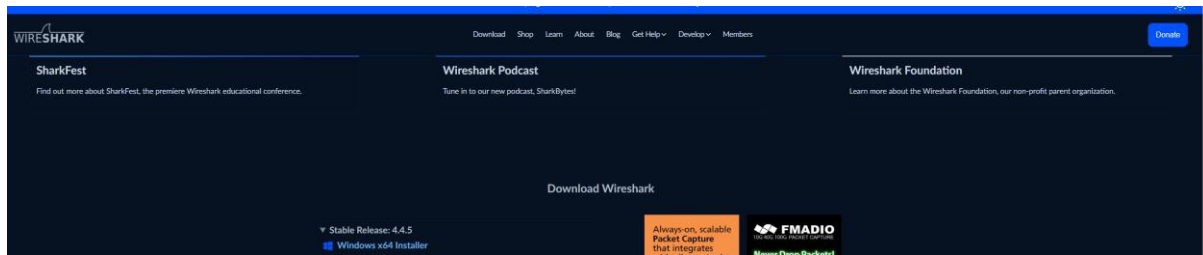
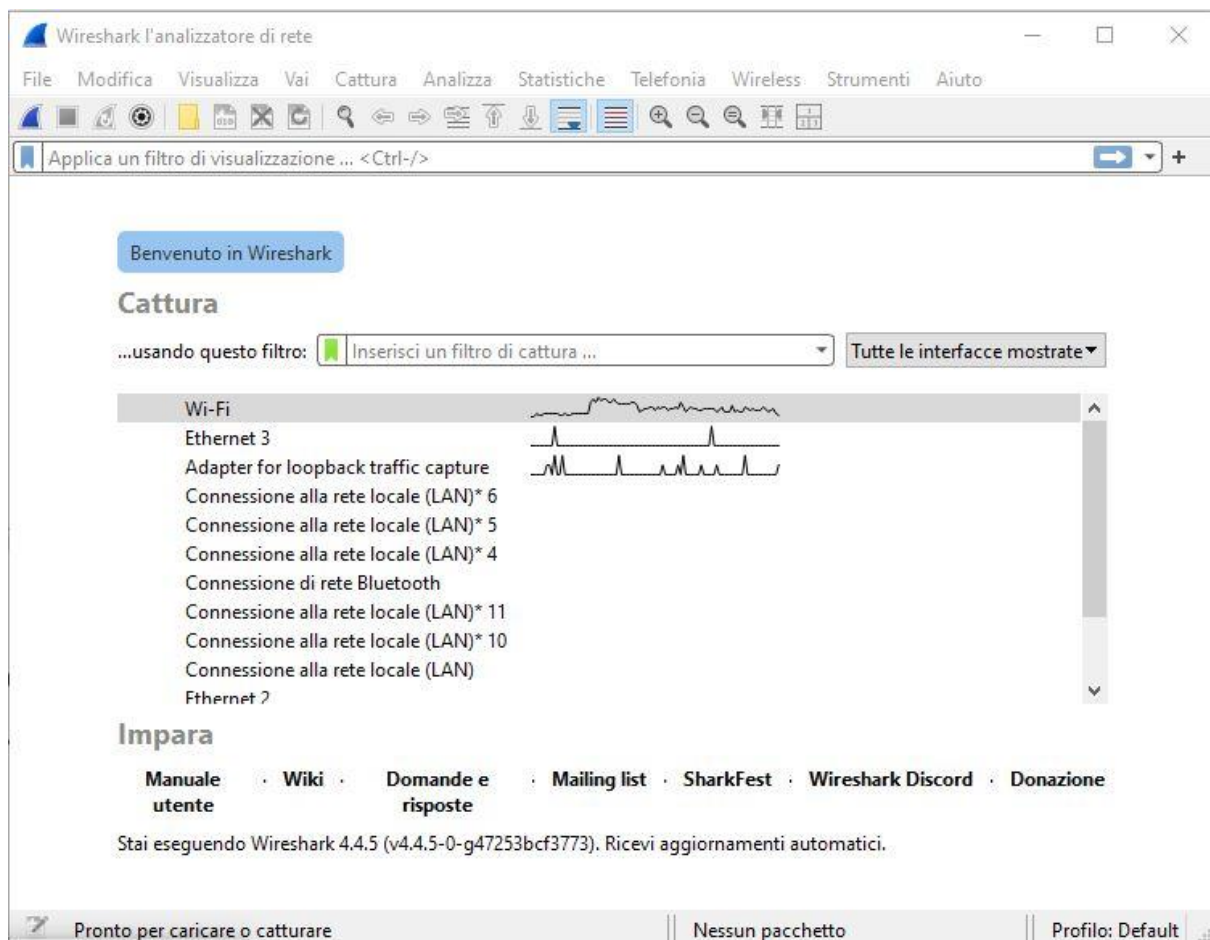


Esplorazione del Traffico DNS



Avviare la cattura in Wireshark

Selezionare un'interfaccia attiva con traffico per la cattura dei pacchetti



Cancellare la cache DNS

Utilizzare i comandi appropriati per il proprio sistema operativo

- Windows: `ipconfig /flushdns`

```

Prompt dei comandi
Microsoft Windows [Versione 10.0.19045.5737]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\giang> ipconfig /flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.

C:\Users\giang>

```

Eseguire query DNS

Utilizzare nslookup per interrogare un dominio come www.cisco.com

```

Prompt dei comandi
Microsoft Windows [Versione 10.0.19045.5737]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\giang> ipconfig /flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.

C:\Users\giang> nslookup www.cisco.com
Server:  vodafone.station
Address:  fe80::1614:59ff:fe38:82b0

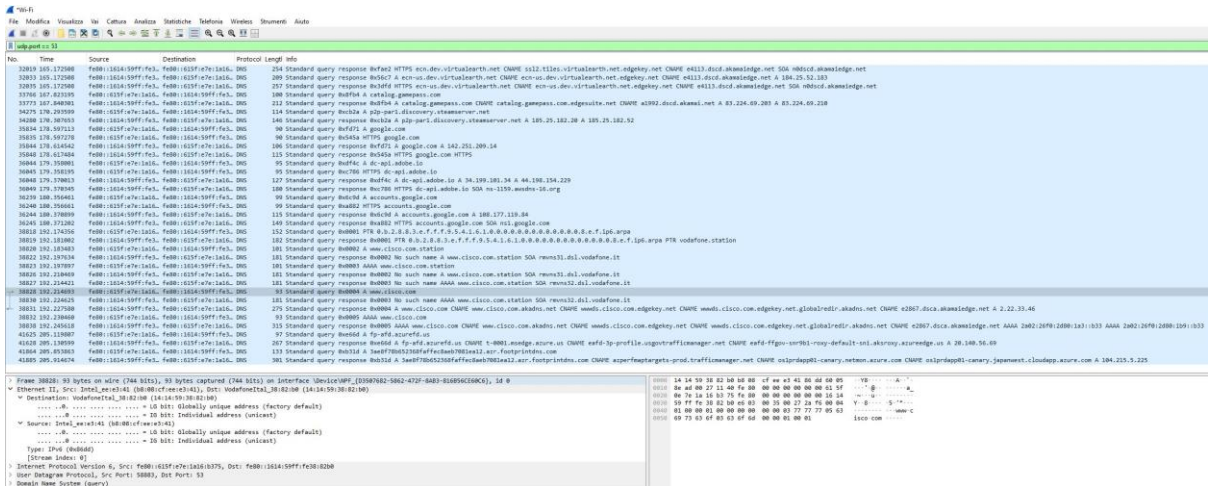
Risposta da un server non autorevole:
Nome:    e2867.dsca.akamaiedge.net
Addresses:  2a02:26f0:2d80:1a3::b33
            2a02:26f0:2d80:1b9::b33
            2.22.33.46
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net

C:\Users\giang>

```

Analisi del Pacchetto DNS

Osservare il traffico catturato nel riquadro Packet List di Wireshark. Inserire `udp.port == 53` nella casella del filtro e fare clic sulla freccia (o premere invio) per visualizzare solo i pacchetti DNS. Selezionare il pacchetto DNS che contiene "Standard query" e "A www.cisco.com" nella colonna Info. Nel riquadro Packet Details, notare che questo pacchetto ha Ethernet II, Internet Protocol Version 4, User Datagram Protocol e Domain Name System (query). Espandere Ethernet II per visualizzare i dettagli. Osservare i campi di origine e destinazione.



In un prompt dei comandi Windows, inserire `arp -a` e `ipconfig /all` per registrare gli indirizzi MAC e IP del PC.

```
C:\Users\giang> arp -a

Interface: 192.168.56.1 --- 0xa
Indirizzo Internet    Indirizzo fisico    Tipo
192.168.56.255        ff-ff-ff-ff-ff-ff  statico
224.0.0.22            01-00-5e-00-00-16  statico
224.0.0.251           01-00-5e-00-00-fb  statico
224.0.0.252           01-00-5e-00-00-fc  statico
239.255.255.250       01-00-5e-7f-ff-fa  statico

Interface: 192.168.1.7 --- 0x11
Indirizzo Internet    Indirizzo fisico    Tipo
192.168.1.1           14-14-59-38-82-b0  dinamico
192.168.1.2           64-66-24-99-c4-a3  dinamico
192.168.1.255         ff-ff-ff-ff-ff-ff  statico
224.0.0.22            01-00-5e-00-00-16  statico
224.0.0.251           01-00-5e-00-00-fb  statico
224.0.0.252           01-00-5e-00-00-fc  statico
239.255.255.250       01-00-5e-7f-ff-fa  statico
255.255.255.255       ff-ff-ff-ff-ff-ff  statico
```

```
C:\Users\giang> ipconfig /all
```

Configurazione IP di Windows

```
Nome host . . . . . : LAPTOP-LIUT6STS
Suffisso DNS primario . . . . . :
Tipo nodo . . . . . : Ibrido
Routing IP abilitato. . . . . : No
Proxy WINS abilitato . . . . . : No
Elenco di ricerca suffissi DNS. . . . : station
```

Scheda Ethernet Ethernet:

```
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione: station
Descrizione . . . . . : Realtek PCIe GBE Family Controller
Indirizzo fisico. . . . . : 10-E7-C6-DF-2F-60
DHCP abilitato. . . . . : Sì
Configurazione automatica abilitata : Sì
```

Scheda Ethernet Ethernet 2:

```
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
Descrizione . . . . . : ExpressVPN TAP Adapter
Indirizzo fisico. . . . . : 00-FF-FE-90-A3-B4
DHCP abilitato. . . . . : Sì
Configurazione automatica abilitata : Sì
```

Scheda sconosciuta Connessione alla rete locale (LAN):

```
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
Descrizione . . . . . : ExpressVPN TUN Driver
Indirizzo fisico. . . . . :
DHCP abilitato. . . . . : No
Configurazione automatica abilitata : Sì
```

Scheda Ethernet Ethernet 3:

```
Suffisso DNS specifico per connessione:
Descrizione . . . . . : VirtualBox Host-Only Ethernet Adapter
Indirizzo fisico. . . . . : 0A-00-27-00-00-0A
DHCP abilitato. . . . . : No
Configurazione automatica abilitata : Sì
Indirizzo IPv6 locale rispetto al collegamento . : fe80::326:ff4d:471e:8b03%10(Preferenziale)
Indirizzo IPv4. . . . . : 192.168.56.1(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . :
IAID DHCPv6 . . . . . : 856293415
DUID Client DHCPv6. . . . . : 00-01-00-01-22-35-C2-20-10-E7-C6-DF-2F-60
Server DNS . . . . . : fec0:0:0:ffff::1%1
                          fec0:0:0:ffff::2%1
                          fec0:0:0:ffff::3%1
NetBIOS su TCP/IP . . . . . : Attivato
```

Scheda LAN wireless Connessione alla rete locale (LAN)* 10:

```
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
Descrizione . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Indirizzo fisico. . . . . : B8-08-CF-EE-E3-42
DHCP abilitato. . . . . : Sì
Configurazione automatica abilitata : Sì
```



```

Scheda LAN wireless Connessione alla rete locale (LAN)* 11:

Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
Descrizione . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Indirizzo fisico. . . . . : BA-08-CF-EE-E3-41
DHCP abilitato. . . . . : No
Configurazione automatica abilitata : Sì

Scheda LAN wireless Wi-Fi:

Suffisso DNS specifico per connessione: station
Descrizione . . . . . : Intel(R) Dual Band Wireless-AC 7265
Indirizzo fisico. . . . . : B8-08-CF-EE-E3-41
DHCP abilitato. . . . . : Sì
Configurazione automatica abilitata : Sì
Indirizzo IPv6 locale rispetto al collegamento . : fe80::615f:e7e:1a16:b375%17(Preferenziale)
Indirizzo IPv4. . . . . : 192.168.1.7(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Lease ottenuto. . . . . : giovedì 10 aprile 2025 13:54:35
Scadenza lease . . . . . : venerdì 11 aprile 2025 13:54:36
Gateway predefinito . . . . . : 192.168.1.1
Server DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 280496335
DUID Client DHCPv6. . . . . : 00-01-00-01-22-35-C2-20-10-E7-C6-DF-2F-60
Server DNS . . . . . : fe80::1614:59ff:fe38:82b0%17
                        192.168.1.1
NetBIOS su TCP/IP . . . . . : Attivato

Scheda Ethernet Connessione di rete Bluetooth:

Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
Descrizione . . . . . : Bluetooth Device (Personal Area Network)
Indirizzo fisico. . . . . : B8-08-CF-EE-E3-45
DHCP abilitato. . . . . : Sì
Configurazione automatica abilitata : Sì

```

Esplorare il Traffico di Risposta DNS

Selezionare il pacchetto DNS di risposta corrispondente che ha "Standard query response" e "A www.cisco.com" nella colonna Info. L'indirizzo IP, l'indirizzo MAC e il numero di porta di origine nel pacchetto di query sono ora indirizzi di destinazione. L'indirizzo IP, l'indirizzo MAC e il numero di porta di destinazione nel pacchetto di query sono ora indirizzi di origine.

Esandere Domain Name System (response). Poi esandere Flags, Queries e Answers. Osservare i risultati. Il DNS pu gestire query ricorsive. Osservare i record CNAME e A nei dettagli delle risposte. I risultati in Wireshark dovrebbero essere gli stessi dei risultati di nslookup nel Prompt dei comandi o nel terminale...

