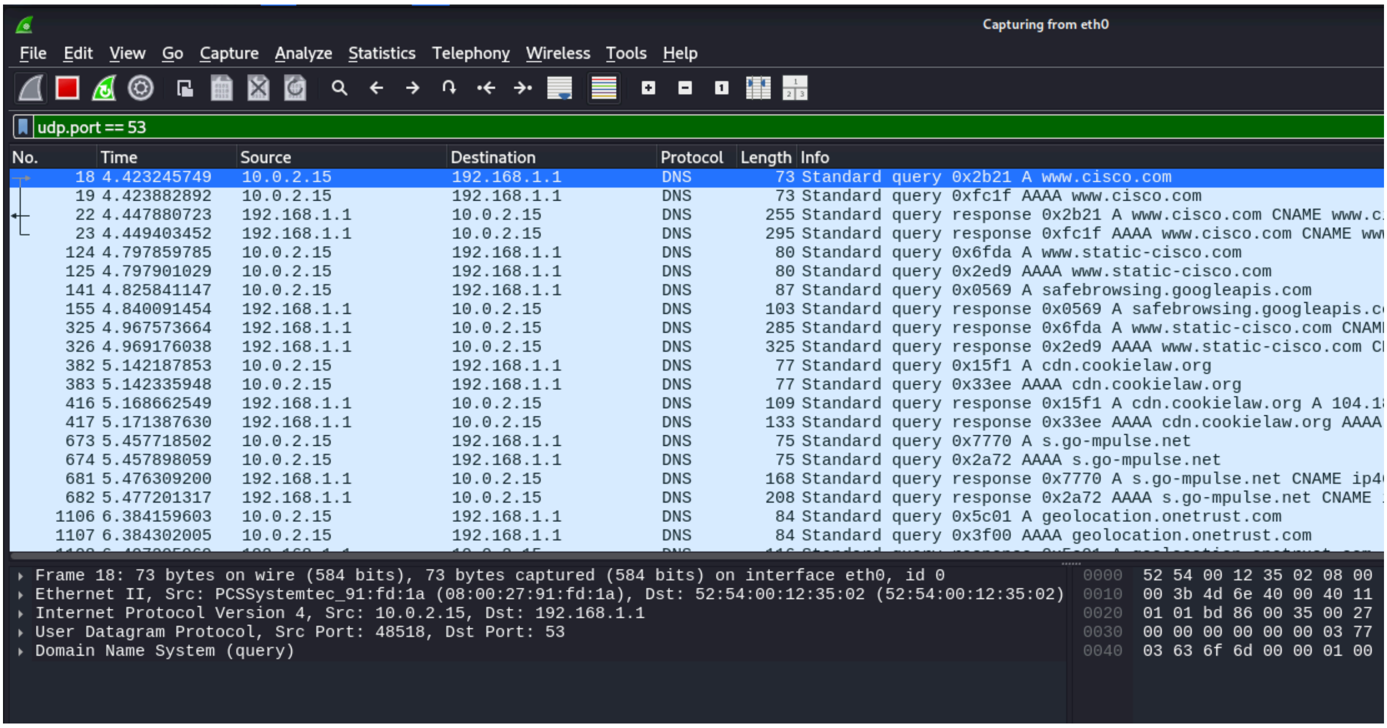
DNS con Wire Shark

Per prima cosa ho deciso di analizzare le richieste DNS connettendomi al sito di CISCO, una volta deciso ho attivato la cattura di Wire Shark applicando il filtro `udp.port == 53` per visualizzare solo i pacchetti DNS.



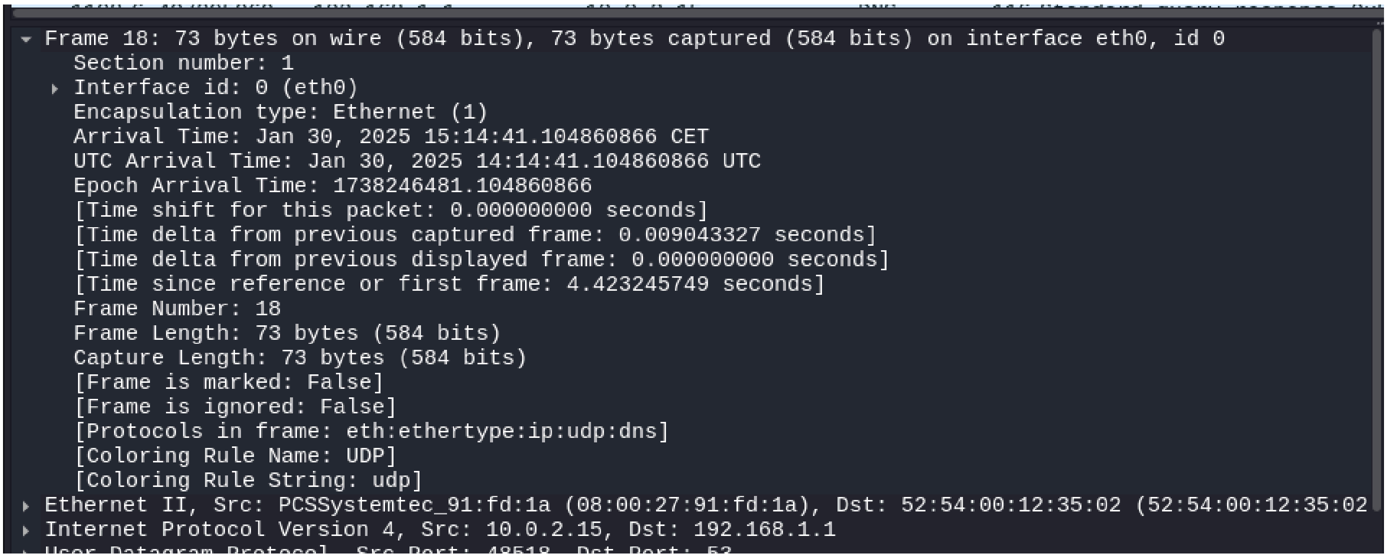
udp.port == 53

```
No.    Time         Source        Destination   Protocol Length Info
    18 4.423245749  10.0.2.15     192.168.1.1   DNS        73 Standard query 0x2b21 A www.cisco.com
    19 4.423882892  10.0.2.15     192.168.1.1   DNS        73 Standard query 0xfc1f AAAA www.cisco.com
    22 4.447880723  192.168.1.1   10.0.2.15     DNS       255 Standard query response 0x2b21 A www.cisco.com CNAME www.c
    23 4.449403452  192.168.1.1   10.0.2.15     DNS       295 Standard query response 0xfc1f AAAA www.cisco.com CNAME ww
   124 4.797859785  10.0.2.15     192.168.1.1   DNS        80 Standard query 0x6fda A www.static-cisco.com
   125 4.797901029  10.0.2.15     192.168.1.1   DNS        80 Standard query 0x2ed9 AAAA www.static-cisco.com
   141 4.825841147  10.0.2.15     192.168.1.1   DNS        87 Standard query 0x0569 A safebrowsing.googleapis.com
   155 4.840091454  192.168.1.1   10.0.2.15     DNS       103 Standard query response 0x0569 A safebrowsing.googleapis.c
   325 4.967573664  192.168.1.1   10.0.2.15     DNS       285 Standard query response 0x6fda A www.static-cisco.com CNAM
   326 4.969176038  192.168.1.1   10.0.2.15     DNS       325 Standard query response 0x2ed9 AAAA www.static-cisco.com C
   382 5.142187853  10.0.2.15     192.168.1.1   DNS        77 Standard query 0x15f1 A cdn.cookielaw.org
   383 5.142335948  10.0.2.15     192.168.1.1   DNS        77 Standard query 0x33ee AAAA cdn.cookielaw.org
   416 5.168662549  192.168.1.1   10.0.2.15     DNS       109 Standard query response 0x15f1 A cdn.cookielaw.org A 104.1
   417 5.171387630  192.168.1.1   10.0.2.15     DNS       133 Standard query response 0x33ee AAAA cdn.cookielaw.org AAAA
   673 5.457718502  10.0.2.15     192.168.1.1   DNS        75 Standard query 0x7770 A s.go-mpulse.net
   674 5.457898059  10.0.2.15     192.168.1.1   DNS        75 Standard query 0x2a72 AAAA s.go-mpulse.net
   681 5.476309200  192.168.1.1   10.0.2.15     DNS       168 Standard query response 0x7770 A s.go-mpulse.net CNAME ip4
   682 5.477201317  192.168.1.1   10.0.2.15     DNS       208 Standard query response 0x2a72 AAAA s.go-mpulse.net CNAME
  1106 6.384159603  10.0.2.15     192.168.1.1   DNS        84 Standard query 0x5c01 A geolocation.onetrust.com
  1107 6.384302005  10.0.2.15     192.168.1.1   DNS        84 Standard query 0x3f00 AAAA geolocation.onetrust.com
```

```
› Frame 18: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_91:fd:1a (08:00:27:91:fd:1a), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.1
› User Datagram Protocol, Src Port: 48518, Dst Port: 53
› Domain Name System (query)
```

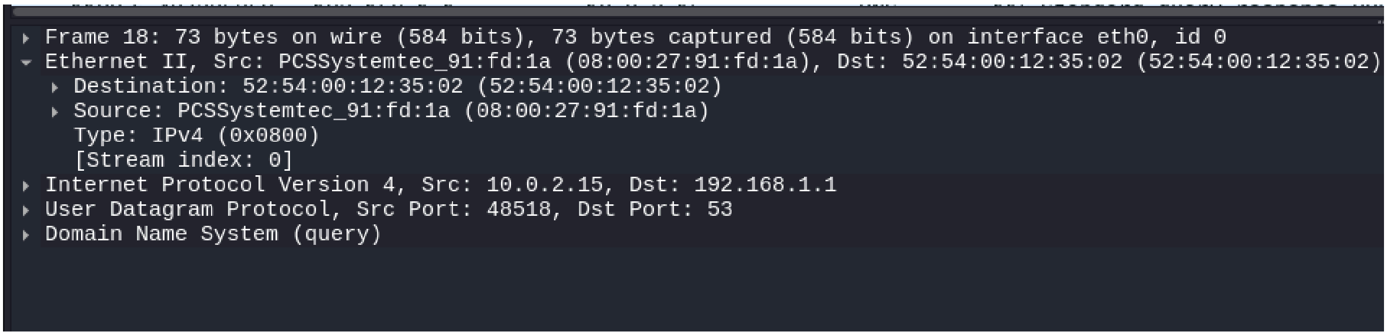
```
0000  52 54 00 12 35 02 08 00
0010  00 3b 4d 6e 40 00 40 11
0020  01 01 bd 86 00 35 00 27
0030  00 00 00 00 00 00 03 77
0040  03 63 6f 6d 00 00 01 00
```

Subito dopo ho selezionato appunto la richiesta di connettermi al sito della CISCO e in basso a sinistra ho esplorato i vari menu' a tendina per avere le info di cui avevo bisogno, in questo caso vedrò il menu' dei frame.



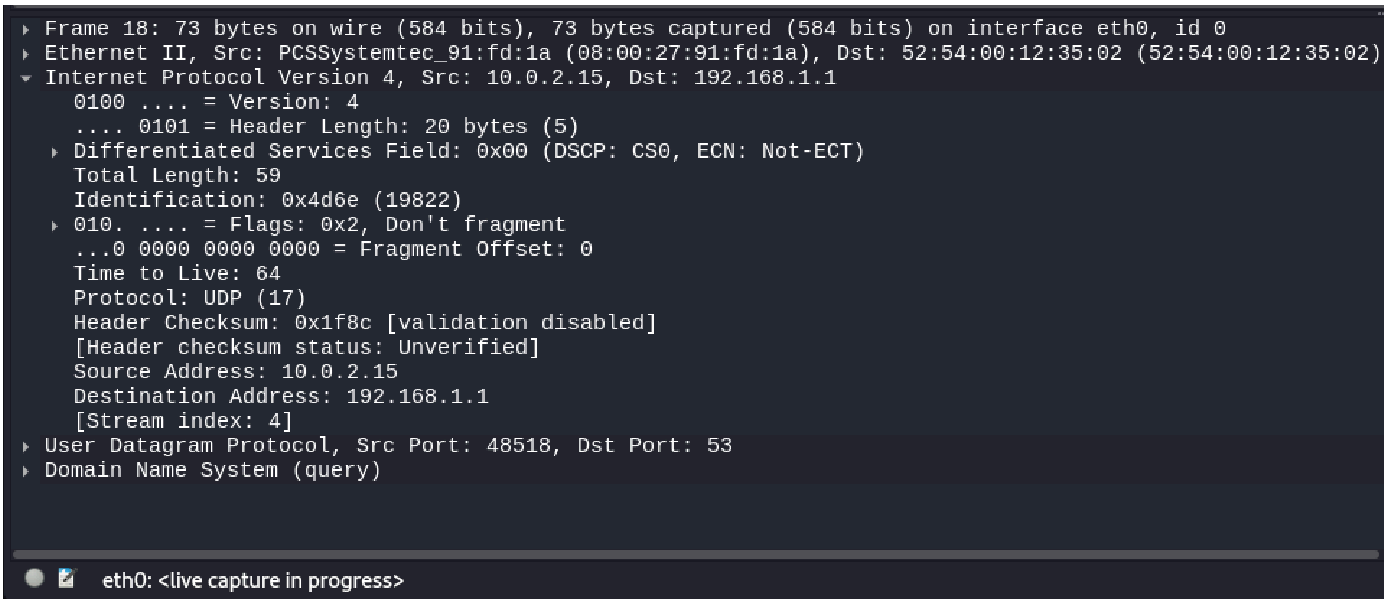
```
▾ Frame 18: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
    Section number: 1
  › Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 30, 2025 15:14:41.104860866 CET
    UTC Arrival Time: Jan 30, 2025 14:14:41.104860866 UTC
    Epoch Arrival Time: 1738246481.104860866
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.009043327 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 4.423245749 seconds]
    Frame Number: 18
    Frame Length: 73 bytes (584 bits)
    Capture Length: 73 bytes (584 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
› Ethernet II, Src: PCSSystemtec_91:fd:1a (08:00:27:91:fd:1a), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.1
```

Poi la tendina Ethernet II



```
Frame 18: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_91:fd:1a (08:00:27:91:fd:1a), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
  Destination: 52:54:00:12:35:02 (52:54:00:12:35:02)
  Source: PCSSystemtec_91:fd:1a (08:00:27:91:fd:1a)
  Type: IPv4 (0x0800)
  [Stream index: 0]
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 48518, Dst Port: 53
Domain Name System (query)
```

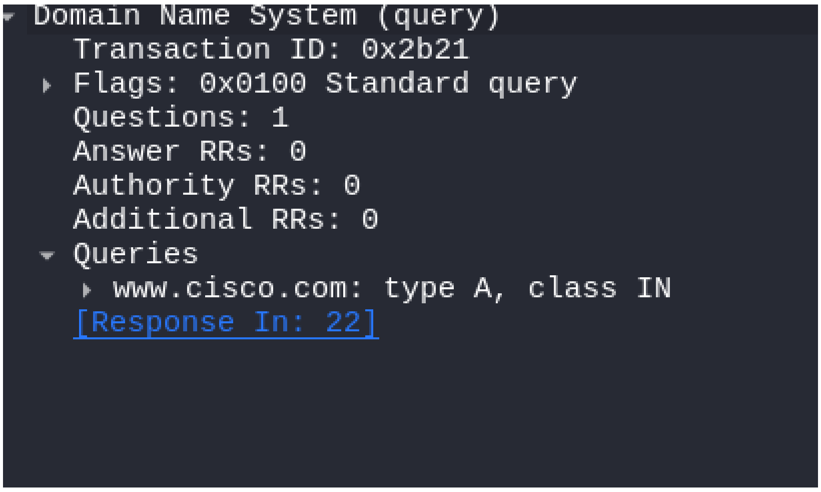
Poi la tendina IPV4 che ci rivela anche la sorgente e la destinazione del pacchetto.



```
Frame 18: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_91:fd:1a (08:00:27:91:fd:1a), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 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: 0x4d6e (19822)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0x1f8c [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.0.2.15
  Destination Address: 192.168.1.1
  [Stream index: 4]
User Datagram Protocol, Src Port: 48518, Dst Port: 53
Domain Name System (query)

eth0: <live capture in progress>
```

E per ultima la tendina della QUERY.



```
Domain Name System (query)
  Transaction ID: 0x2b21
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.cisco.com: type A, class IN
  [Response In: 22]
```