Universidade do Minho

Licenciatura em Ciências da Computação

Sistemas de Comunicações e Redes

Ensaio Escrito

Aplicações e Camada de Transporte

Grupo 28

Davide Santos (A102938)

Edgar Araújo (A102946)

Pedro Augusto Camargo (A102504)

Novembro 2023

Contents

1 Nível aplicacional

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

```
14 10.033359221  172.26.57.176   193.137.16.65    DNS      78 Standard query 0x7b03 A www.scom.uminho.pt
15 10.033386202  172.26.57.176   193.137.16.65    DNS      78 Standard query 0xda1c AAAA www.scom.uminho.pt
16 10.057275198  193.137.16.65    172.26.57.176    DNS      94 Standard query response 0x7b03 A www.scom.uminho.pt A 193.137.9.174
17 10.057275910  193.137.16.65    172.26.57.176    DNS     106 Standard query response 0xda1c AAAA www.scom.uminho.pt AAAA 2001:690:2280:1::105
18 10.058089977  172.26.57.176   193.137.9.174    TCP      74 38734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1449595496 TSecr=0 WS=128
19 10.060328175  193.137.9.174   172.26.57.176    TCP      78 80 → 38734 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1250 WS=1 TSval=0 TSecr=0 SACK_PERM
```

O endereço IP da estação que formulou a query DNS: 172.26.57.176 (O meu computador) Foram enviadas 2 querys dns, uma do tipo A (endereço IPv4) e outra do tipo AAAA (endereço IPv6)

1.2 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

```
14 10.033359221  172.26.57.176   193.137.16.65    DNS      78 Standard query 0x7b03 A www.scom.uminho.pt
15 10.033386202  172.26.57.176   193.137.16.65    DNS      78 Standard query 0xda1c AAAA www.scom.uminho.pt
16 10.057275198  193.137.16.65    172.26.57.176    DNS      94 Standard query response 0x7b03 A www.scom.uminho.pt A 193.137.9.174
17 10.057275910  193.137.16.65    172.26.57.176    DNS     106 Standard query response 0xda1c AAAA www.scom.uminho.pt AAAA 2001:690:2280:1::105
18 10.058089977  172.26.57.176   193.137.9.174    TCP      74 38734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1449595496 TSecr=0 WS=128
19 10.060328175  193.137.9.174   172.26.57.176    TCP      78 80 → 38734 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1250 WS=1 TSval=0 TSecr=0 SACK_PERM
```

O endereço IP do servidor web que respondeu a query DNS: 193.137.16.65 De forma a identificar o servidor de nomes que forneceu a resposta, poderia ter sido usado o utilitario nslookup, como tambem o servico WEB https://whatismyipaddress.com/ip/<ip>, para o ip anterior:

Obtemos que o servidor DNS que forneceu a resposta, tem por hostname: dns3.uminho.pt

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

```
21 10.060450003  172.26.57.176   193.137.9.174    HTTP    439 GET / HTTP/1.1
22 10.120634426  193.137.9.174   172.26.57.176    TCP    2542 80 → 38734 [ACK] Seq=1 Ack=374 Win=65162 Len=2476 TSval=381818 TSecr=1449595498 [TCP
23 10.120710338  172.26.57.176   193.137.9.174    TCP      66 38734 → 80 [ACK] Seq=374 Ack=2477 Win=63360 Len=0 TSval=1449595558 TSecr=381818
24 10.124781915  193.137.9.174   172.26.57.176    TCP    3780 80 → 38734 [ACK] Seq=2477 Ack=374 Win=65162 Len=3714 TSval=381818 TSecr=1449595558 [
25 10.124795390  172.26.57.176   193.137.9.174    TCP      66 38734 → 80 [ACK] Seq=374 Ack=6191 Win=62336 Len=0 TSval=1449595562 TSecr=381818
```

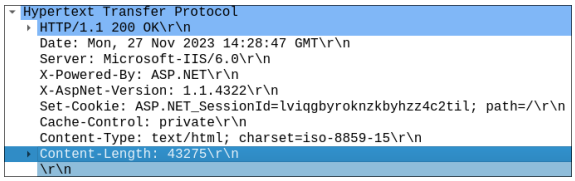
- Temos o endereco IP do cliente, vindo do HTTP GET Request: 172.26.57.176
- Que tem como destino o IP do servidor: 193.137.9.174

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

```
18 10.058089977  172.26.57.176   193.137.9.174    TCP      74 38734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1449595496 TSecr=0 WS=128
19 10.060328175  193.137.9.174   172.26.57.176    TCP      78 80 → 38734 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1250 WS=1 TSval=0 TSecr=0 SACK_PERM
20 10.060351849  172.26.57.176   193.137.9.174    TCP      66 38734 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1449595498 TSecr=0
21 10.060450003  172.26.57.176   193.137.9.174    HTTP    439 GET / HTTP/1.1
```

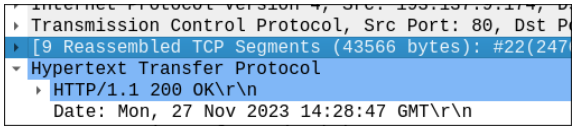
Tal como mostra a imagem, os pacotes 18 e 19 correspondem aos pactoes SYN do cliente e SYN-ACK do servidor, respetivamente. Logo ambos tem oportunidade nestes pacotes de solicitar um MSS, que no caso do servidor é de 1250 bytes.

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



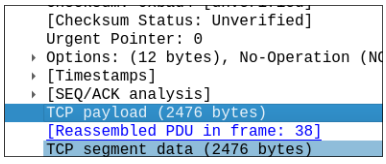
A resposta HTTP do servidor é do tipo 200 OK, e contem 43275 bytes de dados aplicacionais, tal como indica o campo Content-Length.

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

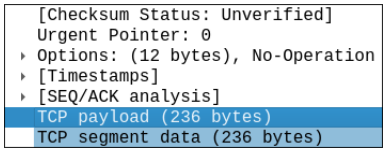


A resposta HTTP foi transmitida em 9 segmentos. A estimativa teórica para essa quantidade é de $43566/1460 = 29.8$, ou seja, 30 segmentos.

1.7 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.



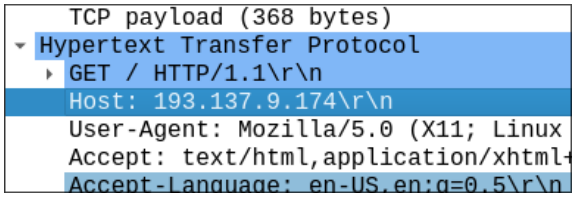
(a) Primeiro Segmento



(b) Último Segmento

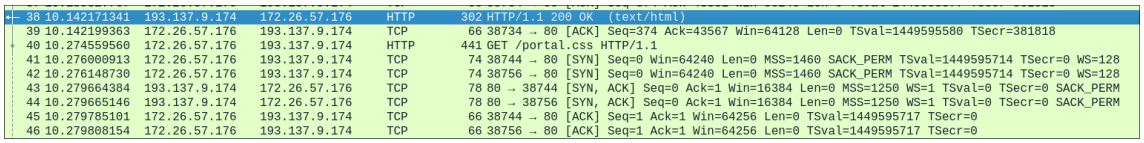
No primeiro segmento TCP, o número de bytes de dados enviados é de 2476 bytes. No último segmento TCP, o número de bytes de dados enviados é de 236 bytes.

1.8 Observe a informação apresentada no campo host do cabeçalho do pedido HTTP e diga qual o seu interesse?



O campo host do cabeçalho do pedido HTTP indica o nome colocado no url do browser, que serve para identificar o website que se pretende aceder, em caso de um servidor conter vários websites diferentes.

1.9 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.



38	10.142171341	193.137.9.174	172.26.57.176	HTTP	302	HTTP/1.1 200 OK (text/html)
39	10.142199363	172.26.57.176	193.137.9.174	TCP	66	38734 → 80 [ACK] Seq=374 Ack=43567 Win=64128 Len=0 TSval=1449595580 TSecr=381818
40	10.274559560	172.26.57.176	193.137.9.174	HTTP	441	GET /portal.css HTTP/1.1
41	10.276000913	172.26.57.176	193.137.9.174	TCP	74	38744 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1449595714 TSecr=0 WS=128
42	10.276148730	172.26.57.176	193.137.9.174	TCP	74	38756 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1449595714 TSecr=0 WS=128
43	10.279664384	193.137.9.174	172.26.57.176	TCP	78	80 → 38744 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1250 WS=1 TSval=0 TSecr=0 SACK_PERM
44	10.279665146	193.137.9.174	172.26.57.176	TCP	78	80 → 38756 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1250 WS=1 TSval=0 TSecr=0 SACK_PERM
45	10.279785101	172.26.57.176	193.137.9.174	TCP	66	38744 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1449595717 TSecr=0
46	10.279808154	172.26.57.176	193.137.9.174	TCP	66	38756 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1449595717 TSecr=0

O servidor HTTP está a funcionar em modo de conexão persistente, pois nenhum dos segmentos TCP tem a flag FIN ativa, entre GET Requests.

1.10 Aceda a https://www.uminho.pt, ao mesmo tempo que captura o tráfego desse acesso com o Wireshark. 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?

A razao pela qual o trafego HTTP nao é identificado como tal no Wireshark, é porque o trafego HTTP está a ser feito sobre o protocolo TLS, que é um protocolo de segurança que encripta o trafego HTTP, de forma a que este não seja visivel a terceiros. O Wireshark sabe que se trata de uma ligação http-over-tls, porque o protocolo TLS é identificado no campo Protocol do pacote.

1.11 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 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

- i) O endereço IP do cliente não é oculto, pois é necessário para que o servidor saiba para onde enviar a resposta.
- ii) O endereço IP do servidor web não é oculto, pois é necessário para que o cliente saiba para onde enviar o pedido.
- iii) O nome do servidor web não é oculto, pois é necessário para que o servidor saiba para que website enviar o pedido.
- iv) O tamanho da mensagem trocada entre o cliente e o servidor não é oculto, pois é necessário para que o cliente saiba se recebeu a mensagem completa.
- v) A identificação da página acedida no servidor web não é oculto. O caminho do URL é parte da solicitação HTTP e, embora a comunicação seja criptografada, a estrutura básica da solicitação permanece visível.
- vi) A frequência das conexões estabelecidas entre o cliente e o servidor não é oculto, pois é necessário para que o servidor saiba se o cliente está a tentar fazer um ataque de negação de serviço.
- vii) Os dados da aplicação trocados entre o servidor e o cliente SÃO ocultos, isso garante que o conteúdo da mensagem, incluindo informações sensíveis, não seja visível para um atacante que possa interceptar a comunicação.

2 Parte 2

2.1 Usando o registo MX

2.1.1 Quais são os servidores de email do domínio "tecnico.ulisboa.pt."?

Utilizando o comando dig MX tecnico.ulisboa.pt, obtemos os seguintes servidores de email:

- 51 smtp1.tecnico.ulisboa.pt.
- 10 smtp.tecnico.ulisboa.pt.
- 61 smtp2.tecnico.ulisboa.pt.

2.1.2 A que sistema são preferencialmente entregues as mensagens dirigidas a geral@tecnico.ulisboa.pt?

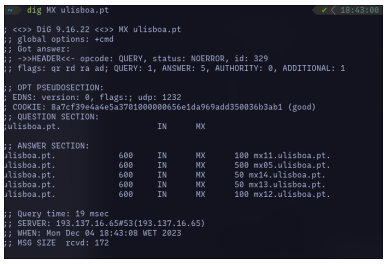
As mensagens sao preferencialmente entregues ao sistema de maior prioridade, isto e, os de menor numero a esquerda do nome do servidor de email, logo as mensagens seriam entregues ao servidor smtp.tecnico.ulisboa.pt, no caso deste estar indisponivel, a mensagem seria entao entregue ao seguintes, por ordem, smtp1.tecnico.ulisboa.pt e por fim smtp2.tecnico.ulisboa.pt.

2.2 A resposta obtida a uma query pode ser classificada como autoritativa ou não-autoritativa.

2.2.1 Qual a diferença fundamental entre ambos os tipos de resposta?

A diferença fundamental entre ambos os tipos de resposta é que uma resposta autoritativa é uma resposta que vem diretamente do servidor DNS que contém a informação sobre o domínio, enquanto que uma resposta não-autoritativa é uma resposta que vem de um servidor DNS que não contém a informação sobre o domínio, mas que obteve essa informação de um servidor DNS autoritativo. Logo enquanto a resposta nao autoritativa pode conter informação desatualizada, a resposta autoritativa contém sempre a informação mais atualizada.

2.2.2 Usando o seu default DNS server, que tipos de resposta obtém se efetuar queries aos registos MX para identificar os servidores de email dos domínios "ulisboa.pt." e "uminho.pt."? Experimente e justifique os tipos de respostas obtidos.



(a) ULisboa

(b) UMinho