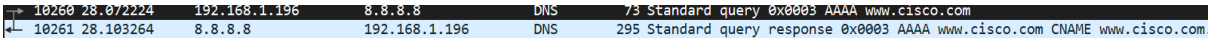
Esercizio S11L4 - Wireshark e cattura di DNS

Dimostrazione di flush e di nslookup su www.cisco.com:

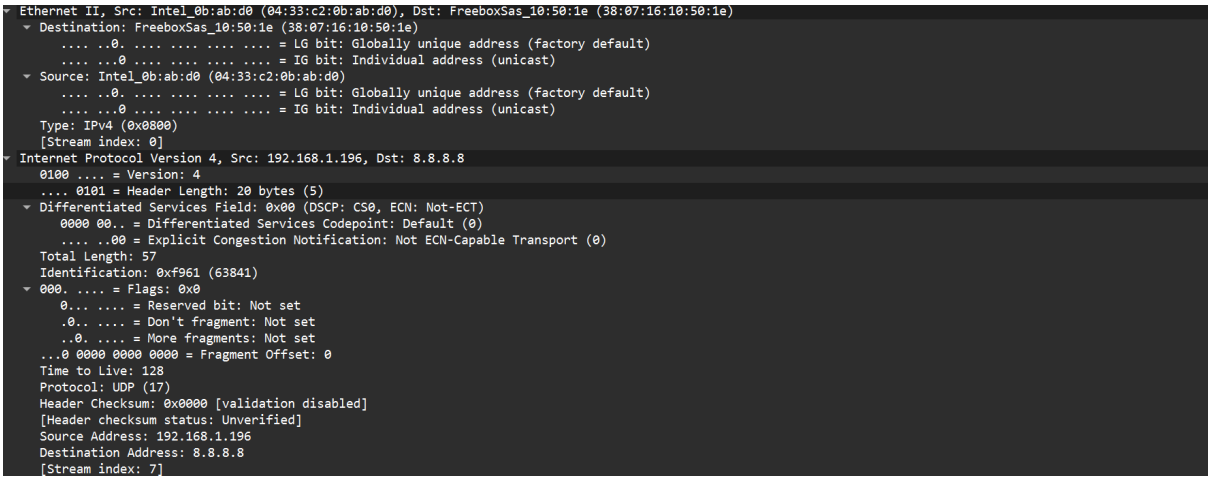
```
C:\Users\uomos>ipconfig /flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.

C:\Users\uomos>nslookup www.cisco.com
Server:  dns.google
Address:  8.8.8.8

Risposta da un server non autorevole:
Nome:    e2867.dsca.akamaiedge.net
Addresses:  2a02:26f0:2d80:280::b33
          2a02:26f0:2d80:281::b33
          92.123.44.98
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net


C:\Users\uomos>
```

Dimostrazione cattura DNS con filtro UDP su porta 53 via Wireshark:



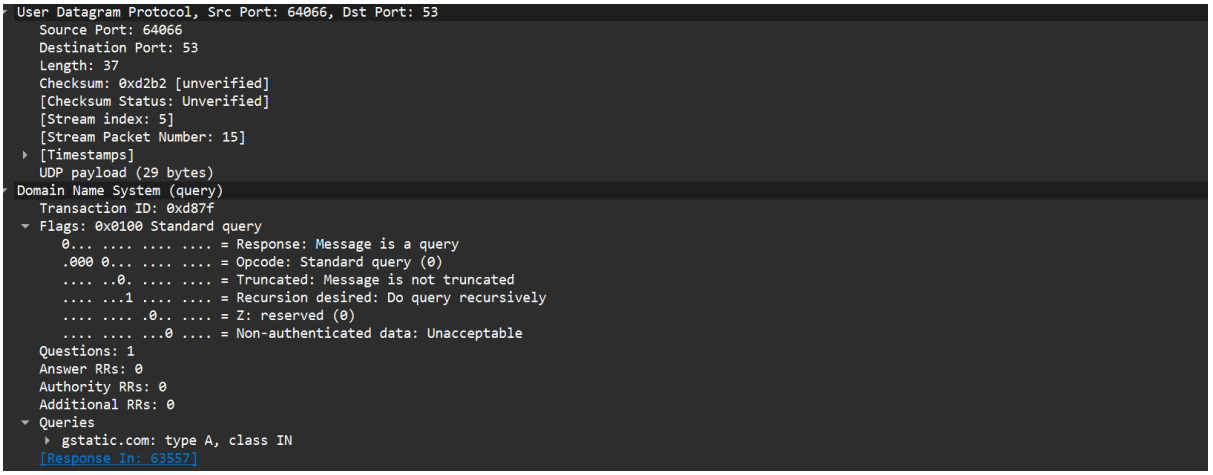
→	10260 28.072224	192.168.1.196	8.8.8.8	DNS	73 Standard query 0x0003 AAAA www.cisco.com
←	10261 28.103264	8.8.8.8	192.168.1.196	DNS	295 Standard query response 0x0003 AAAA www.cisco.com CNAME www.cisco.com

Esplorazione di Ethernet, IPV4 su pacchetto Standard Query (invio):

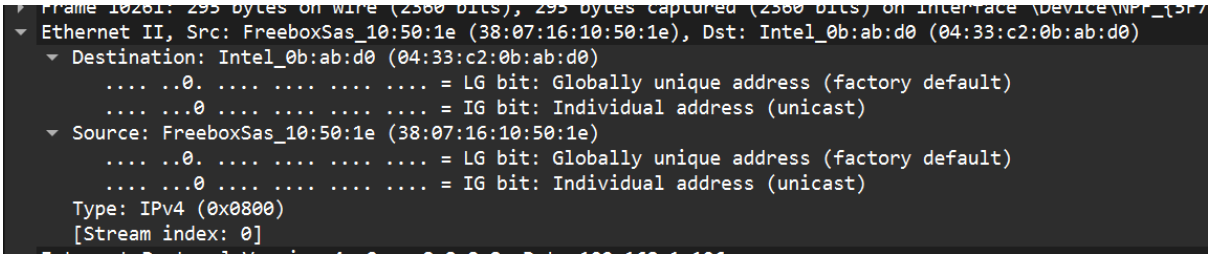


```
▾ Ethernet II, Src: Intel_0b:ab:d0 (04:33:c2:0b:ab:d0), Dst: FreeboxSas_10:50:1e (38:07:16:10:50:1e)
  ▾ Destination: FreeboxSas_10:50:1e (38:07:16:10:50:1e)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Intel_0b:ab:d0 (04:33:c2:0b:ab:d0)
      .... ..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: 192.168.1.196, Dst: 8.8.8.8
    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: 57
    Identification: 0xf961 (63841)
  ▾ 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...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: 192.168.1.196
    Destination Address: 8.8.8.8
    [Stream index: 7]
```

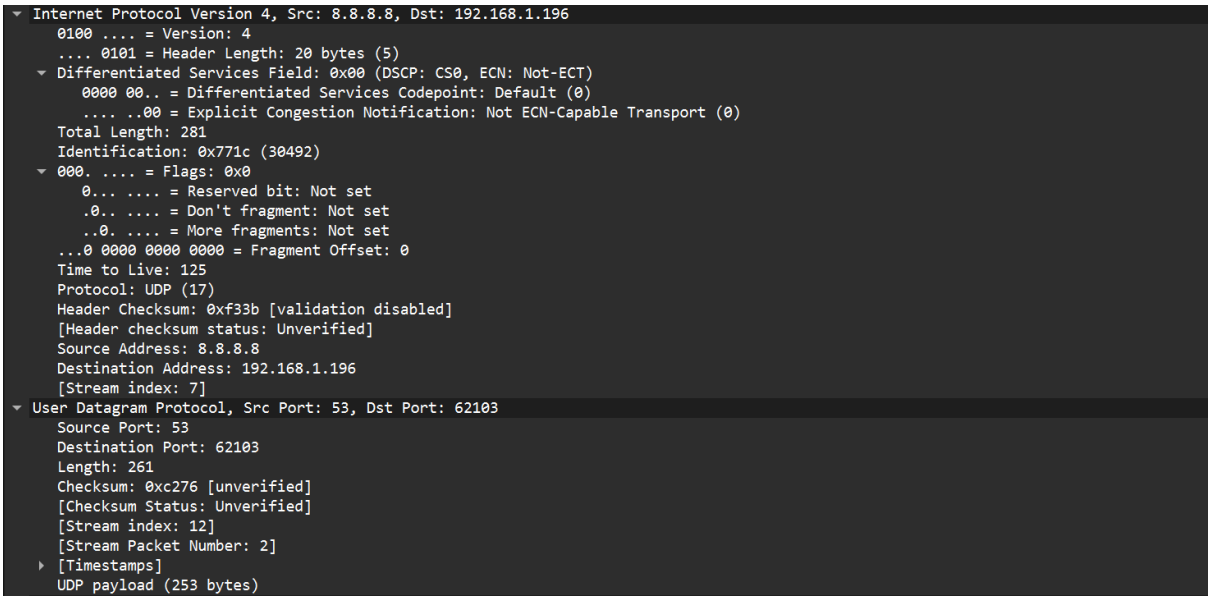
Esplorazione User Datagram Protocol (UDP) con visibilità di utilizzo porta 5 e query per il DNS su pacchtto Standard Query (invio):



Esplorazione Ethernet su pacchetto Standard Query Response (risposta):

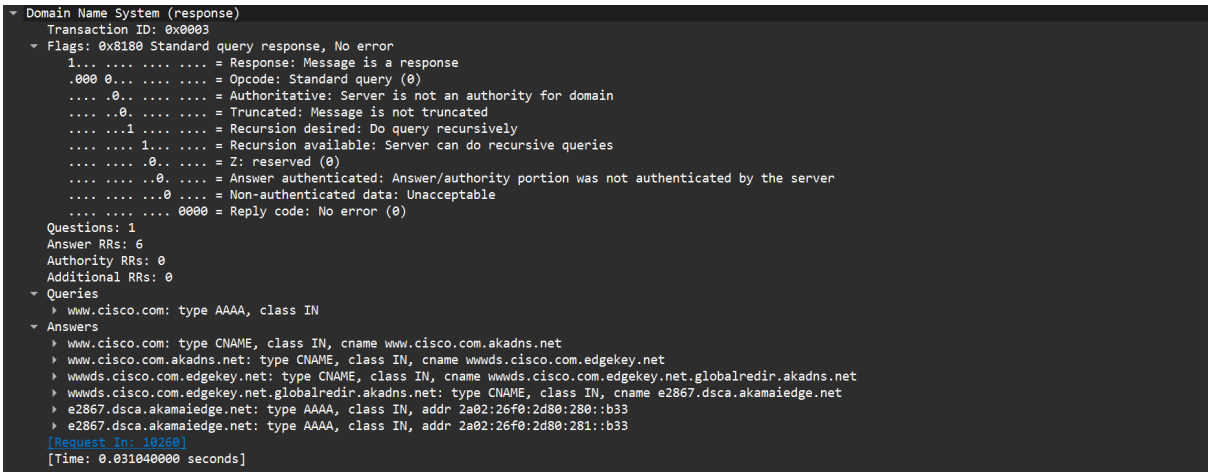


Esplorazione IPV4 e UDP su pacchetto Standard Query Response (risposta), evidenza che ora la porta di origine è 53 come ci aspettiamo da pacchetto UDP:



```
▾ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.196
    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: 281
    Identification: 0x771c (30492)
  ▾ 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 125
    Protocol: UDP (17)
    Header Checksum: 0xf33b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 8.8.8.8
    Destination Address: 192.168.1.196
    [Stream index: 7]
▾ User Datagram Protocol, Src Port: 53, Dst Port: 62103
    Source Port: 53
    Destination Port: 62103
    Length: 261
    Checksum: 0xc276 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 12]
    [Stream Packet Number: 2]
  ▸ [Timestamps]
    UDP payload (253 bytes)
```

Esplorazione DNS su pacchetto Standard Query Response (risposta), con evidenzia di gestione query recursion:



```
▾ Domain Name System (response)
    Transaction ID: 0x0003
  ▾ 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: 6
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.cisco.com: type AAAA, 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.edgekey.net
    ▸ wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadns.net
    ▸ wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
    ▸ e2867.dsca.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:2d80:280::b33
    ▸ e2867.dsca.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:2d80:281::b33
    [Request In: 10260]
    [Time: 0.031040000 seconds]
```