

TP3: Serviço de Resolução de Nomes (DNS)

Comunicações por Computador
Universidade do Minho

André Peixoto, Filipe Cunha, João Monteiro



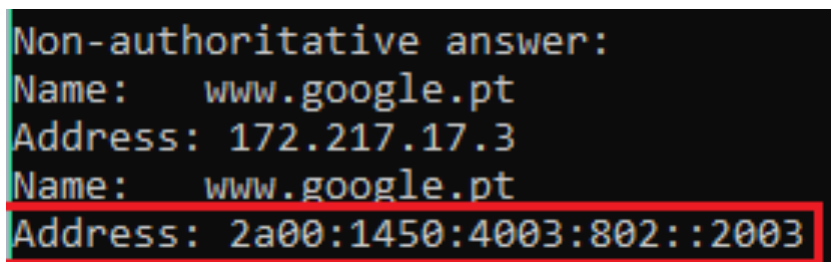
1 Questões e Respostas

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

O ficheiro resolv.conf é um ficheiro de texto de configuração que contém informação que determina os parâmetros operacionais do DNS. Este permite às aplicações fazerem a conversão de nomes de domínio específicos para endereços IP, de modo a ser possível a conexão à internet e à rede local.

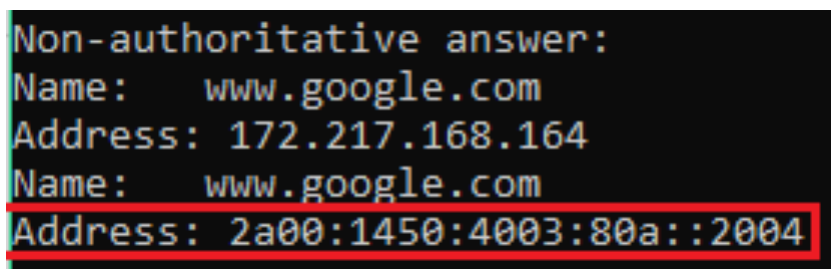
1.2 b) Os servidores **www.google.pt.** e **www.google.com.** têm endereços IPv6? Se sim, quais?

Usando os comandos "nslookup www.google.pt." e "nslookup www.google.com." obtemos a seguinte informação:



```
Non-authoritative answer:
Name:   www.google.pt
Address: 172.217.17.3
Name:   www.google.pt
Address: 2a00:1450:4003:802::2003
```

Figure 1: O endereço IPv6 do servidor **www.google.pt.** é 2a00:1450:4003:802::2003



```
Non-authoritative answer:
Name:   www.google.com
Address: 172.217.168.164
Name:   www.google.com
Address: 2a00:1450:4003:80a::2004
```

Figure 2: O endereço IPv6 do servidor **www.google.com.** é 2a00:1450:4003:80a::2004

1.3 c) Quais os servidores de nomes definidos para os domínios: “**ccg.pt.**”, “**pt.**” e “**.”**?

Usando os comandos "dig ccg.pt.", "dig pt." e "dig .", obtemos os respetivos servidores de nomes:

```

: <<>> DiG 9.11.3-lubuntu1.1-Ubuntu <<>> ccg.pt.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47242
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a17304fd8d7c93ba32ed85695ca38f46c725de36aeb11c5b (good)
;; QUESTION SECTION:
;ccg.pt.                                IN      A

;; ANSWER SECTION:
ccg.pt.                338      IN      A      193.136.14.98

;; AUTHORITY SECTION:
ccg.pt.                3578     IN      NS      ns1.ccg.pt.
ccg.pt.                3578     IN      NS      ns3.ccg.pt.

;; ADDITIONAL SECTION:
ns3.ccg.pt.            1806     IN      A      193.136.11.203
ns1.ccg.pt.            587      IN      A      193.136.11.201

```

Figure 3: Os name servers do domínio ccg.pt. são ns1.ccg.pt e ns3.ccg.pt. (secundário)

```

: <<>> DiG 9.11.3-lubuntu1.1-Ubuntu <<>> pt.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41304
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 8acb17ff6624bef080deffd55ca38f0b068d411a13891645 (good)
;; QUESTION SECTION:
;pt.                                IN      A

;; AUTHORITY SECTION:
pt.                300      IN      SOA      curiosity.dns.pt. request.dns.pt.

```

Figure 4: O name server do domínio pt. é curiosity.dns.pt.

```

: <<>> DiG 9.11.3-lubuntu1.1-Ubuntu <<>> .
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52892
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4020f2d5a9b893e8f80343fb5ca38ec318eabe7674f7247c (good)
;; QUESTION SECTION:
;.                                IN      A

;; AUTHORITY SECTION:
.                3325     IN      SOA      a.root-servers.net. nstld.verisign-grs.com.

```

Figure 5: O name server do domínio . é a.root-servers.net

1.4 d) Existe o domínio eureka.software.? Será que eureka.software. é um host?

De facto, eureka.software. é um Host. Esta afirmação justifica-se com o facto de que, ao utilizar o comando "dig eureka.software.", recebemos resposta a uma query do tipo A, o que nos informa de que se trata de uma máquina com endereço próprio.

```
;<<>> DiG 9.11.3-lubuntu1.1-Ubuntu <<>> eureka.software
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35574
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 3

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
; COOKIE: 2a6bc0e75083ef68eb50bd345ca3b12ae36b53e29dbd0e01 (good)
; QUESTION SECTION:
eureka.software.          IN      A

; ANSWER SECTION:
eureka.software.          300     IN      A      34.214.90.141

; AUTHORITY SECTION:
eureka.software.          724     IN      NS      ns-312.awsdns-39.com.
eureka.software.          724     IN      NS      ns-957.awsdns-55.net.
eureka.software.          724     IN      NS      ns-1624.awsdns-11.co.uk.
eureka.software.          724     IN      NS      ns-1241.awsdns-27.org.

; ADDITIONAL SECTION:
ns-312.awsdns-39.com.     2199    IN      A      205.251.193.56
ns-957.awsdns-55.net.     2811    IN      A      205.251.195.189
```

Figure 6: Comando "dig eureka.software."

1.5 e) Qual é o servidor DNS primário definido para o domínio ami.pt.? Este servidor primário (master) aceita queries recursivas? Porquê?

O servidor DNS primário do domínio ami.pt. é ns1.ami.pt. Para sabermos se este servidor aceita queries recursivas, utilizamos o dig, porque este envia uma query recursiva por defeito. Se o server suporta queries recursivas, a resposta terá uma flag de "recursion available", o que tal se verificou.

```

; <<>> DiG 9.11.3-1ubuntu1.5-Ubuntu <<>> ami.pt.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36945
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 469c2389be1cb8c12ddef02e5ca3926651f38bb08fab8883 (good)
;; QUESTION SECTION:
;ami.pt.                                IN      A

;; ANSWER SECTION:
ami.pt.                                3600    IN      A      80.172.230.97

;; AUTHORITY SECTION:
ami.pt.                                1281    IN      NS      ns1.ami.pt.
ami.pt.                                1281    IN      NS      ns2.ami.pt.

;; ADDITIONAL SECTION:
ns2.ami.pt.                            1281    IN      A      5.199.172.41
ns1.ami.pt.                            1281    IN      A      80.172.230.28

```

Figure 7: Comando "dig ami.pt."

```

; <<>> DiG 9.11.3-1ubuntu1.5-Ubuntu <<>> ami.pt.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36945
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

```

Figure 8: Flags da resposta com "ra"

1.6 f) Obtenha uma resposta "autoritativa" para a questão anterior.

Usando o comando "dig nl.dot2web.com" recebemos agora uma resposta autoritativa do servidor, onde a flag recursion available se mantém (o servidor aceita queries recursivas).

```

; <<>> DiG 9.11.3-1ubuntu1.5-Ubuntu <<>> n1.dot2web.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 2567
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 6f34df67b3170220f2d5272f5ca3a33e6c4e59ca69e438b0 (good)
;; QUESTION SECTION:
;n1.dot2web.com.                IN      A

;; AUTHORITY SECTION:
dot2web.com.                    3123    IN      SOA     ns1.dot2web.com. dc.dot2web.pt.

```

Figure 9: Flags da resposta autoritativa com "ra"

1.7 g) Onde são entregues as mensagens dirigidas a marcelo@presidencia.pt? E a guterres@onu.org?

As mensagens a marcelo@presidencia.pt são entregues a mail1.presidencia.pt e aquelas que são dirigidas a guterres@onu.org são levadas a mail.onu.org.

```

> ^Candregpx@Laptop-André:/mnt/c/Users/André/Desktop$ nslookup
> set type=mx
> presidencia.pt
Server:          193.137.16.65
Address:         193.137.16.65#53

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

```

Figure 10: Sequência de comandos para obter a primeira resposta

```

> ^Candregpx@Laptop-André:/mnt/c/Users/André/Desktop$ nslookup
> set type=mx
> onu.org
Server:          193.137.16.65
Address:         193.137.16.65#53

Non-authoritative answer:
onu.org mail exchanger = 10 mail.onu.org.

```

Figure 11: Sequência de comandos para obter a segunda resposta

1.8 h) Que informação é possível obter acerca de www.whitehouse.gov? Qual é o endereço IPv4 associado?

Ao realizar o comando "dig www.whitehouse.gov" conseguimos obter várias informações.

```

;; ANSWER SECTION:
www.whitehouse.gov. 300 IN CNAME wildeard.whitehouse.gov.edgekey.net.
wildeard.whitehouse.gov.edgekey.net. 900 IN CNAME e4036.dscb.akamaiedge.net.
e4036.dscb.akamaiedge.net. 20 IN A 23.10.65.110 ipv4 do endereço

;; AUTHORITY SECTION:
dscb.akamaiedge.net. 2405 IN NS n0dscb.akamaiedge.net.
dscb.akamaiedge.net. 2405 IN NS n6dscb.akamaiedge.net.
dscb.akamaiedge.net. 2405 IN NS n1dscb.akamaiedge.net.
dscb.akamaiedge.net. 2405 IN NS n5dscb.akamaiedge.net.
dscb.akamaiedge.net. 2405 IN NS n7dscb.akamaiedge.net.
dscb.akamaiedge.net. 2405 IN NS n4dscb.akamaiedge.net.
dscb.akamaiedge.net. 2405 IN NS n3dscb.akamaiedge.net.
dscb.akamaiedge.net. 2405 IN NS n2dscb.akamaiedge.net.

;; ADDITIONAL SECTION:
n5dscb.akamaiedge.net. 2405 IN A 2.16.65.215 ipv4 de name servers
n0dscb.akamaiedge.net. 2405 IN A 88.221.81.192
n3dscb.akamaiedge.net. 2405 IN A 2.16.65.206
n2dscb.akamaiedge.net. 2405 IN A 2.16.65.205
n1dscb.akamaiedge.net. 2405 IN A 2.16.65.214
n7dscb.akamaiedge.net. 2405 IN A 95.101.143.101
n4dscb.akamaiedge.net. 2405 IN A 2.16.65.213
n6dscb.akamaiedge.net. 2405 IN A 88.221.90.156
n0dscb.akamaiedge.net. 2405 IN AAAA 2600:1480:c800::c0 ipv6 de name servers

```

Figure 12: Resultado do comando "dig www.whitehouse.gov".

Primeiramente, temos que www.whitehouse.gov tem como alias "wildeard.whitehouse.gov.edgekey.net." que por sua vez tem como alias "e4036.dscb.akamaiedge.net.". Vemos isto através dos records CNAME que se podem ver na imagem. Para além disso analisando o Record A da resposta à query vemos que e4036.dscb.akamaiedge.net. tem como endereço ipv4 23.10.65.110 o que faz com que todos os outros domínios apontem para este mesmo ipv4.

Vemos ainda que cada um dos registos que fornecem estas informações tem ttl igual a 300 (primerio CNAME), 900 (segundo CNAME) e 20 (Record A) respetivamente. Para além disso conseguimos saber quais os Name Servers responsáveis pelo domínio "e4036.dscb.akamaiedge.net." e os seus endereços ipv4 e ipv6 (Record AAAA) quando existente (n0dscb.akamaiedge.net. neste caso) registrando sempre o ttl de cada record da resposta.

1.9 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?

Usando o comando "dig -x 2001:690:a00:1036:1113::247" conseguimos fazer um reverse DNS lookup. Daqui, obtemos a seguinte informação:

1. O domínio correspondente: www.fccn.pt.
2. Os seus name servers: ns03.fccn.pt., ns02.fccn.pt., ns01.fccn.pt.
3. Os ipv4 (A) e ipv6 (AAAA) destes name servers

```
> ^Candregpx@Laptop-André:/mnt/c/Users/André/Desktop$ dig -x 2001:690:a00:1036:1113::247

;; <<>> DiG 9.11.3-1ubuntu1.5-Ubuntu <<>> -x 2001:690:a00:1036:1113::247
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4935
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 8e19f8b141ab92941452fc775ca3b42fc53e57528b90ee1b (good)
;; QUESTION SECTION:
;7.4.2.0.0.0.0.0.0.0.0.0.0.3.1.1.1.6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa. IN PTR

;; ANSWER SECTION:
7.4.2.0.0.0.0.0.0.0.0.0.0.3.1.1.1.6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa. 3600 IN PTR www.fccn.pt.

;; AUTHORITY SECTION:
0.9.6.0.1.0.0.2.ip6.arpa. 3600 IN NS ns03.fccn.pt.
0.9.6.0.1.0.0.2.ip6.arpa. 3600 IN NS ns02.fccn.pt.
0.9.6.0.1.0.0.2.ip6.arpa. 3600 IN NS ns01.fccn.pt.

;; ADDITIONAL SECTION:
ns02.fccn.pt. 2574 IN A 193.136.2.228
ns03.fccn.pt. 2566 IN A 138.246.255.249
ns01.fccn.pt. 2566 IN A 193.136.192.40
ns02.fccn.pt. 24 IN AAAA 2001:690:a80:4001::200
ns03.fccn.pt. 2566 IN AAAA 2001:4ca0:106:0:250:56ff:fea9:3fd
ns01.fccn.pt. 2566 IN AAAA 2001:690:a00:4001::200
```

Figure 13: Resultado do reverse DNS lookup

1.10 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).

Sendo que é um mecanismo para os administradores replicarem bancos de dados DNS em um conjunto de servidores, uma transferência de zona usa o TCP para transporte e assume a forma de

uma transação cliente-servidor. Tendo por exemplo o domínio di.uminho.pt, iniciar uma solicitação de transferência de zona AXFR é tão simples quanto usar o comando dig, em que di.uminho.pt é o domínio para o qual deseja-se iniciar uma transferência de zona, e dns2.di.uminho.pt é o servidor DNS requerido para consulta. Por exemplo:

1) o comando "dig +short di.uminho.pt" mostra numa lista, de forma resumida, todas os servidores DNS do domínio di.uminho.pt.

2) escolhe-se na lista gerada pelo comando "dig +short di.uminho.pt" um dos servidores DNS. Neste caso o servidor dns2.di.uminho.pt

3) inicia-se a transferência de zona usando o comando "dig axfr di.uminho.pt @dns2.di.uminho.pt."

2 Domínio de Nomes CC.PT

2.1 Nesta secção vamos mostrar vários prints sobre os resultados que obtivemos durante todo o desenvolvimento deste trabalho.

Na figura abaixo apresentamos o ficheiro db.cc.pt onde guardamos os dados do domínio "cc.pt".

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA     dns.cc.pt. grupo04@cc.pt. (
                        6           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )    ; Negative Cache TTL
;
@         IN      NS      dns.cc.pt.
dns       IN      A       10.1.1.1
Servidor1 IN      A       10.1.1.1
dns2      IN      CNAME   Urano
Urano     IN      A       10.2.2.3
imap      IN      CNAME   Servidor2
pop       IN      CNAME   Servidor2
Servidor2 IN      A       10.1.1.2
mail      IN      CNAME   Servidor3
www       IN      CNAME   Servidor3
Servidor3 IN      A       10.1.1.3
Grupo04   IN      CNAME   Cliente1
Cliente1  IN      A       10.4.4.1
Alfa      IN      A       10.3.3.1
Beta      IN      A       10.3.3.2
Gama      IN      A       10.3.3.3
```

Figure 14: Conteúdo do ficheiro db.cc.pt

2.2 A seguir, mostramos os ficheiros que contêm os dados dos domínios reversos das nossas redes.

```
;  
; BIND reverse data file for local loopback interface  
;  
$TTL      604800  
@         IN      SOA      dns.cc.pt. grupo04@cc.pt. (  
                                5          ; Serial  
                                604800     ; Refresh  
                                86400      ; Retry  
                                2419200    ; Expire  
                                604800 )    ; Negative Cache TTL  
;  
@         IN      NS       dns.  
1         IN      PTR      Servidor1  
1         IN      PTR      dns  
2         IN      PTR      Servidor2  
2         IN      PTR      imap  
2         IN      PTR      pop  
3         IN      PTR      Servidor3  
3         IN      PTR      mail  
3         IN      PTR      www
```

Figure 15: Dados do domínio reverso 1.1.10.in-addr.arpa. relativos à rede 10.1.1.0/24

```
;  
; BIND reverse data file for local loopback interface  
;  
$TTL      604800  
@         IN      SOA      dns.cc.pt. grupo04@cc.pt. (  
                                5          ; Serial  
                                604800     ; Refresh  
                                86400      ; Retry  
                                2419200    ; Expire  
                                604800 )    ; Negative Cache TTL  
;  
@         IN      NS       dns.  
1         IN      PTR      Alfa  
2         IN      PTR      Beta  
3         IN      PTR      Gama
```

Figure 16: Dados do domínio reverso 3.3.10.in-addr.arpa.

2.3 De seguida mostramos as zonas que criamos para o nosso dominio.

```
//  
// Do any local configuration here  
//  
  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
  
zone "1.1.10.in-addr.arpa" {  
    type master;  
    notify no;  
    file "/home/core/primario/db.1-1-10.rev";  
    allow-transfer {10.2.2.3;};  
};  
  
zone "3.3.10.in-addr.arpa" {  
    type master;  
    notify no;  
    file "/home/core/primario/db.3-3-10.rev";  
    allow-transfer {10.2.2.3;};  
};  
  
zone "cc.pt" {  
    type master;  
    file "/home/core/primario/db.cc.pt";  
    allow-transfer {10.2.2.3;};  
};
```

Figure 17: Zonas do servidor Primario

2.4 Na figura seguinte mostramos a lista dos hosts da nossa máquina.

```
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
S### begin CORE auto-generated hosts entrie
10.0.0.1          A0
10.0.0.2          A1
10.0.0.3          A2
10.0.0.4          A3
10.0.0.5          A4
10.0.0.6          A5
10.0.0.7          A6
10.0.0.8          A7
10.0.0.9          A8
10.0.0.10         A9
10.0.0.11         A10
10.0.0.12         A11
10.0.0.13         A12
10.0.0.14         A13
10.0.0.15         A14
10.0.0.16         A15
10.0.0.17         A16
10.1.1.1 Servidor1
10.1.1.1 dns.cc.pt
10.2.2.3 Urano
10.2.2.3 dns2.cc.pt
10.1.1.2 Servidor2
10.1.1.3 Servidor3
### end CORE auto-generated hosts entries
```

Figure 18: Lista de Hosts

2.5 Finalmente, nas próximas duas imagens mostramos vários exemplos de interrogações aos servidores que criamos e as suas respostas.

```
> dns.cc.pt.  
Server:      Servidor1  
Address:     10.1.1.1#53  
  
Name:  dns.cc.pt  
Address: 10.1.1.1  
> dns2.cc.pt  
Server:      Servidor1  
Address:     10.1.1.1#53  
  
dns2.cc.pt    canonical name = Urano.cc.pt.  
Name:  Urano.cc.pt  
Address: 10.2.2.3  
> mail.cc.pt.  
Server:      Servidor1  
Address:     10.1.1.1#53  
  
mail.cc.pt    canonical name = Servidor3.cc.pt.  
Name:  Servidor3.cc.pt  
Address: 10.1.1.3  
> Servidor2.cc.pt  
Server:      Servidor1  
Address:     10.1.1.1#53  
  
Name:  Servidor2.cc.pt  
Address: 10.1.1.2  
> █
```

Figure 19: Comando nslookup Servidor1 para dns.cc.pt, dns2.cc.pt e mail.cc.pt

```
> Servidor3.cc.pt.  
Server:      Servidor1  
Address:     10.1.1.1#53  
  
Name:  Servidor3.cc.pt  
Address: 10.1.1.3  
> Grupo04.cc.pt.  
Server:      Servidor1  
Address:     10.1.1.1#53  
  
Grupo04.cc.pt canonical name = Cliente1.cc.pt.  
Name:  Cliente1.cc.pt  
Address: 10.4.4.1  
> Cliente1.cc.pt.  
Server:      Servidor1  
Address:     10.1.1.1#53  
  
Name:  Cliente1.cc.pt  
Address: 10.4.4.1  
> Alfa.cc.pt.  
Server:      Servidor1  
Address:     10.1.1.1#53  
  
Name:  Alfa.cc.pt  
Address: 10.3.3.1  
> Beta.cc.pt.  
Server:      Servidor1  
Address:     10.1.1.1#53  
  
Name:  Beta.cc.pt  
Address: 10.3.3.2  
> Gama.cc.pt.  
Server:      Servidor1  
Address:     10.1.1.1#53  
  
Name:  Gama.cc.pt  
Address: 10.3.3.3  
> █
```

Figure 20: Comando nslookup Servidor1 para Servidor3.cc.pt, Grupo04.cc.pt, Cliente1.cc.pt e outros.

3 Conclusões

Neste trabalho explorámos os vários temas relacionados com DNS. Aprendemos a criar domínios e a utilizar as suas funcionalidades explorando os mecanismos que são usados no dia a dia na maioria dos servidores na Internet. Para além disso, ainda conseguimos utilizar as informações que obtivemos nas aulas teóricas de forma a enriquecer o nosso conhecimento sobre este tema.