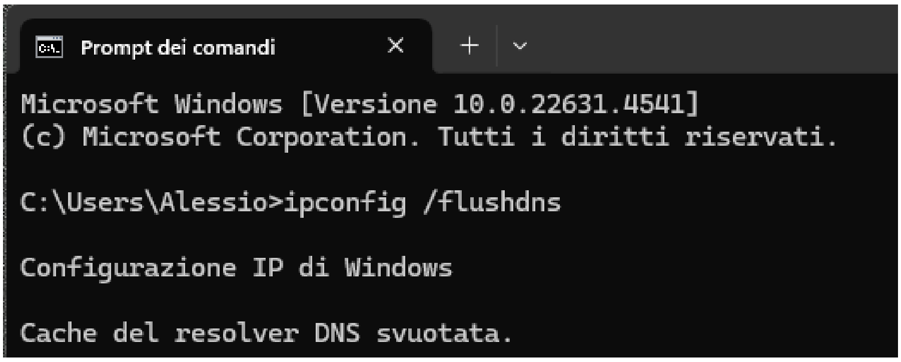
Esplorazione del Traffico DNS

- **Catturare il traffico DNS**
- **Esplorare il traffico delle query DNS**
- **Esplorare il traffico delle risposte DNS**

Capture DNS traffic

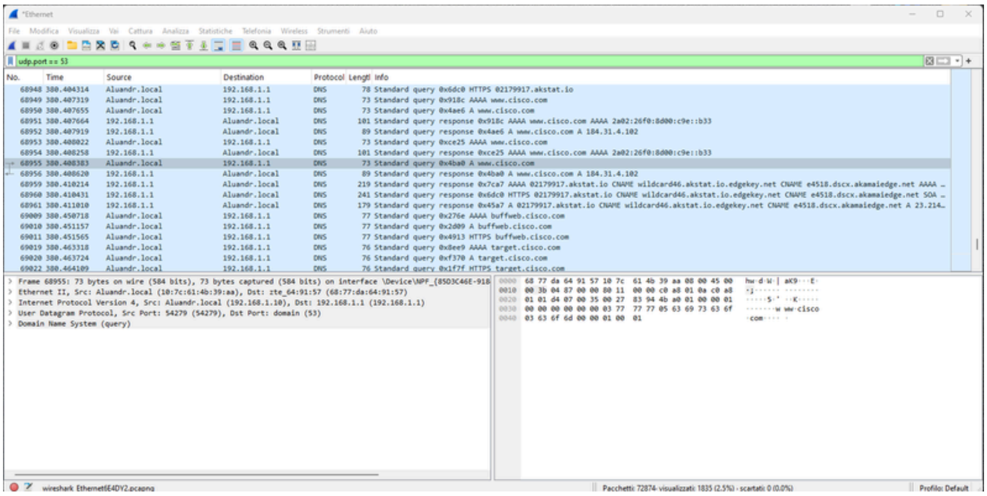
- In Windows, enter ipconfig /flushdns in Command Prompt.



```
Microsoft Windows [Versione 10.0.22631.4541]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\Alessio>ipconfig /flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.
```

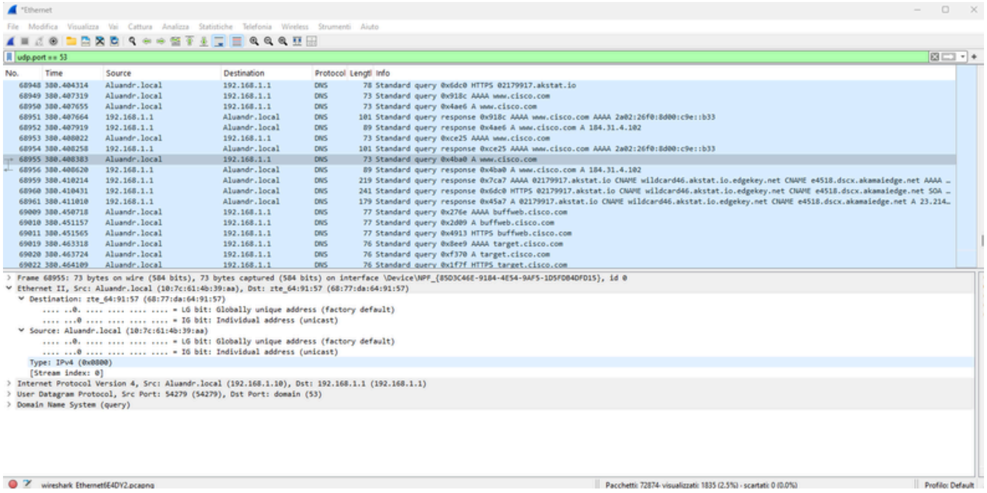
Esplorare il traffico delle query DNS

- Enter the domain name of a website. The domain name www.cisco.com
- Click Stop capturing packets to stop the Wireshark capture
- Observe the traffic captured in the Wireshark Packet List pane. Enter **udp.port == 53** in the filter box and click the arrow (or press enter) to display only DNS packets.



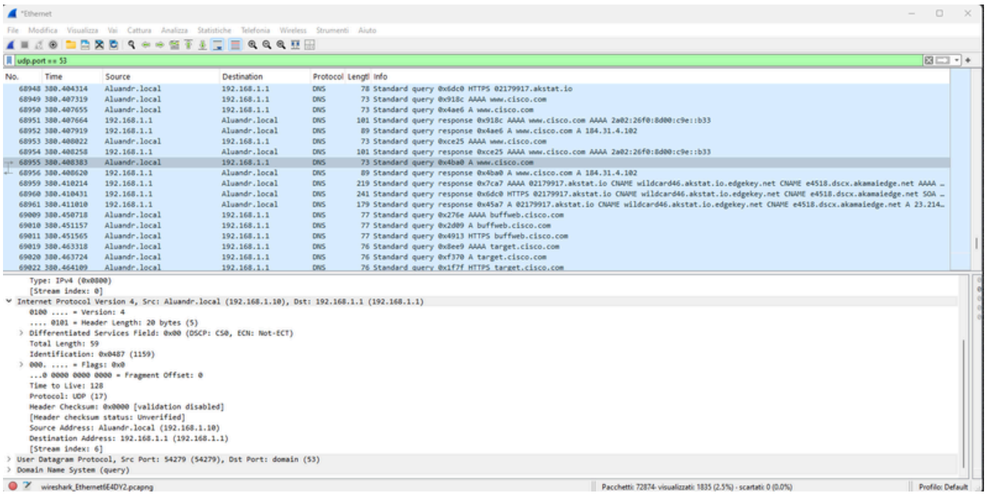
```
udp.port == 53

No.   Time       Source         Destination    Protocol Lengtl Info
68948 380.404314 Aluandr.local  192.168.1.1    DNS       78 Standard query 0x6dc0 HTTPS 02179917.akstat.io
68949 380.407319 Aluandr.local  192.168.1.1    DNS       73 Standard query 0x918c AAAA www.cisco.com
68950 380.407655 Aluandr.local  192.168.1.1    DNS       73 Standard query 0x4ae6 A www.cisco.com
68951 380.407664 192.168.1.1    Aluandr.local  DNS      101 Standard query response 0x918c AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68952 380.407919 192.168.1.1    Aluandr.local  DNS       89 Standard query response 0x4ae6 A www.cisco.com A 184.31.4.102
68953 380.408022 Aluandr.local  192.168.1.1    DNS       73 Standard query 0xce25 AAAA www.cisco.com
68954 380.408258 192.168.1.1    Aluandr.local  DNS      101 Standard query response 0xce25 AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68955 380.408383 Aluandr.local  192.168.1.1    DNS       73 Standard query 0x4ba0 A www.cisco.com
68956 380.408620 192.168.1.1    Aluandr.local  DNS       89 Standard query response 0x4ba0 A www.cisco.com A 184.31.4.102
68959 380.410214 192.168.1.1    Aluandr.local  DNS      219 Standard query response 0x7ca7 AAAA 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net AAAA …
68960 380.410431 192.168.1.1    Aluandr.local  DNS      241 Standard query response 0x6dc0 HTTPS 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net SOA …
68961 380.411010 192.168.1.1    Aluandr.local  DNS      179 Standard query response 0x45a7 A 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net A 23.214…
69009 380.450718 Aluandr.local  192.168.1.1    DNS       77 Standard query 0x276e AAAA buffweb.cisco.com
69010 380.451157 Aluandr.local  192.168.1.1    DNS       77 Standard query 0x2d09 A buffweb.cisco.com
69011 380.451565 Aluandr.local  192.168.1.1    DNS       77 Standard query 0x4913 HTTPS buffweb.cisco.com
69019 380.463318 Aluandr.local  192.168.1.1    DNS       76 Standard query 0x8ee9 AAAA target.cisco.com
69020 380.463724 Aluandr.local  192.168.1.1    DNS       76 Standard query 0xf370 A target.cisco.com
69022 380.464109 Aluandr.local  192.168.1.1    DNS       76 Standard query 0x1f7f HTTPS target.cisco.com

> Frame 68955: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{85D3C46E-918
> Ethernet II, Src: Aluandr.local (10:7c:61:4b:39:aa), Dst: zte_64:91:57 (68:77:da:64:91:57)
> Internet Protocol Version 4, Src: Aluandr.local (192.168.1.10), Dst: 192.168.1.1 (192.168.1.1)
> User Datagram Protocol, Src Port: 54279 (54279), Dst Port: domain (53)
> Domain Name System (query)

0000  68 77 da 64 91 57 10 7c  61 4b 39 aa 08 00 45 00   hw·d·W·| aK9···E·
0010  00 3b 04 87 00 00 80 11  00 00 c0 a8 01 0a c0 a8   ·;······ ········
0020  01 01 d4 07 00 35 00 27  83 94 4b a0 01 00 00 01   ·····5·' ··K·····
0030  00 00 00 00 00 00 03 77  77 77 05 63 69 73 63 6f   ·······w ww·cisco
0040  03 63 6f 6d 00 00 01 00  01                        ·com·····

wireshark_Ethernet6E4DY2.pcapng    Pacchetti: 72874 · visualizzati: 1835 (2.5%) · scartati: 0 (0.0%)    Profilo: Default
```

- Expand Ethernet II to view the details. Observe the source and destination fields.


*Ethernet
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto

```
udp.port == 53

No.   Time       Source          Destination     Protocol Lengtl Info
68948 380.404314 Aluandr.local   192.168.1.1     DNS       78 Standard query 0x6dc0 HTTPS 02179917.akstat.io
68949 380.407319 Aluandr.local   192.168.1.1     DNS       73 Standard query 0x918c AAAA www.cisco.com
68950 380.407655 Aluandr.local   192.168.1.1     DNS       73 Standard query 0x4ae6 A www.cisco.com
68951 380.407664 192.168.1.1     Aluandr.local   DNS      101 Standard query response 0x918c AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68952 380.407919 192.168.1.1     Aluandr.local   DNS       89 Standard query response 0x4ae6 A www.cisco.com A 184.31.4.102
68953 380.408022 Aluandr.local   192.168.1.1     DNS       73 Standard query 0xce25 AAAA www.cisco.com
68954 380.408258 192.168.1.1     Aluandr.local   DNS      101 Standard query response 0xce25 AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68955 380.408383 Aluandr.local   192.168.1.1     DNS       73 Standard query 0x4ba0 A www.cisco.com
68956 380.408620 192.168.1.1     Aluandr.local   DNS       89 Standard query response 0x4ba0 A www.cisco.com A 184.31.4.102
68959 380.410214 192.168.1.1     Aluandr.local   DNS      219 Standard query response 0x7ca7 AAAA 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net AAAA …
68960 380.410431 192.168.1.1     Aluandr.local   DNS      241 Standard query response 0x6dc0 HTTPS 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net SOA …
68961 380.411010 192.168.1.1     Aluandr.local   DNS      179 Standard query response 0x45a7 A 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net A 23.214…
69009 380.450718 Aluandr.local   192.168.1.1     DNS       77 Standard query 0x276e AAAA buffweb.cisco.com
69010 380.451157 Aluandr.local   192.168.1.1     DNS       77 Standard query 0x2d09 A buffweb.cisco.com
69011 380.451565 Aluandr.local   192.168.1.1     DNS       77 Standard query 0x4913 HTTPS buffweb.cisco.com
69019 380.463318 Aluandr.local   192.168.1.1     DNS       76 Standard query 0x8ee9 AAAA target.cisco.com
69020 380.463724 Aluandr.local   192.168.1.1     DNS       76 Standard query 0xf370 A target.cisco.com
69022 380.464109 Aluandr.local   192.168.1.1     DNS       76 Standard query 0x1f7f HTTPS target.cisco.com

> Frame 68955: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{85D3C46E-9184-4E54-9AF5-1D5FD84DFD15}, id 0
v Ethernet II, Src: Aluandr.local (10:7c:61:4b:39:aa), Dst: zte_64:91:57 (68:77:da:64:91:57)
  v Destination: zte_64:91:57 (68:77:da:64:91:57)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Aluandr.local (10:7c:61:4b:39:aa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: Aluandr.local (192.168.1.10), Dst: 192.168.1.1 (192.168.1.1)
> User Datagram Protocol, Src Port: 54279 (54279), Dst Port: domain (53)
> Domain Name System (query)

wireshark Ethernet6E4DY2.pcapng        Pacchetti: 72874· visualizzati: 1835 (2.5%) · scartati: 0 (0.0%)        Profilo: Default
```

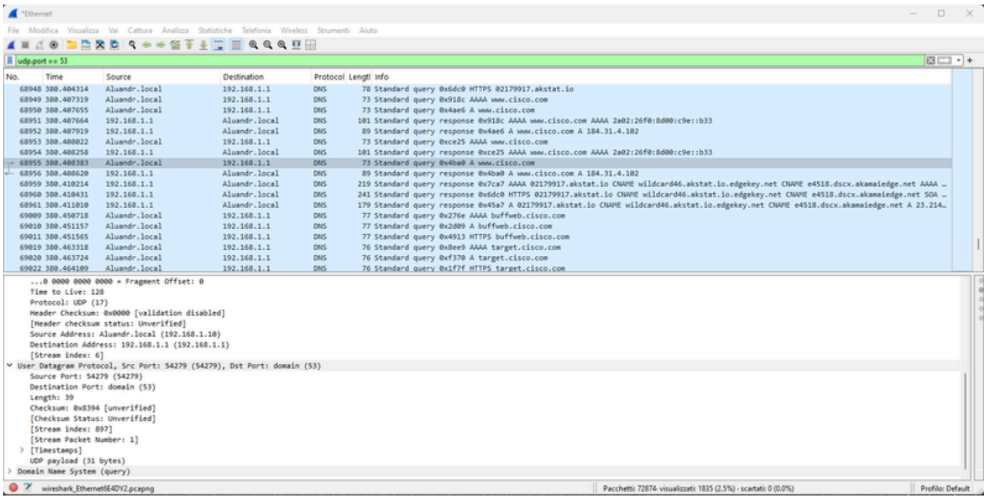
- Expand Internet Protocol Version 4. Observe the source and destination IPv4 addresses.


*Ethernet
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto

```
udp.port == 53

No.   Time       Source          Destination     Protocol Lengtl Info
68948 380.404314 Aluandr.local   192.168.1.1     DNS       78 Standard query 0x6dc0 HTTPS 02179917.akstat.io
68949 380.407319 Aluandr.local   192.168.1.1     DNS       73 Standard query 0x918c AAAA www.cisco.com
68950 380.407655 Aluandr.local   192.168.1.1     DNS       73 Standard query 0x4ae6 A www.cisco.com
68951 380.407664 192.168.1.1     Aluandr.local   DNS      101 Standard query response 0x918c AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68952 380.407919 192.168.1.1     Aluandr.local   DNS       89 Standard query response 0x4ae6 A www.cisco.com A 184.31.4.102
68953 380.408022 Aluandr.local   192.168.1.1     DNS       73 Standard query 0xce25 AAAA www.cisco.com
68954 380.408258 192.168.1.1     Aluandr.local   DNS      101 Standard query response 0xce25 AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68955 380.408383 Aluandr.local   192.168.1.1     DNS       73 Standard query 0x4ba0 A www.cisco.com
68956 380.408620 192.168.1.1     Aluandr.local   DNS       89 Standard query response 0x4ba0 A www.cisco.com A 184.31.4.102
68959 380.410214 192.168.1.1     Aluandr.local   DNS      219 Standard query response 0x7ca7 AAAA 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net AAAA …
68960 380.410431 192.168.1.1     Aluandr.local   DNS      241 Standard query response 0x6dc0 HTTPS 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net SOA …
68961 380.411010 192.168.1.1     Aluandr.local   DNS      179 Standard query response 0x45a7 A 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net A 23.214…
69009 380.450718 Aluandr.local   192.168.1.1     DNS       77 Standard query 0x276e AAAA buffweb.cisco.com
69010 380.451157 Aluandr.local   192.168.1.1     DNS       77 Standard query 0x2d09 A buffweb.cisco.com
69011 380.451565 Aluandr.local   192.168.1.1     DNS       77 Standard query 0x4913 HTTPS buffweb.cisco.com
69019 380.463318 Aluandr.local   192.168.1.1     DNS       76 Standard query 0x8ee9 AAAA target.cisco.com
69020 380.463724 Aluandr.local   192.168.1.1     DNS       76 Standard query 0xf370 A target.cisco.com
69022 380.464109 Aluandr.local   192.168.1.1     DNS       76 Standard query 0x1f7f HTTPS target.cisco.com
```

```
    Type: IPv4 (0x0800)
    [Stream index: 0]
v Internet Protocol Version 4, Src: Aluandr.local (192.168.1.10), Dst: 192.168.1.1 (192.168.1.1)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 59
    Identification: 0x0487 (1159)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: Aluandr.local (192.168.1.10)
    Destination Address: 192.168.1.1 (192.168.1.1)
    [Stream index: 6]
> User Datagram Protocol, Src Port: 54279 (54279), Dst Port: domain (53)
> Domain Name System (query)

wireshark_Ethernet6E4DY2.pcapng        Pacchetti: 72874· visualizzati: 1835 (2.5%) · scartati: 0 (0.0%)        Profilo: Default
```

- Expand the User Datagram Protocol. Observe the source and destination ports.



udp.port == 53

```
No.   Time       Source          Destination     Protocol Lengt Info
68948 380.404314 Aluandr.local   192.168.1.1     DNS       78 Standard query 0x6dc0 HTTPS 02179917.akstat.io
68949 380.407319 Aluandr.local   192.168.1.1     DNS       73 Standard query 0x918c AAAA www.cisco.com
68950 380.407655 Aluandr.local   192.168.1.1     DNS       73 Standard query 0x4ae6 A www.cisco.com
68951 380.407664 192.168.1.1     Aluandr.local   DNS      101 Standard query response 0x918c AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68952 380.407919 192.168.1.1     Aluandr.local   DNS       89 Standard query response 0x4ae6 A www.cisco.com A 184.31.4.102
68953 380.408022 Aluandr.local   192.168.1.1     DNS       73 Standard query 0xce25 AAAA www.cisco.com
68954 380.408258 192.168.1.1     Aluandr.local   DNS      101 Standard query response 0xce25 AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68955 380.408383 Aluandr.local   192.168.1.1     DNS       73 Standard query 0x4ba0 A www.cisco.com
68956 380.408620 192.168.1.1     Aluandr.local   DNS       89 Standard query response 0x4ba0 A www.cisco.com A 184.31.4.102
68959 380.410214 192.168.1.1     Aluandr.local   DNS      219 Standard query response 0x7ca7 AAAA 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net AAAA …
68960 380.410431 192.168.1.1     Aluandr.local   DNS      241 Standard query response 0x6dc0 HTTPS 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net SOA …
68961 380.411010 192.168.1.1     Aluandr.local   DNS      179 Standard query response 0x45a7 A 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net A 23.214…
69009 380.450718 Aluandr.local   192.168.1.1     DNS       77 Standard query 0x276e AAAA buffweb.cisco.com
69010 380.451157 Aluandr.local   192.168.1.1     DNS       77 Standard query 0x2d09 A buffweb.cisco.com
69011 380.451565 Aluandr.local   192.168.1.1     DNS       77 Standard query 0x4913 HTTPS buffweb.cisco.com
69019 380.463318 Aluandr.local   192.168.1.1     DNS       76 Standard query 0x8ee9 AAAA target.cisco.com
69020 380.463724 Aluandr.local   192.168.1.1     DNS       76 Standard query 0xf370 A target.cisco.com
69022 380.464109 Aluandr.local   192.168.1.1     DNS       76 Standard query 0x1f7f HTTPS target.cisco.com
```

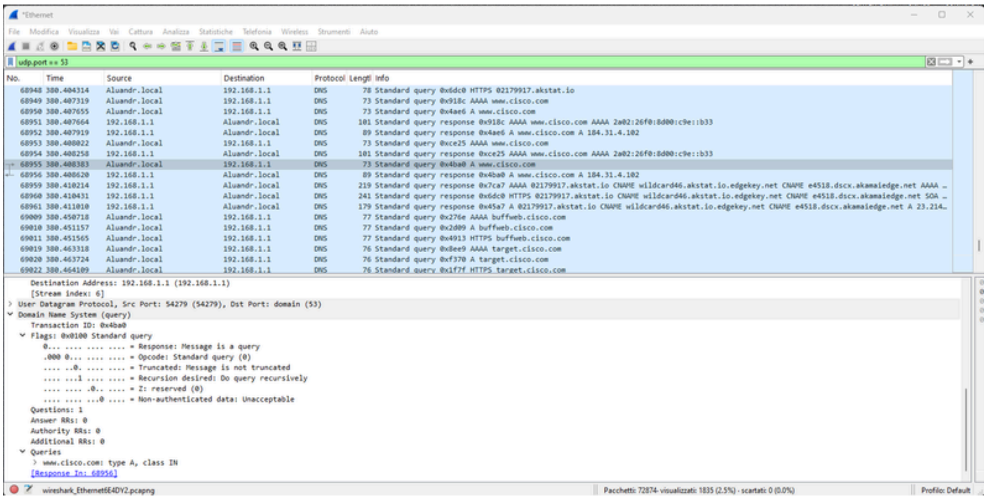
```
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: Aluandr.local (192.168.1.10)
    Destination Address: 192.168.1.1 (192.168.1.1)
    [Stream index: 6]
v User Datagram Protocol, Src Port: 54279 (54279), Dst Port: domain (53)
    Source Port: 54279 (54279)
    Destination Port: domain (53)
    Length: 39
    Checksum: 0x8394 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 897]
    [Stream Packet Number: 1]
  > [Timestamps]
    UDP payload (31 bytes)
> Domain Name System (query)
```

wireshark_Ethernet6E4DY2.pcapng

Pacchetti: 72874 · visualizzati: 1835 (2.5%) · scartati: 0 (0.0%)

Profilo: Default

- Expand Domain Name System (query) in the Packet Details pane. Then expand the Flags and Queries.



udp.port == 53

```
No.   Time       Source          Destination     Protocol Lengt Info
68948 380.404314 Aluandr.local   192.168.1.1     DNS       78 Standard query 0x6dc0 HTTPS 02179917.akstat.io
68949 380.407319 Aluandr.local   192.168.1.1     DNS       73 Standard query 0x918c AAAA www.cisco.com
68950 380.407655 Aluandr.local   192.168.1.1     DNS       73 Standard query 0x4ae6 A www.cisco.com
68951 380.407664 192.168.1.1     Aluandr.local   DNS      101 Standard query response 0x918c AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68952 380.407919 192.168.1.1     Aluandr.local   DNS       89 Standard query response 0x4ae6 A www.cisco.com A 184.31.4.102
68953 380.408022 Aluandr.local   192.168.1.1     DNS       73 Standard query 0xce25 AAAA www.cisco.com
68954 380.408258 192.168.1.1     Aluandr.local   DNS      101 Standard query response 0xce25 AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68955 380.408383 Aluandr.local   192.168.1.1     DNS       73 Standard query 0x4ba0 A www.cisco.com
68956 380.408620 192.168.1.1     Aluandr.local   DNS       89 Standard query response 0x4ba0 A www.cisco.com A 184.31.4.102
68959 380.410214 192.168.1.1     Aluandr.local   DNS      219 Standard query response 0x7ca7 AAAA 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net AAAA …
68960 380.410431 192.168.1.1     Aluandr.local   DNS      241 Standard query response 0x6dc0 HTTPS 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net SOA …
68961 380.411010 192.168.1.1     Aluandr.local   DNS      179 Standard query response 0x45a7 A 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akamaiedge.net A 23.214…
69009 380.450718 Aluandr.local   192.168.1.1     DNS       77 Standard query 0x276e AAAA buffweb.cisco.com
69010 380.451157 Aluandr.local   192.168.1.1     DNS       77 Standard query 0x2d09 A buffweb.cisco.com
69011 380.451565 Aluandr.local   192.168.1.1     DNS       77 Standard query 0x4913 HTTPS buffweb.cisco.com
69019 380.463318 Aluandr.local   192.168.1.1     DNS       76 Standard query 0x8ee9 AAAA target.cisco.com
69020 380.463724 Aluandr.local   192.168.1.1     DNS       76 Standard query 0xf370 A target.cisco.com
69022 380.464109 Aluandr.local   192.168.1.1     DNS       76 Standard query 0x1f7f HTTPS target.cisco.com
```

```
    Destination Address: 192.168.1.1 (192.168.1.1)
    [Stream index: 6]
> User Datagram Protocol, Src Port: 54279 (54279), Dst Port: domain (53)
v Domain Name System (query)
    Transaction ID: 0x4ba0
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.cisco.com: type A, class IN
    [Response In: 68956]
```

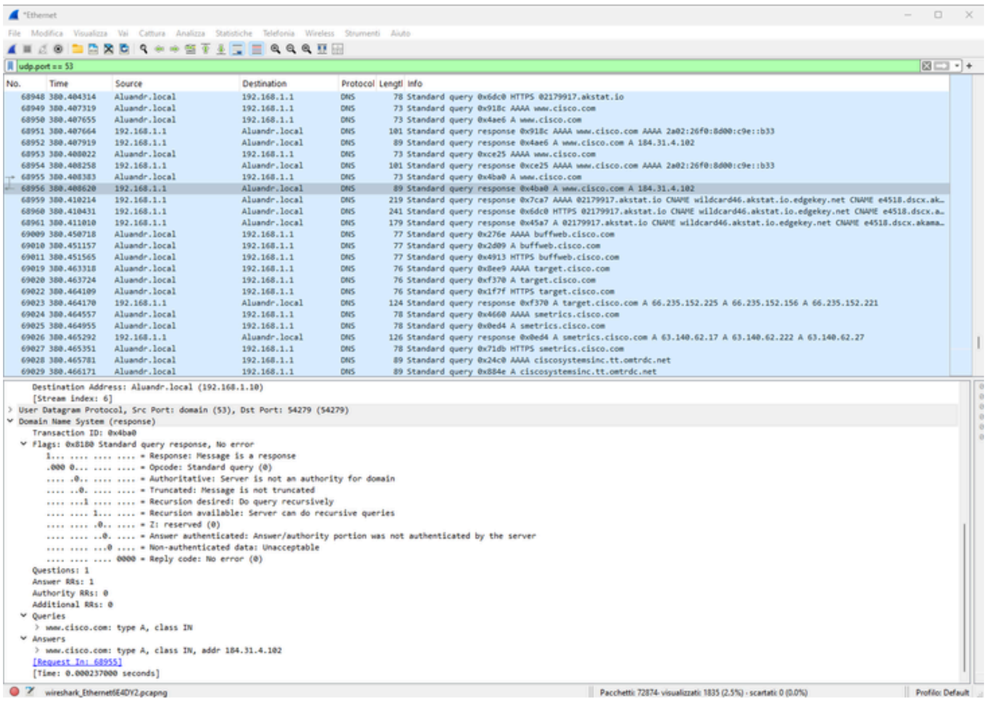
wireshark_Ethernet6E4DY2.pcapng

Pacchetti: 72874 · visualizzati: 1835 (2.5%) · scartati: 0 (0.0%)

Profilo: Default

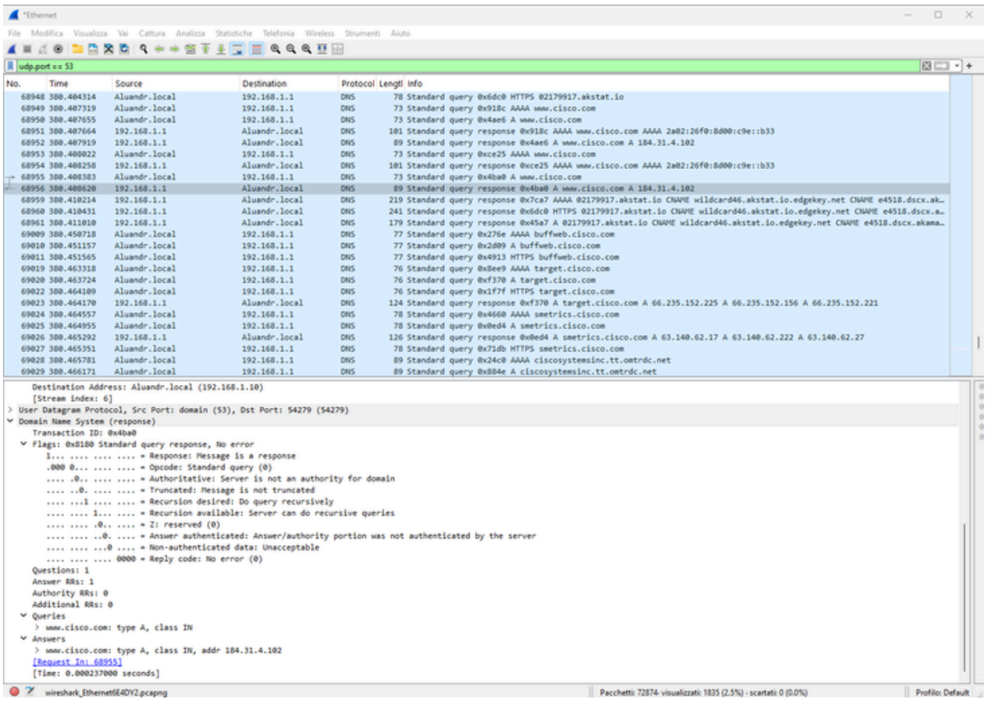
Esplorare il traffico delle risposte DNS

- Select the corresponding response DNS packet has Standard query response and A www.cisco.com in the Info column.



```
udp.port == 53

No.   Time        Source        Destination   Protocol Lengtl Info
68948 380.404314  Aluandr.local 192.168.1.1   DNS       78 Standard query 0x6dc0 HTTPS 02179917.akstat.io
68949 380.407319  Aluandr.local 192.168.1.1   DNS       73 Standard query 0x918c AAAA www.cisco.com
68950 380.407655  Aluandr.local 192.168.1.1   DNS       73 Standard query 0x4ae6 A www.cisco.com
68951 380.407664  192.168.1.1   Aluandr.local DNS      101 Standard query response 0x918c AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68952 380.407919  192.168.1.1   Aluandr.local DNS       89 Standard query response 0x4ae6 A www.cisco.com A 184.31.4.102
68953 380.408022  Aluandr.local 192.168.1.1   DNS       73 Standard query 0xce25 AAAA www.cisco.com
68954 380.408258  192.168.1.1   Aluandr.local DNS      101 Standard query response 0xce25 AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68955 380.408383  Aluandr.local 192.168.1.1   DNS       73 Standard query 0x4ba0 A www.cisco.com
68956 380.408620  192.168.1.1   Aluandr.local DNS       89 Standard query response 0x4ba0 A www.cisco.com A 184.31.4.102
68959 380.410214  192.168.1.1   Aluandr.local DNS      219 Standard query response 0x7ca7 AAAA 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.ak…
68960 380.410431  192.168.1.1   Aluandr.local DNS      241 Standard query response 0x6dc0 HTTPS 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.a…
68961 380.411010  192.168.1.1   Aluandr.local DNS      179 Standard query response 0x45a7 A 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akama…
69009 380.450718  Aluandr.local 192.168.1.1   DNS       77 Standard query 0x276e AAAA buffweb.cisco.com
69010 380.451157  Aluandr.local 192.168.1.1   DNS       77 Standard query 0x2d09 A buffweb.cisco.com
69011 380.451565  Aluandr.local 192.168.1.1   DNS       77 Standard query 0x4913 HTTPS buffweb.cisco.com
69019 380.463318  Aluandr.local 192.168.1.1   DNS       76 Standard query 0x8ee9 AAAA target.cisco.com
69020 380.463724  Aluandr.local 192.168.1.1   DNS       76 Standard query 0xf370 A target.cisco.com
69022 380.464109  Aluandr.local 192.168.1.1   DNS       76 Standard query 0x1f7f HTTPS target.cisco.com
69023 380.464170  192.168.1.1   Aluandr.local DNS      124 Standard query response 0xf370 A target.cisco.com A 66.235.152.225 A 66.235.152.156 A 66.235.152.221
69024 380.464557  Aluandr.local 192.168.1.1   DNS       78 Standard query 0x4660 AAAA smetrics.cisco.com
69025 380.464955  Aluandr.local 192.168.1.1   DNS       78 Standard query 0x0ed4 A smetrics.cisco.com
69026 380.465292  192.168.1.1   Aluandr.local DNS      126 Standard query response 0x0ed4 A smetrics.cisco.com A 63.140.62.17 A 63.140.62.222 A 63.140.62.27
69027 380.465351  Aluandr.local 192.168.1.1   DNS       78 Standard query 0x71db HTTPS smetrics.cisco.com
69028 380.465781  Aluandr.local 192.168.1.1   DNS       89 Standard query 0x24c0 AAAA ciscosystemsinc.tt.omtrdc.net
69029 380.466171  Aluandr.local 192.168.1.1   DNS       89 Standard query 0x884e A ciscosystemsinc.tt.omtrdc.net

    Destination Address: Aluandr.local (192.168.1.10)
    [Stream index: 6]
> User Datagram Protocol, Src Port: domain (53), Dst Port: 54279 (54279)
v Domain Name System (response)
    Transaction ID: 0x4ba0
  v Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.cisco.com: type A, class IN
  v Answers
    > www.cisco.com: type A, class IN, addr 184.31.4.102
    [Request In: 68955]
    [Time: 0.000237000 seconds]

wireshark_Ethernet6E4DY2.pcapng    Pacchetti: 72874 · visualizzati: 1835 (2.5%) · scartati: 0 (0.0%)    Profilo: Default
```

- Expand Domain Name System (response). Then expand the Flags, Queries, and Answers



```
udp.port == 53

No.   Time        Source        Destination   Protocol Lengtl Info
68948 380.404314  Aluandr.local 192.168.1.1   DNS       78 Standard query 0x6dc0 HTTPS 02179917.akstat.io
68949 380.407319  Aluandr.local 192.168.1.1   DNS       73 Standard query 0x918c AAAA www.cisco.com
68950 380.407655  Aluandr.local 192.168.1.1   DNS       73 Standard query 0x4ae6 A www.cisco.com
68951 380.407664  192.168.1.1   Aluandr.local DNS      101 Standard query response 0x918c AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68952 380.407919  192.168.1.1   Aluandr.local DNS       89 Standard query response 0x4ae6 A www.cisco.com A 184.31.4.102
68953 380.408022  Aluandr.local 192.168.1.1   DNS       73 Standard query 0xce25 AAAA www.cisco.com
68954 380.408258  192.168.1.1   Aluandr.local DNS      101 Standard query response 0xce25 AAAA www.cisco.com AAAA 2a02:26f0:8d00:c9e::b33
68955 380.408383  Aluandr.local 192.168.1.1   DNS       73 Standard query 0x4ba0 A www.cisco.com
68956 380.408620  192.168.1.1   Aluandr.local DNS       89 Standard query response 0x4ba0 A www.cisco.com A 184.31.4.102
68959 380.410214  192.168.1.1   Aluandr.local DNS      219 Standard query response 0x7ca7 AAAA 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.ak…
68960 380.410431  192.168.1.1   Aluandr.local DNS      241 Standard query response 0x6dc0 HTTPS 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.a…
68961 380.411010  192.168.1.1   Aluandr.local DNS      179 Standard query response 0x45a7 A 02179917.akstat.io CNAME wildcard46.akstat.io.edgekey.net CNAME e4518.dscx.akama…
69009 380.450718  Aluandr.local 192.168.1.1   DNS       77 Standard query 0x276e AAAA buffweb.cisco.com
69010 380.451157  Aluandr.local 192.168.1.1   DNS       77 Standard query 0x2d09 A buffweb.cisco.com
69011 380.451565  Aluandr.local 192.168.1.1   DNS       77 Standard query 0x4913 HTTPS buffweb.cisco.com
69019 380.463318  Aluandr.local 192.168.1.1   DNS       76 Standard query 0x8ee9 AAAA target.cisco.com
69020 380.463724  Aluandr.local 192.168.1.1   DNS       76 Standard query 0xf370 A target.cisco.com
69022 380.464109  Aluandr.local 192.168.1.1   DNS       76 Standard query 0x1f7f HTTPS target.cisco.com
69023 380.464170  192.168.1.1   Aluandr.local DNS      124 Standard query response 0xf370 A target.cisco.com A 66.235.152.225 A 66.235.152.156 A 66.235.152.221
69024 380.464557  Aluandr.local 192.168.1.1   DNS       78 Standard query 0x4660 AAAA smetrics.cisco.com
69025 380.464955  Aluandr.local 192.168.1.1   DNS       78 Standard query 0x0ed4 A smetrics.cisco.com
69026 380.465292  192.168.1.1   Aluandr.local DNS      126 Standard query response 0x0ed4 A smetrics.cisco.com A 63.140.62.17 A 63.140.62.222 A 63.140.62.27
69027 380.465351  Aluandr.local 192.168.1.1   DNS       78 Standard query 0x71db HTTPS smetrics.cisco.com
69028 380.465781  Aluandr.local 192.168.1.1   DNS       89 Standard query 0x24c0 AAAA ciscosystemsinc.tt.omtrdc.net
69029 380.466171  Aluandr.local 192.168.1.1   DNS       89 Standard query 0x884e A ciscosystemsinc.tt.omtrdc.net

    Destination Address: Aluandr.local (192.168.1.10)
    [Stream index: 6]
> User Datagram Protocol, Src Port: domain (53), Dst Port: 54279 (54279)
v Domain Name System (response)
    Transaction ID: 0x4ba0
  v Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.cisco.com: type A, class IN
  v Answers
    > www.cisco.com: type A, class IN, addr 184.31.4.102
    [Request In: 68955]
    [Time: 0.000237000 seconds]

wireshark_Ethernet6E4DY2.pcapng    Pacchetti: 72874 · visualizzati: 1835 (2.5%) · scartati: 0 (0.0%)    Profilo: Default
```