

# 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
```

```
Selecionar Administrador: Linha de comandos

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Physical Address. . . . . : AE-50-DE-88-B0-95
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi 2:

Connection-specific DNS Suffix . : ualg.pt
Description . . . . . : RZ616 Wi-Fi 6E 160MHz
Physical Address. . . . . : AC-50-DE-88-80-A5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::6843:9be0:35cc:edbc%15(Preferred)
IPv4 Address. . . . . : 10.20.77.220(Preferred)
Subnet Mask . . . . . : 255.255.224.0
Lease Obtained. . . . . : 17 de março de 2025 10:07:25
Lease Expires . . . . . : 17 de março de 2025 20:05:05
Default Gateway . . . . . : 10.20.95.254
DHCP Server . . . . . : 10.2.2.1
DHCPv6 IAID . . . . . : 229396702
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-66-61-66-9C-2D-CD-42-F9-82
DNS Servers . . . . . : 193.136.224.101
                        193.136.228.10
                        193.136.224.100
Primary WINS Server . . . . . : 193.136.224.100
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ligação de Rede Bluetooth:
```

## 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 acessar a informação)

## 3

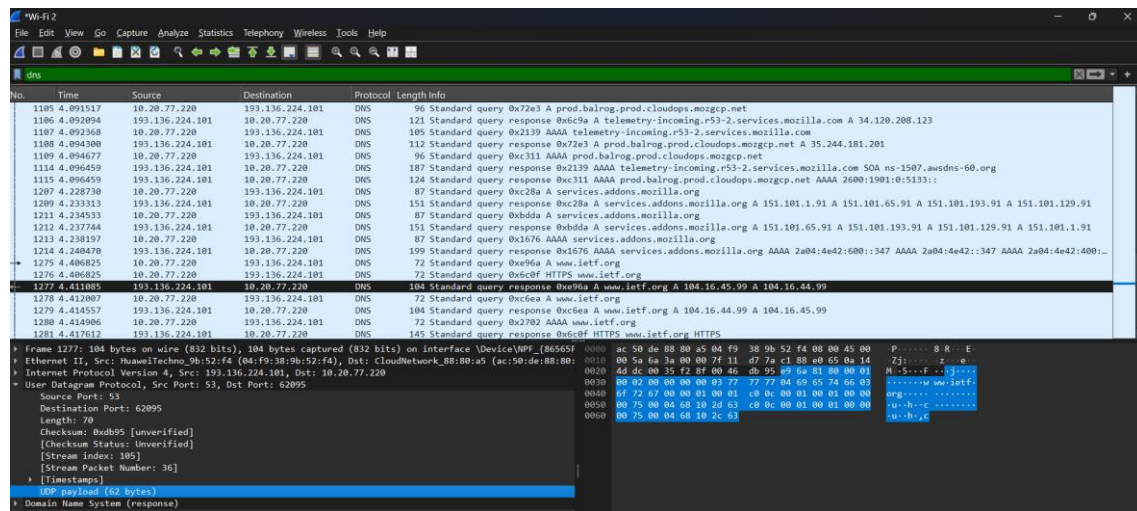
```
C:\Windows\System32>nslookup -type=MX ua.pt 193.136.224.100
Server:  SI-SDC-01.ualg.pt
Address:  193.136.224.100

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

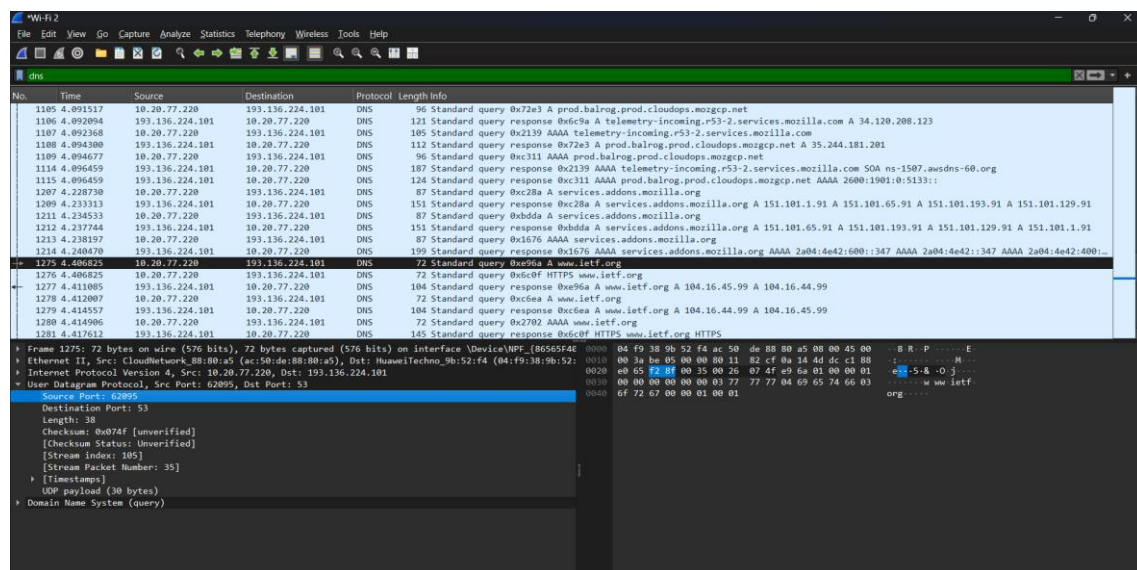
Trata-se de UDP, demonstrado em baixo



## 5

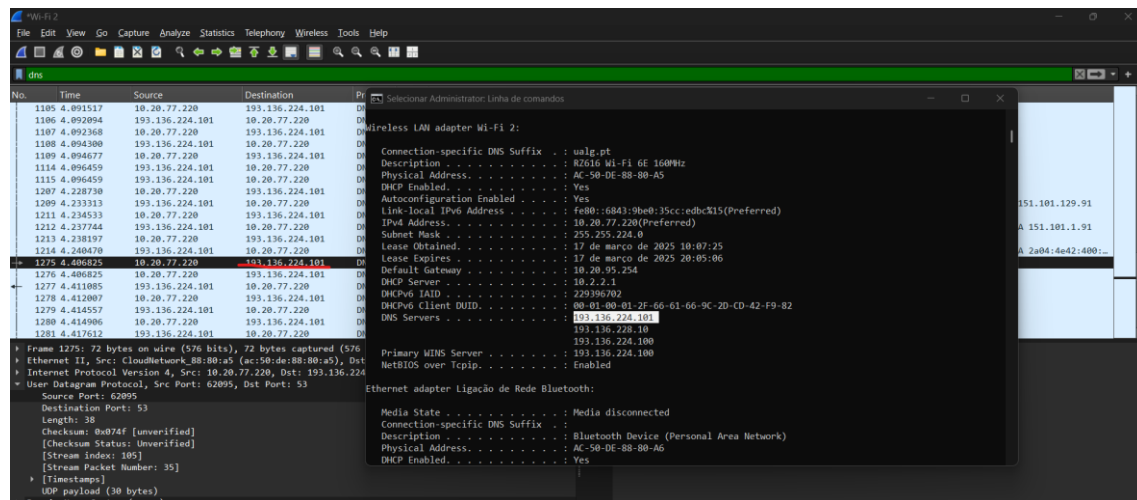
A porta de destino: 53

A porta de envio: 62095



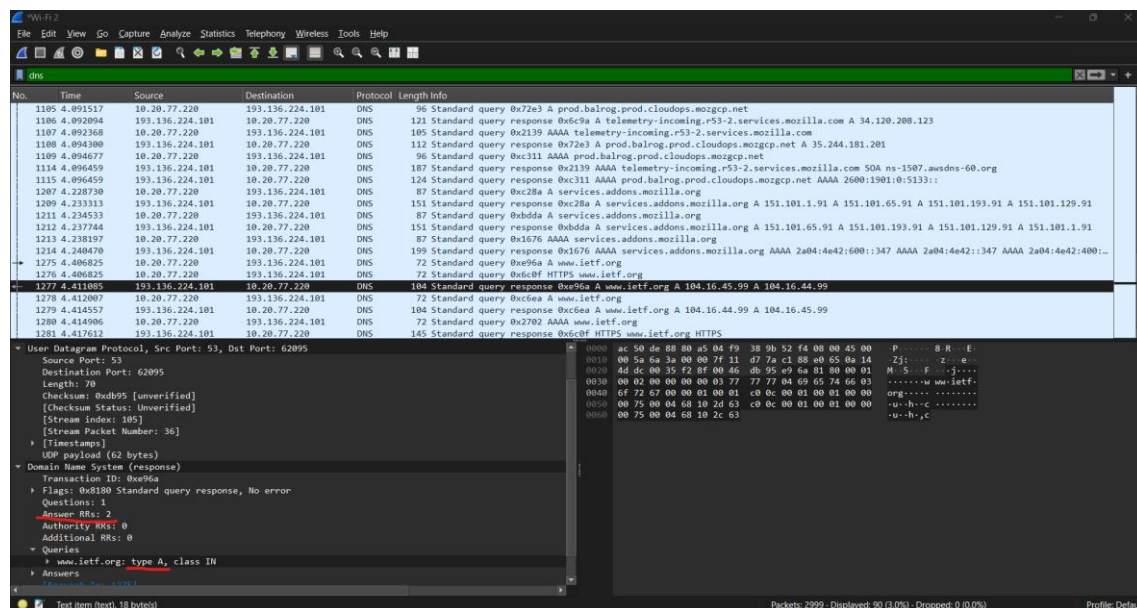
6

São iguais



7

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



8

Obteve 2 respostas (VER IMAGEM ANTERIOR)

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes:

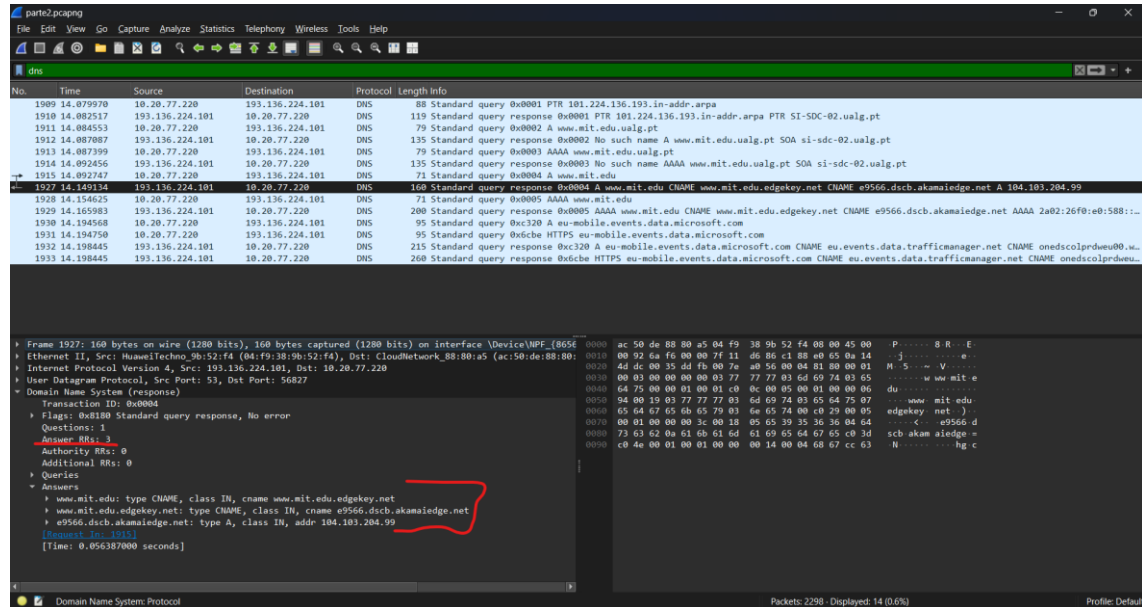
- Packet List Pane:** Shows a list of captured packets. The selected packet is #1915, a DNS Standard query response from 193.136.224.101 to 10.20.77.220. The list includes several other DNS queries and responses, some from MIT and some from Microsoft.
- Packet Details Pane:** Provides a hierarchical view of the selected packet's structure. It shows the DNS Standard query response format, including the Transaction ID (0x0004), Flags (0x0100), Questions (1), Answer RRs (0), Authority RRs (0), and Additional RRs (0). The selected item is the first question, which is a query for www.mit.edu.
- Packet Bytes Pane:** Displays the raw data of the selected packet in hexadecimal and ASCII. The data shows the DNS query structure, including the transaction ID, flags, and the query name.



14

Obteve 3 respostas

15

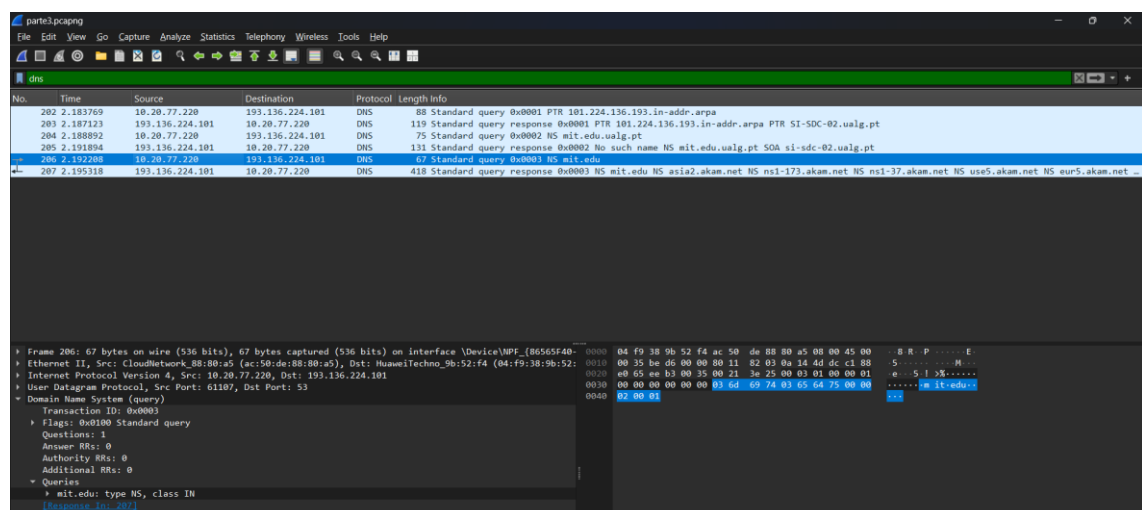


16

É o nosso default DNS server: 193.136.224.101

17

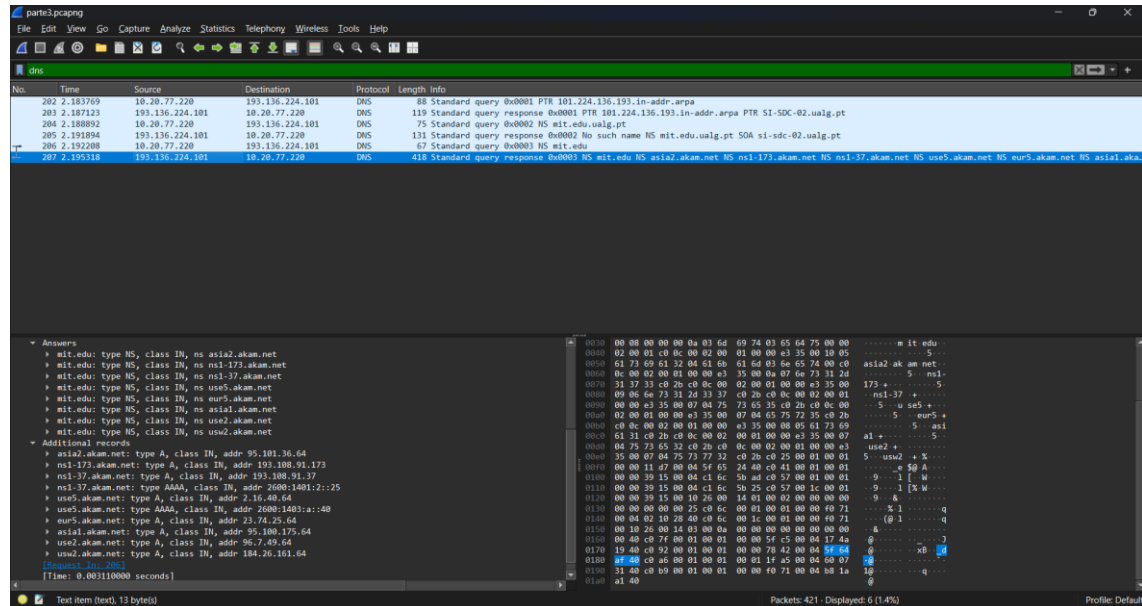
Type=NS



## 18

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

## 19



## 20

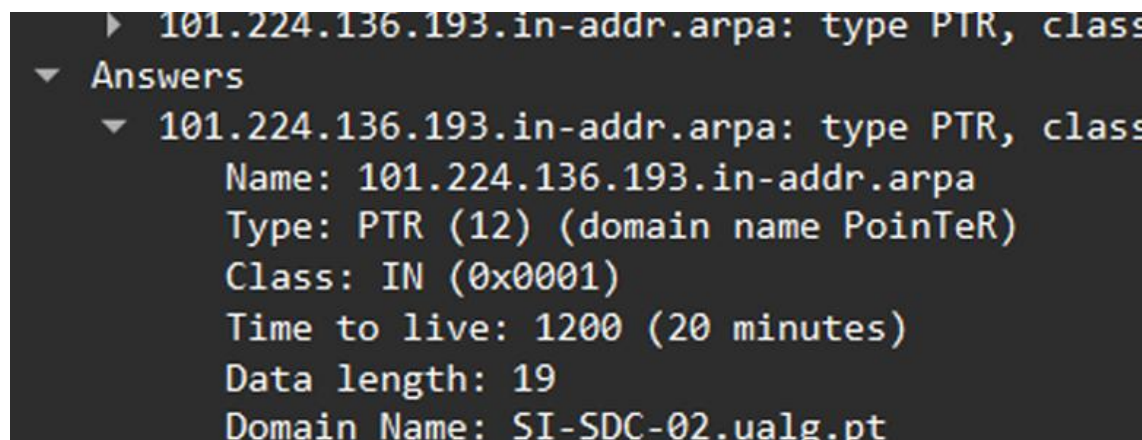
IP adress dest: 143.136.224.100

## 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, Dst: 10.20.67.199	0000	fe 7d d1 80 54 87 04 f9 38 9b 52 f4 08 00 45 00
User Datagram Protocol, Src Port: 53, Dst Port: 5163	0010	00 69 11 74 00 00 7f 11 3a 47 c1 88 e0 65 0a 14
Domain Name System (response)	0020	43 c7 00 35 c9 af 00 55 b5 d9 00 01 85 80 00 01
Transaction ID: 0x0001	0030	00 01 00 00 00 00 03 31 30 31 03 32 32 34 03 31
Flags: 0x8580 Standard query response, No error	0040	33 36 03 31 39 33 07 69 6e 2d 61 64 64 72 04 61
Questions: 1	0050	72 70 61 00 00 0c 00 01 c0 0c 00 0c 00 01 00 00
Answer RRs: 1	0060	04 b0 00 13 09 53 49 2d 53 44 43 2d 30 32 04 75
Authority RRs: 0	0070	61 6c 67 02 70 74 00
Additional RRs: 0		
Queries		
101.224.136.193.in-addr.arpa: type PTR, class IN		
Answers		
101.224.136.193.in-addr.arpa: type PTR, class IN		
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.uaig.pt		
[Request In: 106]		
[Time: 0.003195000 seconds]		