

Comunicações por Computadores (3º ano MIEI)

Trabalho Prático nº3

Serviço de Resolução de Nomes (DNS) - PL 2 Grupo 3

Henrique Paz (a84372), José Santos (a84288), Pedro Gomes (a84220)

5 de Abril de 2020

Conteúdo

1	Questoes e respostas	3
1.1	1-a)	3
1.2	1-b)	3
1.3	1-c)	4
1.4	1-d)	5
1.5	1-e)	6
1.6	1-f)	7
1.7	1-g)	8
1.8	1-h)	9
1.9	1-i)	10
1.10	1-j)	10
2	Parte II: Instalação, configuração e teste de um domínio CC.PT	11
2.1	Cricacao de um dominio CC.PT	11
3	Conclusão	14

1 Questões e respostas

1.1 1-a)

Qual o conteúdo do ficheiro `/etc/resolv.conf` e para que serve essa informação?

O ficheiro `resolv.conf` contém os servidores que DNS que servem para resolver problemas de nomes de domínio e de endereços IP.

```
core@XubunCORE:~$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 127.0.0.1
search home
core@XubunCORE:~$
```

1.2 1-b)

Os servidores `www.sapo.pt` e `www.yahoo.com` têm endereços IPv6? Se sim, quais?

Sim tem endereços IPv6 que no caso do `www.sapo.pt` é `2001:8a0:2102:c:213:13:146:142` e no caso do `www.yahoo.com` é `2001:8a0:2102:c:213:13:146:142`

```
pedro@DESKTOP-2T5G8H6:~$ nslookup -query=AAAA www.sapo.pt
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
Name:   www.sapo.pt
Address: 2001:8a0:2102:c:213:13:146:142
```

```
pedro@DESKTOP-2T5G8H6:~$ nslookup -query=AAAA www.yahoo.com
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
www.yahoo.com canonical name = atsv2-fp-shed.wg1.b.yahoo.com.
Name:   atsv2-fp-shed.wg1.b.yahoo.com
Address: 2a00:1288:110:1c::4
Name:   atsv2-fp-shed.wg1.b.yahoo.com
Address: 2a00:1288:110:1c::3

pedro@DESKTOP-2T5G8H6:~$
```

1.3 1-c)

Quais os servidores de nomes definidos para os domínios: “uminho.pt.”, “pt.” e “?”?

Atravez do comando nslookup é possível ver os servidores de nomes definidos para cada um dos dominios tal como é visível nas imagens

```
pedro@DESKTOP-2T5G8H6:~$ nslookup -q=ns uminho.pt.  
Server:          192.168.1.1  
Address:         192.168.1.1#53  
  
Non-authoritative answer:  
uminho.pt        nameserver = dns3.uminho.pt.  
uminho.pt        nameserver = dns2.uminho.pt.  
uminho.pt        nameserver = ns02.fccn.pt.  
uminho.pt        nameserver = dns.uminho.pt.  
  
Authoritative answers can be found from:
```

```
pedro@DESKTOP-2T5G8H6:~$ nslookup -q=ns pt.  
Server:          192.168.1.1  
Address:         192.168.1.1#53  
  
Non-authoritative answer:  
pt               nameserver = c.dns.pt.  
pt               nameserver = d.dns.pt.  
pt               nameserver = a.dns.pt.  
pt               nameserver = ns.dns.br.  
pt               nameserver = e.dns.pt.  
pt               nameserver = ns2.nic.fr.  
pt               nameserver = f.dns.pt.  
pt               nameserver = b.dns.pt.  
pt               nameserver = g.dns.pt.  
pt               nameserver = h.dns.pt.  
  
Authoritative answers can be found from:
```

```

pedro@DESKTOP-2T5G8H6:~$ nslookup -q=ns .
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
.           nameserver = i.root-servers.net.
.           nameserver = d.root-servers.net.
.           nameserver = g.root-servers.net.
.           nameserver = l.root-servers.net.
.           nameserver = a.root-servers.net.
.           nameserver = m.root-servers.net.
.           nameserver = c.root-servers.net.
.           nameserver = k.root-servers.net.
.           nameserver = b.root-servers.net.
.           nameserver = h.root-servers.net.
.           nameserver = f.root-servers.net.
.           nameserver = j.root-servers.net.
.           nameserver = e.root-servers.net.

Authoritative answers can be found from:

```

1.4 1-d)

Existe o domínio nice.software.? Será que nice.software. é um host ou um domínio?

Sim o domínio nice.software. existe visto que tem um endereço IP associado como se pode ver na imagem

```

pedro@DESKTOP-2T5G8H6:~$ host nice.software.
nice.software has address 213.212.81.71
pedro@DESKTOP-2T5G8H6:~$

```

1.5 1-e)

Qual é o servidor DNS primário definido para o domínio msf.org.? Este servidor primário (master) aceita queries recursivas? Porquê?

Pela primeira imagem sabemos que o servidor Dns primario definido é ns1.dds.nl. e pela segunda imagem na parte das flags verificamos que esta presente o simbolo 'ra' o que significa recursion available logo o servidor aceita queries recursivas.

```
pedro@DESKTOP-2T5G8H6:~$ nslookup -q=soa msf.org
Server:                192.168.1.1
Address:               192.168.1.1#53

Non-authoritative answer:
msf.org
    origin = ns1.dds.nl
    mail addr = postmaster.msf.org
    serial = 1407464621
    refresh = 16384
    retry = 2048
    expire = 1048576
    minimum = 2560

Authoritative answers can be found from:
```

```

pedro@DESKTOP-2T5G8H6:~$ dig ns1.dds.nl.

; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> ns1.dds.nl.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62705
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 2048
;; QUESTION SECTION:
;ns1.dds.nl.                IN      A

;; ANSWER SECTION:
ns1.dds.nl.                86400   IN      A      91.142.253.70

;; Query time: 151 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Apr 15 16:45:01 WEST 2020
;; MSG SIZE rcvd: 55

```

1.6 1-f)

Obtenha uma resposta “autoritativa” para a questão anterior

1.7 1-g)

Onde são entregues as mensagens de correio eletrônico dirigidas aos presidentes **marcelo@presidencia.pt** e **bolsonaro@casacivil.gov.br**?

presidencia.pt: as mensagens de correio eletrônico são entregues nos servidores mail1.presidencia.pt. e mail2.presidencia.pt.

casacivil.gov.br: as mensagens de correio eletrônico são entregues em esa01.presidencia.gov.br e em esa02.presidencia.gov.br, ambas as respostas são podem ser confirmadas nas imagens que se seguem

```
pedro@DESKTOP-2T5G8H6:~$ nslookup
> set query=MX
> presidencia.pt
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
presidencia.pt mail exchanger = 50 mail1.presidencia.pt.
presidencia.pt mail exchanger = 10 mail2.presidencia.pt.

Authoritative answers can be found from:
>
```

```
pedro@DESKTOP-2T5G8H6:~$ nslookup
> set query=MX
> casacivil.gov.br
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
casacivil.gov.br mail exchanger = 5 esa01.presidencia.gov.br.
casacivil.gov.br mail exchanger = 10 esa02.presidencia.gov.br.

Authoritative answers can be found from:
>
```


1.8 1-h)

Que informação é possível obter, via DNS, acerca de **whitehouse.gov**?

Para além da identificação dos nomes dos servidores, o IPv4 associado(69.192.66.35) e também olhando para as flags sabemos que as queries recursivas são aceites pelo servidor.

```
pedro@DESKTOP-2T5G8H6:~$ dig whitehouse.gov

; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> whitehouse.gov
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46646
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 2048
;; QUESTION SECTION:
;whitehouse.gov.                IN      A

;; ANSWER SECTION:
whitehouse.gov.                20      IN      A      69.192.66.35

;; Query time: 32 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Apr 15 20:23:07 WEST 2020
;; MSG SIZE rcvd: 59

pedro@DESKTOP-2T5G8H6:~$
```

1.9 1-i)

Consegue interrogar o DNS sobre o endereço IPv6 2001:690:a00:1036:1113::247 usando algum dos clientes DNS? Que informação consegue obter? Supondo que teve problemas com esse endereço, consegue obter um contacto do responsável por esse IPv6?

Sim, é possível interrogar o DNS sobre o endereço IPv6 2001:690:a00:1036:1113::247 e desta forma obter o nome de domínio que é www.fccn.pt. No entanto não conseguimos entrar em contacto com ninguém responsável como é verificável na imagem

```
pedro@DESKTOP-2T5G8H6:~$ nslookup 2001:690:a00:1036:1113::247
7.4.2.0.0.0.0.0.0.0.3.1.1.1.6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa      name = www.fccn.pt.

Authoritative answers can be found from:

pedro@DESKTOP-2T5G8H6:~$
```

1.10 1-j)

Os secundários usam um mecanismo designado por “Transferência de zona” para se atualizarem automaticamente a partir do primário, usando os parâmetros definidos no Record do tipo SOA do domínio. Descreve sucintamente esse mecanismo com base num exemplo concreto (ex: di.uminho.pt ou o domínio cc.pt que vai ser criado na topologia virtual).

Transferência de zona no Dns é uma query IXFR ou AXFR que é usada para replicar uma parte contínua, zona, ou até mesmo a totalidade da base de dados do Dns do servidor.

2 Parte II: Instalação, configuração e teste de um domínio CC.PT

2.1 Cricacao de um dominio CC.PT

```
include "/home/core/primario/named.conf.options";
include "/home/core/primario/named.conf.local";
include "/home/core/primario/named.conf.default-zones";

zone "cc.pt"{
    type master;
    file "/home/core/primario/db.cc.pt";
    allow-transfer {10.4.4.1};
};

zone "3.3.10.in-addr.arpa" {
    type master;
    file "/home/core/primario/db.3-3-10.rev";
    allow-transfer{10.4.4.1};
};
```

Figura 1: primario/named.conf

```
$TTL 604800
@      IN      SOA     dns.cc.pt. grupo03.cc.pt. (
                        2           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )    ; Negative Cache TTL
;
@      IN      NS      dns.cc.pt.
@      IN      NS      dns2.cc.pt.

Serv1  IN      A       10.3.3.1
dns    IN      A       10.3.3.1
dns2   IN      A       10.4.4.1

Serv3  IN      A       10.3.3.3
www    IN      CNAME   Serv3
mail   IN      MX      20      Serv3

Serv2  IN      A       10.3.3.2
pop    IN      CNAME   Serv2
imap   IN      CNAME   Serv2
mail   IN      MX      10      Serv3
```

Figura 2: primario/db.cc.pt

```

$TTL      604800
@         IN      SOA      dns.cc.pt. admin.cc.pt. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@         IN      NS       dns.cc.pt.
@         IN      NS       dns2.cc.pt.
1.3       IN      PTR      dns.cc.pt.
1.4       IN      PTR      dns2.cc.pt.

```

Figura 3: primario/db.3-3-3.rev

```

include "/home/core/secundario/named.conf.options";
include "/home/core/secundario/named.conf.local";
include "/home/core/secundario/named.conf.default-zones";

zone "cc.pt" {
    type slave;
    file "/home/core/primario/db.cc.pt";
    masters {10.3.3.1;};
};

zone "3.3.10.in-addr.arpa" {
    type slave;
    file "/home/core/primario/db.3-3-10.rev";
    masters {10.3.3.1;};
};

```

Figura 4: secundario/named.conf.local

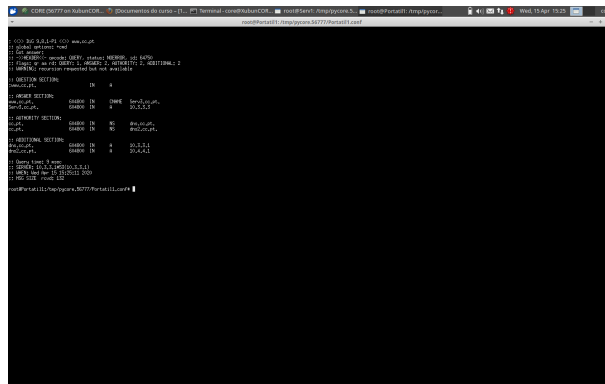
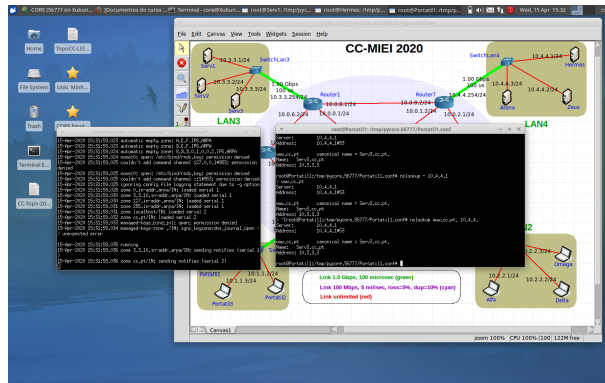


Figura 5: Queries aos servidores DNS

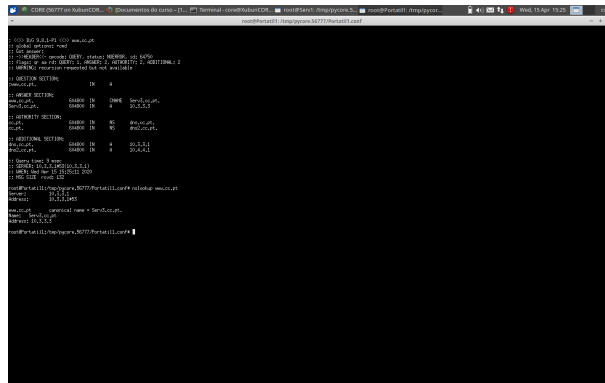
A terminal window with a dark background and light-colored text. It displays the output of several DNS-related commands. The first command is 'nslookup', which shows the default settings for the nslookup utility. The second command is 'nslookup www.google.com', which returns the IP address of www.google.com (74.125.233.100) and lists the DNS servers used for the lookup. The third command is 'nslookup -type=NS www.google.com', which returns the names of the authoritative DNS servers for the google.com domain. The fourth command is 'nslookup -type=A www.google.com', which returns the IP address of www.google.com. The fifth command is 'nslookup -type=AAAA www.google.com', which returns the IPv6 address of www.google.com. The sixth command is 'nslookup -type=CNAME www.google.com', which returns the canonical name for www.google.com. The seventh command is 'nslookup -type=MX www.google.com', which returns the mail exchange records for google.com. The eighth command is 'nslookup -type=SOA www.google.com', which returns the start of authority records for google.com. The ninth command is 'nslookup -type=PTR www.google.com', which returns the pointer records for google.com. The tenth command is 'nslookup -type=SRV www.google.com', which returns the service records for google.com. The eleventh command is 'nslookup -type=TXT www.google.com', which returns the text records for google.com. The twelfth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The thirteenth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The fourteenth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The fifteenth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The sixteenth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The seventeenth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The eighteenth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The nineteenth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The twentieth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The twenty-first command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The twenty-second command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The twenty-third command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The twenty-fourth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The twenty-fifth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The twenty-sixth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The twenty-seventh command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The twenty-eighth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The twenty-ninth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The thirtieth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The thirty-first command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The thirty-second command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The thirty-third command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The thirty-fourth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The thirty-fifth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The thirty-sixth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The thirty-seventh command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The thirty-eighth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The thirty-ninth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The fortieth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The forty-first command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The forty-second command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The forty-third command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The forty-fourth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The forty-fifth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The forty-sixth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The forty-seventh command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The forty-eighth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The forty-ninth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The fiftieth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The fifty-first command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The fifty-second command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The fifty-third command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The fifty-fourth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The fifty-fifth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The fifty-sixth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The fifty-seventh command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The fifty-eighth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The fifty-ninth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The sixtieth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The sixty-first command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The sixty-second command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The sixty-third command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The sixty-fourth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The sixty-fifth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The sixty-sixth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The sixty-seventh command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The sixty-eighth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The sixty-ninth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The seventieth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The seventy-first command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The seventy-second command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The seventy-third command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The seventy-fourth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The seventy-fifth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The seventy-sixth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The seventy-seventh command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The seventy-eighth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The seventy-ninth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The eightieth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The eighty-first command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The eighty-second command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The eighty-third command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The eighty-fourth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The eighty-fifth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The eighty-sixth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The eighty-seventh command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The eighty-eighth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The eighty-ninth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The ninetieth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The ninety-first command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The ninety-second command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The ninety-third command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The ninety-fourth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The ninety-fifth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The ninety-sixth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The ninety-seventh command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The ninety-eighth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com. The ninety-ninth command is 'nslookup -type=ALL www.google.com', which returns all the records for google.com. The hundredth command is 'nslookup -type=ANY www.google.com', which returns all the records for google.com.

Figura 6: Queries aos servidores DNS

3 Conclusão

Dado concludido o trabalho pratico 3, sobre o dns,nós achamos que obtivemos bastantes conhecimentos sobre este sistema de gestao de nomes distribuido e hierarquico.

Na primeira fase trabalhamos com diferentes formas de interrogar o dns.Começamos por investigar o ficheiro que contem os servidores de dns root, e depois usamos varios comandos para interrogar o sistema, desde o nslookup, ao dig, host, em que poderiamos fazer queries especificas por exemplo o registo 'NS', que devolve os nomes dos servidores do dominio, ou 'A' para saber o endereço neste caso o Ipv4 entre outros registos.

Na segunda parte do trabalho fizemos a instalação, configuração e teste de um dominio que neste caso era o cc.pt o que ainda nos criou algumas dificuldades principalmente na parte da configuração mas no final achamos que conseguimos ultrapassar os obstaculos que nos foram aparecendo e deste modo achamos que tivemos um resultado positivo.