Serviço de Nomes (DNS)

Consulta simples ao DNS gerada a partir de um comando ping

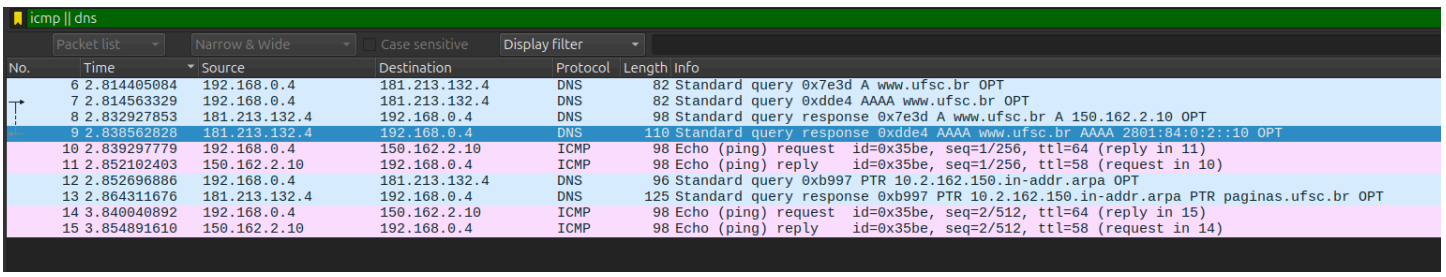
1. Quem são os servidores DNS da sua máquina?

181.213.132.4
181.213.132.5
2804:14d:1:0:181:213:132:4 (IPv6)
2804:14d:1:0:181:213:132:5 (IPv6)

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ resolvectl status
Global
         Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: stub

Link 2 (wlo1)
    Current Scopes: DNS
         Protocols: +DefaultRoute -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
Current DNS Server: 181.213.132.5
       DNS Servers: 181.213.132.4 181.213.132.5 2804:14d:1:0:181:213:132:4 2804:14d:1:0:181:213:132:5
        DNS Domain: home

Link 3 (docker0)
    Current Scopes: none
         Protocols: -DefaultRoute -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported

Link 4 (br-c7577b95616b)
    Current Scopes: none
         Protocols: -DefaultRoute -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported

Link 5 (br-f15b30ebf387)
    Current Scopes: none
         Protocols: -DefaultRoute -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
```

2. O ping gerou pergunta para cada um deles?

Não, o ping foi enviado diretamente ao IP **150.162.2.10**. O tráfego ICMP não interage diretamente com os servidores DNS, e sim resolve os nomes de domínio (caso necessário) antes de enviar os pacotes ICMP.



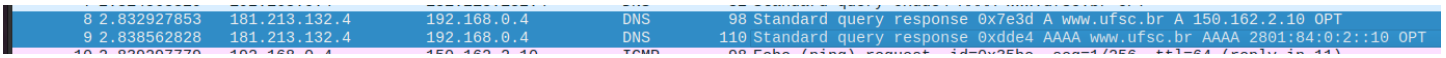
3. Qual o tipo da RR associada a pergunta (*Queries*). O que significa?

Tipos A, AAAA e PTR.

A: Retorna o endereço IPv4 associado a um domínio.
AAAA: Retorna o endereço IPv6 associado a um domínio.
PTR: Faz o mapeamento reverso de um endereço IP para um nome de domínio.

4. Qual endereço IP retornado da solicitação da resolução de www.ufsc.br?

No pacote 9, a resposta à consulta AAAA retorna o endereço **2801:84:0:2::10** e no pacote 8, a resposta à consulta A é o endereço **150.162.2.10.**

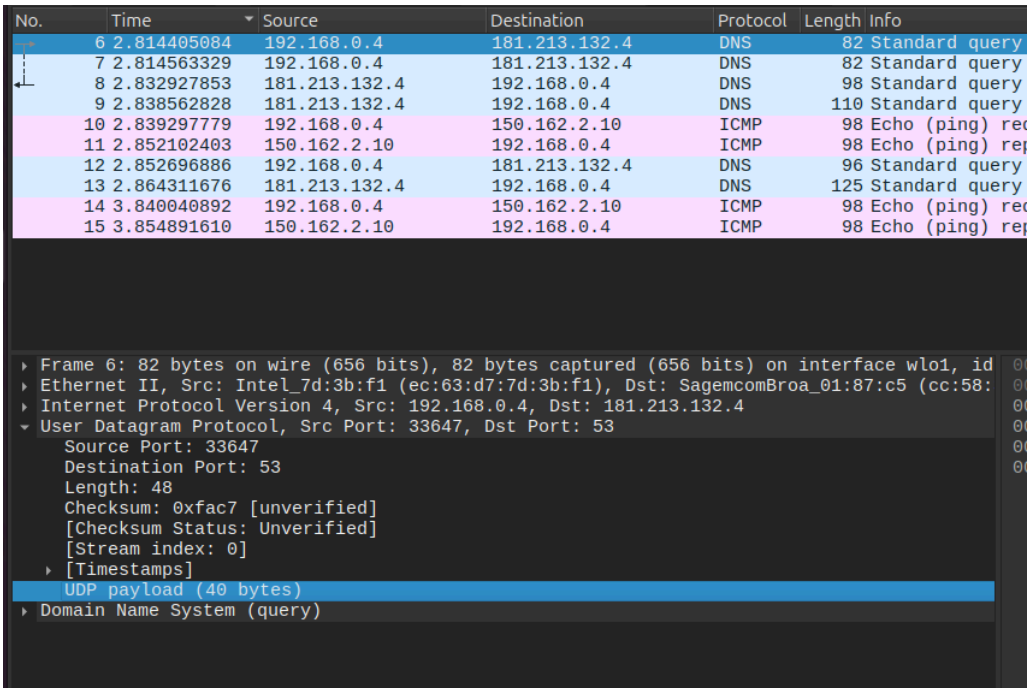


5. Qual endereço IP usado no ping (ver pacote REQUEST ICMP)?

O endereço IP de destino usado no ping é **150.162.2.10**.

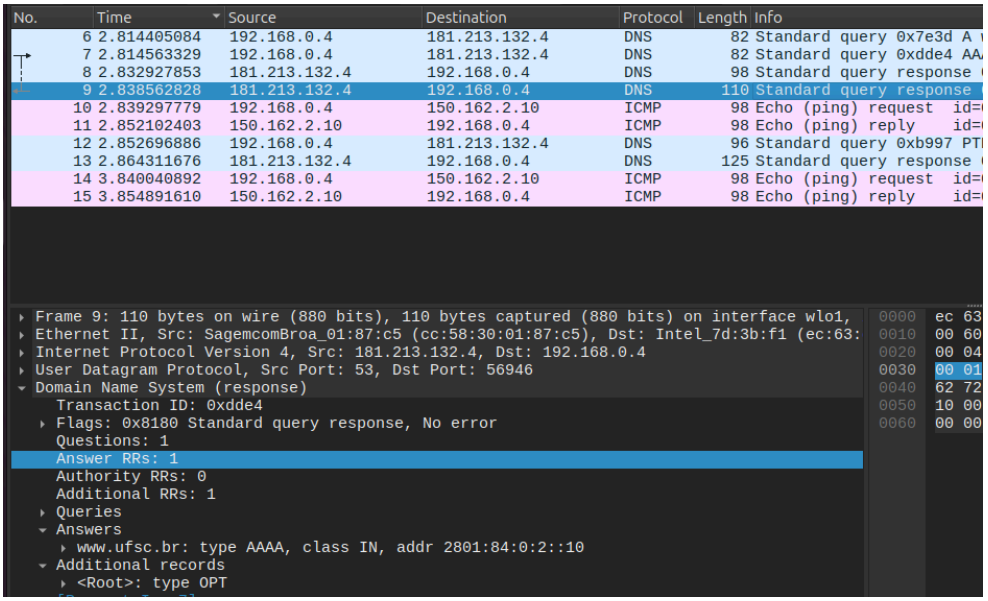
6. Qual protocolo de transporte, camada 4, que foi usado para transportar as mensagens de aplicação DNS?

O protocolo de transporte utilizado foi o **UDP**.



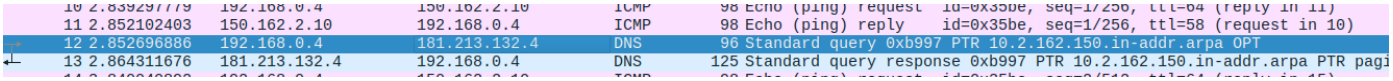
7. No QUERY realizado foi solicitado consulta recursiva. O servidor aceitou esta solicitação? (ver a resposta do servidor)

Sim, pois houve uma resposta correspondente.



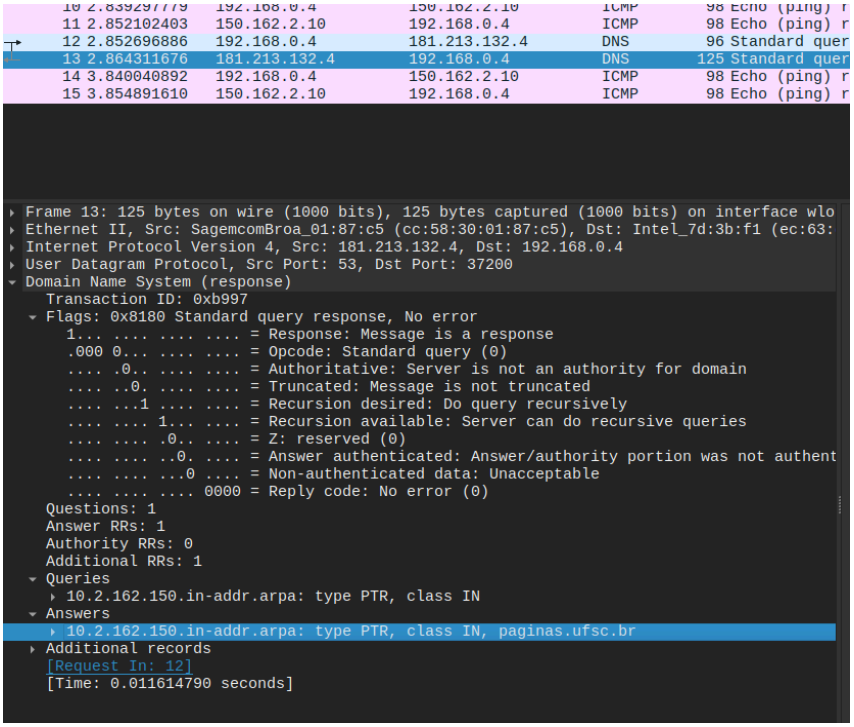
8. Qual o IP que se pretende resolver?

O IP que se pretende resolver é 10.2.162.150, conforme a consulta PTR vista no pacote 12.



9. Qual o nome retornado?

“paginas.ufsc.br”, conforme a resposta do servidor DNS no pacote 13.



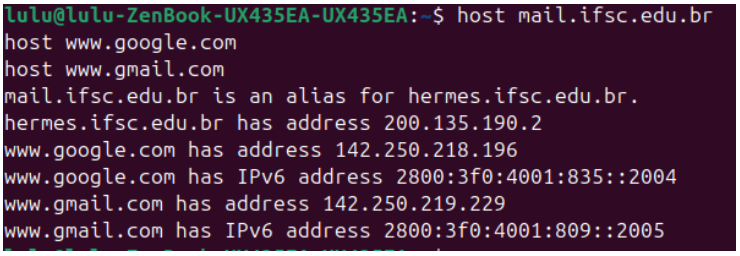
10. O nome retornado é www.ufsc.br? Sim ou não? Explique.

Não Isso acontece porque a consulta PTR resolve o nome do domínio associado diretamente ao IP fornecido, e o IP 10.2.162.150 está associado ao subdomínio paginas.ufsc.br, que pode ser uma parte diferente da infraestrutura de servidores da UFSC.

Consultas DNS por meio de ferramentas especializadas

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):**

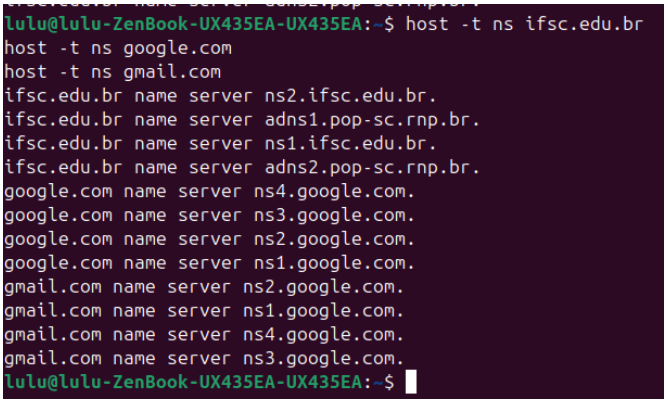
- mail.ifsc.edu.br:
  - Endereço IPv4 de hermes.ifsc.edu.br: 200.135.190.2
- www.google.com:
  - Endereço IPv4: 142.250.218.196
  - Endereço IPv6: 2800:3f0:4001:835::2004
- www.gmail.com:
  - Endereço IPv4: 142.250.219.229
  - Endereço IPv6: 2800:3f0:4001:809::2005



2. Agora descubra e anote no relatório quem é o servidor DNS responsável por cada um dos domínios (p.e.: ifsc.edu.br) dos nomes acima. Para isso consulte o valor do registro NS associado a esses domínios. Por exemplo, com o programa *host* ou *dig* isso pode ser feito assim: host -t ns ifsc.edu.br

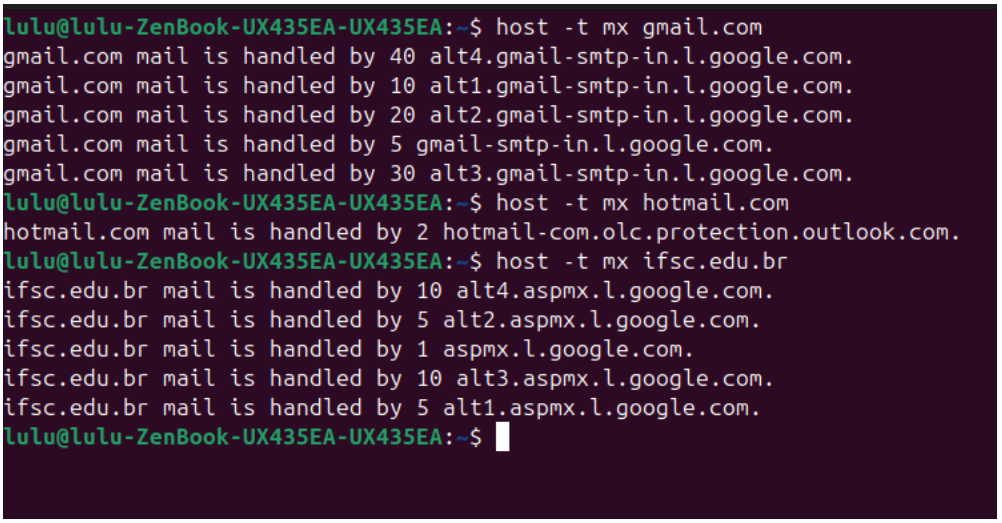
- ifsc.edu.br
  - ns2.ifsc.edu.br
  - adns1.pop-sc.rnp.br
  - ns1.ifsc.edu.br
  - adns2.pop-sc.rnp.br
- google.com

    - ns4.google.com
    - ns3.google.com
    - ns2.google.com
    - ns1.google.com
- gmail.com
    - ns1.google.com
    - ns4.google.com
    - ns3.google.com
    - ns2.google.com



3. Descubra e anote no relatório quem é o servidor de emails nos seguintes domínios:

- **gmail.com**
- **hotmail.com**
- **ifsc.edu.br**



3. Faça uma consulta iterativa com *dig* e responda:

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

Representado pelos servidores root-servers.net.

3.2. Qual o TLD (*Top Level Domain*) consultado?

Foi .ru.

3.3. Qual o SLD (*Second Level Domain*) consultado?

Foi o mail.

3.4.. Como você sabe que foram esses os LDs consultados?

A partir das respostas mostradas no comando dig +trace, ele mostra cada etapa da consulta DNS.

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ dig +trace mail.ru.

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> +trace mail.ru.
;; global options: +cmd
.                       489227  IN      NS      a.root-servers.net.
.                       489227  IN      NS      h.root-servers.net.
.                       489227  IN      NS      i.root-servers.net.
.                       489227  IN      NS      j.root-servers.net.
.                       489227  IN      NS      l.root-servers.net.
.                       489227  IN      NS      f.root-servers.net.
.                       489227  IN      NS      k.root-servers.net.
.                       489227  IN      NS      g.root-servers.net.
.                       489227  IN      NS      c.root-servers.net.
.                       489227  IN      NS      b.root-servers.net.
.                       489227  IN      NS      m.root-servers.net.
.                       489227  IN      NS      d.root-servers.net.
.                       489227  IN      NS      e.root-servers.net.
;; Received 239 bytes from 127.0.0.53#53(127.0.0.53) in 59 ms

ru.                     172800  IN      NS      a.dns.ripn.net.
ru.                     172800  IN      NS      b.dns.ripn.net.
ru.                     172800  IN      NS      d.dns.ripn.net.
ru.                     172800  IN      NS      e.dns.ripn.net.
ru.                     172800  IN      NS      f.dns.ripn.net.
ru.                     86400   IN      DS      43786 8 2 3C59747544090BC74419D5F69E32D8C9E
ru.                     86400   IN      RRSIG   DS 8 1 86400 20241020210000 20241007200000
C6KCF3koXMpPa8DktQ1NyupTLbhuIF2 rRQ37hCdNRFZUH5osh5SGqxWyb3mzpd7Wsb5Cfvh6evyNeOjUOaCcsbC uN
;; Received 683 bytes from 2801:1b8:10::b#53(b.root-servers.net) in 182 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 - J21LULR2UNPA28SERE28OVNJNJ67QP7V
J20C0QKDHUA3CUMNKST289FF06U2SQ91.ru. 3600 IN RRSIG NSEC3 8 2 3600 20241110155306 2024093012
Evwr59QnOp3G/HeUJGnLAr/xNfHBggJZdoG3qJ QvA=
UI68RDB76N8TRSIHGPGCK981SK28G1U8.ru. 3600 IN NSEC3 1 1 0 - UI8S9USHP4V1P4E3SJCV9QALB7CO4K2V
UI68RDB76N8TRSIHGPGCK981SK28G1U8.ru. 3600 IN RRSIG NSEC3 8 2 3600 20241109111608 2024093012
J13GkMiC8ba+9dZ5kGHywHFWU36YfZmMO/Z74k Xvw=
;; Received 601 bytes from 2001:678:15:0:193:232:142:17#53(e.dns.ripn.net) in 242 ms

mail.ru.                60      IN      A       217.69.139.202
mail.ru.                60      IN      A       217.69.139.200
mail.ru.                60      IN      A       94.100.180.201
mail.ru.                60      IN      A       94.100.180.200
mail.ru.                600     IN      NS      ns1.mail.ru.
mail.ru.                600     IN      NS      ns2.mail.ru.
;; Received 224 bytes from 217.69.139.112#53(ns1.mail.RU) in 308 ms
```

Algumas Consultas AAAA

1. **No terminal de sua máquina faça uma consulta e responda: qual o endereço IPv6 dos hosts? Por exemplo: host -t AAAA google.com**
    1. **www.ufsc.br**
    2. **ipv6.br**

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ host -t AAAA www.ufsc.br
www.ufsc.br has IPv6 address 2801:84:0:2::10
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ host -t AAAA ipv6.br
ipv6.br has IPv6 address 2001:12ff:0:4::9
lulu@lulu-ZenBook-UX435EA-UX435EA:~$
```

2. Agora vamos fazer a consulta reversa. Qual é o nome de host dos seguintes endereços? Por exemplo: host 2600:1419:1e00:38e::356e

1. **2801:84:0:2::10**
2. **2001:12d0:0:126::183:244**

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ 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.
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ host 2001:12ff:0:4::9
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer seminarioprivacidade.cgi.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer icannsaopaulo.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer pttforum.nic.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer ipv6.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer igfbrazil2007.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer antispam.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer internetsegura.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer www.xn--icannsopaulo-7bb.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer cetic.br.
lulu@lulu-ZenBook-UX435EA-UX435EA:~$
```