

ESPLORAZIONE DEL TRAFFICO DNS

Dopo aver installato Wireshark, cancelliamo la cache DNS inserendo nel terminale comando specifico per Windows "ipconfig /flushdns".

```
Microsoft Windows [Versione 10.0.26100.3775]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\andre>ipconfig /flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.

C:\Users\andre>
```

Avviamo Wireshark e attiviamo la cattura del traffico dei pacchetti. Sul terminale inseriamo il comando "nslookup www.cisco.com" per interrogare il dominio.

```
Microsoft Windows [Versione 10.0.26100.3775]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\andre>ipconfig /flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.

C:\Users\andre>nslookup www.cisco.com
Server:  UnKnown
Address:  10.2.0.1

Risposta da un server non autorevole:
Nome:      e2867.dsca.akamaiedge.net
Addresses: 2001:41a8:47:a83::b33
           2001:41a8:47:a81::b33
           2.18.1.94
Aliases:   www.cisco.com
           www.cisco.com.akadns.net
           wwwds.cisco.com.edgekey.net
           wwwds.cisco.com.edgekey.net.globalredir.akadns.
net

C:\Users\andre>
```

Su Wireshark stoppiamo la cattura ed inseriamo il filtro “udp.port == 53”. Tra i pacchetti che vi vengono proposti, andiamo a selezionare la stringa che ha “Standard query 0x0002 A www.cisco.com” tra le info.

udp.port == 53

No.	Time	Source	Destination	Protocol	Length	Info
259	5.775491	192.168.1.8	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
260	5.776865	192.168.1.1	192.168.1.8	DNS	128	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR H388X.homenet.telecomitalia.it
261	5.777584	192.168.1.8	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
263	5.786182	192.168.1.1	192.168.1.8	DNS	271	Standard query response 0x0002 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME
264	5.788696	192.168.1.8	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
266	5.811797	192.168.1.1	192.168.1.8	DNS	311	Standard query response 0x0003 AAAA www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net C
285	6.118869	192.168.1.8	192.168.1.1	DNS	79	Standard query 0x74ca A clients4.google.com
286	6.119162	192.168.1.8	192.168.1.1	DNS	79	Standard query 0x080f HTTPS clients4.google.com
287	6.127311	192.168.1.1	192.168.1.8	DNS	129	Standard query response 0x74ca A clients4.google.com CNAME clients1.google.com A 216.58.204.238
288	6.129441	192.168.1.1	192.168.1.8	DNS	163	Standard query response 0x080f HTTPS clients4.google.com CNAME clients1.google.com SOA ns1.google.com

> Frame 259: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{ABCC8F15-0000-4459-436F-0084} 49 43 6F 00 84 4C 49 6C 5C 70 0B 08 00 45 00 DYCo...LI l\p...E-
> Ethernet II, Src: Intel_5c:70:0b (4c:49:6c:5c:70:0b), Dst: zte_6f:00:84 (44:59:43:6f:00:84) 0010 00 46 1f 5e 00 00 00 11 00 00 c0 a8 01 08 c0 a8 :F... ..
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 192.168.1.1 0020 01 01 fe fe 00 35 00 32 83 9d 00 01 01 00 00 01S.2.....
> User Datagram Protocol, Src Port: 65278, Dst Port: 53 0030 00 00 00 00 00 01 31 01 31 03 31 36 38 03 311.1.168.1
> Domain Name System (query) 0040 39 32 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 92-in-ad dr-arpa-
0050 00 0c 00 01 00 0c 00 01

Qui notiamo nel riquadro Packet Details che questo pacchetto ha:

Ethernet II, Internet Protocol Version 4, User Datagram Protocol e Domain Name System (query).

Andando ad espandere la sezione Ethernet II noteremo gli indirizzi MAC di origine (4c:49:6c:5c:70:0b riferito alla NIC del PC) e di destinazione (44:59:43:6f:00:84 riferito al Gateway).

ANALISI DEGLI INDIRIZZI IP E PORTE

ELEMENTO	ORIGINE	DESTINAZIONE
INDIRIZZO MAC	NIC DEL PC	GATEWAY PREDEFINITO
INDIRIZZO IP	192.168.1.8	192.168.1.1
PORTA	65279	53

Come controprova sul terminale sul terminale inseriamo i comandi “arp -a” e “ipconfig /all”

Noteremo che l'indirizzo MAC del nostro PC è lo stesso catturato da Wireshark

```
Scheda LAN wireless Wi-Fi:

Suffisso DNS specifico per connessione: homenet.telecomitalia.it
Descrizione . . . . . : Intel(R) Wi-Fi 6 AX101
Indirizzo fisico. . . . . : 4C-49-6C-5C-70-0B
DHCP abilitato. . . . . : Sì
Configurazione automatica abilitata : Sì
Indirizzo IPv4. . . . . : 192.168.1.8(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Lease ottenuto. . . . . : mercoledì 9 aprile 2025 21:07:32
Scadenza lease . . . . . : venerdì 11 aprile 2025 08:32:35
Gateway predefinito . . . . . : 192.168.1.1
Server DHCP . . . . . : 192.168.1.1
Server DNS . . . . . : 192.168.1.1
NetBIOS su TCP/IP . . . . . : Attivato
```

DETTAGLI DELLA QUERY DNS

Analisi Domain Name System (query)

```
> User Datagram Protocol, Src Port: 65279, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x0002
  ▼ 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
    [Response In: 263]
```

Espandendo Domain Name System (query), ed espandere Flags e Queries, possiamo notare che la query DNS contiene:

- Identificatore della transazione
- Flag per la query ricorsiva
- Dominio richiesto (www.cisco.com)
- Tipo di record richiesto (A)

ESPLORAZIONE DEL TRAFFICO DI RISPOSTA DNS

Per questo passaggio prendiamo in esame il pacchetto DNS di risposta che ha “Standard query response – A www.cisco.com” nella colonna info

No.	Time	Source	Destination	Protocol	Leng	Info
259	5.775491	192.168.1.8	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
260	5.776865	192.168.1.1	192.168.1.8	DNS	128	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR H388X.homenet.telecomitalia.it
261	5.777584	192.168.1.8	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
263	5.786182	192.168.1.1	192.168.1.8	DNS	271	Standard query response 0x0002 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME www.cisco.com.edgekey.net CNAME www.cisco.com.edgekey..
264	5.788696	192.168.1.8	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
266	5.811797	192.168.1.1	192.168.1.8	DNS	311	Standard query response 0x0003 AAAA www.cisco.com CNAME www.cisco.com.akadns.net CNAME www.cisco.com.edgekey.net CNAME www.cisco.com.edge..
285	6.118860	192.168.1.8	192.168.1.1	DNS	79	Standard query 0x74ca A clients4.google.com
286	6.119162	192.168.1.8	192.168.1.1	DNS	79	Standard query 0x880f HTTPS clients4.google.com
287	6.127311	192.168.1.1	192.168.1.8	DNS	129	Standard query response 0x74ca A clients4.google.com CNAME clients.l.google.com A 216.58.204.238
288	6.129441	192.168.1.1	192.168.1.8	DNS	163	Standard query response 0x880f HTTPS clients4.google.com CNAME clients.l.google.com SOA ns1.google.com

> Frame 263: 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits) on interface \Device\NPF_{ABCC8F15-1A6F-4E77-87B9-1B2EBF22FEB8}, id 0	0000	4c 49 6c 5c 70 0b 44 59 43 6f e
▼ Ethernet II, Src: zte_6f:00:84 (44:59:43:6f:00:84), Dst: Intel_5c:70:0b (4c:49:6c:5c:70:0b)	0010	01 01 b3 03 40 00 40 11 03 8f c
> Destination: Intel_5c:70:0b (4c:49:6c:5c:70:0b)	0020	01 08 00 35 fe ff 00 ed ce f7 e
> Source: zte_6f:00:84 (44:59:43:6f:00:84)	0030	00 05 00 00 00 00 03 77 77 77 e
Type: IPv4 (0x0800)	0040	03 63 6f 6d 00 00 01 00 01 c0 e
[Stream index: 0]	0050	00 08 67 00 1a 03 77 77 77 05 e
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.8	0060	63 6f 6d 06 61 6b 61 64 6e 73 e
> User Datagram Protocol, Src Port: 53, Dst Port: 65279	0070	2b 00 05 00 01 00 00 01 12 00 1
> Domain Name System (response)	0080	73 05 63 69 73 63 6f 03 63 6f e
	0090	6b 65 79 03 6e 65 74 00 c0 51 e
	00a0	44 2b 00 34 05 77 77 77 64 73 e
	00b0	03 63 6f 6d 07 65 64 67 65 6b e
	00c0	0b 67 6c 6f 62 61 6c 72 65 64 e
	00d0	64 6e 73 03 6e 65 74 00 c0 7a e
	00e0	09 6e 00 1b 05 65 32 38 36 37 e
	00f0	61 6b 61 6d 61 69 65 64 67 65 e
	0100	ba 00 01 00 01 00 00 00 0b 00 e

ANALISI DEGLI INDIRIZZI IP E PORTE

ELEMENTO	ORIGINE	DESTINAZIONE
INDIRIZZO MAC	GATEWAY PREDEFINITO	NIC DEL PC
INDIRIZZO IP	192.168.1.1	192.168.1.8
PORTA	53	65279

Espandendo Domain Name System (response), poi Flags, Queries e Answers potremmo vedere quanto segue

```

> Frame 263: 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits) on interface
> Ethernet II, Src: zte_6f:00:84 (44:59:43:6f:00:84), Dst: Intel_5c:70:0b (4c:49:6c:5
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.8
> User Datagram Protocol, Src Port: 53, Dst Port: 65279
✓ Domain Name System (response)
  Transaction ID: 0x0002
  ✓ 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 a
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 5
  Authority RRs: 0
  Additional RRs: 0
  ✓ Queries
    > www.cisco.com: type A, 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.
    > wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey
    > wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname
    > e2867.dsca.akamaiedge.net: type A, class IN, addr 23.32.112.103
  [Request In: 261]
  [Time: 0.008598000 seconds]

```

Possiamo notare che il DNS può gestire query ricorsive.