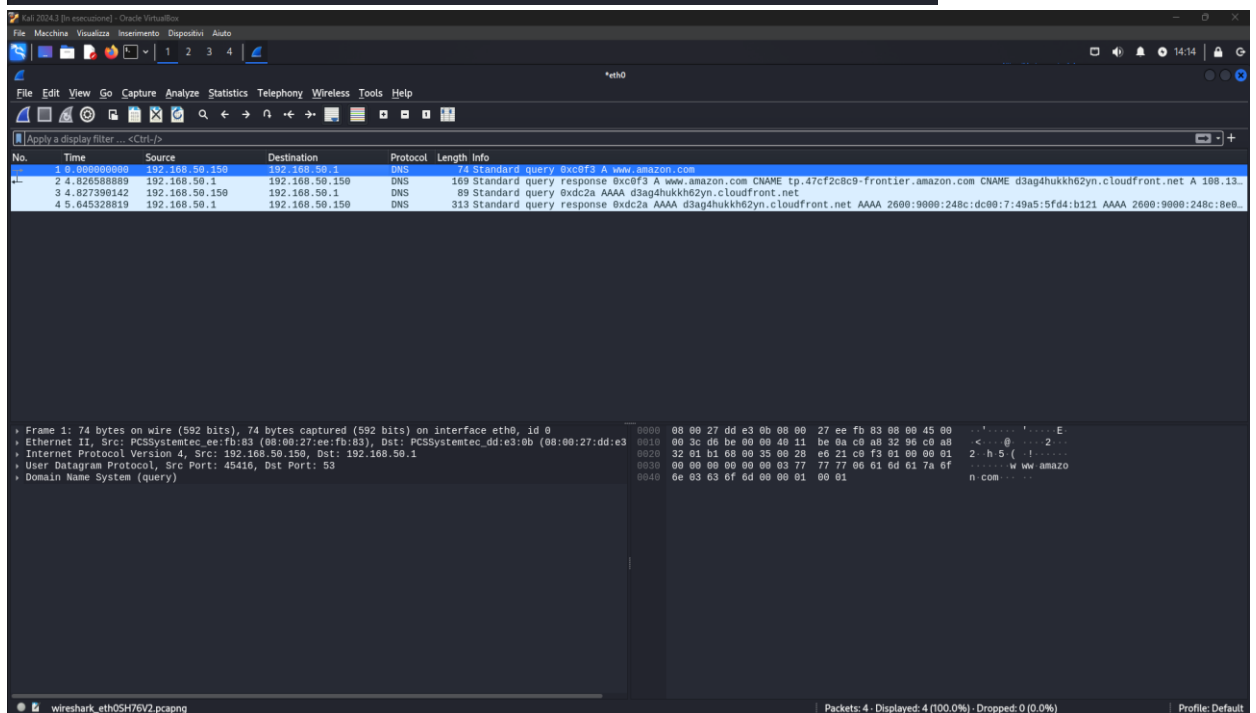


Esercizio 24/10/2024

1. Come primo step seleziono l'interfaccia da monitorare con Wireshark e procedo su terminale con il comando nslookup www.amazon.com per interrogare il dominio amazon:

```
(kali㉿kali)-[~]
$ nslookup www.amazon.com
Server:      192.168.50.1
Address:     192.168.50.1#53

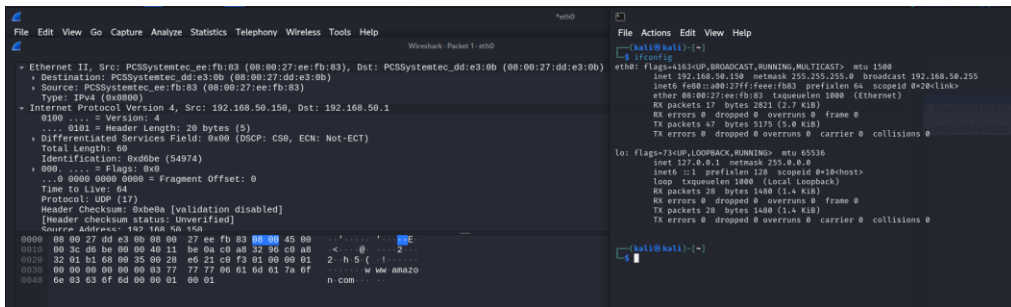
Non-authoritative answer:
www.amazon.com canonical name = tp.47cf2c8c9-frontier.amazon.com.
tp.47cf2c8c9-frontier.amazon.com canonical name = d3ag4hukkh62yn.cloudfront.net.
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 108.138.190.178
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:dc00:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:8e00:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:d800:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:3c00:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:3600:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:200:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:8200:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:3e00:7:49a5:5fd4:b121
```



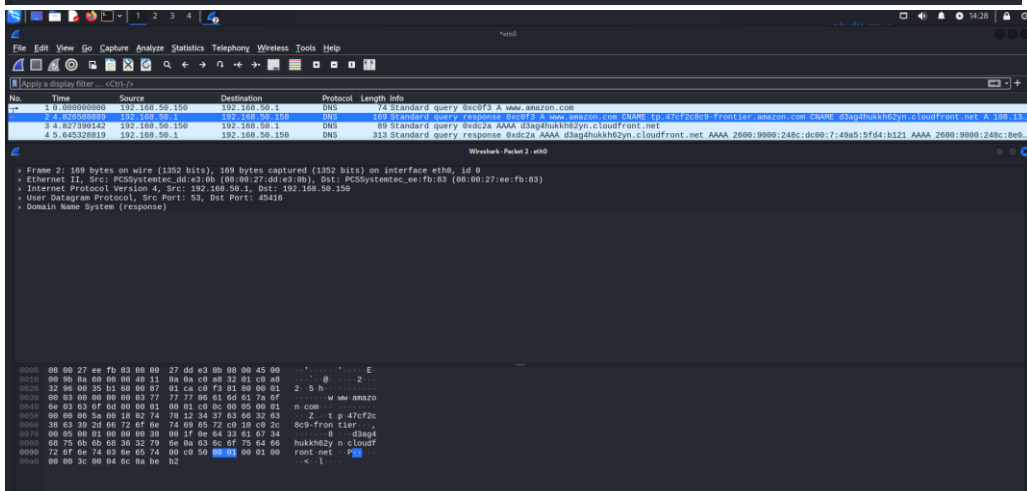
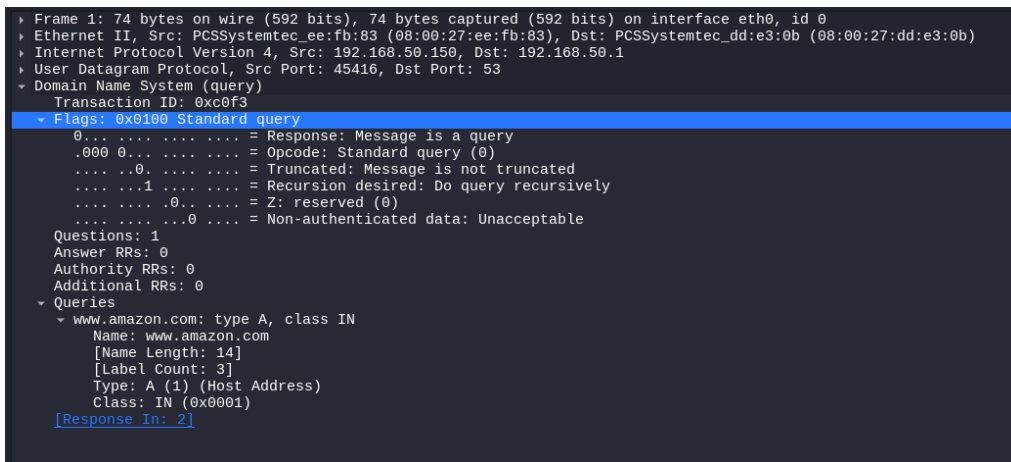
2. Una volta applicati i filtri di cattura passo ad esaminare le query di richiesta e di risposta con i dettagli appropriati:

a- Query di richiesta:





b- Query di risposta:



Wireshark - Packet 2: eth0

- Frame 2: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits) on interface eth0, id 0
- Ethernet II, Src: PCSysintec, dd:e3:0b (08:00:27:dd:e3:0b), Dst: PCSysintec, ee:fb:83 (08:00:27:ee:fb:83)
 - Destination: PCSysintec, ee:fb:83 (08:00:27:ee:fb:83)
 - Address: PCSysintec, ee:fb:83 (08:00:27:ee:fb:83)
 - 0 = 16 bit: Globally unique address (factory default)
 - 0 = 10 bit: Individual address (unicast)
 - Address: PCSysintec, dd:e3:0b (08:00:27:dd:e3:0b)
 - 0 = 10 bit: Globally unique address (factory default)
 - 0 = 10 bit: Individual address (unicast)
- Type: IPv4 (60080)
 - Internet Protocol Version 4, Src: 192.168.50.1, Dst: 192.168.50.150
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (8)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total length: 150
 - Identification: 0x0000 (35424)
 - 0000 = Flags: 0x0
 - 0 0000 0000 = Fragment Offset: 0
 - Time to live: 64
 - Protocol: UDP (17)
 - Header Checksum: 0x0000 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.50.1
 - Destination Address: 192.168.50.150
 - User Datagram Protocol, Src Port: 53, Dst Port: 45416
 - Domain Name System (response)

Wireshark - Packet 2: eth0

- Frame 2: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits) on interface eth0, id 0
- Ethernet II, Src: PCSysintec, dd:e3:0b (08:00:27:dd:e3:0b), Dst: PCSysintec, ee:fb:83 (08:00:27:ee:fb:83)
 - Internet Protocol Version 4, Src: 192.168.50.1, Dst: 192.168.50.150
 - User Datagram Protocol, Src Port: 53, Dst Port: 45416
 - Domain Name System (response)
 - Transaction ID: 0xc0f3
 - Flags: 0x0100 Standard query response, No error
 - 0 = Response: Message is a response
 - 0000 0 = Opcode: Standard query (0)
 - 0 = Authoritative: Server is not an authority for domain
 - 0 = Truncated: Message is not truncated
 - 0 = 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
 - 0000 = Reply code: No error (0)
 - Questions: 1
 - Answer RRs: 3
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.amazon.com type A, class IN
 - Name: www.amazon.com
 - (Name Length: 14)
 - (Label Count: 3)
 - Type: A (1) (Host Address)
 - Class: IN (0x0001)
 - Answers
 - www.amazon.com type CNAME, class IN, cname tp.47cf2c8c9-frontier.amazon.com
 - tp.47cf2c8c9-frontier.amazon.com type CNAME, class IN, cname d3ag4hukkh62yn.cloudfront.net
 - d3ag4hukkh62yn.cloudfront.net type A, class IN, addr 108.138.190.178

```
(kali@kali)~]$ nslookup www.amazon.com
Server:      192.168.50.1
Address:     192.168.50.1#53

Non-authoritative answer:
www.amazon.com canonical name = tp.47cf2c8c9-frontier.amazon.com.
tp.47cf2c8c9-frontier.amazon.com canonical name = d3ag4hukkh62yn.cloudfront.net.
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 108.138.190.178
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:dc00:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:8e00:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:d800:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:3c00:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:3600:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:200:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:8200:7:49a5:5fd4:b121
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:248c:3e00:7:49a5:5fd4:b121
```

Confrontando i risultati di Wireshark con nslookup notiamo che i risultati sono gli stessi.