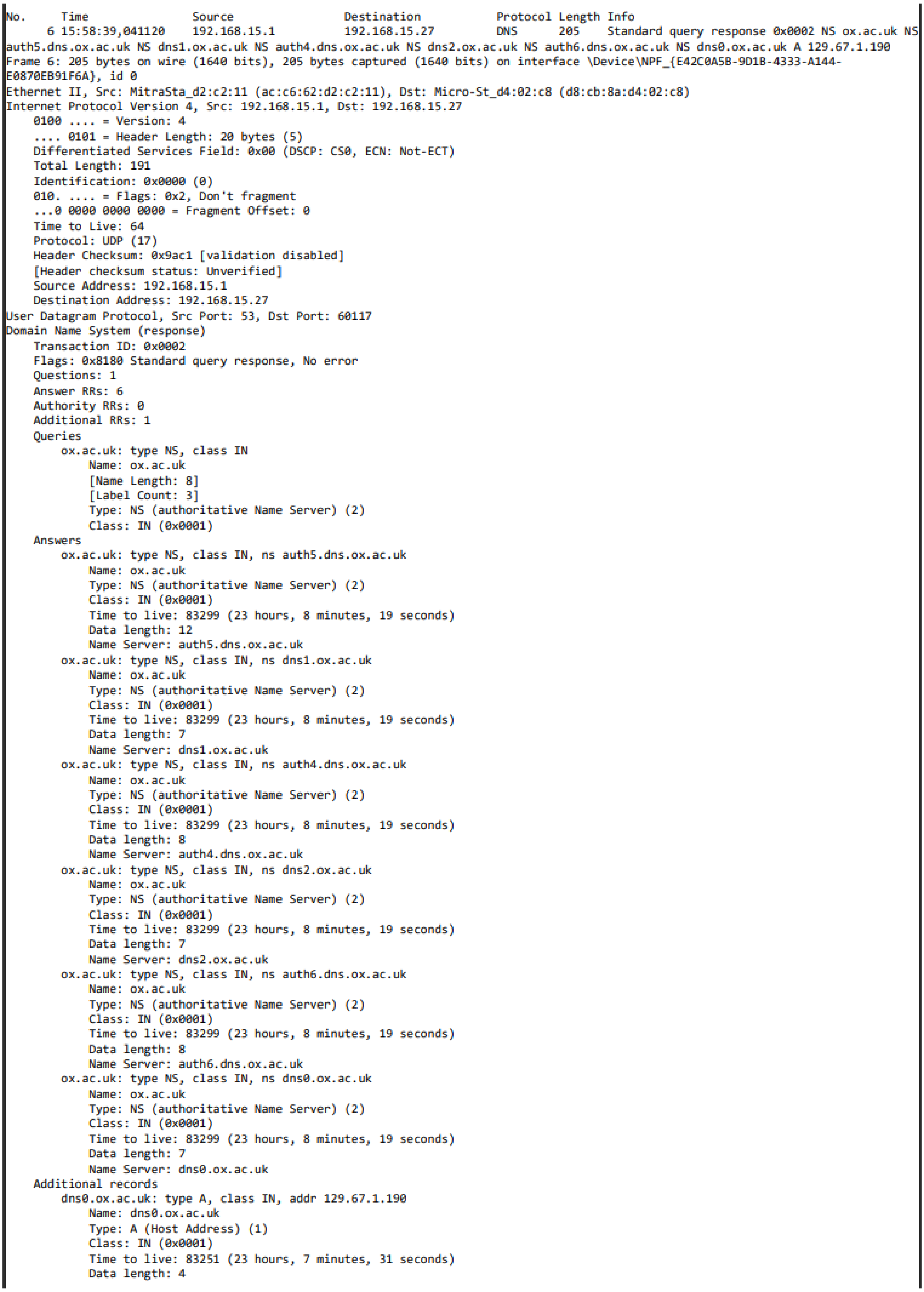
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

Sim, ele apresenta os namesers:



```
⌄ Answers
  ⌄ ox.ac.uk: type NS, class IN, ns auth5.dns.ox.ac.uk
      Name: ox.ac.uk
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 83299 (23 hours, 8 minutes, 19 seconds)
      Data length: 12
      Name Server: auth5.dns.ox.ac.uk
  ⌄ ox.ac.uk: type NS, class IN, ns dns1.ox.ac.uk
      Name: ox.ac.uk
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 83299 (23 hours, 8 minutes, 19 seconds)
      Data length: 7
      Name Server: dns1.ox.ac.uk
  ⌄ ox.ac.uk: type NS, class IN, ns auth4.dns.ox.ac.uk
      Name: ox.ac.uk
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 83299 (23 hours, 8 minutes, 19 seconds)
      Data length: 8
      Name Server: auth4.dns.ox.ac.uk
  ⌄ ox.ac.uk: type NS, class IN, ns dns2.ox.ac.uk
      Name: ox.ac.uk
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 83299 (23 hours, 8 minutes, 19 seconds)
      Data length: 7
      Name Server: dns2.ox.ac.uk
  ⌄ ox.ac.uk: type NS, class IN, ns auth6.dns.ox.ac.uk
      Name: ox.ac.uk
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 83299 (23 hours, 8 minutes, 19 seconds)
      Data length: 8
      Name Server: auth6.dns.ox.ac.uk
  ⌄ ox.ac.uk: type NS, class IN, ns dns0.ox.ac.uk
      Name: ox.ac.uk
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 83299 (23 hours, 8 minutes, 19 seconds)
      Data length: 7
      Name Server: dns0.ox.ac.uk
⌄ Additional records
  ⌄ dns0.ox.ac.uk: type A, class IN, addr 129.67.1.190
      Name: dns0.ox.ac.uk
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 83251 (23 hours, 7 minutes, 31 seconds)
      Data length: 4
```

19. Provide a screenshot.



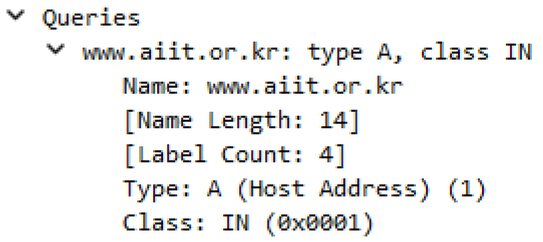
```
No.     Time               Source                Destination           Protocol Length Info
      6 15:58:39,041120    192.168.15.1          192.168.15.27         DNS      205    Standard query response 0x0002 NS ox.ac.uk NS
auth5.dns.ox.ac.uk NS dns1.ox.ac.uk NS auth4.dns.ox.ac.uk NS dns2.ox.ac.uk NS auth6.dns.ox.ac.uk NS dns0.ox.ac.uk A 129.67.1.190
Frame 6: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11), Dst: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8)
Internet Protocol Version 4, Src: 192.168.15.1, Dst: 192.168.15.27
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 191
    Identification: 0x0000 (0)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x9ac1 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.15.1
    Destination Address: 192.168.15.27
User Datagram Protocol, Src Port: 53, Dst Port: 60117
Domain Name System (response)
    Transaction ID: 0x0002
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 1
    Queries
        ox.ac.uk: type NS, class IN
            Name: ox.ac.uk
            [Name Length: 8]
            [Label Count: 3]
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
    Answers
        ox.ac.uk: type NS, class IN, ns auth5.dns.ox.ac.uk
            Name: ox.ac.uk
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 83299 (23 hours, 8 minutes, 19 seconds)
            Data length: 12
            Name Server: auth5.dns.ox.ac.uk
        ox.ac.uk: type NS, class IN, ns dns1.ox.ac.uk
            Name: ox.ac.uk
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 83299 (23 hours, 8 minutes, 19 seconds)
            Data length: 7
            Name Server: dns1.ox.ac.uk
        ox.ac.uk: type NS, class IN, ns auth4.dns.ox.ac.uk
            Name: ox.ac.uk
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 83299 (23 hours, 8 minutes, 19 seconds)
            Data length: 8
            Name Server: auth4.dns.ox.ac.uk
        ox.ac.uk: type NS, class IN, ns dns2.ox.ac.uk
            Name: ox.ac.uk
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 83299 (23 hours, 8 minutes, 19 seconds)
            Data length: 7
            Name Server: dns2.ox.ac.uk
        ox.ac.uk: type NS, class IN, ns auth6.dns.ox.ac.uk
            Name: ox.ac.uk
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 83299 (23 hours, 8 minutes, 19 seconds)
            Data length: 8
            Name Server: auth6.dns.ox.ac.uk
        ox.ac.uk: type NS, class IN, ns dns0.ox.ac.uk
            Name: ox.ac.uk
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 83299 (23 hours, 8 minutes, 19 seconds)
            Data length: 7
            Name Server: dns0.ox.ac.uk
    Additional records
        dns0.ox.ac.uk: type A, class IN, addr 129.67.1.190
            Name: dns0.ox.ac.uk
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 83251 (23 hours, 7 minutes, 31 seconds)
            Data length: 4
```

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?

Foi enviado para o IP de número 18.0.72.3. Não corresponde ao meu servidor de

DNS padrão. Corresponde ao endereço do www.aiit.or.kr

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



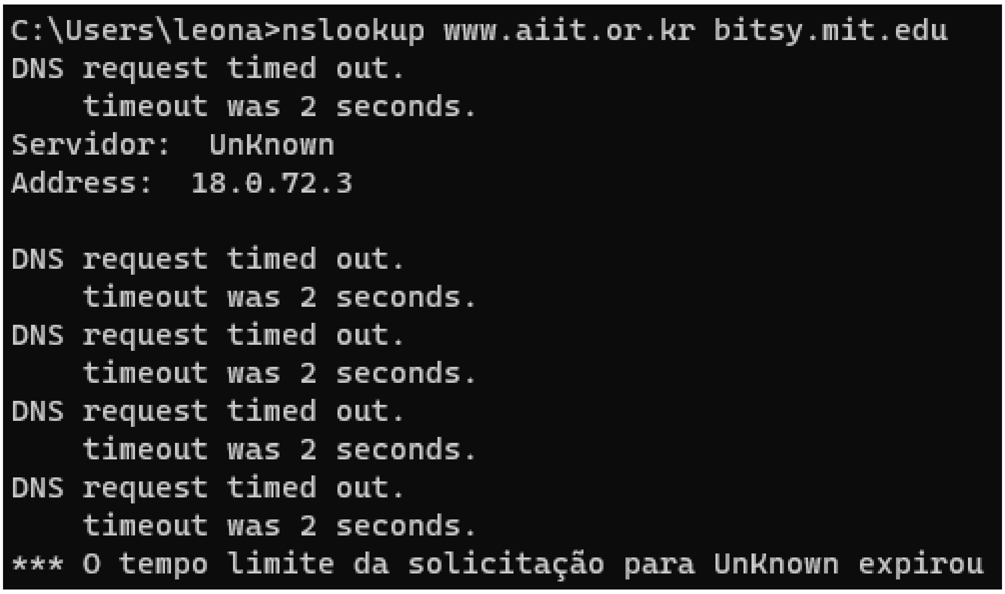
```
⌄ Queries
   ⌄ www.aiit.or.kr: type A, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Type A, naõ contém answers

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

Não teve DNS de resposta. Pois deu time out

23. Provide a screenshot.



```
C:\Users\leona>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Servidor:  UnKnown
Address:  18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** O tempo limite da solicitação para UnKnown expirou
```