



Cybersecurity Specialist

Cyber Security & Ethical Hacking

GIORNO 3 – CISCO CYBEROPS

**Alejandro Cristino
S13-L3**

TRACCIA

Exploring DNS Traffic

In this lab, you will complete the following objectives:

- Capture DNS Traffic
- Explore DNS Query Traffic
- Explore DNS Response

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

Parte 1: Acquisisci il traffico DNS

1. Avvia Wireshark e prepararsi all'avvio dell'acquisizione dei pacchetti
2. In windows inserisci ip config /flushdns nel prompt dei comandi



```
Prompt dei comandi
Microsoft Windows [Versione 10.0.22631.4112]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\aless>ipconfig/flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.
```

3. Al prompt dei comandi o al terminale, digitare nslookup per accedere alla modalità interattiva, seguito dal nome di dominio di un sito web. In questo esempio viene utilizzato il nome di dominio www.cisco.com.
4. Avviare l'acquisizione dei pacchetti con Wireshark.



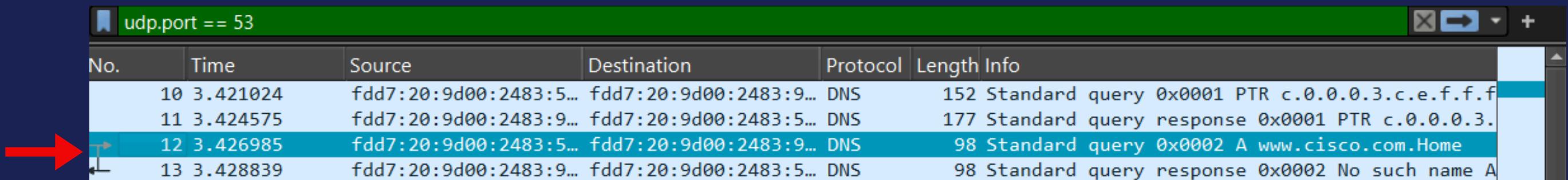
```
C:\Users\aless>nslookup www.cisco.com
Server: myrouter.io
Address: fdd7:20:9d00:2483:9e00:1ff:fe:c

Risposta da un server non autorevole:
Nome: e2867.dsca.akamaiedge.net
Addresses: 2001:41a8:28:5ae::b33
          2001:41a8:28:585::b33
          23.205.50.103
Aliases: www.cisco.com
         www.cisco.com.akadns.net
         wwwds.cisco.com.edgekey.net
         wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

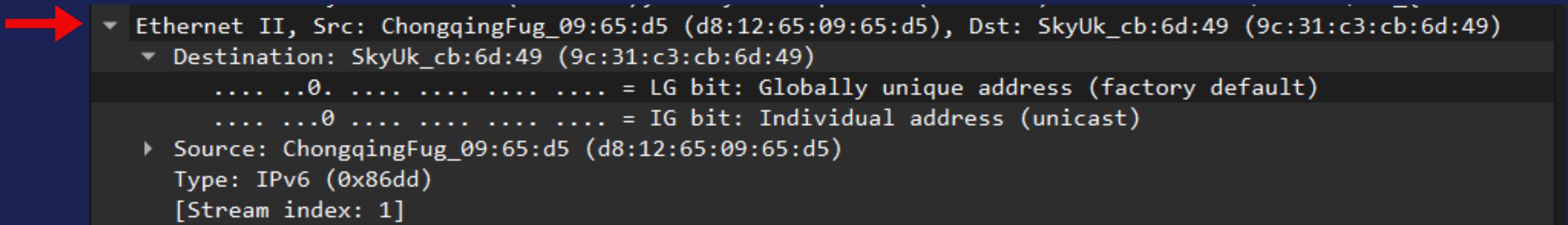
4. Fare clic su Interrompi acquisizione dei pacchetti su Wireshark.

Parte 2: Esplora il traffico delle query DNS

- Osserva il traffico catturato nel riquadro Wireshark Packet List. Inserisci **udp.port == 53** nella casella filtro e fai clic sulla freccia (o premi invio) per visualizzare solo i pacchetti DNS.
- Selezionare il pacchetto DNS contenente **la query standard e A www.cisco.com** nella colonna Info.



- Espandi Ethernet II per visualizzare i dettagli. Osserva i campi di origine e destinazione.



Quali sono gli indirizzi MAC di origine e destinazione?

- Indirizzo MAC di origine: d8:12:65:09:65:d5
- Indirizzo MAC di destinazione: 9c:31:c3:cb:6d:49

A quali interfacce di rete sono associati questi indirizzi MAC?

- Indirizzo MAC di origine (d8:12:65:09:65:d5): È associato alla tua interfaccia di rete locale.
- Indirizzo MAC di destinazione (9c:31:c3:cb:6d:49): Probabilmente è associato a un dispositivo remoto nella rete esterna, come un router o server appartenente a Sky UK, dato il nome associato all'indirizzo (SkyUk).

4. Espandi Protocollo Internet versione 6. Osserva gli indirizzi di origine e di destinazione.

```
► Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{81E92277-9
► Ethernet II, Src: ChongqingFug_09:65:d5 (d8:12:65:09:65:d5), Dst: SkyUk_cb:6d:49 (9c:31:c3:cb:6d:49)
▼ Internet Protocol Version 6, Src: fdd7:20:9d00:2483:559d:1835:30ab:6697, Dst: fdd7:20:9d00:2483:9e00:1ff
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 00.. .... .... .... .... = Differentiated Services Codepoint: Default (0)
    .... .... ..00 .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport
  .... 0011 1111 0000 0010 1111 = Flow Label: 0x3f02f
  Payload Length: 44
  Next Header: UDP (17)
  Hop Limit: 64
  ▼ Source Address: fdd7:20:9d00:2483:559d:1835:30ab:6697
    [Address Space: Unique Local Unicast]
    ▶ [Special-Purpose Allocation: Unique-Local]
  ▼ Destination Address: fdd7:20:9d00:2483:9e00:1ff:fec3:c
    [Address Space: Unique Local Unicast]
    ▶ [Special-Purpose Allocation: Unique-Local]
  [Destination SLAAC MAC: 9c:00:01:c3:00:0c (9c:00:01:c3:00:0c)]
  [Stream index: 0]
```

Quali sono gli indirizzi IP di origine e destinazione?

- Indirizzo IP di origine: fdd7:20:9d00:2483:559d:1835:30ab:6697
- Indirizzo IP di destinazione: fdd7:20:9d00:2483:9e00:1ff

A quali interfacce di rete sono associati questi indirizzi IP?

- Indirizzo IP di origine: È associato all'interfaccia di rete del dispositivo che ha originato il pacchetto, che potrebbe essere il computer o un altro dispositivo della rete locale.
- Indirizzo IP di destinazione: È associato a un dispositivo della stessa rete locale, con lo stesso prefisso di indirizzo IP, che potrebbe essere un altro computer, un server o un router nella rete locale.

5. Espandi il protocollo User Datagram . Osserva le porte di origine e di destinazione.

```
▶ Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{81E92277-999
▶ Ethernet II, Src: ChongqingFug_09:65:d5 (d8:12:65:09:65:d5), Dst: SkyUk_cb:6d:49 (9c:31:c3:cb:6d:49)
▶ Internet Protocol Version 6, Src: fdd7:20:9d00:2483:559d:1835:30ab:6697, Dst: fdd7:20:9d00:2483:9e00:1ff:f
▼ User Datagram Protocol, Src Port: 64693, Dst Port: 53
  Source Port: 64693
  Destination Port: 53
  Length: 44
  Checksum: 0x4610 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
  [Stream Packet Number: 1]
  ▶ [Timestamps]
  UDP payload (36 bytes)
  ▶ Domain Name System (query)
```

Quali sono le porte di origine e destinazione?

- Porta di origine: 64693
- Porta di destinazione: 53

Qual è il numero di porta DNS predefinito?

- Il numero di porta DNS predefinito è 53

6. Determinare l'indirizzo IP e MAC del PC.

- Nel prompt dei comandi di Windows, digitare arp –a e ipconfig /all per registrare gli indirizzi MAC e IP del PC.
- Confronta gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC.

Qual è la tua osservazione?

Gli indirizzi IP e MAC acquisiti nei risultati di Wireshark sono gli stessi indirizzi elencati nel comando ipconfig /all.

7. Espandi Domain Name System (query) nel riquadro Packet Details. Quindi espandi Flags and Queries .

- Osserva i risultati. Il flag è impostato per eseguire la query in modo ricorsivo per interrogare l'indirizzo IP su www.cisco.com.

```

>User Datagram Protocol, Src Port: 64693, 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.Home: type A, class IN
      [Response In: 13]

```

Parte 3: Esplora il traffico di risposta DNS

1. Selezionare il pacchetto DNS di risposta corrispondente con Risposta query standard e A www.cisco.com nella colonna Informazioni.

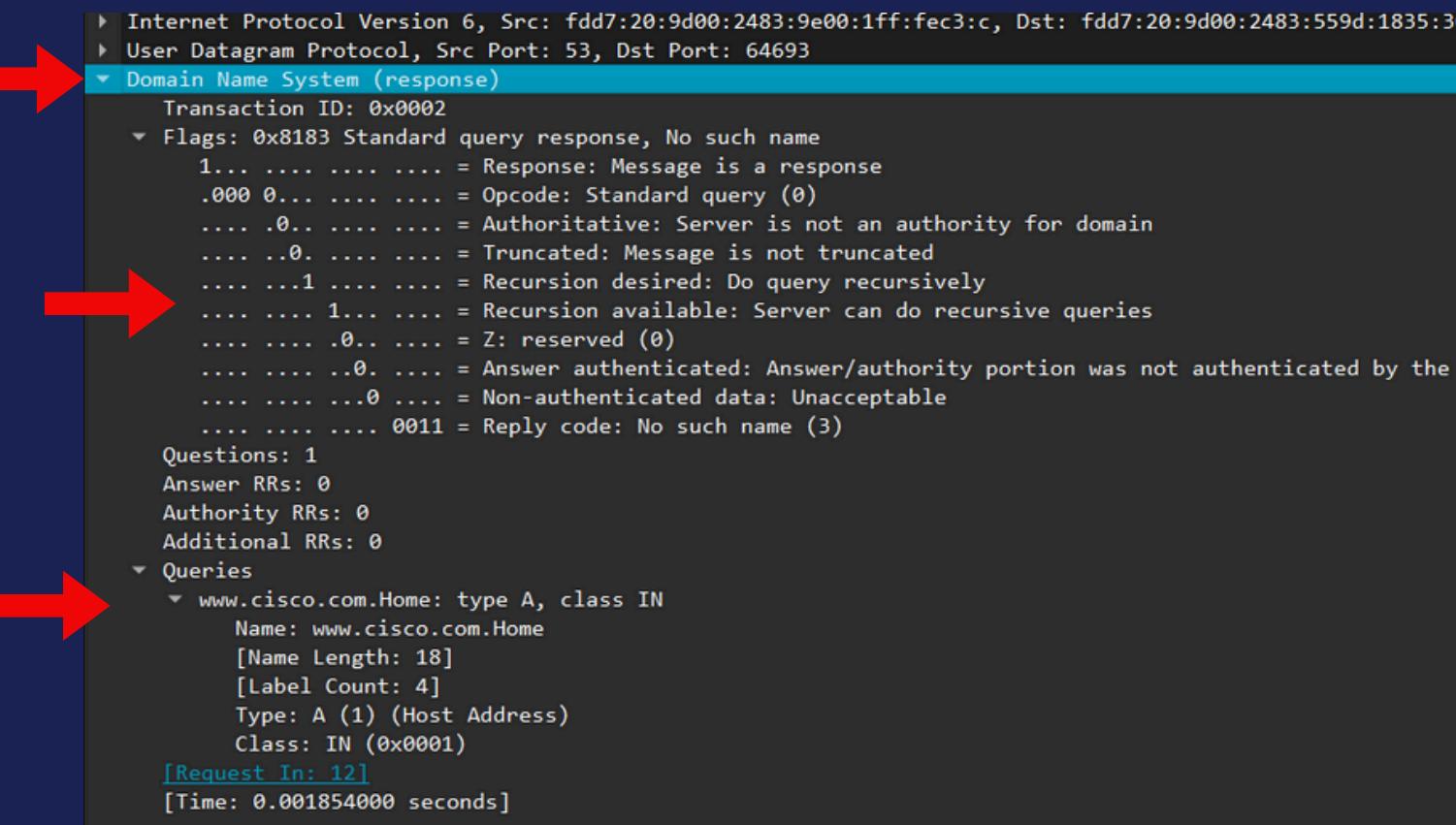
→

11 3.424575	fdd7:20:9d00:2483:9... fdd7:20:9d00:2483:5... DNS	177 Standard query response 0x0001 PTR c.0.0.0.3.c.e.1.1.1.1.0.0.0.e.9.
12 3.426985	fdd7:20:9d00:2483:5... fdd7:20:9d00:2483:9... DNS	98 Standard query 0x0002 A www.cisco.com.Home
13 3.428839	fdd7:20:9d00:2483:9... fdd7:20:9d00:2483:5... DNS	98 Standard query response 0x0002 No such name A www.cisco.com.Home
14 3.429203	fdd7:20:9d00:2483:5... fdd7:20:9d00:2483:9... DNS	98 Standard query 0x0003 AAAA www.cisco.com.Home
15 3.431256	fdd7:20:9d00:2483:9... fdd7:20:9d00:2483:5... DNS	98 Standard query response 0x0003 No such name AAAA www.cisco.com.Home
16 3.431612	fdd7:20:9d00:2483:5... fdd7:20:9d00:2483:9... DNS	93 Standard query 0x0004 A www.cisco.com
17 4.365035	fdd7:20:9d00:2483:9... fdd7:20:9d00:2483:5... DNS	275 Standard query response 0x0004 A www.cisco.com CNAME www.cisco.com.
20 4.372851	fdd7:20:9d00:2483:5... fdd7:20:9d00:2483:9... DNS	93 Standard query 0x0005 AAAA www.cisco.com
21 4.976678	fdd7:20:9d00:2483:9... fdd7:20:9d00:2483:5... DNS	315 Standard query response 0x0005 AAAA www.cisco.com CNAME www.cisco.com
23 5.813857	fdd7:20:9d00:2483:5... fdd7:20:9d00:2483:9... DNS	112 Standard query 0x1efc A mobile.events.data.microsoft.com
24 5.814750	fdd7:20:9d00:2483:5... fdd7:20:9d00:2483:9... DNS	112 Standard query 0x33c8 AAAA mobile.events.data.microsoft.com
▶ Frame 13: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{81E92277-999		
▶ Ethernet II, Src: SkyUk_cb:6d:49 (9c:31:c3:cb:6d:49), Dst: ChongqingFug_09:65:d5 (d8:12:65:09:65:d5)		
▶ Internet Protocol Version 6, Src: fdd7:20:9d00:2483:9e00:1ff:fec3:c, Dst: fdd7:20:9d00:2483:559d:1835:30ab		
▶ User Datagram Protocol, Src Port: 53, Dst Port: 64693		
▶ Domain Name System (response)		
0000 d8 12 65 09 65 d5 9c 31 c3 cb		
0010 00 00 00 2c 11 40 fd d7 00 26		
0020 01 ff fe c3 00 0c fd d7 00 26		
0030 18 35 30 ab 66 97 00 35 fc b5		
0040 81 83 00 01 00 00 00 00 00 00		
0050 00 72 02 05 02 05 01 01 00 00		

Quali sono gli indirizzi MAC e IP di origine e destinazione e i numeri di porta? Come si confrontano con gli indirizzi nei pacchetti di query DNS?

- L'IP sorgente, l'indirizzo MAC e il numero di porta nel pacchetto di query sono ora indirizzi di destinazione. L'IP destinazione, l'indirizzo MAC e il numero di porta nel pacchetto di query sono ora indirizzi di origine.

2. Espandi Domain Name System (response)



```
Internet Protocol Version 6, Src: fdd7:20:9d00:2483:9e00:1ff:fec3:c, Dst: fdd7:20:9d00:2483:559d:1835:30
User Datagram Protocol, Src Port: 53, Dst Port: 64693
Domain Name System (response)
  Transaction ID: 0x0002
  Flags: 0x8183 Standard query response, No such name
    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
    .... .... 0011 = Reply code: No such name (3)
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.cisco.com.Home: type A, class IN
      Name: www.cisco.com.Home
      [Name Length: 18]
      [Label Count: 4]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      [Request In: 121]
      [Time: 0.001854000 seconds]
```

3. Osservare i risultati.

Il server DNS può eseguire query ricorsive?

- Sì, il DNS può gestire query ricorsive.

4. Osservare i record CNAME e A nei dettagli delle risposte.

Come si confrontano i risultati con quelli di nslookup?

- I risultati in Wireshark dovrebbero essere gli stessi dei risultati di nslookup nel prompt dei comandi o nel terminale poiché entrambi si affidano alle risposte del server DNS.



Cybersecurity Specialist

Cyber Security & Ethical Hacking

GRAZIE.