

## REPORT S11/L4

Sistema operativo utilizzato: kali linux

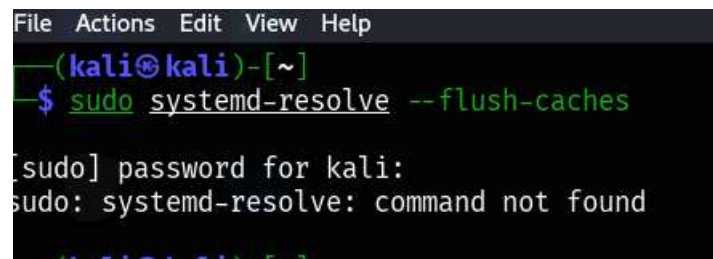
**Obiettivo del laboratorio:**

- 1 - Pulizia delle cache
  - 2 - Catturare pacchetti DNS (query e risposta)
  - 3 - Analizzare i risultati con Wireshark
  - 4 - Capire come funzionano e cosa rivelano
- 

**1- Pulizia cache:** tecnicamente il sistema kali linux non memorizza la cache ma per essere sicuri eseguiamo il comando:

`sudo systemd-resolve --flush-caches`

risultato:



```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo systemd-resolve --flush-caches
[sudo] password for kali:
sudo: systemd-resolve: command not found
```

questo comando funziona su sistemi operativi come Ubuntu...

Ma Kali Linux, di default, non usa un caching DNS come detto in precedenza, quindi il comando non esiste.

### 2 - Catturare pacchetti DNS (query e risposta)

Avviamo wireshark con il comando:

`sudo whireshark`

selezioniamo eth0 e poi clicchiamo start capturing packet

```
(kali㉿kali)-[~]
$ sudo wireshark

** (wireshark:6501) 14:52:02.814174 [Capture MESSAGE] -- Capture Start ...
** (wireshark:6501) 14:52:02.951919 [Capture MESSAGE] -- Capture started
** (wireshark:6501) 14:52:02.951978 [Capture MESSAGE] -- File: "/tmp/wireshark_eth04RQW42.pcapng"
```

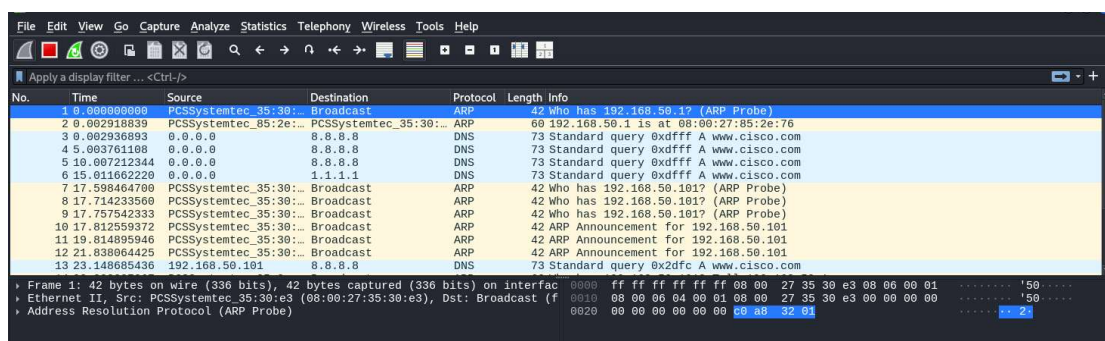
Nel frattempo su un altro terminale facciamo partire la connessione al sito [www.cisco.com](http://www.cisco.com)

```
(kali㉿kali)-[~]
$ nslookup www.cisco.com

Server:      8.8.8.8
Address:     8.8.8.8#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: 2.22.33.46
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:dc:396::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:dc:39b::b33
```

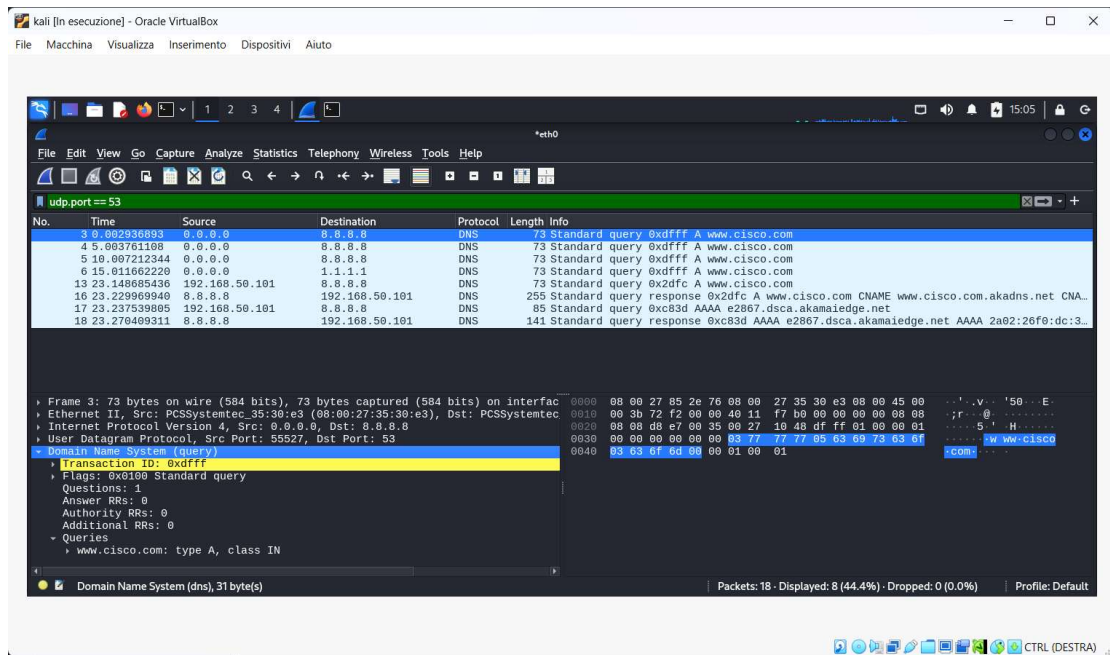
Nel frattempo su whiresark:



### 3 - Analizzare i risultati con Wireshark

dopo aver cliccato su "Stop capturing packets" per interrompere la cattura di Wireshark, passiamo ora all' Analisi del Pacchetto DNS con il filtro:

**udp.port == 53**



1) ethernet II: dà gli indirizzi MAC

+

2) Internet protocol version 4: ci da gli indirizzi IP

```

▼ Ethernet II, Src: PCSSystemtec_35:30:e3 (08:00:27:35:30:e3), Dst: PCSSystemtec
  ▼ Destination: PCSSystemtec_85:2e:76 (08:00:27:85:2e:76)
    .... 0. .... = LG bit: Globally unique address (factory)
    .... 0. .... = IG bit: Individual address (unicast)
  ▼ Source: PCSSystemtec_35:30:e3 (08:00:27:35:30:e3)
    .... 0. .... = LG bit: Globally unique address (factory)
    .... 0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 1]
▼ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 8.8.8.8
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 59
  Identification: 0x72f2 (29426)
  ▶ 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0xf7b0 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 0.0.0.0
  Destination Address: 8.8.8.8
  [Stream index: 0]

```

3 . User Datagram Protocol : ci da la porta SORGENTE e la DESTINAZIONE

```

▼ User Datagram Protocol, Src Port: 55527, Dst Port: 53
  Source Port: 55527
  Destination Port: 53
  Length: 39
  Checksum: 0x1048 [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 (31 bytes)

```

#### 4. Domain Name System (query)

```

  UDP payload (31 bytes)
▼ Domain Name System (query)
  ▼ Transaction ID: 0xdfff
    ▼ [Expert Info (Warning/Protocol): DNS response missing]
      [DNS response missing]
      [Severity level: Warning]
      [Group: Protocol]
    ▼ 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

```