TP3: Aplicações e Camada de Transporte

Ana Silva (a91678), Paulo Freitas (a100053) e Rúben Machado (a91656)

Questões e Respostas

1 Nível aplicacional

1) Identifique o endereço IP da estação que formulou a *query* DNS e o tipo de *query* realizada.

O endereço IP 172.26.42.81 (Fig.1 – vermelho) da estação formulou a *query* DNS, sendo do tipo A (Fig.1 – verde)

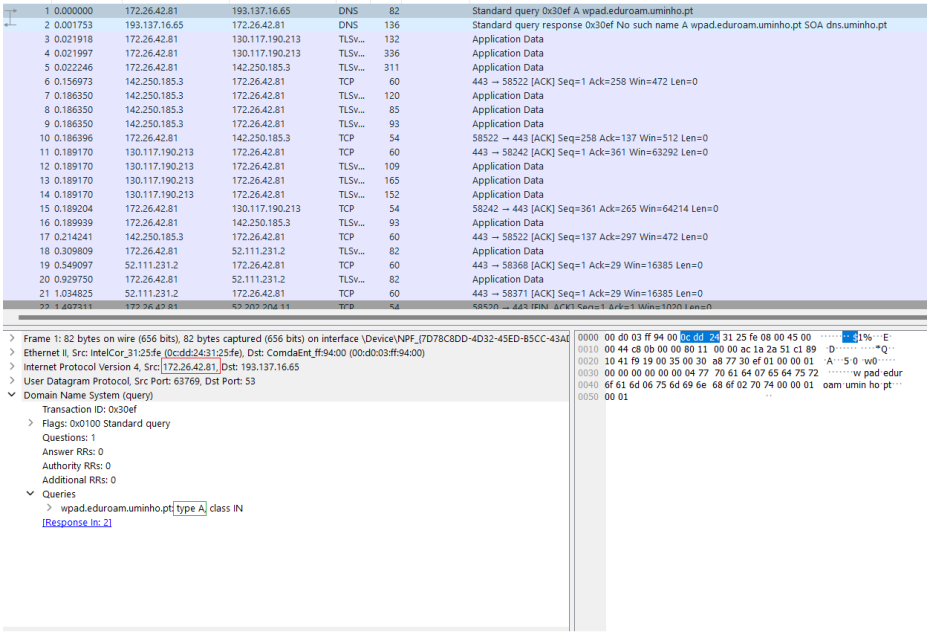

Fig. 1. Campo *Domain Name System* numa *query* DNS

2) Localize a trama com a resposta à *query* DNS formulada. Identifique nesta trama o endereço IP do servidor *web*. Identifique também o servidor de nomes que forneceu a resposta, através do seu IP e nome.

O endereço IP 172.26.42.81 (Fig.2 -vermelho) corresponde ao servidor *web*. O servidor dns3.uminho.pt (Fig.2 – verde) forneceu a resposta, com o endereço IP 193.137.16.65.

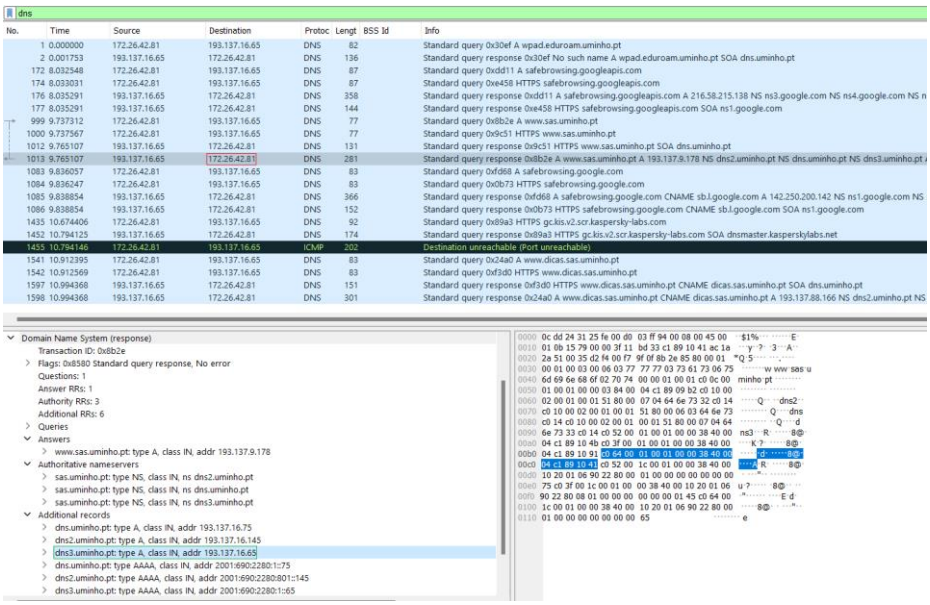

Fig. 2. Nome de servidores e os seus respetivos endereços IP

1.1 HTTP e TCP

3) Aplique o filtro aos protocolos *http // tcp*. Identifique os endereços IP do cliente e do servidor HTTP.

O endereço IP do cliente corresponde ao endereço IP de origem, enquanto o endereço IP do servidor HTTP corresponde ao endereço IP de destino, ou seja, os endereços 172.26.42.81 e 193.137.9.178, respetivamente (Fig. 3).

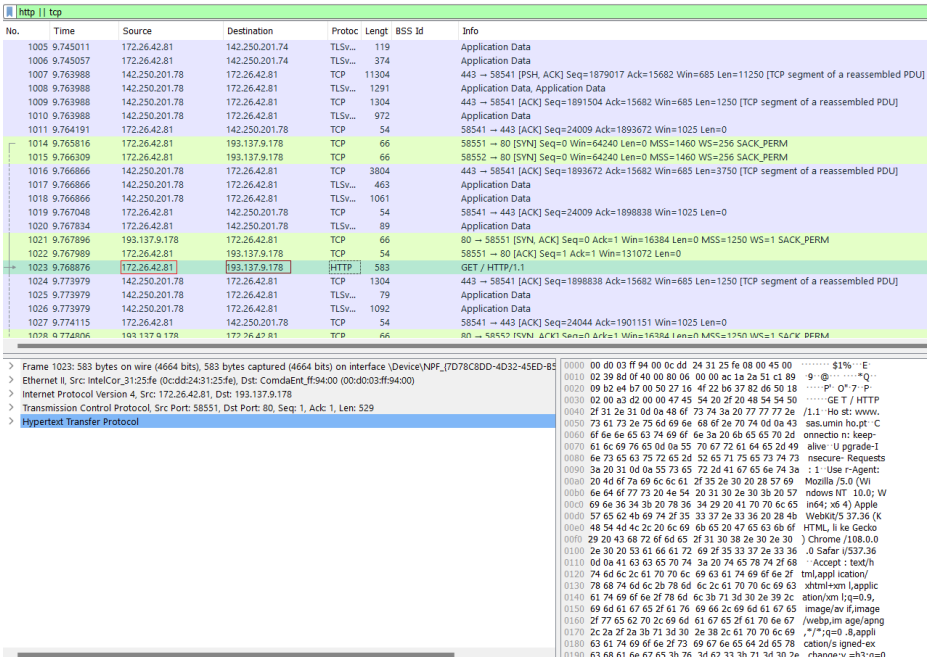

Fig. 3. Endereços IP do cliente e do servidor HTTP

4) Identifique os segmentos TCP correspondentes ao estabelecimento da ligação entre o cliente e o servidor HTTP. Qual o tamanho máximo de segmento (MSS) que o servidor aceita receber?

O tamanho máximo de segmento (MSS) corresponde a 1460 *bytes* a MTU, em que apresenta uma taxa de transmissão de 1500 *bytes* e, como o cabeçalho do TCP e IP apresentam 20 *bytes* cada. Logo, a subtração entre a MTU e os cabeçalhos corresponde a 1460 *bytes* (Fig.4).

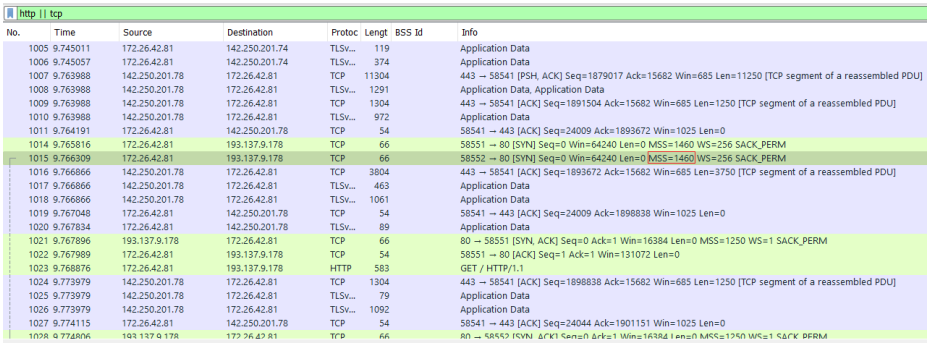

Fig. 4. MSS do TCP

5) Identifique a resposta HTTP do servidor respeitante ao primeiro pedido GET efetuado pelo cliente. Quantos *bytes* de dados aplicacionais contém essa resposta HTTP?

A resposta HTTP do servidor respeitante ao primeiro pedido GET apresenta com um tamanho de 924 *bytes* (Fig.5).

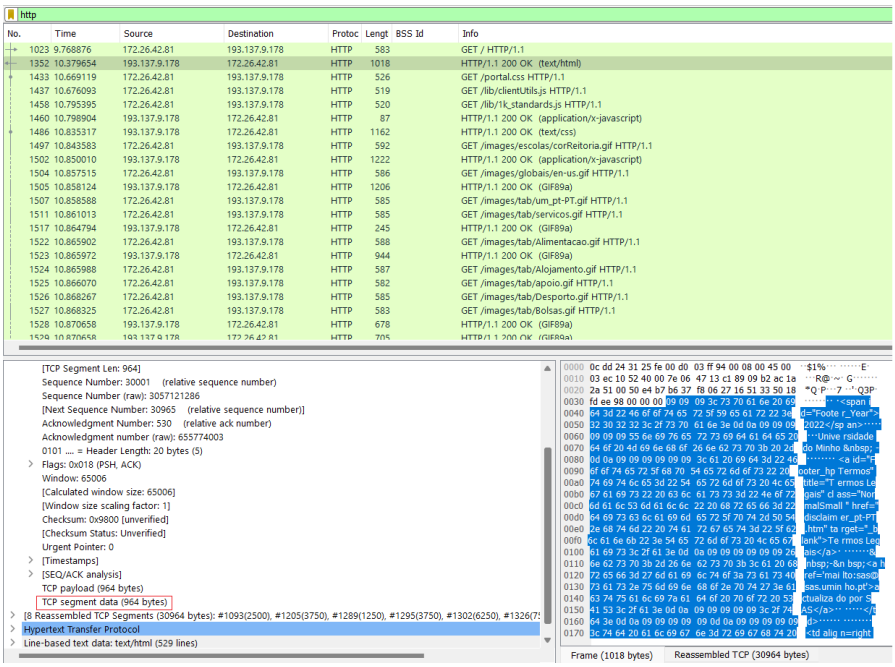

Fig. 5. Campo TCP da resposta HTTP ao pedido GET

6) A resposta HTTP identificada na alínea anterior foi transmitida em quantos segmentos TCP? Apresente também uma estimativa teórica para essa quantidade.

A resposta HTTP foi transmitida em 8 segmentos TCP (Fig.6). Teoricamente, sabendo que o MSS corresponde a 1460 *bytes* e o tamanho da resposta é de 30964 *bytes*. Logo, a divisão entre o tamanho total e o MSS corresponde a 22 segmentos TCP possíveis.

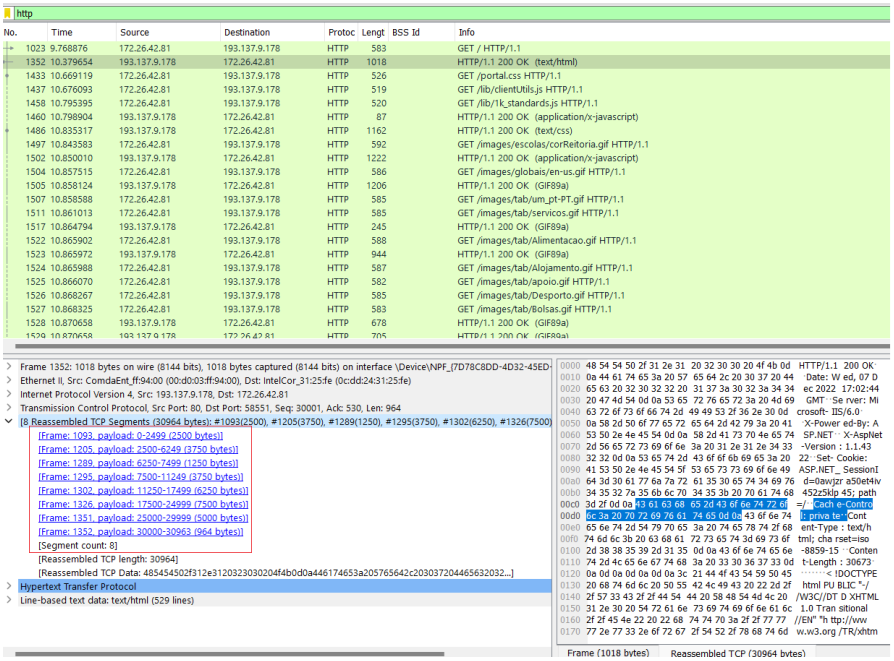

Fig. 6. Segmentos TCP de uma resposta HTTP

7) A partir da informação contida nos cabeçalhos dos protocolos IP e TCP, determine o número de *bytes* de dados enviados no primeiro e no último segmento TCP respeitantes à resposta HTTP.

O primeiro e último fragmento TCP respeitante à resposta HTTP foi 2500 *bytes* e 964 *bytes*, respetivamente (Fig.6).

8) Observe a informação apresentada no campo *host* do cabeçalho do pedido HTTP e diga qual o seu interesse? Experimente aceder à mesma página *web* através de *http://endereço_IP*, em que *endereço_IP* é o respeitante a *www.sas.uminho.pt* (identificado na alínea 2). Justifique o comportamento observado.

O campo *host* do cabeçalho do pedido HTTP permite identificar o *host* do destinatário, neste caso, corresponde ao *www.sas.uminho.pt* (Fig.7).
Contudo, quando se acede novamente à página, a quantidade de mensagens HTTP e significantemente menor, isto deve-se ao facto, da *cache* do *browser* que armazena essas mensagens, permitindo assim que as mensagens HTTP sejam num número reduzido.

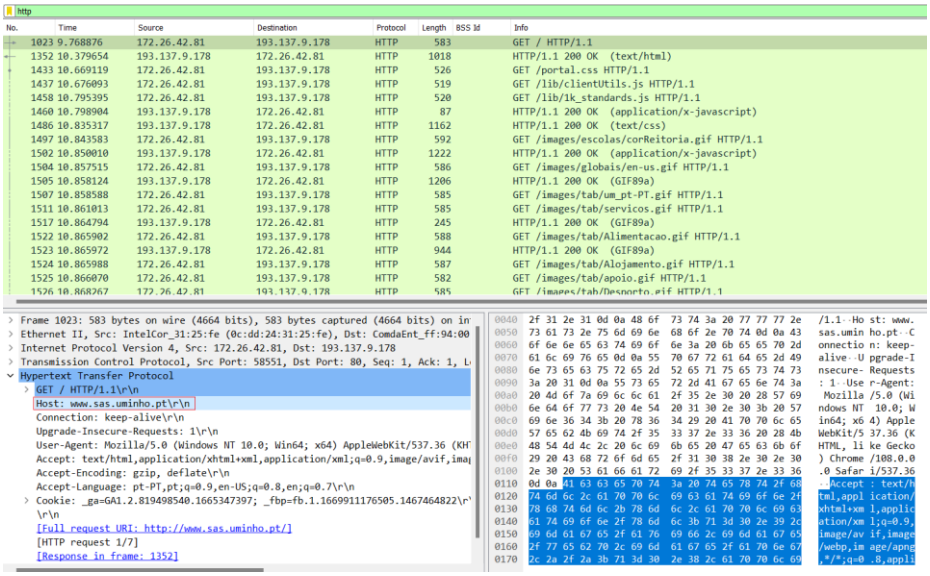

Fig. 7. *Host* do pedido HTTP

9) Com base na sequência de dados trocados entre o cliente e o servidor diga, justificando, se o servidor HTTP está a funcionar em modo de conexão persistente ou não persistente.

O servidor está a funcionar em modo de conexão persistente, visto que o HTTP utiliza por definição a conexão persistente, mas em paralelo (vários envios ao mesmo tempo). Isto é, a conexão TCP fica aberta e disponível para o envio de mensagens do servidor ou do cliente. As conexões são encerradas quando ao fim de um certo tempo não existe envio ou pedidos.

10) Aplique o filtro apenas ao protocolo *http*. O *hard refresh* permite limpar a cache do *browser* para uma determinada página, forçando o browser a carregar a última versão da página existente no servidor. Normalmente o *hard refresh* duma página faz-se com CTRL+F5 ou SHIFT+*page reload*. 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*. Qual é a principal vantagem e desvantagem inerente ao *hard refresh*.

O *hard refresh* vai limpar a *cache* do *browser*, e por isso, terá de realizar novamente todas as trocas de mensagens como fosse a primeira vez a aceder a página. (Fig.8)
De seguida, ao procurar a mesma página, a informação estará guardada na *cache* o que torna a troca de mensagens mínima (Fig.9)

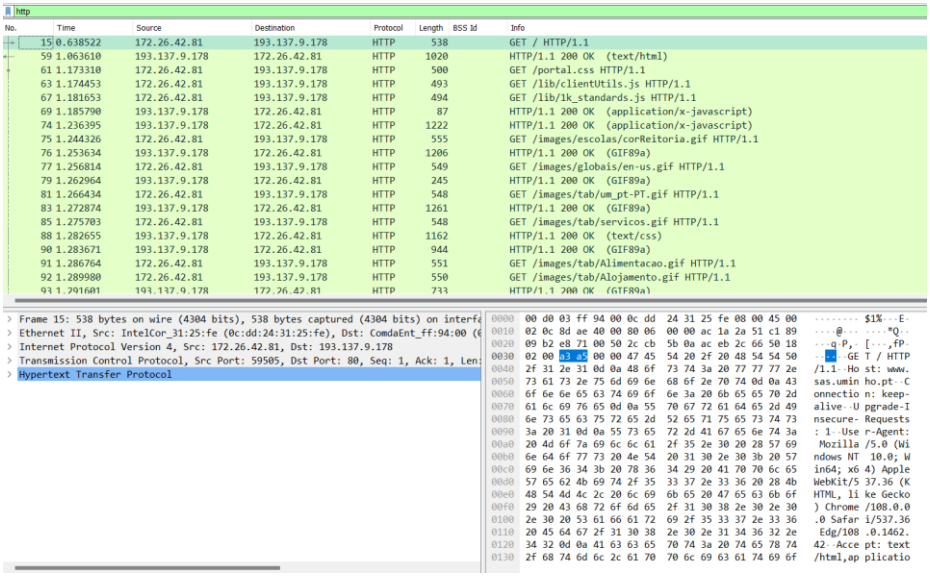

Fig. 8. Tráfego HTTP com *hard refresh*

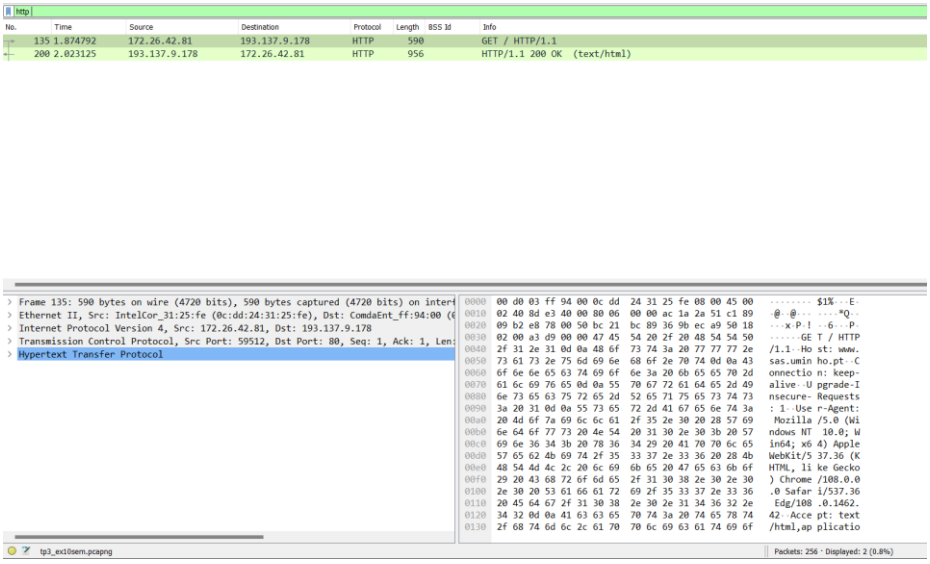

Fig. 9. Tráfego HTTP sem *hard refresh*

1.2 HTTPS

11) Aceda a *https://elearning.uminho.pt* , ao mesmo tempo que captura tráfego desse acesso com o *Wireshark*.

a) De que forma o seu *browser* assinala que o utilizador está perante, ou não, uma ligação HTTP ao servidor segura? Apresente uma captura de écran com essa indicação.

O *browser* assinala que o utilizador está perante uma ligação HTTP segura ao servidor através da imagem de um "cadeado fechado"(Fig.10).

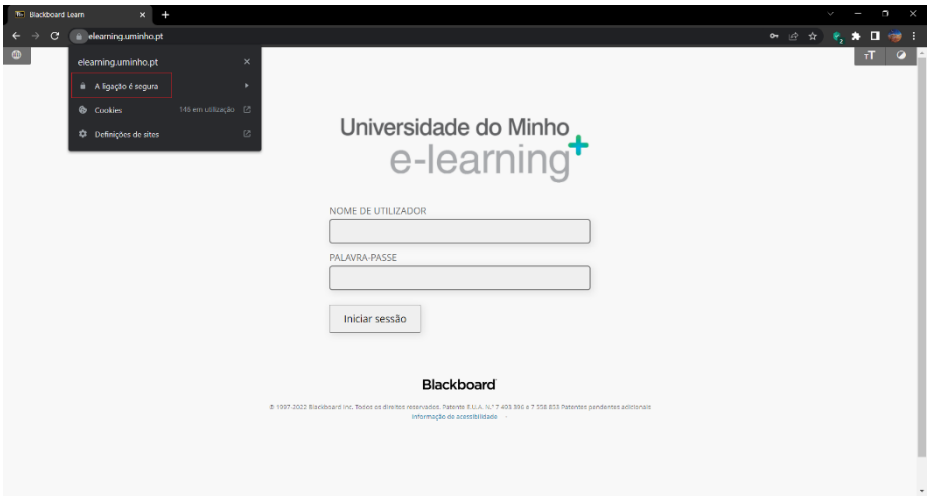

Fig. 10. Ligação segura

b) Porque razão o tráfego HTTP não é identificado como tal no *Wireshark*? Apesar disso, pode detetar-se qual o protocolo aplicacional. Como é que o *Wireshark* sabe que se trata duma ligação *http-over-tls*?

O tráfego HTTP não é identificado como tal no *Wireshark*, porque a informação encontra-se cifrada, tratando assim de uma ligação *http-over-tls*. Porém, através das portas de atendimento, consegue identificar se se trata de um canal seguro (443) ou não (80).

12) Diga, justificando, quais dos seguintes elementos uma comunicação HTTPS permite manter ocultos dum atacante: *i*) o endereço IP do cliente, *ii*) o endereço IP do servidor *web*, *iii*) o nome do servidor *web*, *iv*) o tamanho da mensagem trocada entre o cliente e o servidor, *v*) a identificação da página acedida no servidor *web*, *vi*) a frequência das conexões estabelecidas entre o cliente e o servidor, *vii*) os dados da aplicação trocados entre o servidor e o cliente.

Uma comunicação HTTPS para se manter oculta dum atacante necessita de conter a informação cifrada quando se utiliza um *sniffer*, ou seja, a informação oculta corresponde ao nome de servidor *web* e aos dados da aplicação trocados entre o servidor e o cliente.

2 Consultas ao serviço de resolução de nome DNS

1) Indique qual o servidor de nomes que a sua máquina está a usar?

O servidor de nomes que a máquina está a usar é *dns3.uminho.pt*.

2) Usando o registo do tipo A, identifique os endereços IPv4 dos servidores *www.sas.uminho.pt*, *marco.uminho.pt* e *www.google.com*? Usando o registo AAAA, identifique o endereço IPv6 do servidor *www.fccn.pt*.

Os servidores *www.sas.uminho.pt*, *marco.uminho.pt* e *www.google.com* têm como endereços IPv4: *193.137.9.178*, *193.136.9.240* e *172.217.168.164*, respetivamente. O servidor *www.fccn.pt* têm como endereço IPv6: *2001:690:a00:1036:1113:247*.

3) Experimente fazer uma *query* aos registos PTR para os nomes 240.9.136.193.in-addr.arpa. e 7.4.2.0.0.0.0.0.0.0.0.0.3.1.1.1.6.3.0.1.0.0.2.ip6.arpa. Comente os resultados face aos obtidos na alínea anterior.

Os nomes no enunciado correspondem a: *marco.uminho.pt* e *www.fcnn.pt*, respetivamente.
Estes nomes correspondem aos servidores de nomes, na alínea anterior.

4) Usando os registos NS, identifique os servidores de nomes definidos para os domínios:"uminho.com", "sas.uminho.pt", "pt." e "." (*root*).

Os nomes definidos para os domínios correspondem a :"uminho.com" os servidores de nome: *dns2.uminho.pt, dns3.uminho.pt, dns.uminho.pt, ns02.fcnn.pt;* "sas.uminho.pt" os servidores de nome: *dns.uminho.pt*, *dns2.uminho.pt* e *dns.uminho.pt*; "pt." Os servidores de nome: *ns2.nic.fr*, *b.dns.pt, ns.dns.br, d.dns.pt, g.dns.pt, c.dns.pt, h.dns.pt, e.dns.pt* e *a.dns.pt*; "." (*root*) os servidores de nomes: *d.root-servers.net, h.root-servers.net, k.root-servers.net, b.root-servers.net, g.root-servers.net, e.root-servers.net, l.root-servers.net, a.root-servers.net, m.root-servers.net, f.root-servers.net, c.root-servers.net, j.root-servers.net* e *i.root-servers.net*.

a) Perante a informação obtida, diga, justificando, se os servidores de nomes de diferentes domínios podem coexistir numa mesma máquina física.

Os servidores de nomes de diferentes domínios podem coexistir numa mesma máquina física, caso ambos possuem os mesmos servidores de nomes, neste caso, temos o *sas.uminho.pt* e o *uminho.pt*.

b) Encontra domínios geridos por servidores de nomes localizados em redes IP distintas? Se sim, apresente esses domínios e diga qual a vantagem resultante desse procedimento?

Os domínios *uminho.pt* e *sas.uminho.pt* apresentam IP iguais, ou seja, a mesma máquina pode gerir vários domínios, como também ser possível máquinas distintas gerir o mesmo domínio.

5) Usando o registo SOA, identifique o servidor DNS primário definido para os domínios "uminho.pt", "pt." e "."? Em que difere o servidor primário de um servidor secundário e qual o significado dos parâmetros temporais associados ao servidor primário?

O servidor DNS primário para os domínios "uminho.pt", "pt." e "." Correspondem a: *dns.uminho.pt, curiosity.dns.pt* e *a.root-servers.net*.
Os servidores primários contêm todos os registos de recursos relevantes e administram as consultas DNS para um domínio, no qual os tempos indicados correspondem ao tempo de execução diferentes tarefas, ou, seja, (recarregar) *refresh*, (tentar) *retry* e (expirar) *expire* ao fim de um determinado tempo. Por outro lado, os servidores secundários de DNS contêm cópias de arquivos de zona somente para leitura, o que significa que não podem ser modificados.

6) Usando o registo MX, diga qual(quais) o(s) servidor(es) de email do domínio *edu.ulisboa.pt*? A que sistema são entregues preferencialmente as mensagens dirigidas a *geral@edu.ulisboa.pt*?

Os servidores de email do domínio *edu.ulisboa.pt* são: *ASPMX.L.GOOGLE.COM*, *ASPM3.GOOGLEMAIL.COM*, *ALT2.ASPMX.L.GOOGLE.COM*, *ASPMX2.GOOGLEMAIL.COM* e *ALT1.ASPMX.L.GOOGLE.COM*.
As mensagens dirigidas a *geral@edu.ulisboa.pt* são entregues preferencialmente a *sistemas.reitoria.ulisboa.pt*.

7) Usando o registo CNAME, diga qual(quais) o(s) *aliases* do nome *www.ebay.com*? O que é que isso significa?

O nome dos *aliases de www.ebay.com* corresponde a *slot9428.ebay.com.edgekey.net* (*canonical name*).

8) Qual a diferença entre uma resposta adjetivada como *non-authoritative answer* ("não-autorativa") e uma resposta "autoritativa" para uma determinada *query*?

Uma resposta é autoritativa quando esta é gerada por um servidor de nomes em que recebe um pedido de resolução de endereços para um domínio numa zona em que este tem autoridade. Pelo mesmo raciocínio, uma resposta não autoritativa é obtida quando um servidor de nomes recebe um pedido referente a um domínio numa zona sobre a qual este não tem autoridade, ou seja, a resposta não pertence ao servidor primário ou secundário.

3 Uso da camada de transporte por parte das aplicações

1) Preencha a seguinte tabela com base nos resultados que obteve:

Comando/aplicação	Canal seguro?	Protocolo de transporte (se aplicável)	Porta de atendimento (se aplicável)
browser http://	Sim	TCP	80
browser https://	Sim	TCP	443
ftp	Sim	TCP	21
Ping	Não	Não aplicável	Não aplicável
Ssh	Sim	TCP	22
nslookup/dig	Não	UDP	53
Traceroute	Não	UDP	33434
telnet	Sim	TCP	23

2) Comente as principais diferenças entre os protocolos TCP e UDP. Relacione-as com as experiências realizadas onde observou os campos dos cabeçalhos respetivos e o *overhead* protocolar. Em particular, identifique os campos do TCP responsáveis pelo controlo de fluxo, ordenação e fiabilidade do protocolo.

O TCP (*Transmission Control Protocol*) é um protocolo de transporte fiável de dados ponto-a-ponto orientado por conexão, enquanto o UDP (*User Datagram Protocol*) é um protocolo de transporte ponto-a-ponto não fiável que não usa conexões. Contudo, o UDP apresenta uma maior velocidade do que TCP, sendo este último responsável pelo controlo de fluxo e congestionamento de erros.
Os diferentes campos do TCP são a porta Origem/Destino, número de sequência, número de ACK (*Acknowledgements*), o comprimento do cabeçalho, as *Flags* (que são indicações especificas que podem ser: ACK, PDH, RST, SYN, FIN, URG), a janela, a soma de controlo, e ainda o apontador de emergência, podendo ainda haver outas opcionais.
Destes campos, a janela é a responsável pelo controlo de fluxo, e é através deste campo que o software TCP indica a quantidade de dados que tem capacidade de receber.
A soma de controlo é usada para verificar a integridade/fiabilidade do cabeçalho e dos dados do segmento TCP.
O número de sequência e o número de ACK são usados para a ordenação dos octetos, visto que o número de ACK vai identificar a posição do último *byte* recebido e vai especificar o número do próximo *byte* que o recetor espera receber; enquanto o número de sequência vai identificar a posição, no fluxo de *bytes*, do segmento que foi enviado pelo transmissor, ou seja, refere-se ao fluxo de dados que vai na mesma direção do segmento.

4 Conclusão

Os temas abordados neste trabalho prático têm como finalidade a exposição de conhecimentos dos autores ao docente da Unidade Curricular. Apesar dos percalços durante o trabalho, não impediu a realização do mesmo. Os autores com recurso ao *Wireshark* proporcionou uma ajuda indispensável no estudo do *http*, assim como, nos protocolos de transporte, TCP e UDP, não esquecendo do serviço de resolução de nome DNS. No seu geral, o estudo contribui de forma pedagógica nos temas abordados, proporcionando grande interessante aos autores e elevando o grau de conhecimento dos mesmos.