**TP2 – PL19**

**Tiago Matos Guedes**

**Eduardo Manuel Sousa Pereira**

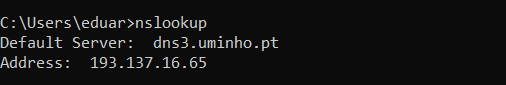
Questões e respostas

Nível aplicacional

1. **Aceda à página http://www.scom.uminho.pt e espere que o conteúdo seja carregado. Pare a captura. Para localizar mais facilmente o tráfego correspondente ao acesso web realizado, comece por filtrar pelo protocolo dns. Para tal, introduza dns na caixa do display filter e aplique o filtro. Localize a resolução do nome www.scom.uminho.pt. Identifique o endereço IP da estação que formulou a query e o tipo de query realizada.**
2. **Identifique a trama com resposta à query formulada. Identifique também o servidor de nomes que deu a resposta, através do seu IP e nome.**
3. **Limpe o filtro anteriormente estabelecido e filtre agora pelos protocolos http // tcp.**
4. **Tente identificar as tramas correspondentes ao estabelecimento da ligação entre o cliente e o servidor HTTP.**
5. **Com base na sequência de dados trocados entre cliente e servidor explique se o servidor HTTP está a funcionar em modo de conexão persistente ou não persistente.**
6. **Limpe o filtro anteriormente estabelecido e filtre agora pelo protocolo http.**
7. **Coloque o wireshark a capturar tráfego e faça hard refresh da página indicada anteriormente. Depois volte a aceder à mesma página mas sem fazer hard refresh. Pare a captura de tráfego. Identifique a principal diferença observada no tráfego HTTP entre carregar a referida página com e sem hard refresh. Quais os campos do cabeçalho HTTP envolvidos nesta ação? Qual a principal vantagem e desvantagem inerente ao hard refresh?**
8. **Aceda a https://alunos.uminho.pt, ao mesmo tempo que captura o tráfego desse acesso com o wireshark. Porque razão o tráfego HTTP não é identificado como tal?**

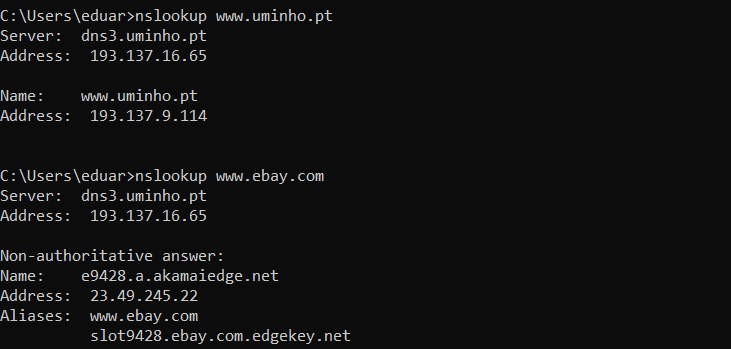
**Consultas ao serviço de resolução de nomes DNS**

1. **Abra uma janela de comandos e execute nslookup. Para que serve a informação apresentada?**

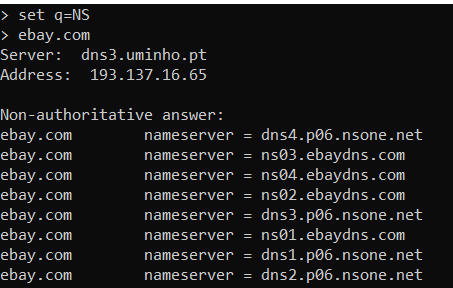


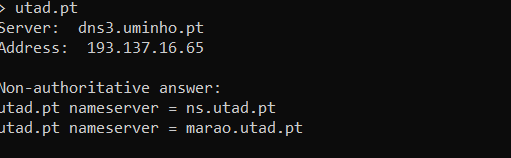
A informação serve para informar o servidor que se vai trabalhar com este IP.

1. **Usando os registos do tipo A, identifique os endereços IPv4 dos servidores ww.uminho.pt e www.ebay.com.**



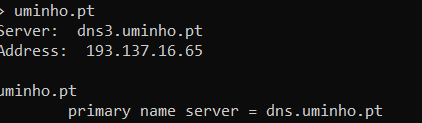
1. **Usando os registos NS, identifique os servidores de nomes definidos para os domínios: “ebay.com”, “utad.pt” e “.”.**





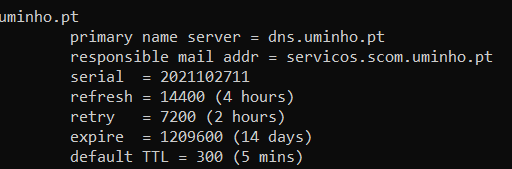


1. **Usando o registo SOA, identifique o servidor DNS primário definido para o domínio uminho.pt. Em que difere o servidor primário de um servidor secundário? Qual o significado dos parâmetros temporais associados ao servidor primário?**



Tanto o DNS primário como o DNS secundário contêm informação, incluindo IP’s, a identidade do administrador do domínio e informação de outros recursos.

A principal diferença entre eles, é que o DNS primário pode fazer alterações necessárias às informações contidas nos servidores DNS, enquanto que o DNS secundário, contém apenas cópias dos ficheiros, sendo que estas cópias são read-only. O DNS secundário só pode fazer pedidos ao DNS primário após este fazer as atualizações necessárias.



Serial: Número que se dá cada vez que o DNS primário faz alguma atualização. Como o número tem de aumentar a cada atualização, normalmente este número corresponde à data da atualização.

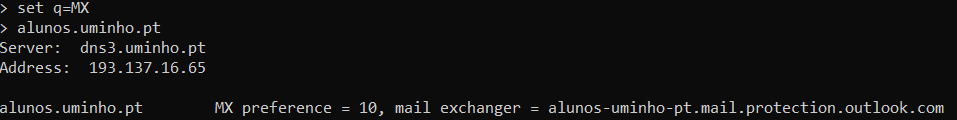
**Refresh**: Tempo que o DNS primário demora a informar o DNS secundário se tem alguma atualização (14400 - 4 horas)

**Retry**: Tempo que demora até tentar dar Refresh novamente, caso o DNS primário não retorne nenhuma resposta em 4 horas. (7200 - 2 horas)

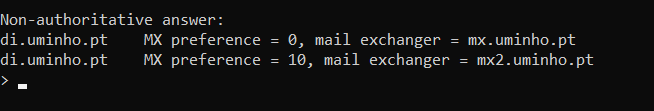
**Expire**: Tempo durante o qual o DNS secundário da Retry até determinar que não consegue comunicar com o DNS primário. Quando isto acontece o DNS secundário não dá resposta. (1209600 - 14 dias)

**Default TTL**: Tempo que o pacote pode permanecer na cache. Evita casos em que o pacote ficaria “perdido” na rede. (300 - 5 minutos)

1. **Usando os registos MX, diga quais os servidores de mail do domínio de mail alunos.uminho.pt. A que sistema são entregues preferencialmente as mensagens dirigidas a user@di.uminho.pt?**

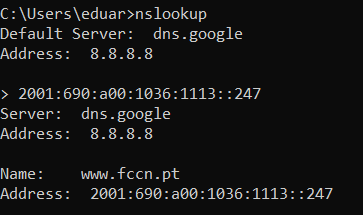


O servidor de mail do domínio de mail alunos.uminho.pt é alunos.uminho.pt.mail.protection@outlook.com.

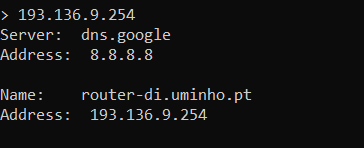


As mensagens dirigidas a user@di.uminho.pt são entregues preferencialmente a mx.uminho.pt.

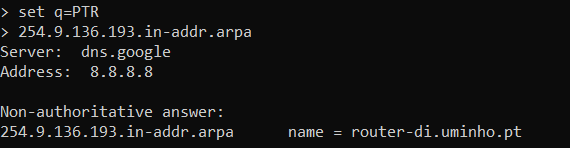
1. **Consegue interrogar o DNS sobre o endereço IPv6 2001:690:a00:1036:1113::247? E sobre o endereço IPv4 193.136.9.254? A que sistemas correspondem? Experimente fazer uma query aos registos PTR para o nome 254.9.136.193.in-addr.arpa. E comente o resultado obtido.**



Este IP corresponde ao www.fccn.pt.



Este IP corresponde ao router-di.uminho.pt.



Se fizermos nslookup do IP 193.136.9.254 dá o mesmo resultado de fazer uma query aos registos PTR de 254.9.136.193.in-addr.arpa.

Ao fazermos nslookup de um IP, o sistema sabe que tem de aceder aos registos PTR para dar a resposta, daí a resposta, fazendo de uma forma ou de outra, ser a mesma.

1. **Qual a diferença entre uma resposta adjetivada como *non-authorative answer* e uma *authorative answer* para uma determinada query?**

**Uso da camada de transportes por parte das aplicações**