

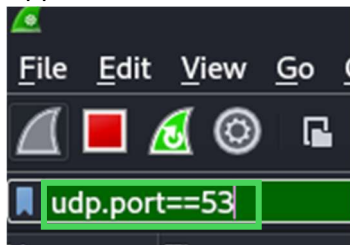
<https://itexamanswers.net/17-1-7-lab-exploring-dns-traffic-answers.html>

```

sudo systemctl status systemd-resolved
systemd-resolved.service - Network Name Resolution
  Loaded: loaded (/usr/lib/systemd/system/systemd-resolved.service; enabled; preset: enabled)
  Active: active (running) since Wed 2025-02-19 10:00:48 EST; 1min 43s ago
  Invocation: bf45db7d000942a08c9f8c13172a98b3
  Docs: man:systemd-resolved.service(8)
       man:org.freedesktop.resolve1(5)
       https://systemd.io/Writing_Network_Configuration_Managers
       https://systemd.io/Writing_Resolver_Clients
  Main PID: 18374 (systemd-resolve)
  Status: "Processing requests..."
  Tasks: 1 (limit: 2211)
  Memory: 3.5M (peak: 4M)
  CPU: 86ms
  CGroup: /system.slice/systemd-resolved.service
          └─18374 /usr/lib/systemd/systemd-resolved

```

Applico il filtro su wireshark:



Nella cattura non era presente [www.cisco.com](http://www.cisco.com) e quindi ho preso come riferimento [www.google.com](http://www.google.com)

No.	Time	Source	Destination	Protocol	Length	Info
166	6.392138451	192.168.214.30	192.168.214.110	DNS	74	Standard query 0x2357 A www.google.com
168	6.406911514	192.168.214.30	192.168.214.110	DNS	70	Standard query 0xa0be A adncdn.net
170	6.407107986	192.168.214.30	192.168.214.110	DNS	84	Standard query 0x72b6 A www.googletagmanager.com
179	6.494442521	192.168.214.110	192.168.214.30	DNS	90	Standard query response 0x2357 A www.google.com A 216.58.205.36
180	6.494443636	192.168.214.110	192.168.214.30	DNS	100	Standard query response 0x72b6 A www.googletagmanager.com A 216.58.205.40
191	6.511151003	192.168.214.110	192.168.214.30	DNS	134	Standard query response 0xa0be A adncdn.net A 108.138.199.90 A 108.138.199.60 A 108.138.1
290	6.924873506	192.168.214.30	192.168.214.110	DNS	75	Standard query 0xbbea A www.gstatic.com
294	6.95614537	192.168.214.110	192.168.214.30	DNS	91	Standard query response 0xbbea A www.gstatic.com A 142.250.180.131
500	58.608019632	192.168.214.30	192.168.214.110	DNS	76	Standard query 0xf7f0 A aus5.mozilla.org
501	58.608446727	192.168.214.30	192.168.214.110	DNS	76	Standard query 0xd758 AAAA aus5.mozilla.org
502	58.662767223	192.168.214.110	192.168.214.30	DNS	194	Standard query response 0xf7f0 A aus5.mozilla.org CNAME balrog-aus5-r53-2.services.mozill
503	58.666597397	192.168.214.110	192.168.214.30	DNS	206	Standard query response 0xd758 AAAA aus5.mozilla.org CNAME balrog-aus5-r53-2.services.moz
514	58.806326216	192.168.214.30	192.168.214.110	DNS	77	Standard query 0xeebe A ocsdp.digicert.com
515	58.806674801	192.168.214.30	192.168.214.110	DNS	77	Standard query 0x957a AAAA ocsdp.digicert.com
516	58.853320534	192.168.214.110	192.168.214.30	DNS	213	Standard query response 0xeebe A ocsdp.digicert.com CNAME ocsdp.edge.digicert.com CNAME cac
517	58.856038430	192.168.214.110	192.168.214.30	DNS	273	Standard query response 0x957a AAAA ocsdp.digicert.com CNAME ocsdp.edge.digicert.com CNAME
518	58.856426562	192.168.214.30	192.168.214.110	DNS	83	Standard query 0x3ede AAAA e3913.cd.akamaiedge.net
521	58.863599822	192.168.214.110	192.168.214.30	DNS	83	Standard query response 0x3ede AAAA e3913.cd.akamaiedge.net
545	59.082817325	192.168.214.30	192.168.214.110	DNS	95	Standard query 0x0165 A content-signature-2.cdn.mozilla.net
546	59.145430239	192.168.214.110	192.168.214.30	DNS	255	Standard query response 0x0165 A content-signature-2.cdn.mozilla.net CNAME content-signat

Da notare che nella sezione in basso, è presente la dicitura Ethernet II che se la espando:

```

Frame 166: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
  Ethernet II, Src: PCSSystemtec_6e:13:6e (08:00:27:00:13:6e), Dst: fe:c9:65:ca:8b:59 (fe:c9:65:ca:8b:59)
    Destination: fe:c9:65:ca:8b:59 (fe:c9:65:ca:8b:59)
      ... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
      ... ..0. .... = IG bit: Individual address (unicast)
    Source: PCSSystemtec_6e:13:6e (08:00:27:00:13:6e)
      ... ..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: 192.168.214.30, Dst: 192.168.214.110

```

Possiamo notare come sono presenti informazioni riguardo gli indirizzi mac sorgente e destinazione.

Andando ad espandere invece la sezione Internet Protocol Version 4:

```

Internet Protocol Version 4, Src: 192.168.214.30, Dst: 192.168.214.110
  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: 60
  Identification: 0x8c0c (35852)
  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: 64
  Protocol: UDP (17)
  Header Checksum: 0xc0c6 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.214.30
  Destination Address: 192.168.214.110
  [Stream index: 3]
  User Datagram Protocol, Src Port: 56005, Dst Port: 53

```

Sono presenti informazioni riguardo agli indirizzi IP sorgente e destinazione.

Espandendo poi User Datagram Protocol:

```

User Datagram Protocol, Src Port: 56005, Dst Port: 53
  Source Port: 56005
  Destination Port: 53
  Length: 40
  Checksum: 0x2e18 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Stream Packet Number: 1]
  [Timestamps]
    [Time since first frame: 0.000000000 seconds]
    [Time since previous frame: 0.000000000 seconds]
  UDP payload (32 bytes)

```

Sono presenti informazioni riguardo le porte di origine e destinazione.

se andiamo a confrontare gli indirizzi indicati, sono gli stessi se andiamo a scrivere sul terminale il comando `ip a`

espandendo Domain Name System:

```
▼ Domain Name System (query)
  Transaction ID: 0x2357
  ▼ 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.google.com: type A, class IN
      Name: www.google.com
      [Name Length: 14]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      [Response In: 179]
```

Possiamo notare come il flag è impostato per eseguire la query in maniera ricorsiva.

Adesso analizzo il pacchetto di risposta dal dominio [www.google.com](http://www.google.com)

No.	Time	Source	Destination	Protocol	Length	Info
166	6.397138451	192.168.214.30	192.168.214.110	DNS	74	Standard query 0x2357 A www.google.com
168	6.400911514	192.168.214.30	192.168.214.110	DNS	70	Standard query 0xa0be A adncdn.net
170	6.407107986	192.168.214.30	192.168.214.110	DNS	84	Standard query 0x72b6 A www.googletagmanager.com
179	6.494442521	192.168.214.110	192.168.214.30	DNS	90	Standard query response 0x2357 A www.google.com A 216.58.205.36
180	6.494443636	192.168.214.110	192.168.214.30	DNS	100	Standard query response 0x72b6 A www.googletagmanager.com A 216.58.205.36
191	6.511151003	192.168.214.110	192.168.214.30	DNS	134	Standard query response 0xa0be A adncdn.net A 108.138.199.90 A
290	6.924873506	192.168.214.30	192.168.214.110	DNS	75	Standard query 0xbbea A www.gstatic.com
294	6.985614537	192.168.214.110	192.168.214.30	DNS	91	Standard query response 0xbbea A www.gstatic.com A 142.250.180.101
500	58.608019632	192.168.214.30	192.168.214.110	DNS	76	Standard query 0xf7f0 A aus5.mozilla.org
501	58.608446727	192.168.214.30	192.168.214.110	DNS	76	Standard query 0xd758 AAAA aus5.mozilla.org

Frame 179: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface eth0  
 Ethernet II, Src: fe:c9:65:ca:8b:59 (fe:c9:65:ca:8b:59), Dst: PCSSystemtec\_6e:13:0e  
 Internet Protocol Version 4, Src: 192.168.214.110, Dst: 192.168.214.30  
 User Datagram Protocol, Src Port: 53, Dst Port: 56005  
 Domain Name System (response)

Possiamo notare come gli indirizzi mac sono ora invertiti dato che si tratta di una risposta.

Analizzando Domain Name System:

```

Domain Name System (response)
  Transaction ID: 0x2357
  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
  Queries
    www.google.com: type A, class IN
      Name: www.google.com
      [Name Length: 14]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  Answers
    www.google.com: type A, class IN, addr 216.58.205.36
    [Request In: 166]
    [Time: 0.097304070 seconds]
  
```

Possiamo notare che il DNS può gestire le query ricorsive e che il flag di risposta è attivo.