Nome: Nathan Medeiros Cristiano.
Turma: **RED129005**

LABORATÓRIO 5

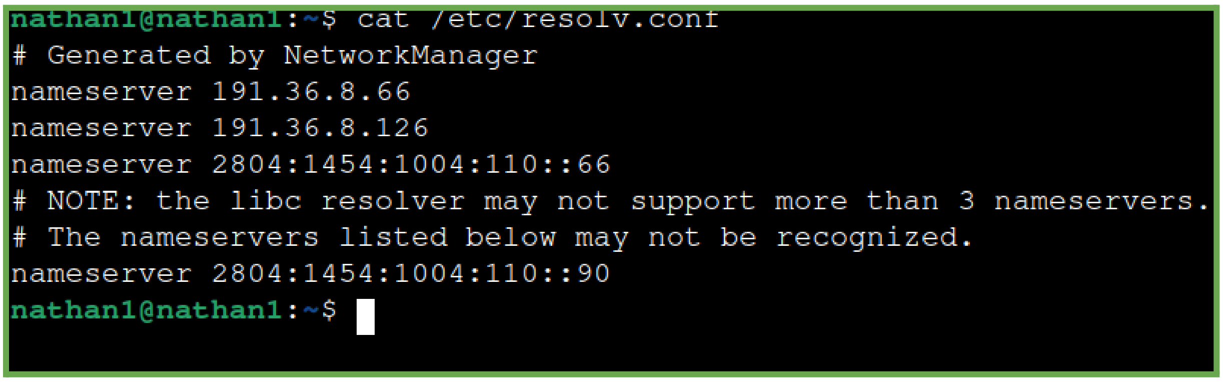
USANDO MINHA MÁQUINA / IFSC

SERVIÇOS DE NOMES (DNS)

1.0

Perguntas a serem respondidas, baseado nos pacotes "*Standard query*", "*Standard query response*" e leitura do arquivo resolv.conf:

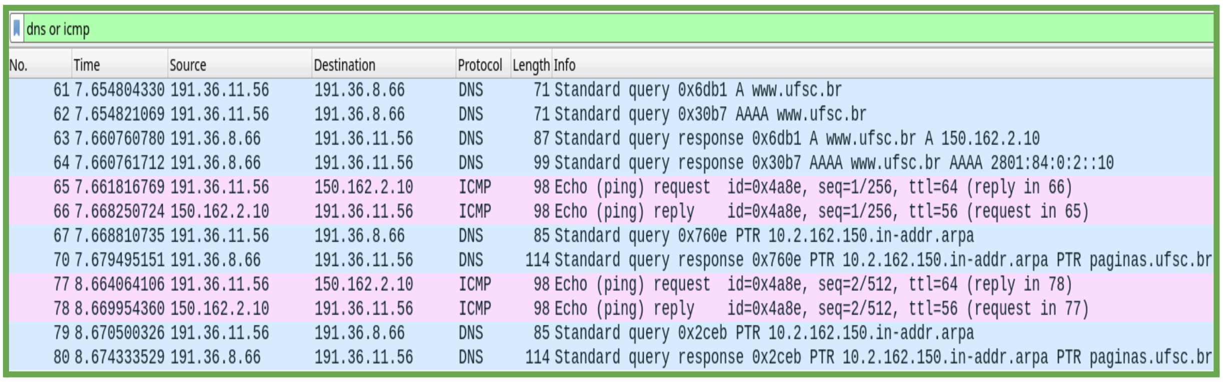
1.1- Quem são os servidores DNS da sua máquina (DNS local)?



```
nathan1@nathan1:~$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 191.36.8.66
nameserver 191.36.8.126
nameserver 2804:1454:1004:110::66
# NOTE: the libc resolver may not support more than 3 nameservers.
# The nameservers listed below may not be recognized.
nameserver 2804:1454:1004:110::90
nathan1@nathan1:~$
```

1.2- O ping gerou perguntas para cada um deles, ou somente para um?

- Somente para um!



dns or icmp

No.	Time	Source	Destination	Protocol	Length	Info
61	7.654804330	191.36.11.56	191.36.8.66	DNS	71	Standard query 0x6db1 A www.ufsc.br
62	7.654821069	191.36.11.56	191.36.8.66	DNS	71	Standard query 0x30b7 AAAA www.ufsc.br
63	7.660760780	191.36.8.66	191.36.11.56	DNS	87	Standard query response 0x6db1 A www.ufsc.br A 150.162.2.10
64	7.660761712	191.36.8.66	191.36.11.56	DNS	99	Standard query response 0x30b7 AAAA www.ufsc.br AAAA 2801:84:0:2::10
65	7.661816769	191.36.11.56	150.162.2.10	ICMP	98	Echo (ping) request id=0x4a8e, seq=1/256, ttl=64 (reply in 66)
66	7.668250724	150.162.2.10	191.36.11.56	ICMP	98	Echo (ping) reply id=0x4a8e, seq=1/256, ttl=56 (request in 65)
67	7.668810735	191.36.11.56	191.36.8.66	DNS	85	Standard query 0x760e PTR 10.2.162.150.in-addr.arpa
70	7.679495151	191.36.8.66	191.36.11.56	DNS	114	Standard query response 0x760e PTR 10.2.162.150.in-addr.arpa PTR paginas.ufsc.br
77	8.664064106	191.36.11.56	150.162.2.10	ICMP	98	Echo (ping) request id=0x4a8e, seq=2/512, ttl=64 (reply in 78)
78	8.669954360	150.162.2.10	191.36.11.56	ICMP	98	Echo (ping) reply id=0x4a8e, seq=2/512, ttl=56 (request in 77)
79	8.670500326	191.36.11.56	191.36.8.66	DNS	85	Standard query 0x2ceb PTR 10.2.162.150.in-addr.arpa
80	8.674333529	191.36.8.66	191.36.11.56	DNS	114	Standard query response 0x2ceb PTR 10.2.162.150.in-addr.arpa PTR paginas.ufsc.br

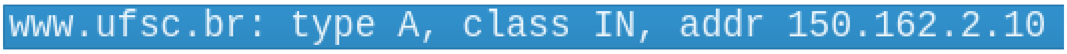
1.3- Qual o tipo da RR associada a pergunta (*Queries*). O que significa?

- Associado às “Queries” , temos dois tipos diferentes de RR.

- **Pacote 61:** A, mapeia um nome de domínio ipv4
- **Pacote 62:** AAAA, mapeia um nome de domínio para ipv6

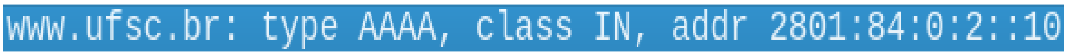
1.4- Qual endereço IP retornado para o www.ufsc.br?

- Para IPV4



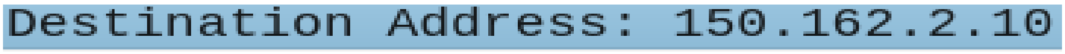
```
www.ufsc.br: type A, class IN, addr 150.162.2.10
```

- Para IPV6



```
www.ufsc.br: type AAAA, class IN, addr 2801:84:0:2::10
```

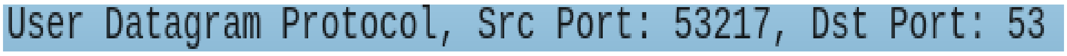
1.5- Qual endereço IP, de destino, usado no ping (ver pacote REQUEST ICMP)?



```
Destination Address: 150.162.2.10
```

1.6- Qual é o número da porta do servidor DNS?

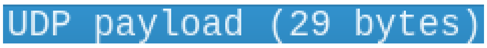
- A porta de destino padrão é 53



```
User Datagram Protocol, Src Port: 53217, Dst Port: 53
```

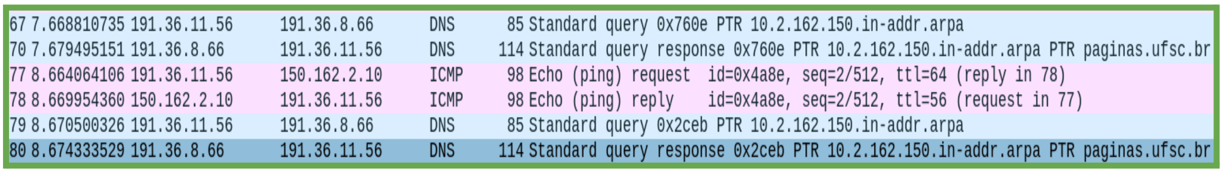
1.7- Qual protocolo de transporte, camada 4, que foi usado para transportar as mensagens de aplicação DNS?

- O protocolo padrão utilizado pela aplicação DNS é o UDP.



```
UDP payload (29 bytes)
```

1.8- Uso do PTR:



```
67 7.668810735 191.36.11.56    191.36.8.66     DNS    85 Standard query 0x760e PTR 10.2.162.150.in-addr.arpa
70 7.679495151 191.36.8.66     191.36.11.56    DNS   114 Standard query response 0x760e PTR 10.2.162.150.in-addr.arpa PTR paginas.ufsc.br
77 8.664064106 191.36.11.56    150.162.2.10    ICMP   98 Echo (ping) request  id=0x4a8e, seq=2/512, ttl=64 (reply in 78)
78 8.669954360 150.162.2.10    191.36.11.56    ICMP   98 Echo (ping) reply    id=0x4a8e, seq=2/512, ttl=56 (request in 77)
79 8.670500326 191.36.11.56    191.36.8.66     DNS    85 Standard query 0x2ceb PTR 10.2.162.150.in-addr.arpa
80 8.674333529 191.36.8.66     191.36.11.56    DNS   114 Standard query response 0x2ceb PTR 10.2.162.150.in-addr.arpa PTR paginas.ufsc.br
```

- **Qual o IP que se pretende resolver?**

  O IP -> 10.2.162.150 porém aqui está invertido característica do PTR, então o endereço é 150.162.2.10.

- **Qual o nome retornado?**

  O nome -> paginas.ufsc.br

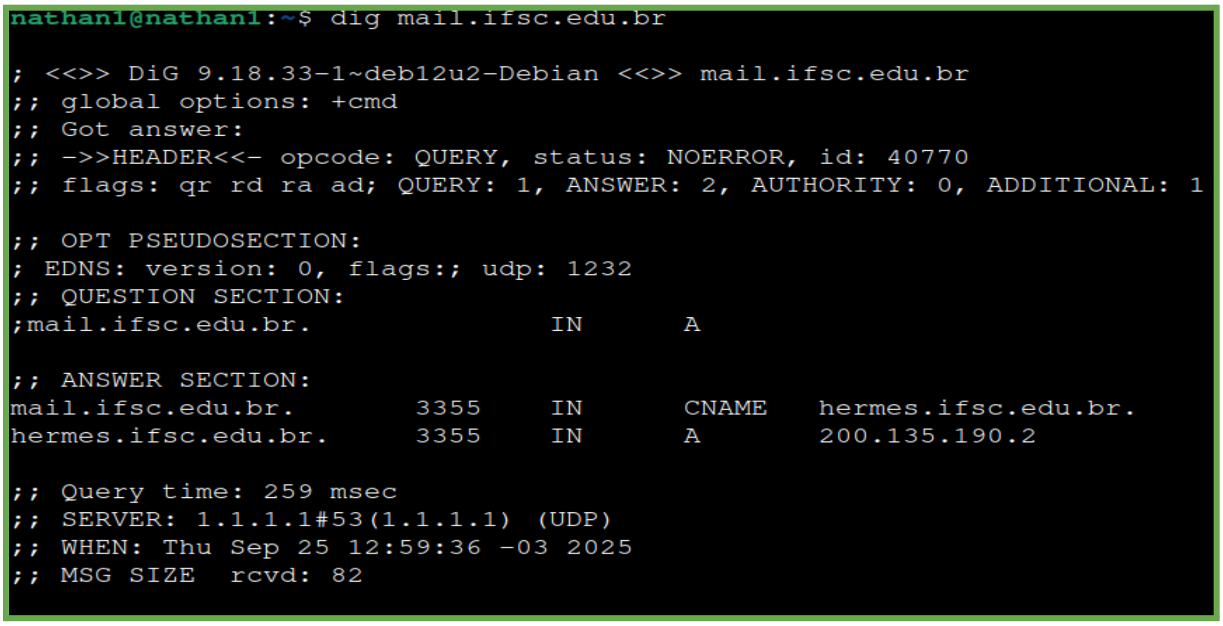
- **O nome retornado é www.ufsc.br? Sim ou não? Explique.**

  Não, pois, um único endereço IP pode ser associado a múltiplos nomes de domínio, tendo geralmente um registro de "fachada" de DNS reverso (PTR).

2.0- Consultas DNS por meio e ferramentas especializadas:

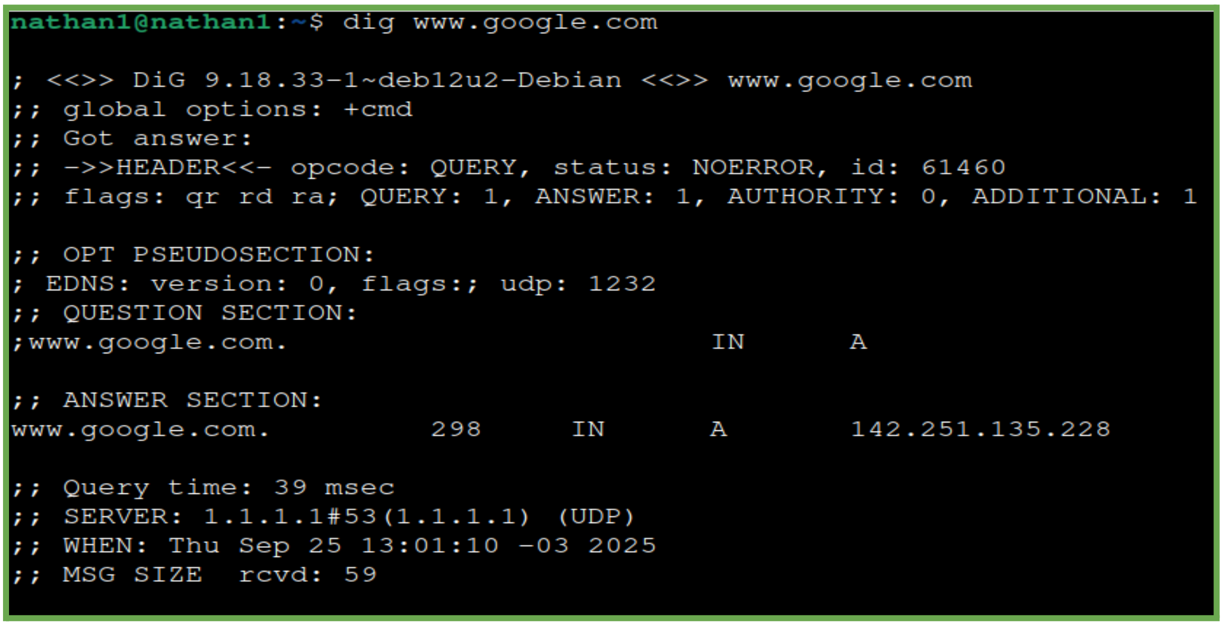
2.1- Usando o programa host ou dig, que são executados no terminal, descubra e anote no relatório os endereços IP associados aos seguintes nomes de hosts (máquinas):

- mail.ifsc.edu.br:



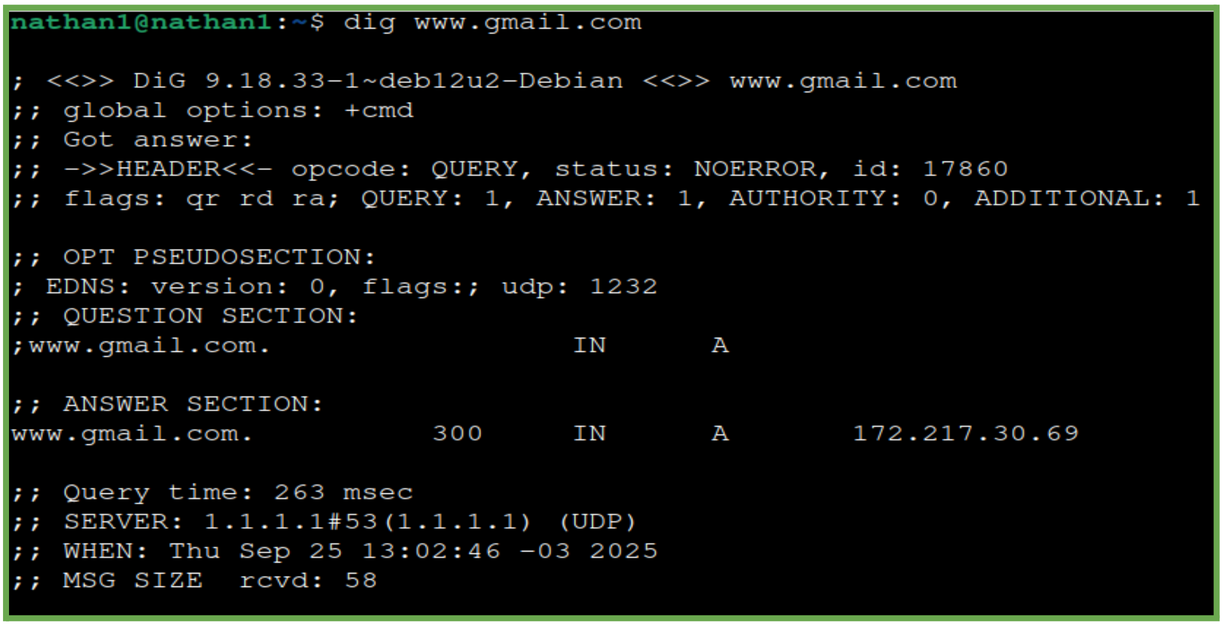
```
nathan1@nathan1:~$ dig mail.ifsc.edu.br

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> mail.ifsc.edu.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40770
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;mail.ifsc.edu.br.              IN      A

;; ANSWER SECTION:
mail.ifsc.edu.br.       3355    IN      CNAME   hermes.ifsc.edu.br.
hermes.ifsc.edu.br.     3355    IN      A       200.135.190.2

;; Query time: 259 msec
;; SERVER: 1.1.1.1#53(1.1.1.1) (UDP)
;; WHEN: Thu Sep 25 12:59:36 -03 2025
;; MSG SIZE  rcvd: 82
```

- www.google.com



```
nathan1@nathan1:~$ dig www.google.com

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61460
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         298     IN      A       142.251.135.228

;; Query time: 39 msec
;; SERVER: 1.1.1.1#53(1.1.1.1) (UDP)
;; WHEN: Thu Sep 25 13:01:10 -03 2025
;; MSG SIZE  rcvd: 59
```

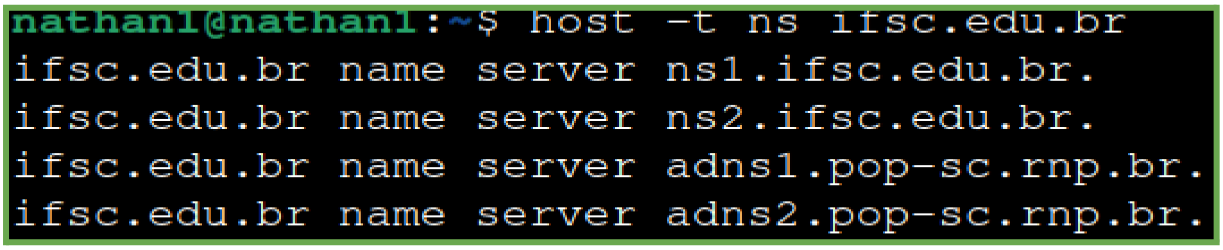
- www.gmail.com



```
nathan1@nathan1:~$ dig www.gmail.com

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> www.gmail.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17860
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.gmail.com.                 IN      A

;; ANSWER SECTION:
www.gmail.com.          300     IN      A       172.217.30.69

;; Query time: 263 msec
;; SERVER: 1.1.1.1#53(1.1.1.1) (UDP)
;; WHEN: Thu Sep 25 13:02:46 -03 2025
;; MSG SIZE  rcvd: 58
```

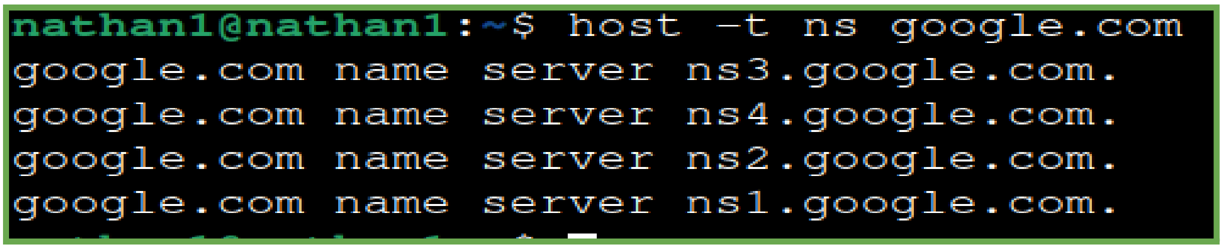
2.2- Agora descubra e anote no relatório quais são os servidores DNS responsáveis por cada um dos domínios dos nomes acima.

- ifsc.edu.br



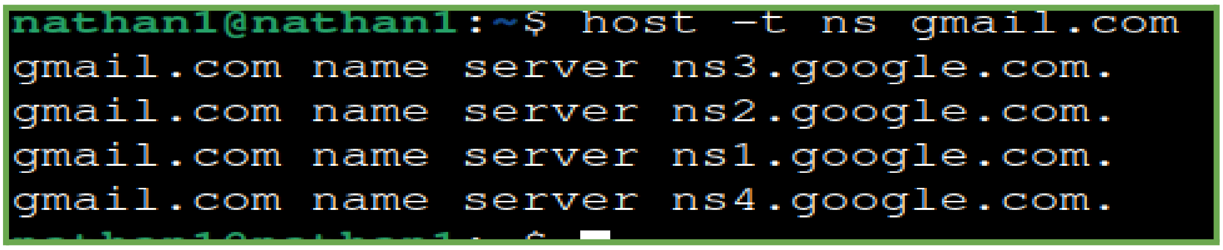
```
nathan1@nathan1:~$ host -t ns ifsc.edu.br
ifsc.edu.br name server ns1.ifsc.edu.br.
ifsc.edu.br name server ns2.ifsc.edu.br.
ifsc.edu.br name server adns1.pop-sc.rnp.br.
ifsc.edu.br name server adns2.pop-sc.rnp.br.
```

- google.com



```
nathan1@nathan1:~$ host -t ns google.com
google.com name server ns3.google.com.
google.com name server ns4.google.com.
google.com name server ns2.google.com.
google.com name server ns1.google.com.
```

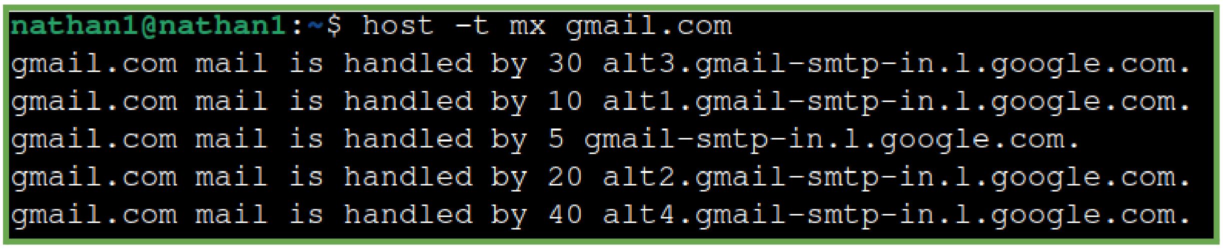
- gmail.com



```
nathan1@nathan1:~$ host -t ns gmail.com
gmail.com name server ns3.google.com.
gmail.com name server ns2.google.com.
gmail.com name server ns1.google.com.
gmail.com name server ns4.google.com.
```

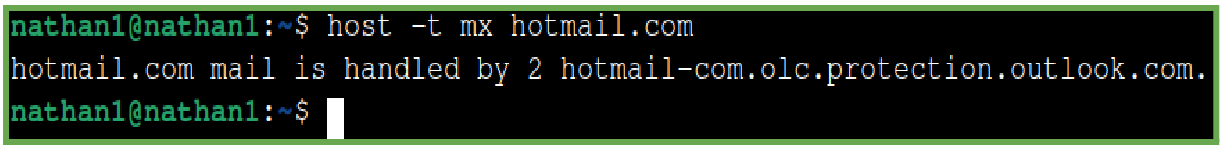
2.3- Descubra e anote no relatório quem é o servidor de emails nos seguintes domínios:

- gmail.com



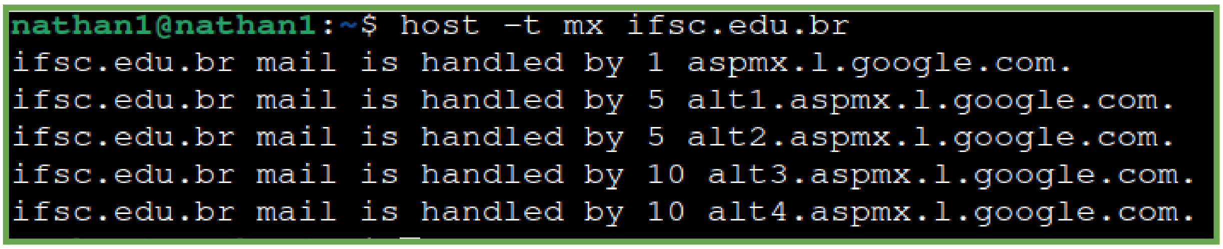
```
nathan1@nathan1:~$ host -t mx gmail.com
gmail.com mail is handled by 30 alt3.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 10 alt1.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 5 gmail-smtp-in.l.google.com.
gmail.com mail is handled by 20 alt2.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 40 alt4.gmail-smtp-in.l.google.com.
```

- hotmail.com



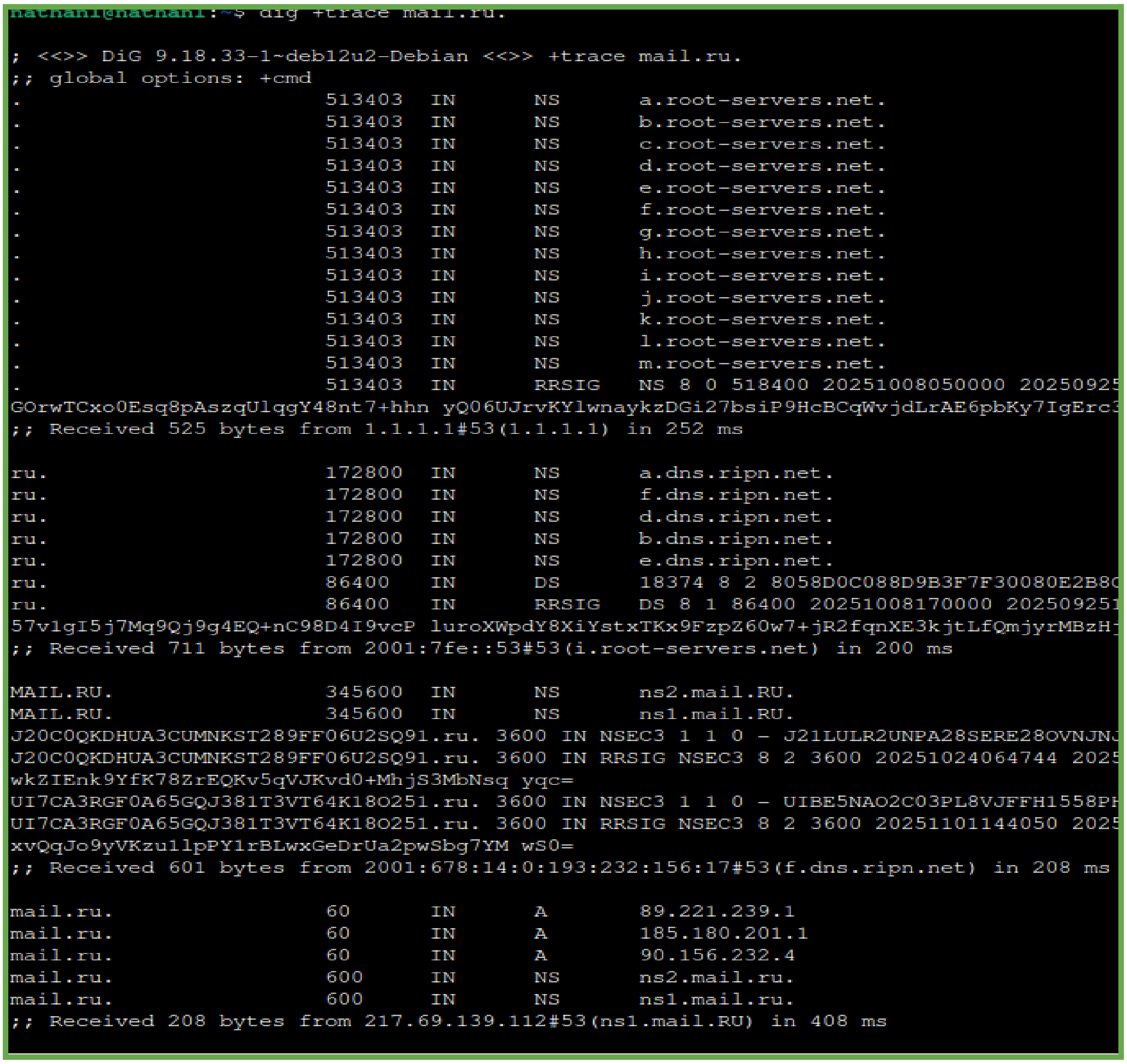
```
nathan1@nathan1:~$ host -t mx hotmail.com
hotmail.com mail is handled by 2 hotmail-com.olc.protection.outlook.com.
nathan1@nathan1:~$
```

- ifsc.edu.br



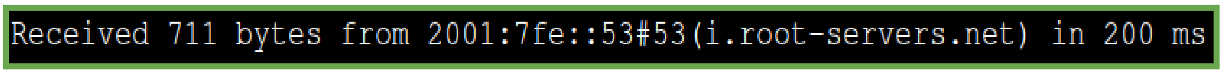
```
nathan1@nathan1:~$ host -t mx ifsc.edu.br
ifsc.edu.br mail is handled by 1 aspmx.l.google.com.
ifsc.edu.br mail is handled by 5 alt1.aspmx.l.google.com.
ifsc.edu.br mail is handled by 5 alt2.aspmx.l.google.com.
ifsc.edu.br mail is handled by 10 alt3.aspmx.l.google.com.
ifsc.edu.br mail is handled by 10 alt4.aspmx.l.google.com.
```

2.4- Faça uma consulta iterativa com dig, faça um print de toda a saída e responda:



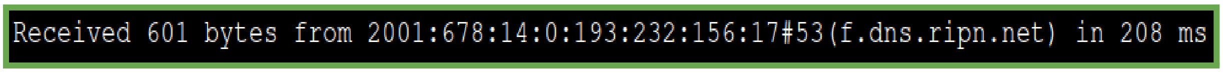
```
nathani@nathani:~$ dig +trace mail.ru.

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> +trace mail.ru.
;; global options: +cmd
.                       513403  IN      NS      a.root-servers.net.
.                       513403  IN      NS      b.root-servers.net.
.                       513403  IN      NS      c.root-servers.net.
.                       513403  IN      NS      d.root-servers.net.
.                       513403  IN      NS      e.root-servers.net.
.                       513403  IN      NS      f.root-servers.net.
.                       513403  IN      NS      g.root-servers.net.
.                       513403  IN      NS      h.root-servers.net.
.                       513403  IN      NS      i.root-servers.net.
.                       513403  IN      NS      j.root-servers.net.
.                       513403  IN      NS      k.root-servers.net.
.                       513403  IN      NS      l.root-servers.net.
.                       513403  IN      NS      m.root-servers.net.
.                       513403  IN      RRSIG   NS 8 0 518400 20251008050000 20250925
GOrwTCxo0Esq8pAszqUlqgY48nt7+hhn yQ06UJrvKYlwnaykzDGi27bsiP9HcBCqWvjdLrAE6pbKy7IgErc3
;; Received 525 bytes from 1.1.1.1#53(1.1.1.1) in 252 ms

ru.                     172800  IN      NS      a.dns.ripn.net.
ru.                     172800  IN      NS      f.dns.ripn.net.
ru.                     172800  IN      NS      d.dns.ripn.net.
ru.                     172800  IN      NS      b.dns.ripn.net.
ru.                     172800  IN      NS      e.dns.ripn.net.
ru.                     86400   IN      DS      18374 8 2 8058D0C088D9B3F7F30080E2B8C
ru.                     86400   IN      RRSIG   DS 8 1 86400 20251008170000 202509251
57v1gI5j7Mq9Qj9g4EQ+nC98D4I9vcP luroXWpdY8XiYstxTKx9FzpZ60w7+jR2fqnXE3kjtLfQmjyrMBzHj
;; Received 711 bytes from 2001:7fe::53#53(i.root-servers.net) in 200 ms

MAIL.RU.                345600  IN      NS      ns2.mail.RU.
MAIL.RU.                345600  IN      NS      ns1.mail.RU.
J20C0QKDHUA3CUMNKST289FF06U2SQ91.ru. 3600 IN NSEC3 1 1 0 - J21LULR2UNPA28SERE28OVNJNJ
J20C0QKDHUA3CUMNKST289FF06U2SQ91.ru. 3600 IN RRSIG NSEC3 8 2 3600 20251024064744 2025
wkZIEnk9YfK78ZrEQKv5qVJKvd0+MhjS3MbNsq yqc=
UI7CA3RGF0A65GQJ381T3VT64K18O251.ru. 3600 IN NSEC3 1 1 0 - UIBE5NAO2C03PL8VJFFH1558PH
UI7CA3RGF0A65GQJ381T3VT64K18O251.ru. 3600 IN RRSIG NSEC3 8 2 3600 20251101144050 2025
xvQqJo9yVKzu1lpPY1rBLwxGeDrUa2pwSbg7YM wS0=
;; Received 601 bytes from 2001:678:14:0:193:232:156:17#53(f.dns.ripn.net) in 208 ms

mail.ru.                60      IN      A       89.221.239.1
mail.ru.                60      IN      A       185.180.201.1
mail.ru.                60      IN      A       90.156.232.4
mail.ru.                600     IN      NS      ns2.mail.ru.
mail.ru.                600     IN      NS      ns1.mail.ru.
;; Received 208 bytes from 217.69.139.112#53(ns1.mail.RU) in 408 ms
```

- **Qual foi o RLD (*Root Level Domain*) consultado?**



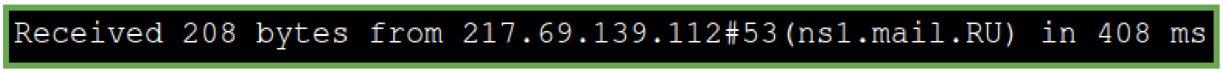
```
Received 711 bytes from 2001:7fe::53#53(i.root-servers.net) in 200 ms
```

- **Qual o TLD (*Top Level Domain*) consultado?**



```
Received 601 bytes from 2001:678:14:0:193:232:156:17#53(f.dns.ripn.net) in 208 ms
```

- **Qual o SLD (*Second Level Domain*) consultado?**



```
Received 208 bytes from 217.69.139.112#53(ns1.mail.RU) in 408 ms
```

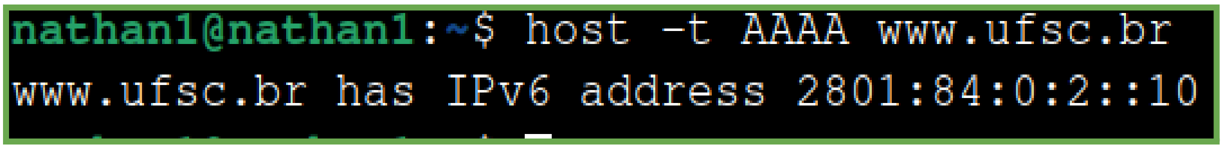
- **Como você sabe que foram esses os LDs consultados?**

  Pelas respostas de Received.

2.5- Algumas consultas AAAA:

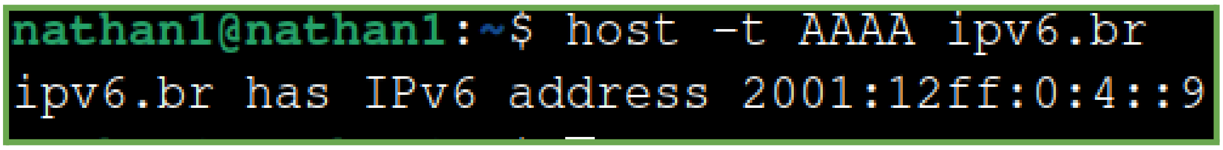
2.5.1- No terminal de sua máquina faça uma consulta e responda: qual o endereço IPv6 dos hosts?

- www.ufsc.br



```
nathan1@nathan1:~$ host -t AAAA www.ufsc.br
www.ufsc.br has IPv6 address 2801:84:0:2::10
```

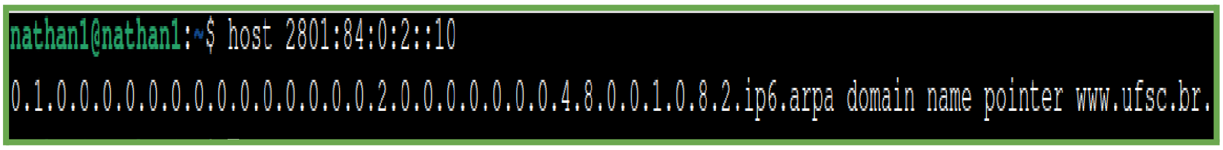
- ipv6.br



```
nathan1@nathan1:~$ host -t AAAA ipv6.br
ipv6.br has IPv6 address 2001:12ff:0:4::9
```

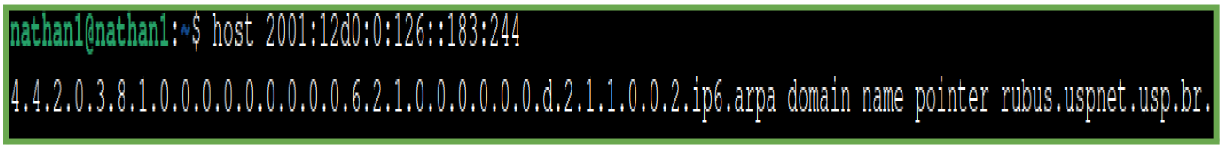
2.5.2- Agora vamos fazer a consulta reversa.Qual é o nome de host dos seguintes endereços?

- 2801:84:0:2::10



```
nathan1@nathan1:~$ host 2801:84:0:2::10
0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.0.0.0.0.4.8.0.0.1.0.8.2.ip6.arpa domain name pointer www.ufsc.br.
```

- 2001:12d0:0:126::183:244



```
nathan1@nathan1:~$ host 2001:12d0:0:126::183:244
4.4.2.0.3.8.1.0.0.0.0.0.0.0.0.0.6.2.1.0.0.0.0.0.0.d.2.1.1.0.0.2.ip6.arpa domain name pointer rubus.uspnet.usp.br.
```