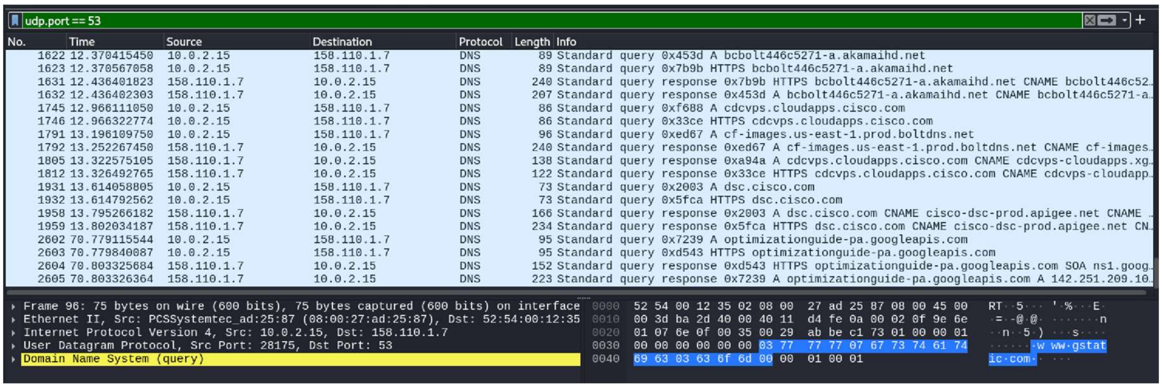
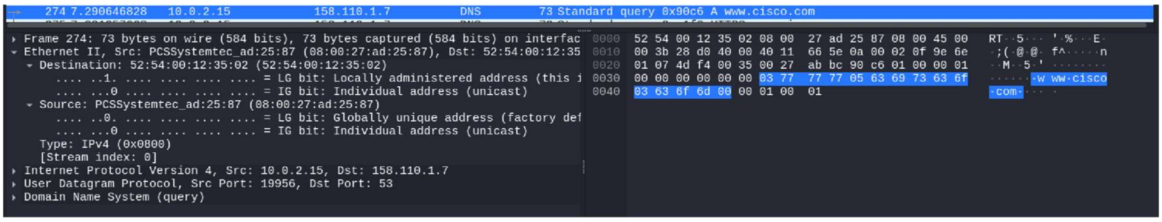
Navighiamo sul sito www.cisco.com e impostiamo il filtro **udp.port == 53 su wireshark**



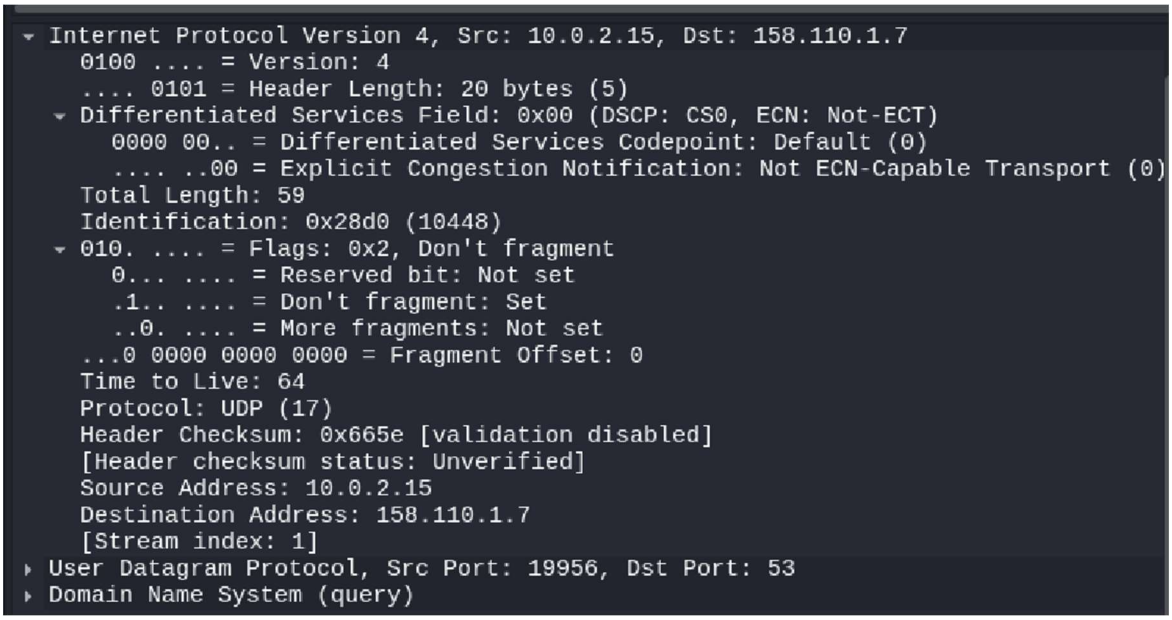
```
udp.port == 53
No.   Time           Source          Destination     Protocol  Length Info
 1622 12.370415450   10.0.2.15       158.110.1.7     DNS        89 Standard query 0x453d A bcbolt446c5271-a.akamaihd.net
 1623 12.370567058   10.0.2.15       158.110.1.7     DNS        89 Standard query 0x7b9b HTTPS bcbolt446c5271-a.akamaihd.net
 1631 12.436401823   158.110.1.7     10.0.2.15       DNS       240 Standard query response 0x7b9b HTTPS bcbolt446c5271-a.akamaihd.net CNAME bcbolt446c52…
 1632 12.436402303   158.110.1.7     10.0.2.15       DNS       207 Standard query response 0x453d A bcbolt446c5271-a.akamaihd.net CNAME bcbolt446c5271-a…
 1745 12.966111050   10.0.2.15       158.110.1.7     DNS        86 Standard query 0xf688 A cdcvps.cloudapps.cisco.com
 1746 12.966322774   10.0.2.15       158.110.1.7     DNS        86 Standard query 0x33ce HTTPS cdcvps.cloudapps.cisco.com
 1791 13.196109750   10.0.2.15       158.110.1.7     DNS        96 Standard query 0xed67 A cf-images.us-east-1.prod.boltdns.net
 1792 13.252267450   158.110.1.7     10.0.2.15       DNS       240 Standard query response 0xed67 A cf-images.us-east-1.prod.boltdns.net CNAME cf-images…
 1805 13.322575105   158.110.1.7     10.0.2.15       DNS       138 Standard query response 0xa94a A cdcvps.cloudapps.cisco.com CNAME cdcvps-cloudapps.xg…
 1812 13.326492765   158.110.1.7     10.0.2.15       DNS       122 Standard query response 0x33ce HTTPS cdcvps.cloudapps.cisco.com CNAME cdcvps-cloudapp…
 1931 13.614058805   10.0.2.15       158.110.1.7     DNS        73 Standard query 0x2003 A dsc.cisco.com
 1932 13.614792562   10.0.2.15       158.110.1.7     DNS        73 Standard query 0x5fca HTTPS dsc.cisco.com
 1958 13.795266182   158.110.1.7     10.0.2.15       DNS       166 Standard query response 0x2003 A dsc.cisco.com CNAME cisco-dsc-prod.apigee.net CNAME …
 1959 13.802034187   158.110.1.7     10.0.2.15       DNS       234 Standard query response 0x5fca HTTPS dsc.cisco.com CNAME cisco-dsc-prod.apigee.net CN…
 2602 70.779115544   10.0.2.15       158.110.1.7     DNS        95 Standard query 0x7239 A optimizationguide-pa.googleapis.com
 2603 70.779840087   10.0.2.15       158.110.1.7     DNS        95 Standard query 0xd543 HTTPS optimizationguide-pa.googleapis.com
 2604 70.803325684   158.110.1.7     10.0.2.15       DNS       152 Standard query response 0xd543 HTTPS optimizationguide-pa.googleapis.com SOA ns1.goog…
 2605 70.803326364   158.110.1.7     10.0.2.15       DNS       223 Standard query response 0x7239 A optimizationguide-pa.googleapis.com A 142.251.209.10…

▸ Frame 96: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface    0000  52 54 00 12 35 02 08 00  27 ad 25 87 08 00 45 00   RT··5···'·%···E·
▸ Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: 52:54:00:12:35   0010  00 3d ba 2d 40 00 40 11  d4 fe 0a 00 02 0f 9e 6e   ·=·-@·@········n
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 158.110.1.7                       0020  01 07 6e 0f 00 35 00 29  ab be c1 73 01 00 00 01   ··n··5·)···s····
▸ User Datagram Protocol, Src Port: 28175, Dst Port: 53                               0030  00 00 00 00 00 00 03 77  77 77 07 67 73 74 61 74   ·······www·gstat
▸ Domain Name System (query)                                                          0040  69 63 03 63 6f 6d 00 00  01 00 01                  ic·com·····
```

Selezioniamo un pacchetto standard query A www.cisco.com e apriamo le informazioni del interfaccia ETH2



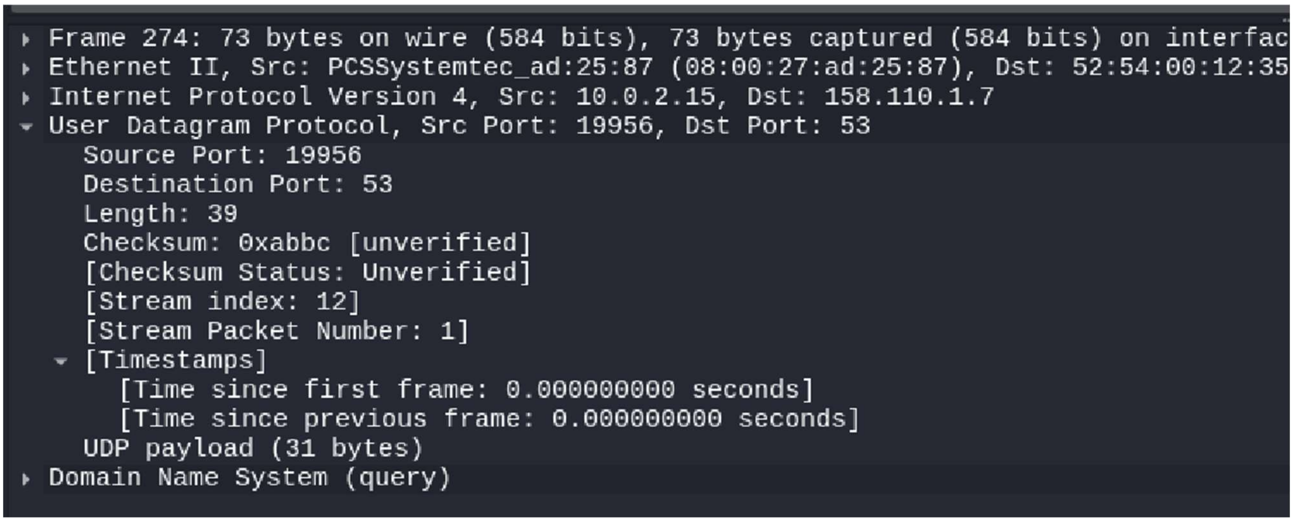
```
  274 7.290646828    10.0.2.15       158.110.1.7     DNS        73 Standard query 0x90c6 A www.cisco.com

▸ Frame 274: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interfac   0000  52 54 00 12 35 02 08 00  27 ad 25 87 08 00 45 00   RT··5···'·%···E·
▾ Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: 52:54:00:12:35   0010  00 3b 28 d0 40 00 40 11  66 5e 0a 00 02 0f 9e 6e   ·;(·@·@·f^·····n
  ▾ Destination: 52:54:00:12:35:02 (52:54:00:12:35:02)                               0020  01 07 4d f4 00 35 00 27  ab bc 90 c6 01 00 00 01   ··M··5·'········
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this i   0030  00 00 00 00 00 00 03 77  77 77 05 63 69 73 63 6f   ·······www·cisco
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)           0040  03 63 6f 6d 00 00 01 00  01                        ·com·····
  ▾ Source: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory def
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 0]
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 158.110.1.7
▸ User Datagram Protocol, Src Port: 19956, Dst Port: 53
▸ Domain Name System (query)
```

Espandiamo poi IPV4



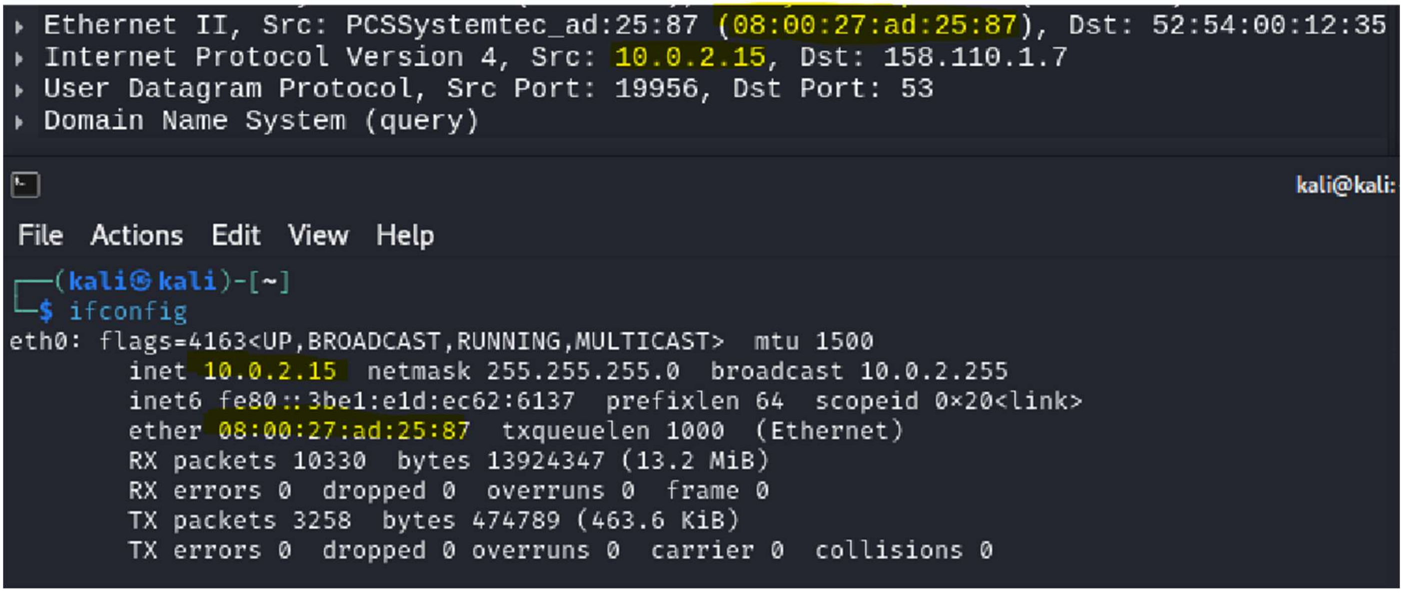
```
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 158.110.1.7
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 59
    Identification: 0x28d0 (10448)
  ▾ 010. .... = Flags: 0x2, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x665e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 158.110.1.7
    [Stream index: 1]
▸ User Datagram Protocol, Src Port: 19956, Dst Port: 53
▸ Domain Name System (query)
```

Espandiamo poi l'User Datagram Protocol



```
▸ Frame 274: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interfac
▸ Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: 52:54:00:12:35
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 158.110.1.7
▾ User Datagram Protocol, Src Port: 19956, Dst Port: 53
    Source Port: 19956
    Destination Port: 53
    Length: 39
    Checksum: 0xabbc [unverified]
    [Checksum Status: Unverified]
    [Stream index: 12]
    [Stream Packet Number: 1]
  ▾ [Timestamps]
      [Time since first frame: 0.000000000 seconds]
      [Time since previous frame: 0.000000000 seconds]
    UDP payload (31 bytes)
▸ Domain Name System (query)
```

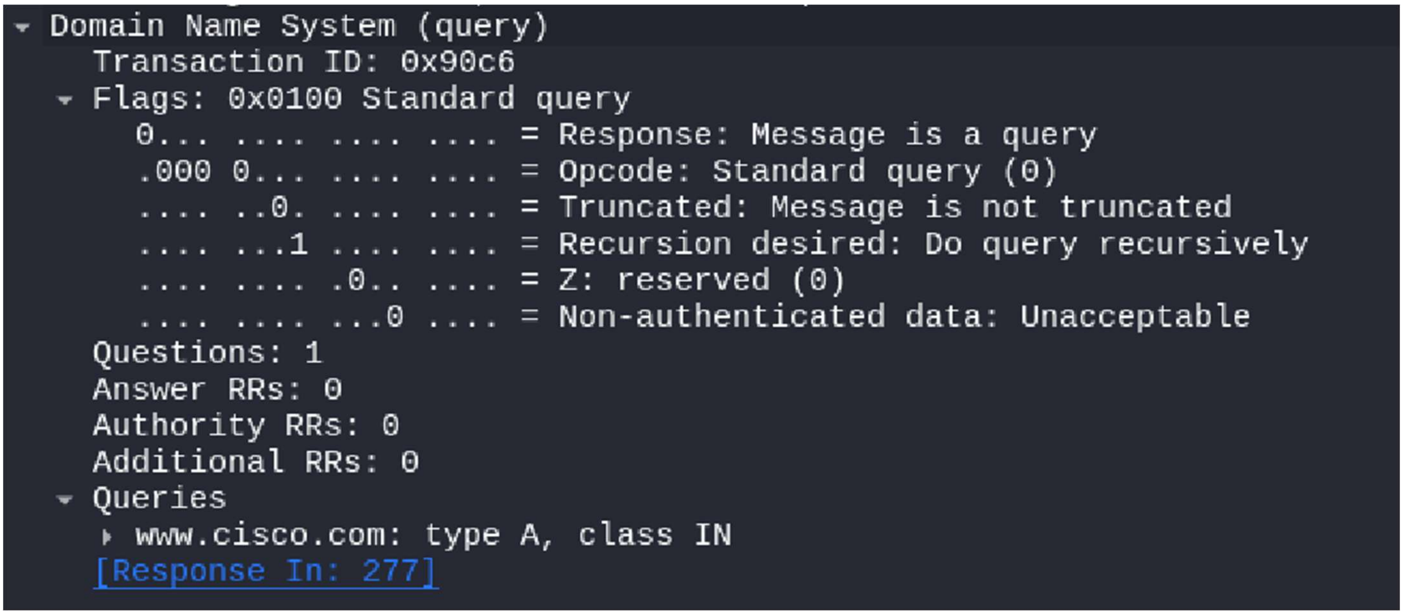
Andiamo a paragonare IP e indirizzo MAC di ifconfig con quelli di wireshark:



```
▸ Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: 52:54:00:12:35
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 158.110.1.7
▸ User Datagram Protocol, Src Port: 19956, Dst Port: 53
▸ Domain Name System (query)
```

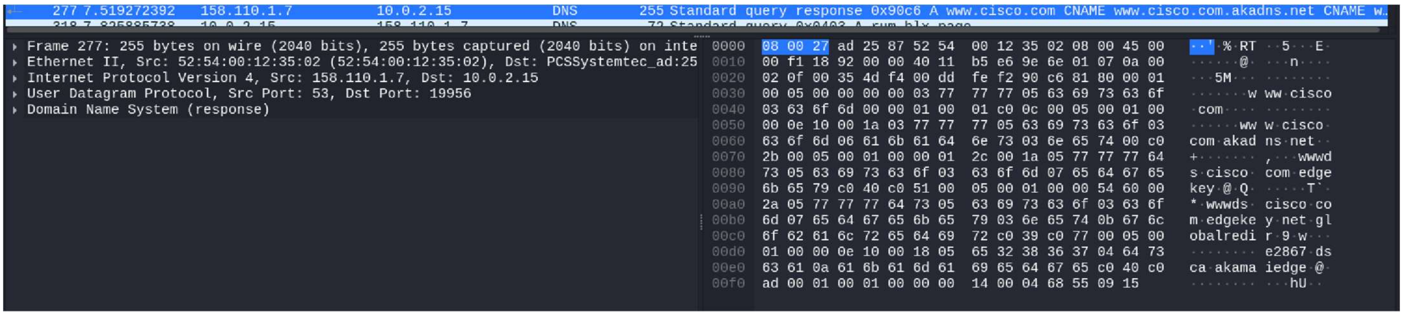
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::3be1:e1d:ec62:6137  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:ad:25:87  txqueuelen 1000  (Ethernet)
        RX packets 10330  bytes 13924347 (13.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3258  bytes 474789 (463.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Espandiamo Domain Name System:



```
▾ Domain Name System (query)
    Transaction ID: 0x90c6
  ▾ 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
  ▾ Queries
    ▸ www.cisco.com: type A, class IN
    [Response In: 277]
```

Selezioniamo il pacchetto di risposta a quello selezionato sopra:



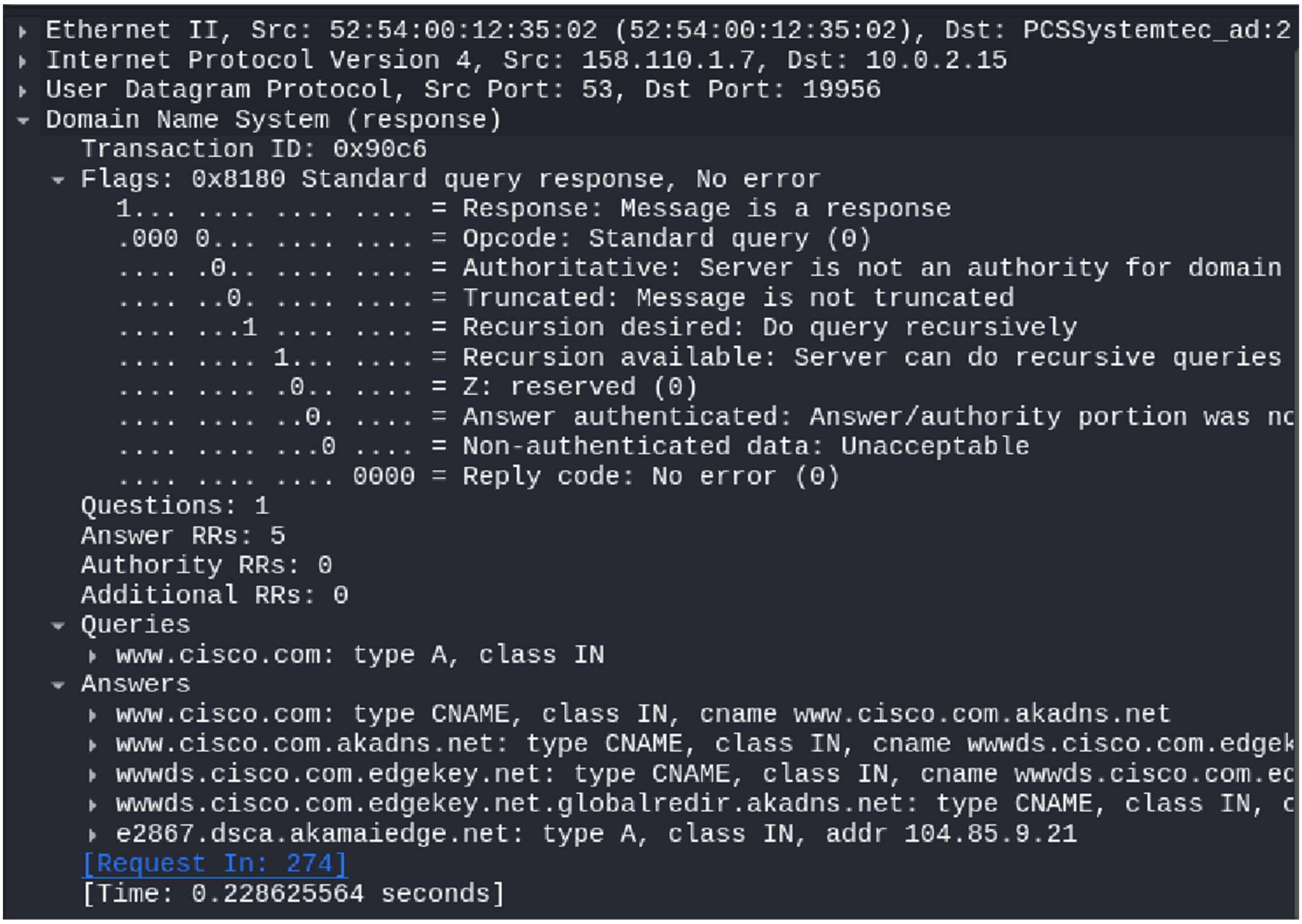
```
277 7.519272392   158.110.1.7     10.0.2.15      DNS    255 Standard query response 0x90c6 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME w…
318 7.825885738   10.0.2.15       158.110.1.7    DNS     72 Standard query 0x0403 A rum.hlx.page
```

```
▸ Frame 277: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on inte
▸ Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_ad:25
▸ Internet Protocol Version 4, Src: 158.110.1.7, Dst: 10.0.2.15
▸ User Datagram Protocol, Src Port: 53, Dst Port: 19956
▸ Domain Name System (response)
```

```
0000  08 00 27 ad 25 87 52 54  00 12 35 02 08 00 45 00   ··'·%·RT ··5···E·
0010  00 f1 18 92 00 00 40 11  b5 e6 9e 6e 01 07 0a 00   ······@· ···n····
0020  02 0f 00 35 4d f4 00 dd  fe f2 90 c6 81 80 00 01   ···5M··· ········
0030  00 05 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 c0 0c 00 05 00 01 00   ·com···· ········
0050  00 0e 10 00 1a 03 77 77  77 05 63 69 73 63 6f 03   ······ww w·cisco·
0060  63 6f 6d 06 61 6b 61 64  6e 73 03 6e 65 74 00 c0   com·akad ns·net··
0070  2b 00 05 00 01 00 00 01  2c 00 1a 05 77 77 77 64   +······· ,···wwwd
0080  73 05 63 69 73 63 6f 03  63 6f 6d 07 65 64 67 65   s·cisco· com·edge
0090  6b 65 79 c0 40 c0 51 00  05 00 01 00 00 54 60 00   key·@·Q· ·····T`·
00a0  2a 05 77 77 77 64 73 05  63 69 73 63 6f 03 63 6f   *·wwwds· cisco·co
00b0  6d 07 65 64 67 65 6b 65  79 03 6e 65 74 0b 67 6c   m·edgeke y·net·gl
00c0  6f 62 61 6c 72 65 64 69  72 c0 39 c0 77 00 05 00   obalredi r·9·w···
00d0  01 00 00 0e 10 00 18 05  65 32 38 36 37 04 64 73   ········ e2867·ds
00e0  63 61 0a 61 6b 61 6d 61  69 65 64 67 65 c0 40 c0   ca·akama iedge·@·
00f0  ad 00 01 00 01 00 00 00  14 00 04 68 55 09 15      ········ ···hU··
```

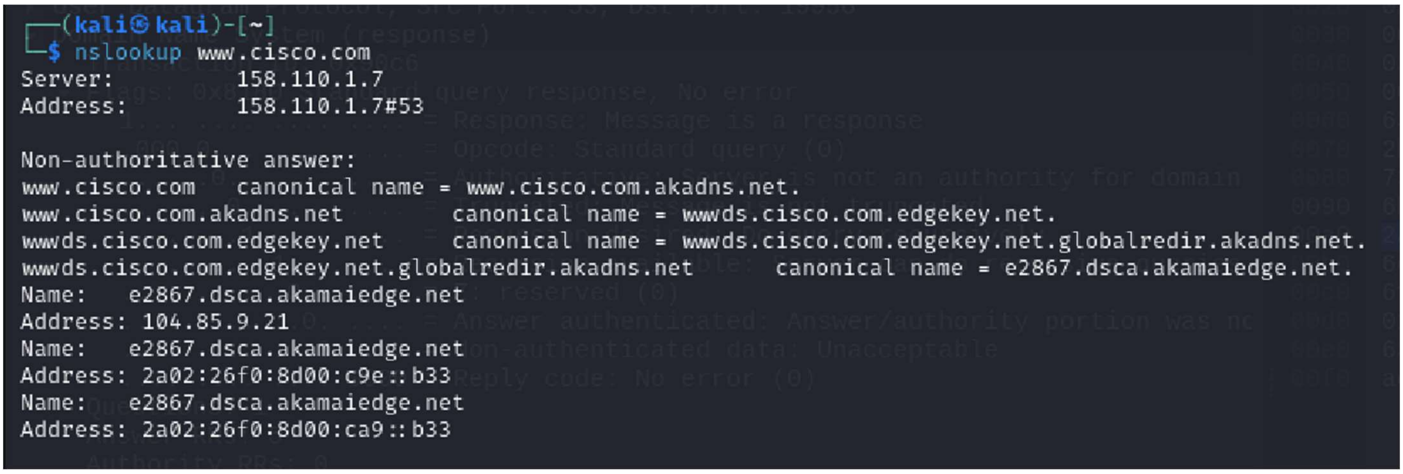
Gli indirizzi di destinazione e partenza sono ora invertiti

Espandiamo Domain Name System:



```
▸ Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_ad:2
▸ Internet Protocol Version 4, Src: 158.110.1.7, Dst: 10.0.2.15
▸ User Datagram Protocol, Src Port: 53, Dst Port: 19956
▾ Domain Name System (response)
    Transaction ID: 0x90c6
  ▾ 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 nc
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.cisco.com: type A, class IN
  ▾ Answers
    ▸ www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
    ▸ www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgek
    ▸ wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.ec
    ▸ wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, c
    ▸ e2867.dsca.akamaiedge.net: type A, class IN, addr 104.85.9.21
    [Request In: 274]
    [Time: 0.228625564 seconds]
```

Confrontiamo i risultati con quelli di nslookup



```
┌──(kali㉿kali)-[~]
└─$ nslookup www.cisco.com
Server:         158.110.1.7
Address:        158.110.1.7#53

Non-authoritative answer:
www.cisco.com   canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net        canonical name = wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net     canonical name = wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net      canonical name = e2867.dsca.akamaiedge.net.
Name:   e2867.dsca.akamaiedge.net
Address: 104.85.9.21
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:8d00:c9e::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:8d00:ca9::b33
```