

# CAPTURE DNS TRAFFIC

```
(kali㉿kali)-[~]
$ nslookup
> www.cisco.com
Server:      192.168.50.1
Address:     192.168.50.1#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: 23.51.50.61
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:df:6b3::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:df:692::b33
```

Osservo il traffico catturato nel pannello Packet List di Wireshark. Inserisco il filtro **udp.port == 53** nell'apposita barra dei filtri per visualizzare esclusivamente i pacchetti DNS.

No.	Time	Source	Destination	Protocol	Length	Info
13	5.349440947	192.168.50.100	192.168.50.1	DNS	87	Standard query 0x0291 A service
14	5.349536855	192.168.50.100	192.168.50.1	DNS	87	Standard query 0xb39e AAAA serv
15	5.392883640	192.168.50.100	192.168.50.1	DNS	89	Standard query 0xefc9 A locatio
16	5.392970328	192.168.50.100	192.168.50.1	DNS	89	Standard query 0x59c5 AAAA loca
80	5.892395590	192.168.50.1	192.168.50.100	DNS	151	Standard query response 0x0291
81	6.044888672	192.168.50.1	192.168.50.100	DNS	167	Standard query response 0xefc9
82	6.054951906	192.168.50.1	192.168.50.100	DNS	168	Standard query response 0xb39e
91	6.149914511	192.168.50.1	192.168.50.100	DNS	241	Standard query response 0x59c5
120	6.253590449	192.168.50.100	192.168.50.1	DNS	76	Standard query 0x854b A aus5.mc
121	6.253692143	192.168.50.100	192.168.50.1	DNS	76	Standard query 0x684d AAAA aus5
154	7.208257084	192.168.50.1	192.168.50.100	DNS	268	Standard query response 0x684d
155	7.274083061	192.168.50.1	192.168.50.100	DNS	194	Standard query response 0x854b
176	7.387674864	192.168.50.100	192.168.50.1	DNS	77	Standard query 0x935c A ocs.p.d
177	7.387751586	192.168.50.100	192.168.50.1	DNS	77	Standard query 0x6b59 AAAA ocs.p
178	7.389830254	192.168.50.1	192.168.50.100	DNS	77	Standard query response 0x6b59
179	7.389830476	192.168.50.1	192.168.50.100	DNS	77	Standard query response 0x935c
180	7.389996515	192.168.50.100	8.8.8.8	DNS	77	Standard query 0x935c A ocs.p.d
181	7.390053587	192.168.50.100	8.8.8.8	DNS	77	Standard query 0x6b59 AAAA ocs.p
184	7.441387189	8.8.8.8	192.168.50.100	DNS	182	Standard query response 0x935c
185	7.441387211	8.8.8.8	192.168.50.100	DNS	194	Standard query response 0x6b59
226	7.791249891	192.168.50.100	192.168.50.1	DNS	79	Standard query 0x95b3 A archive
229	7.791317741	192.168.50.100	192.168.50.1	DNS	79	Standard query 0xbcb1 AAAA arch
245	7.859023767	192.168.50.1	192.168.50.100	DNS	95	Standard query response 0x95b3

▶ Frame 13: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface eth0, id 0  
 ▶ Ethernet II, Src: PCSSystemtec\_d2:26:79 (08:00:27:d2:26:79), Dst: PCSSystemtec\_9a:45:1e (08:00:27:9a:45:1e)  
 ▶ Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.1  
 ▶ User Datagram Protocol, Src Port: 39875, Dst Port: 53  
 ▶ Domain Name System (query)

What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?

765	36.432437482	192.168.50.100	192.168.50.1	DNS	76	Standard query 0x7d20 A target.ci
766	36.432647745	192.168.50.100	192.168.50.1	DNS	76	Standard query 0xdf26 AAAA target
767	36.433824949	192.168.50.100	192.168.50.1	DNS	78	Standard query 0xd858 A smetrics.
768	36.433903187	192.168.50.100	192.168.50.1	DNS	78	Standard query 0x5555 AAAA smetri
769	36.435018885	192.168.50.100	192.168.50.1	DNS	89	Standard query 0x568a A ciscosyst
770	36.435088038	192.168.50.100	192.168.50.1	DNS	89	Standard query 0x5c8d AAAA ciscos
771	36.435912906	192.168.50.1	192.168.50.100	DNS	76	Standard query response 0x7d20 Se
772	36.438027661	192.168.50.1	192.168.50.100	DNS	76	Standard query response 0xdf26 Se
773	36.439506629	192.168.50.100	8.8.8.8	DNS	76	Standard query 0x7d20 A target.ci
774	36.439573009	192.168.50.100	8.8.8.8	DNS	76	Standard query 0xdf26 AAAA target
775	36.439833202	192.168.50.1	192.168.50.100	DNS	78	Standard query response 0xd858 Se
776	36.440519401	192.168.50.1	192.168.50.100	DNS	78	Standard query response 0x5555 Se
777	36.440581590	192.168.50.100	8.8.8.8	DNS	78	Standard query 0xd858 A smetrics.
778	36.440710239	192.168.50.100	8.8.8.8	DNS	78	Standard query 0x5555 AAAA smetri
779	36.440903281	192.168.50.1	192.168.50.100	DNS	89	Standard query response 0x568a Se
780	36.441361420	192.168.50.1	192.168.50.100	DNS	89	Standard query response 0x5c8d Se
781	36.441489221	192.168.50.100	8.8.8.8	DNS	89	Standard query 0x568a A ciscosyst
782	36.441542797	192.168.50.100	8.8.8.8	DNS	89	Standard query 0x5c8d AAAA ciscos
783	36.460017670	192.168.50.100	192.168.50.1	DNS	72	Standard query 0xd8a8 A rum.hlx.p

▶ Frame 765: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0  
 ▶ Ethernet II, Src: PCSSystemtec\_d2:26:79 (08:00:27:d2:26:79), Dst: PCSSystemtec\_9a:45:1e (08:00:27:9a:45:1e)  
 ▶ Destination: PCSSystemtec\_9a:45:1e (08:00:27:9a:45:1e)  
 Address: PCSSystemtec\_9a:45:1e (08:00:27:9a:45:1e)  
 .... 0. .... = LG bit: Globally unique address (factory default)  
 .... 0. .... = IG bit: Individual address (unicast)  
 ▶ Source: PCSSystemtec\_d2:26:79 (08:00:27:d2:26:79)  
 Address: PCSSystemtec\_d2:26:79 (08:00:27:d2:26:79)  
 .... 0. .... = LG bit: Globally unique address (factory default)  
 .... 0. .... = IG bit: Individual address (unicast)  
 Type: IPv4 (0x0800)  
 ▶ Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.1  
 ▶ User Datagram Protocol, Src Port: 46699, Dst Port: 53  
 ▶ Domain Name System (query)

What are the source and destination IP addresses? Which network interfaces are these IP addresses associated with?

No.	Time	Source	Destination	Protocol	Length	Info
709	35.783985861	8.8.8.8	192.168.50.100	DNS	255	Standard query response 0x0c91
722	35.940859818	192.168.50.100	192.168.50.1	DNS	73	Standard query 0x34e4 A www.cis
723	35.941008326	192.168.50.100	192.168.50.1	DNS	73	Standard query 0x9ae6 AAAA www.
724	35.943738811	192.168.50.1	192.168.50.100	DNS	73	Standard query response 0x9ae6
725	35.943739262	192.168.50.1	192.168.50.100	DNS	73	Standard query response 0x34e4
726	35.943985402	192.168.50.100	8.8.8.8	DNS	73	Standard query 0x34e4 A www.cis
727	35.944342518	192.168.50.100	8.8.8.8	DNS	73	Standard query 0x9ae6 AAAA www.
728	36.050138552	8.8.8.8	192.168.50.100	DNS	295	Standard query response 0x9ae6
729	36.050138764	8.8.8.8	192.168.50.100	DNS	255	Standard query response 0x34e4
765	36.432437482	192.168.50.100	192.168.50.1	DNS	76	Standard query 0x7d20 A target.
766	36.432647745	192.168.50.100	192.168.50.1	DNS	76	Standard query 0xdf26 AAAA targ
767	36.433824949	192.168.50.100	192.168.50.1	DNS	78	Standard query 0xd858 A smetric
768	36.433903187	192.168.50.100	192.168.50.1	DNS	78	Standard query 0x5555 AAAA smet
769	36.435018885	192.168.50.100	192.168.50.1	DNS	89	Standard query 0x568a A ciscosy
770	36.435088038	192.168.50.100	192.168.50.1	DNS	89	Standard query 0x5c8d AAAA cisc
771	36.435912906	192.168.50.1	192.168.50.100	DNS	76	Standard query response 0x7d20
772	36.438027661	192.168.50.1	192.168.50.100	DNS	76	Standard query response 0xdf26
773	36.439506629	192.168.50.100	8.8.8.8	DNS	76	Standard query 0x7d20 A target.
774	36.439573009	192.168.50.100	8.8.8.8	DNS	76	Standard query 0xdf26 AAAA targ
775	36.439833202	192.168.50.1	192.168.50.100	DNS	78	Standard query response 0xd858
776	36.440519401	192.168.50.1	192.168.50.100	DNS	78	Standard query response 0x5555
777	36.440581590	192.168.50.100	8.8.8.8	DNS	78	Standard query 0xd858 A smetric
778	36.440710239	192.168.50.100	8.8.8.8	DNS	78	Standard query 0x5555 AAAA smet

▶ Frame 765: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0  
 ▶ Ethernet II, Src: PCSSystemtec\_d2:26:79 (08:00:27:d2:26:79), Dst: PCSSystemtec\_9a:45:1e (08:00:27:9a:45:1e)  
 ▶ Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.1  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 62  
 Identification: 0x28be (10430)  
 ▶ 010. .... = Flags: 0x2, Don't fragment  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 64  
 Protocol: UDP (17)  
 Header Checksum: 0x2c3b [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 192.168.50.100  
 Destination Address: 192.168.50.1  
 ▶ User Datagram Protocol, Src Port: 46699, Dst Port: 53  
 ▶ Domain Name System (query)

What are the source and destination ports? What is the default DNS port number?

765	36.432437482	192.168.50.100	192.168.50.1	DNS	76	Standard query 0x7d20 A target.c
766	36.432647745	192.168.50.100	192.168.50.1	DNS	76	Standard query 0xdf26 AAAA target.c
767	36.433824949	192.168.50.100	192.168.50.1	DNS	78	Standard query 0xd858 A smetrics
768	36.433903187	192.168.50.100	192.168.50.1	DNS	78	Standard query 0x5555 AAAA smet
769	36.435018885	192.168.50.100	192.168.50.1	DNS	89	Standard query 0x568a A ciscosys
770	36.435088038	192.168.50.100	192.168.50.1	DNS	89	Standard query 0x5c8d AAAA cisco
771	36.435912906	192.168.50.1	192.168.50.100	DNS	76	Standard query response 0x7d20 S
772	36.438027661	192.168.50.1	192.168.50.100	DNS	76	Standard query response 0xdf26 S
773	36.439506629	192.168.50.100	8.8.8.8	DNS	76	Standard query 0x7d20 A target.c
774	36.439573009	192.168.50.100	8.8.8.8	DNS	76	Standard query 0xdf26 AAAA target.c
775	36.439833202	192.168.50.1	192.168.50.100	DNS	78	Standard query response 0xd858 S
776	36.440519401	192.168.50.1	192.168.50.100	DNS	78	Standard query response 0x5555 S
777	36.440581590	192.168.50.100	8.8.8.8	DNS	78	Standard query 0xd858 A smetrics
778	36.440710239	192.168.50.100	8.8.8.8	DNS	78	Standard query 0x5555 AAAA smet
779	36.440903281	192.168.50.1	192.168.50.100	DNS	89	Standard query response 0x568a S
780	36.441361420	192.168.50.1	192.168.50.100	DNS	89	Standard query response 0x5c8d S
781	36.441489221	192.168.50.100	8.8.8.8	DNS	89	Standard query 0x568a A ciscosys
782	36.441542797	192.168.50.100	8.8.8.8	DNS	89	Standard query 0x5c8d AAAA cisco
783	36.460017670	192.168.50.100	192.168.50.1	DNS	72	Standard query 0xd8a8 A rum.hlx

▶ Frame 765: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0  
▶ Ethernet II, Src: PCSSystemtec\_d2:26:79 (08:00:27:d2:26:79), Dst: PCSSystemtec\_9a:45:1e (08:00:27:9a:45:1e)  
▶ Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.1  
▼ User Datagram Protocol, Src Port: 46699, Dst Port: 53  
    Source Port: 46699  
    Destination Port: 53  
    Length: 42  
    Checksum: 0xe5f1 [unverified]  
    [Checksum Status: Unverified]  
    [Stream index: 18]  
    ▶ [Timestamps]  
        UDP payload (34 bytes)  
▶ Domain Name System (query)

Determine the IP and MAC address of the PC.

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255
    inet6 fe80::6777:46f0:35e4:3bfa prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:d2:26:79 txqueuelen 1000 (Ethernet)
    RX packets 6647 bytes 6777691 (6.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4187 bytes 568799 (555.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 48 bytes 2480 (2.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 48 bytes 2480 (2.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Expand **Domain Name System (query)** in the Packet Details pane. Then expand the **Flags** and **Queries**.

```
▼ Domain Name System (query)
  Transaction ID: 0x7d20
  ▼ 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
    ▼ target.cisco.com: type A, class IN
      Name: target.cisco.com
      [Name Length: 16]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
```

Expand **Domain Name System (response)**. Then expand the **Flags**, **Queries**, and **Answers**.

```
▼ Domain Name System (response)
  Transaction ID: 0x7d20
  ▼ Flags: 0x8182 Standard query response, Server failure
    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
    .... ....0010 = Reply code: Server failure (2)
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
```

```
▼ Domain Name System (response)
  Transaction ID: 0xdf6
  ► Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ e2867.dsca.akamaiedge.net: type AAAA, class IN
      Name: e2867.dsca.akamaiedge.net
      [Name Length: 25]
      [Label Count: 4]
      Type: AAAA (28) (IP6 Address)
      Class: IN (0x0001)
  ▼ Answers
    ► e2867.dsca.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:df:6b3::b33
    ► e2867.dsca.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:df:692::b33
  [Request In: 3]
  [Time: 0.137299038 seconds]
```