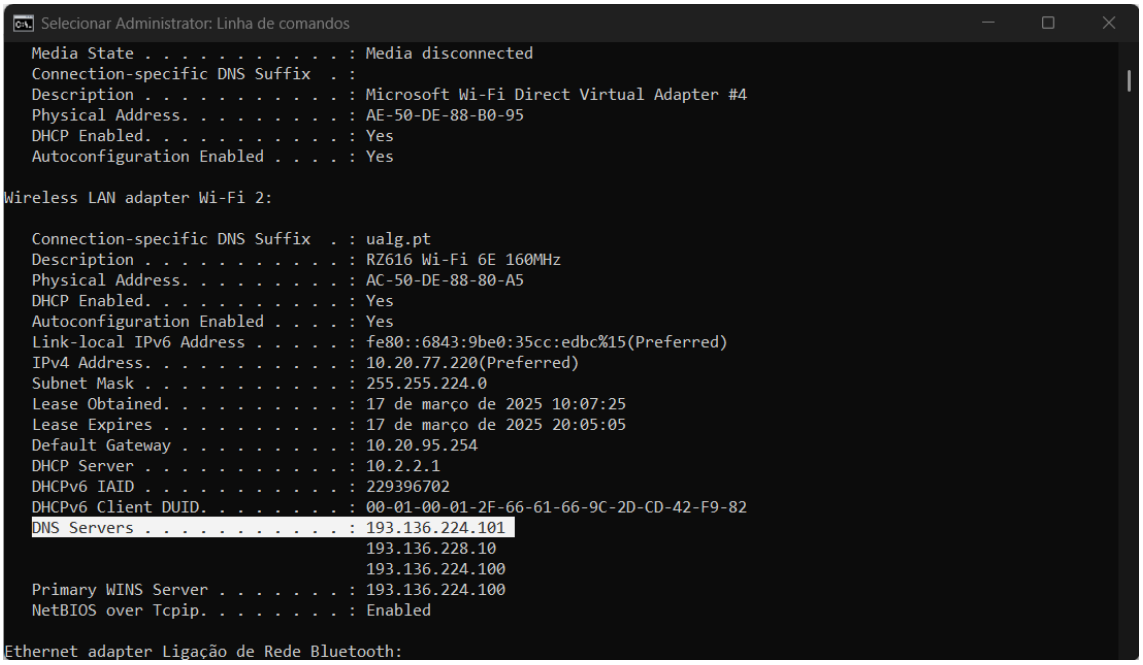
DNS

1

Default -> type A (especifica o IP do servidor e o endereço)

```
C:\Windows\System32>nslookup ua.pt
Server:  SI-SDC-02.ualg.pt
Address:  193.136.224.101

DNS request timed out.
    timeout was 2 seconds.
Name:    ua.pt
```



2

Domínio específico (servidor de nome -> name server NS)

```
C:\Windows\System32>nslookup -type=NS ua.pt
Server:  SI-SDC-02.ualg.pt
Address:  193.136.224.101

Non-authoritative answer:
ua.pt   nameserver = ns2.ua.pt
ua.pt   nameserver = ns.ua.pt

ns2.ua.pt       internet address = 193.136.172.19
ns.ua.pt        internet address = 193.136.172.18
```

Os últimos 2 referem-se ao authorized (quer dizer os ips que são autorizados a acessas a informação)

3

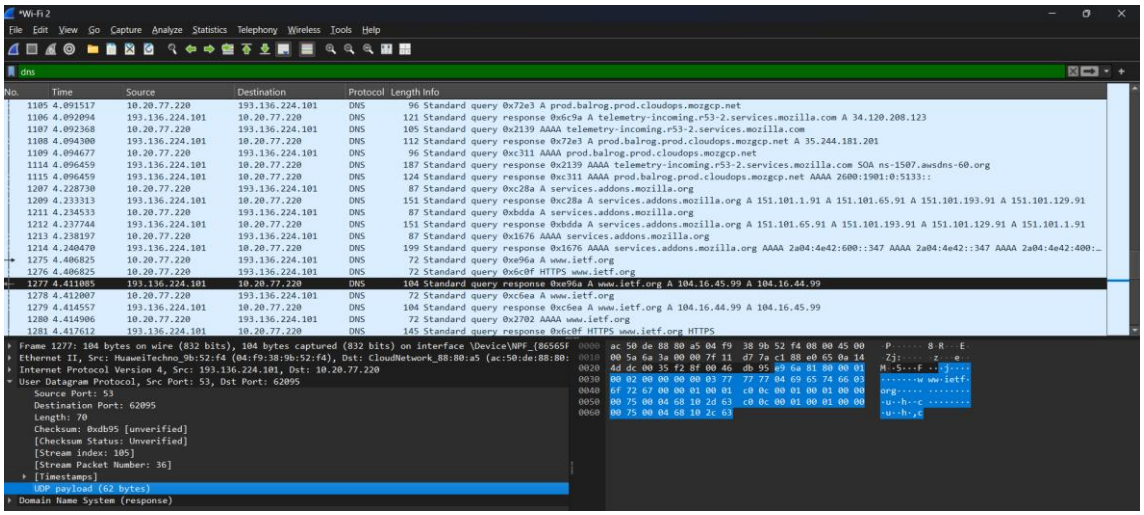
```
C:\Windows\System32>nslookup -type=MX ua.pt 193.136.224.100
Server:  SI-SDC-01.ualg.pt
Address:  193.136.224.100

Non-authoritative answer:
ua.pt   MX preference = 5, mail exchanger = mx4.ua.pt
ua.pt   MX preference = 5, mail exchanger = mx1.ua.pt

mx4.ua.pt       internet address = 193.136.173.27
mx1.ua.pt       internet address = 193.136.173.5
```

4

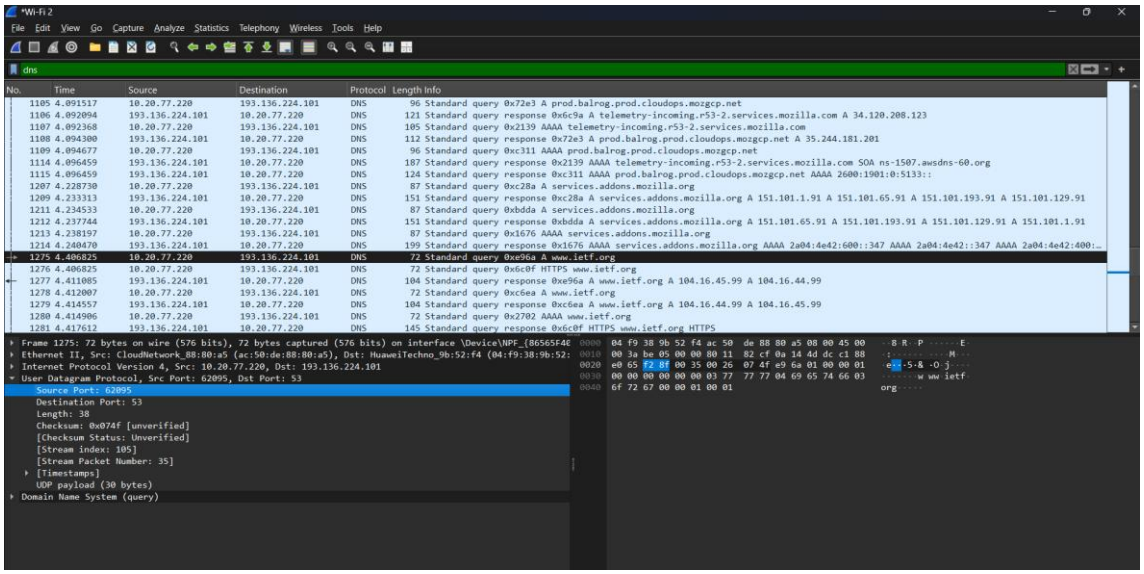
Trata-se de UDP, demonstrado em baixo



5

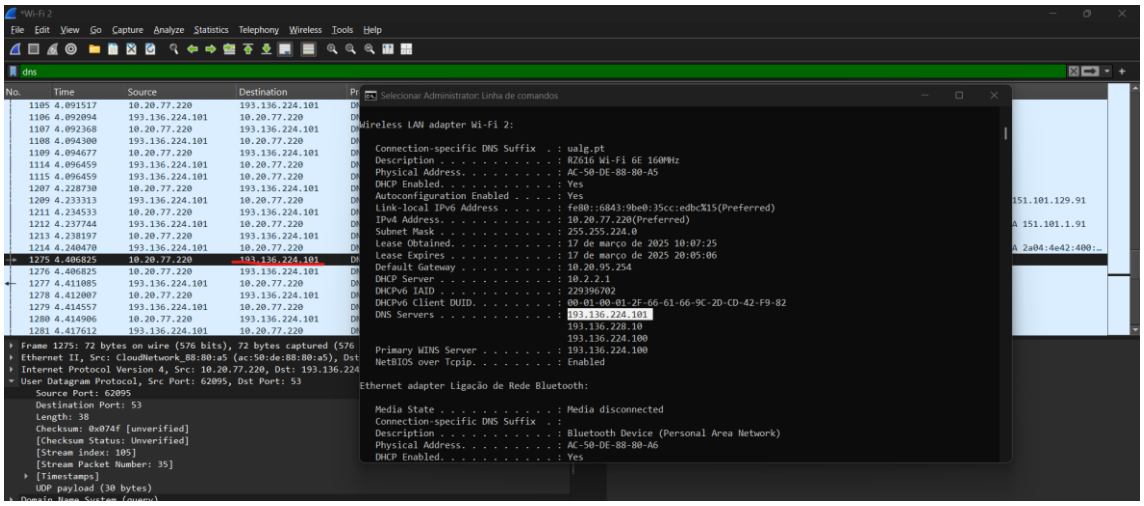
A porta de destino: 53

A porta de envio: 62095



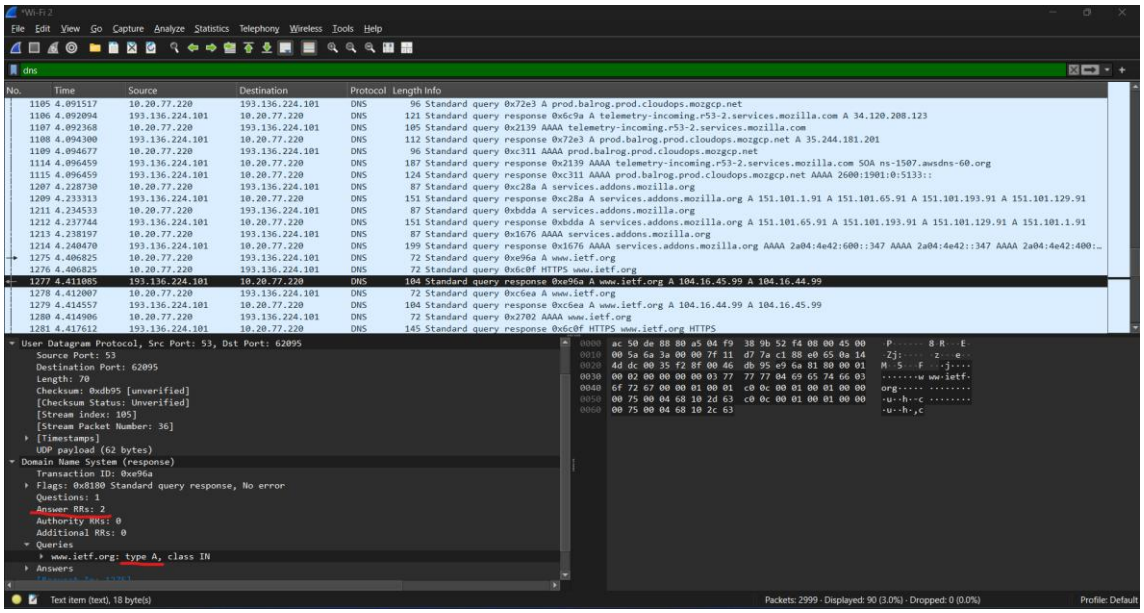
6

São iguais



7

O tipo de DNS query é o A, e contem respostas

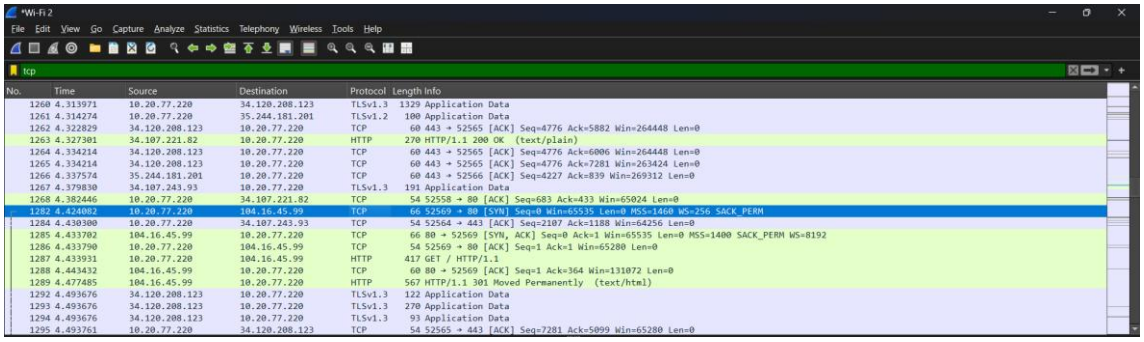


8

Obteve 2 respostas (VER IMAGEM ANTERIOR)

9

Fez hand shake com o IP 104.16.45.99



10

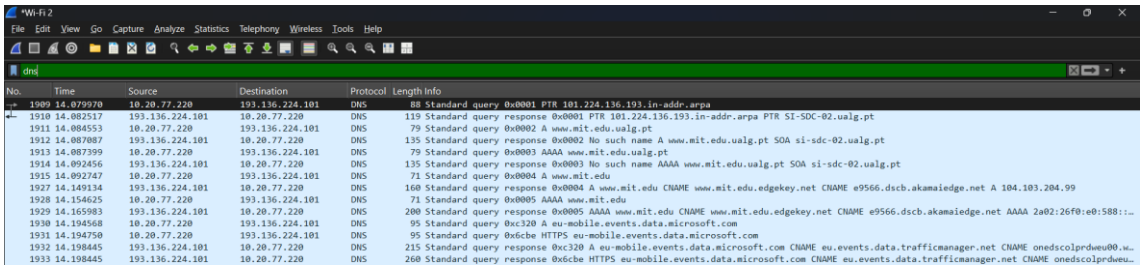
Pode desencadear DNS queries abc.person.com

11

Ambas as portas são 53

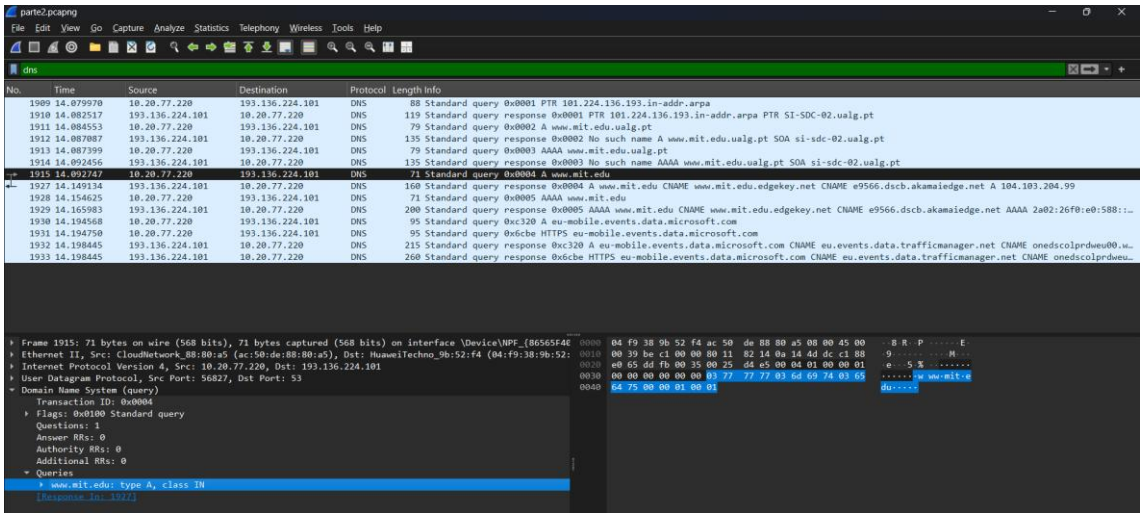
12

Vai para o nosso DNS: 193.136.224.101



13

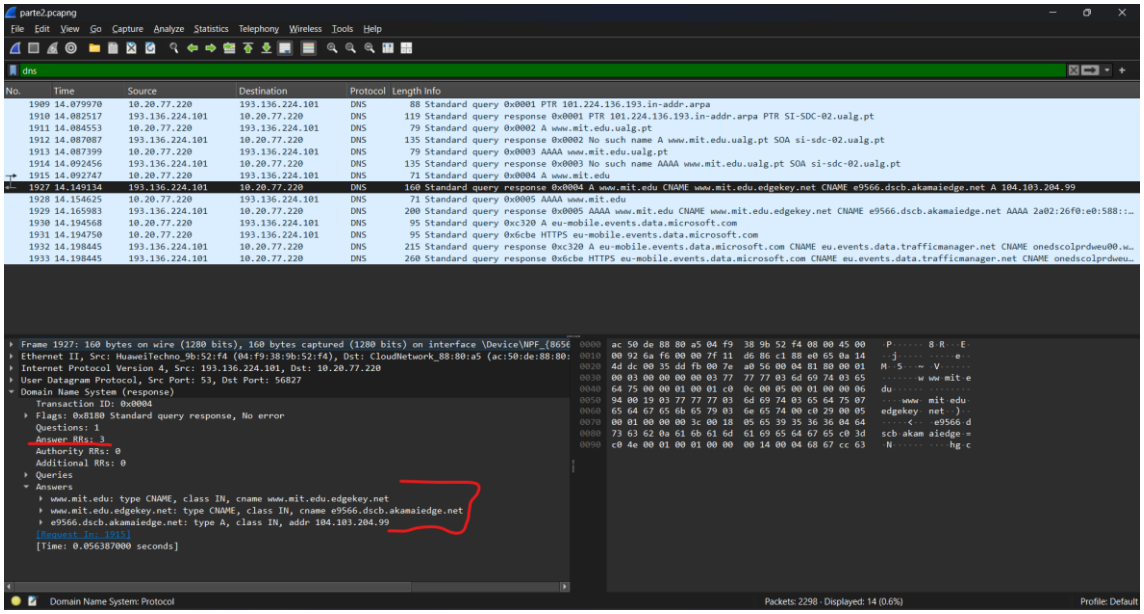
Type A, não contendo nenhuma resposta



14

Obteve 3 respostas

15

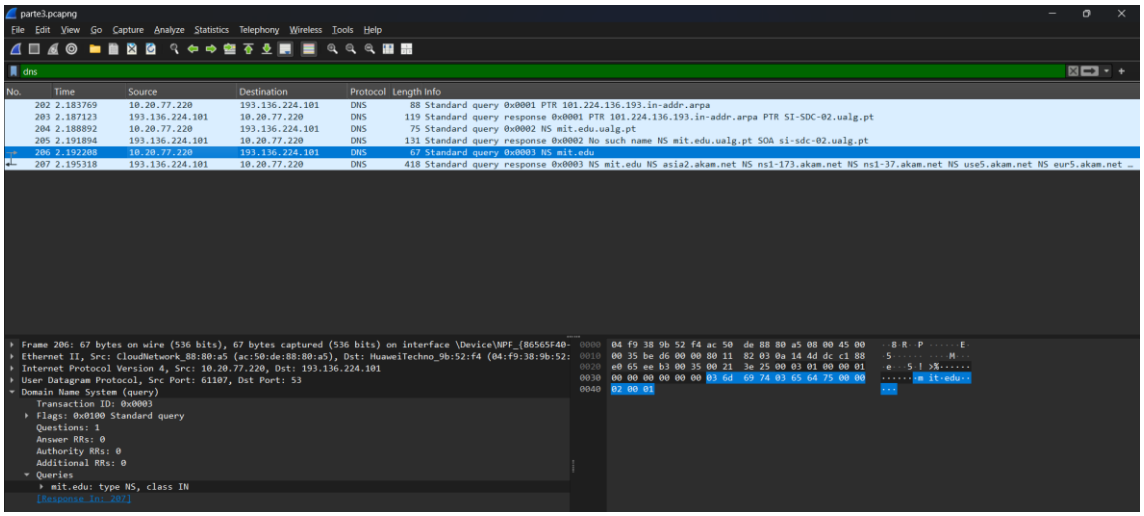


16

É o nosso default DNS server: 193.136.224.101

17

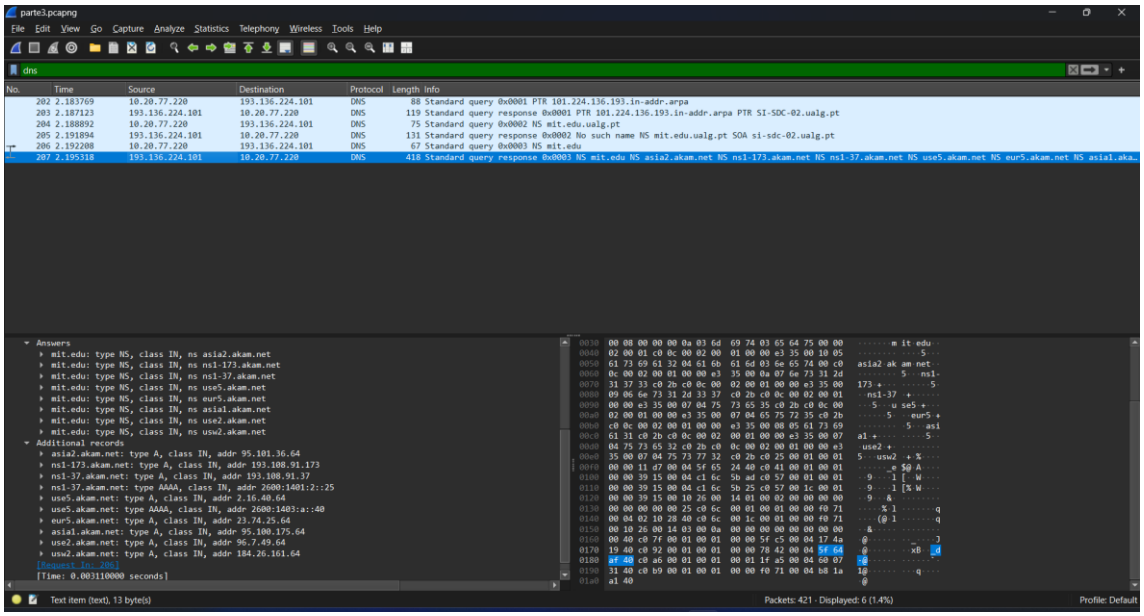
Type=NS



18

Existem vários nameservers e consequentemente vários ips associados (VER PRINT ABAIXO)

19



20

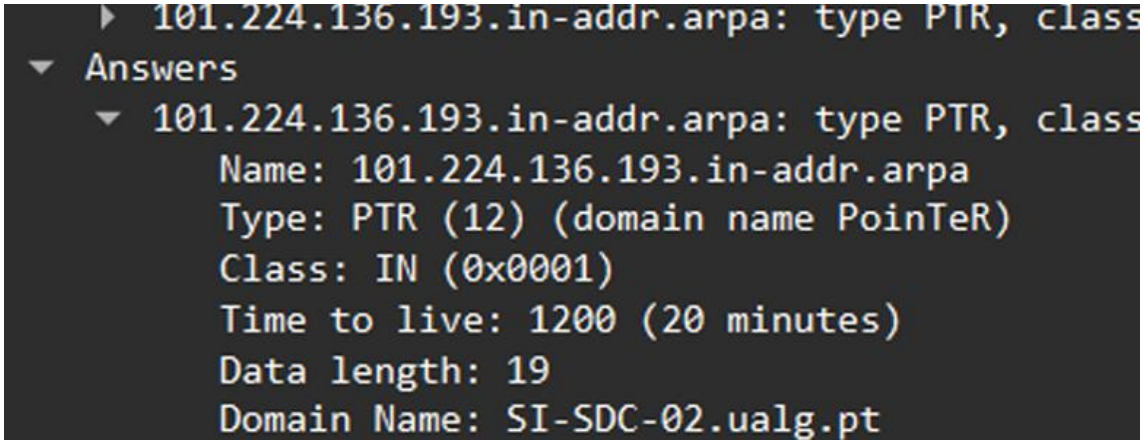
IP adress dest: 143.136.224.100

21

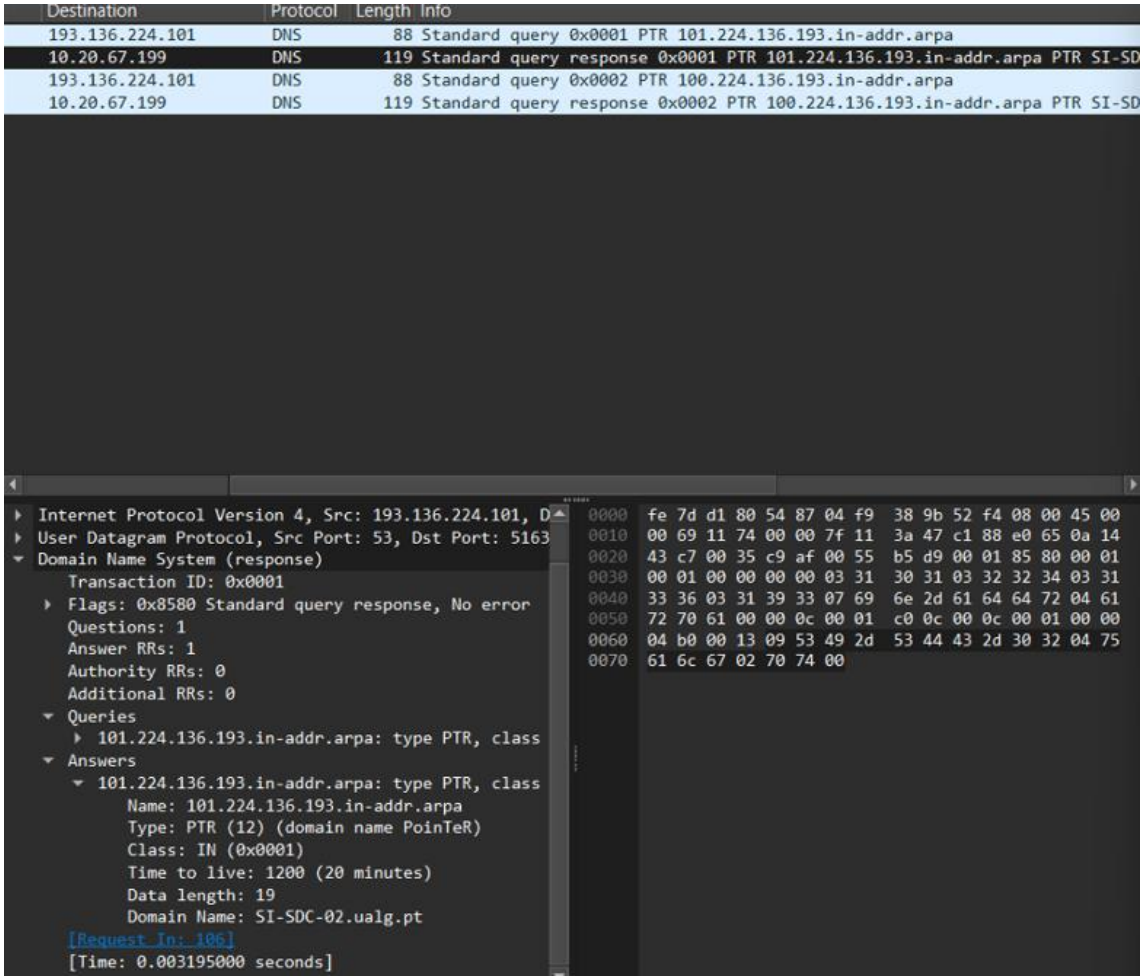
Type=A

22

12 respostas



23


Destination Protocol Length Info
193.136.224.101 DNS 88 Standard query 0x0001 PTR 101.224.136.193.in-addr.arpa
10.20.67.199 DNS 119 Standard query response 0x0001 PTR 101.224.136.193.in-addr.arpa PTR SI-SD
193.136.224.101 DNS 88 Standard query 0x0002 PTR 100.224.136.193.in-addr.arpa
10.20.67.199 DNS 119 Standard query response 0x0002 PTR 100.224.136.193.in-addr.arpa PTR SI-SD
Internet Protocol Version 4, Src: 193.136.224.101, D
User Datagram Protocol, Src Port: 53, Dst Port: 5163
Domain Name System (response)
Transaction ID: 0x0001
Flags: 0x8580 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
101.224.136.193.in-addr.arpa: type PTR, class
Answers
101.224.136.193.in-addr.arpa: type PTR, class
Name: 101.224.136.193.in-addr.arpa
Type: PTR (12) (domain name PoinTeR)
Class: IN (0x0001)
Time to live: 1200 (20 minutes)
Data length: 19
Domain Name: SI-SDC-02.ualg.pt
[Request In: 106]
[Time: 0.003195000 seconds]
0000 fe 7d d1 80 54 87 04 f9 38 9b 52 f4 08 00 45 00
0010 00 69 11 74 00 00 7f 11 3a 47 c1 88 e0 65 0a 14
0020 43 c7 00 35 c9 af 00 55 b5 d9 00 01 85 80 00 01
0030 00 01 00 00 00 00 03 31 30 31 03 32 32 34 03 31
0040 33 36 03 31 39 33 07 69 6e 2d 61 64 64 72 04 61
0050 72 70 61 00 00 0c 00 01 c0 0c 00 0c 00 01 00 00
0060 04 b0 00 13 09 53 49 2d 53 44 43 2d 30 32 04 75
0070 61 6c 67 02 70 74 00