

## QUESTÃO 0

De forma a determinar o endereço IP de cada um dos servidores de DNS de raiz, procedeu-se, através do terminal, à introdução do comando:

### 1. *dig*

```
;; ANSWER SECTION:
.      454606  IN      NS      k.root-servers.net.
.      454606  IN      NS      l.root-servers.net.
.      454606  IN      NS      m.root-servers.net.
.      454606  IN      NS      a.root-servers.net.
.      454606  IN      NS      b.root-servers.net.
.      454606  IN      NS      c.root-servers.net.
.      454606  IN      NS      d.root-servers.net.
.      454606  IN      NS      e.root-servers.net.
.      454606  IN      NS      f.root-servers.net.
.      454606  IN      NS      g.root-servers.net.
.      454606  IN      NS      h.root-servers.net.
.      454606  IN      NS      i.root-servers.net.
.      454606  IN      NS      j.root-servers.net.
```

**FIG. 1:** Parte do *output* do comando *dig*.

Através dos resultados obtidos (**FIG. 1**) – uma lista dos servidores mencionados, bem como uma lista com o endereços de alguns dos servidores – é possível proceder a um novo *dig*, desta vez passando como parâmetro o ‘nome’ do servidor. Efectou-se este passo apenas para os servidores que, por ter sido atingido o tamanho máximo da resposta, não constam da mesma, nomeadamente a partir do servidor *i.root-servers.net*. A título de exemplo, indica-se o comando utilizado para determinar o endereço IP do servidor *j.root-servers.net*.

### 2. *dig j.root-servers.net*.

Os resultados são apresentados abaixo, na **Tabela 1**.

**TABELA 1:** Parte do *output* do comando *dig*

| SERVIDOR                   | ENDEREÇO IP    |
|----------------------------|----------------|
| <i>a.root-servers.net.</i> | 1.198.41.0.4   |
| <i>b.root-servers.net.</i> | 192.228.79.201 |
| <i>c.root-servers.net.</i> | 192.33.4.12    |
| <i>d.root-servers.net.</i> | 128.8.10.90    |
| <i>e.root-servers.net.</i> | 192.203.230.10 |
| <i>f.root-servers.net.</i> | 192.5.5.241    |
| <i>g.root-servers.net.</i> | 192.112.36.4   |

|                            |               |
|----------------------------|---------------|
| <i>h.root-servers.net.</i> | 128.63.2.53   |
| <i>i.root-servers.net.</i> | 192.36.148.17 |
| <i>j.root-servers.net.</i> | 192.58.128.30 |
| <i>k.root-servers.net.</i> | 193.0.14.129  |
| <i>l.root-servers.net.</i> | 199.7.83.42   |
| <i>m.root-servers.net.</i> | 202.12.27.33  |

## QUESTÃO 1

Primeiramente, de forma a resolver a questão, recorreu-se à ferramenta *nslookup*, utilizada para obter informações sobre registos de DNS (*Domain System Name*).

### 3. *nslookup*

No sentido de obter os nomes dos servidores requeridos, foi necessário definir o tipo de consulta, através do comando:

### 4. *set type=ns*

Após as operações descritas, foi possível obter, para cada um dos domínios, os respectivos nomes dos servidores. É importante realçar que um servidor DNS não é necessariamente *master* ou *slave*, podendo assumir o papel de *master* para alguns domínios e *slave* para outros [1].

Apresentam-se, nas **FIG. 2-4**, os resultados relativos às alíneas propostas.

```
Non-authoritative answer:
di.uminho.pt      nameserver = marco.uminho.pt.
di.uminho.pt      nameserver = dns.di.uminho.pt.
di.uminho.pt      nameserver = dns.uminho.pt.
di.uminho.pt      nameserver = ns1.eurotux.com.
di.uminho.pt      nameserver = ns3.eurotux.com.
di.uminho.pt      nameserver = alfa.di.uminho.pt.
di.uminho.pt      nameserver = dns2.di.uminho.pt.
di.uminho.pt      nameserver = dns2.uminho.pt.
di.uminho.pt      nameserver = dns3.uminho.pt.

Authoritative answers can be found from:
dns.di.uminho.pt  internet address = 193.136.19.1
dns.di.uminho.pt  has AAAA address 2001:690:2280:28::1
dns.uminho.pt     internet address = 193.137.16.75
dns.uminho.pt     has AAAA address 2001:690:2280:1::75
ns1.eurotux.com   internet address = 194.107.127.1
ns3.eurotux.com   internet address = 216.75.63.6
alfa.di.uminho.pt internet address = 193.136.19.3
dns2.di.uminho.pt internet address = 193.136.19.2
dns2.di.uminho.pt has AAAA address 2001:690:2280:28::2
dns2.uminho.pt    internet address = 193.137.16.145
dns2.uminho.pt    has AAAA address 2001:690:2280:801::145
dns3.uminho.pt    internet address = 193.137.16.65
dns3.uminho.pt    has AAAA address 2001:690:2280:1::65
marco.uminho.pt   internet address = 193.136.9.240
```

**FIG. 2:** Output do comando *nslookup nameserver* para o servidor *di.uminho.pt*.

```

Non-authoritative answer:
uminho.pt      nameserver = ns02.fccn.pt.
uminho.pt      nameserver = dns.uminho.pt.
uminho.pt      nameserver = dns2.uminho.pt.
uminho.pt      nameserver = dns3.uminho.pt.

Authoritative answers can be found from:
dns.uminho.pt  internet address = 193.137.16.75
dns.uminho.pt  has AAAA address 2001:690:2280:1::75
dns2.uminho.pt internet address = 193.137.16.145
dns2.uminho.pt has AAAA address 2001:690:2280:801::145
dns3.uminho.pt internet address = 193.137.16.65
dns3.uminho.pt has AAAA address 2001:690:2280:1::65
ns02.fccn.pt   internet address = 193.136.2.228

```

**FIG. 3:** Output do comando *nslookup nameserver* para o servidor *uminho.pt*.

```

Non-authoritative answer:
google.com     nameserver = ns2.google.com.
google.com     nameserver = ns3.google.com.
google.com     nameserver = ns4.google.com.
google.com     nameserver = ns1.google.com.

Authoritative answers can be found from:
ns1.google.com internet address = 216.239.32.10
ns2.google.com internet address = 216.239.34.10
ns3.google.com internet address = 216.239.36.10
ns4.google.com internet address = 216.239.38.10

```

**FIG. 4:** Output do comando *nslookup nameserver* para o *google.com*.

Por intermédio da análise dos *outputs*, verifica-se que existem respostas não autoritativas (*non-authoritative*) – teoricamente associadas a servidores primários ou *masters* – e autoritativas (*authoritative*) – por sua vez, associadas a servidores secundários ou *slaves*. A existência de respostas não autoritativas significam que o servidor DNS usado não responde através deste domínio, isto é, foi realizada uma consulta externa aos servidores do domínio pesquisado. Um servidor não autoritativo detém a informação porque, anteriormente, inquiriu um servidor autoritativo e a resposta ficou guardada em *cache*.

De forma a inverter esta situação, utilizou-se um dos servidores providenciados, observando-se agora que não é obtida qualquer resposta não autoritativa, devido ao facto de se utilizar um servidor DNS que possui os registos do domínio *di.uminho.pt*.

5. *server dns.di.uminho.pt.;*
6. *set type=ns;*
7. *di.uminho.pt..*

```

di.uminho.pt      nameserver = dns2.uminho.pt.
di.uminho.pt      nameserver = dns3.uminho.pt.
di.uminho.pt      nameserver = dns2.di.uminho.pt.
di.uminho.pt      nameserver = ns3.eurotux.com.
di.uminho.pt      nameserver = alfa.di.uminho.pt.
di.uminho.pt      nameserver = ns1.eurotux.com.
di.uminho.pt      nameserver = dns.uminho.pt.
di.uminho.pt      nameserver = marco.uminho.pt.
di.uminho.pt      nameserver = dns.di.uminho.pt.

```

**FIG. 5:** Output obtido para o exemplo descrito, referente a *di.uminho.pt*.

## QUESTÃO 2

Para a resolução desta questão, foi usado o comando que permite fazer *queries* sobre nomes de servidores de forma interactiva no terminal:

### 8. *nslookup*

Numa primeira parte da questão, pretendia-se obter respostas autoritativas de um servidor **SOA** - Start Of (a zone of) Authority record - para *sapo.pt.*, *yahoo.com.* e *publico.pt.*. De modo a cumprir o objectivo, utilizou-se o seguinte comando, que especifica o tipo da *query* a efectuar:

### 9. *set querytype=soa*

```

tav@ubuntu:~$ nslookup
> set querytype=soa
> sapo.pt.
Server:          127.0.0.1
Address:         127.0.0.1#53

Non-authoritative answer:
sapo.pt
      origin = ns.sapo.pt
      mail addr = root.sapo.pt
      serial = 1352802129
      refresh = 3600
      retry = 7200
      expire = 360000
      minimum = 18000

Authoritative answers can be found from:
sapo.pt nameserver = ns.sapo.pt.
sapo.pt nameserver = ns2.sapo.pt.
sapo.pt nameserver = dns01.sapo.pt.
sapo.pt nameserver = dns02.sapo.pt.
ns.sapo.pt      internet address = 212.55.154.202
ns2.sapo.pt     internet address = 212.55.154.194
dns01.sapo.pt   internet address = 213.13.28.116
dns01.sapo.pt   has AAAA address 2001:8a0:2106:4:213:13:28:116
dns02.sapo.pt   internet address = 213.13.30.116
dns02.sapo.pt   has AAAA address 2001:8a0:2206:4:213:13:30:116
> server ns2.sapo.pt
Default server: ns2.sapo.pt
Address: 212.55.154.194#53
> sapo.pt.
;; connection timed out; no servers could be reached
>

```

**FIG. 6:** Exemplo de uma *query* do tipo **SOA**.

Como é possível observar no *output* representado na **FIG. 6**, a resposta obtida não é uma resposta autoritativa, mas sim uma indicação de servidores que a podem dar. Escolher um desses servidores e fazer a mesma *query* permite obter uma resposta autoritativa. Não foi possível concluir este passo por falta de acesso a um endereço **IP** público, uma vez que a rede utilizada funciona por intermédio de um *proxy*. Para as restantes *queries* propostas - *yahoo.com*. e *publico.pt*. -, os resultados obtidos foram semelhantes.

A segunda parte da questão tinha também como objectivo obter respostas autoritativas, desta vez a partir de um registo **MX** – Mail Exchange Record –, pelo que se usou o seguinte comando:

**10.** *set querytype=mx*

```
tav@ubuntu:~$ nslookup
> set querytype=mx
> di.uminho.pt.
Server:      127.0.0.1
Address:     127.0.0.1#53

Non-authoritative answer:
di.uminho.pt mail exchanger = 20 mx-fe1.di.uminho.pt.
di.uminho.pt mail exchanger = 20 mx-fe2.di.uminho.pt.

Authoritative answers can be found from:
di.uminho.pt nameserver = dns3.uminho.pt.
di.uminho.pt nameserver = marco.uminho.pt.
di.uminho.pt nameserver = dns.di.uminho.pt.
di.uminho.pt nameserver = dns.uminho.pt.
di.uminho.pt nameserver = ns1.eurotux.com.
di.uminho.pt nameserver = ns3.eurotux.com.
di.uminho.pt nameserver = alfa.di.uminho.pt.
di.uminho.pt nameserver = dns2.di.uminho.pt.
di.uminho.pt nameserver = dns2.uminho.pt.
mx-fe1.di.uminho.pt internet address = 193.136.19.251
mx-fe2.di.uminho.pt internet address = 193.136.19.252
dns.di.uminho.pt    internet address = 193.136.19.1
dns.di.uminho.pt    has AAAA address 2001:690:2280:28::1
dns.uminho.pt       internet address = 193.137.16.75
dns.uminho.pt       has AAAA address 2001:690:2280:1::75
ns1.eurotux.com     internet address = 194.107.127.1
ns3.eurotux.com     internet address = 216.75.63.6
alfa.di.uminho.pt   internet address = 193.136.19.3
dns2.di.uminho.pt   internet address = 193.136.19.2
dns2.di.uminho.pt   has AAAA address 2001:690:2280:28::2
dns2.uminho.pt      internet address = 193.137.16.145
dns2.uminho.pt      has AAAA address 2001:690:2280:801::145
> server dns2.uminho.pt
Default server: dns2.uminho.pt
Address: 193.137.16.145#53
> di.uminho.pt.
;; connection timed out; no servers could be reached
>
```

**FIG. 7:** Exemplo de uma *query* do tipo **MX**.

Como é possível observar a partir do *output* (**FIG. 7**), não foi possível obter resposta autoritativa, pelos mesmos motivos explicitados no exemplo anterior.

### QUESTÃO 3

Réseaux IP Européens - RIPE - é a entidade responsável pelos dados administrativos europeus. Para aceder a informação inteiramente administrativa de supostos atacantes foi necessário recorrer à ferramenta disponível em *ripe.net/whois*. Inserindo os endereços de IP fornecidos na caixa de pesquisa, foi possível obter uma lista de informações (**FIG. 8**).

```
inetnum:      193.136.16.0 - 193.136.19.255
netname:      PTUMGUA-1
descr:        Universidade do Minho
descr:        Centro de Informatica
descr:        Campus de Gualtar
descr:        Braga
country:      PT
admin-c:      AS215
tech-c:       JAR36-RIPE
tech-c:       JMG41-RIPE
tech-c:       PAG10-RIPE
tech-c:       PVC8-RIPE
remarks:      rev-srv:          torga.ci.uminho.pt
status:       ASSIGNED PA
remarks:      created 19930305
mnt-by:       AS1930-MNT
mnt-lower:    AS1930-MNT
source:       RIPE #Filtered
remarks:      rev-srv attribute deprecated by RIPE NCC on 02/09/2009

person:       Alexandre Santos
address:      Universidade do Minho
address:      Departamento de Informatica
address:      P-4710-057 Braga
address:      Portugal
phone:        +351 253604474
fax-no:       +351 253612954
nic-hdl:      AS215
mnt-by:       AS1930-MNT
source:       RIPE #Filtered

person:       Jose Antonio Ramada
address:      Servico de Comunicacoes
address:      Universidade do Minho
```

**FIG. 8:** Excerto da lista de informações obtida com a ferramenta

No primeiro campo da lista está o intervalo de endereços IP relativos à informação obtida e, no segundo, o domínio. Por exemplo, para a pessoa Alexandre Santos, encontra-se disponível a sua morada, número de telefone e *fax*. Seguindo o *link* **AS215**, é possível obter mais informação (**FIG. 9**), como, por exemplo, o endereço de e-mail.

```

person:      Alexandre Santos
address:     Universidade do Minho
address:     Departamento de Informatica
address:     P-4710-057 Braga
address:     Portugal
phone:       +351 253604474
fax-no:      +351 253612954
e-mail:      alex@di.uminho.pt
nic-hdl:     AS215
mnt-by:      AS1930-MNT
changed:     alex@uminho.pt 19920512
changed:     ip-adm@ce.fccn.pt 19930704
changed:     ipadm@rccn.net 19991130
changed:     ipadm@fccn.pt 20000208
changed:     ipadm@fccn.pt 20000209
changed:     ipadm@fccn.pt 20000210
changed:     ipadm@fccn.pt 20000211
changed:     ipadm@fccn.pt 20050621
source:      RIPE

```

FIG. 9: Informação mostrada seguindo o *link* **AS215** da Fig. 4.

## QUESTÃO 4

A identificação dos parâmetros temporais associados ao domínio *gcom.di.uminho.pt* passa por executar o seguinte comando:

**11.** *dig gcom.di.uminho.pt SOA*

Na secção de resposta, é possível identificar os parâmetros referidos, neste caso específico '2012010901 86400 7200 604800 86400'. Decompondo o *output*, é possível isolar o seu significado individual [2]:

- **2012010901:** Número de série, composto, por defeito, pela data inversa da última modificação– 9 de Janeiro de 2012 – e por um inteiro que especifica a versão de alteração dentro desse mesmo dia. Este parâmetro é, então, incrementado de cada vez que o ficheiro é alterado, comunicando aos servidores secundários que houve uma modificação e que estes devem actualizar a informação;
- **86400:** Parâmetro temporal de *refresh*, que veicula a frequência com que os servidores secundários devem inquirir o servidor primário de forma a aferir se o número de série sofreu qualquer incrementação e se necessitam, consequentemente, de efectuar uma actualização;
- **7200:** Parâmetro temporal de *retry*, que indica quanto tempo um servidor secundário deve aguardar antes de poder voltar a inquirir o servidor primário relativamente ao número de série, caso a primeira tentativa tenha falhado. Este parâmetro nunca deve ser superior ao valor indicado para o *refresh*;
- **604800:** Parâmetro temporal de *expire*, que diz respeito ao período de tempo durante o qual os servidores secundários podem utilizar os dados actualmente disponíveis, caso não se vejam impedidos de verificar se os dados necessitam de ser actualizados

(por exemplo, devido a uma desconexão prolongada do servidor primário). Este parâmetro nunca deve ser inferior ao valor indicado para o *refresh* nem superior a 1 ano;

- **86400:** *Minimum TTL*, que determina o tempo durante o qual um recurso é considerado válido, sendo fornecido nas respostas aos inquirimentos de forma a informar os servidores secundários acerca do tempo que devem manter os dados em *cache*.

Os parâmetros temporais podem, assim, ser agrupados (**Tabela 2**), de forma a clarificar o caso específico do domínio *gcom.di.uminho.pt*.

**TABELA 2:** Parâmetros temporais associados ao domínio *gcom-di.uminho.pt*

| PARÂMETROS      | PERÍODO                                   |
|-----------------|-------------------------------------------|
| NÚMERO DE SÉRIE | Actualizado pela última vez em 09/01/2012 |
| REFRESH         | 24 horas                                  |
| RETRY           | 2 horas                                   |
| EXPIRE          | 1 semana                                  |
| MINIMUM TTL     | 24 horas                                  |



## BIBLIOGRAFIA

[1] *DNS Configuration Types*. Zytrax. Disponível em: <<http://www.zytrax.com/books/dns/ch4/#master>>.

[2] *Record Types and Parameters*. DNS-Master. Disponível em: <[http://www.dns-master.ru/help/en/help.html#p8\\_2](http://www.dns-master.ru/help/en/help.html#p8_2)>.