

S11L4

Questa relazione documenta i passaggi effettuati per catturare e analizzare il traffico DNS, includendo l'argomentazione e le spiegazioni necessarie, come richiesto dalla traccia.

Obiettivi del laboratorio

1. Catturare il traffico DNS
 2. Esplorare il traffico delle query DNS
 3. Esplorare il traffico delle risposte DNS
-

Passaggio 1: Preparazione dell'ambiente

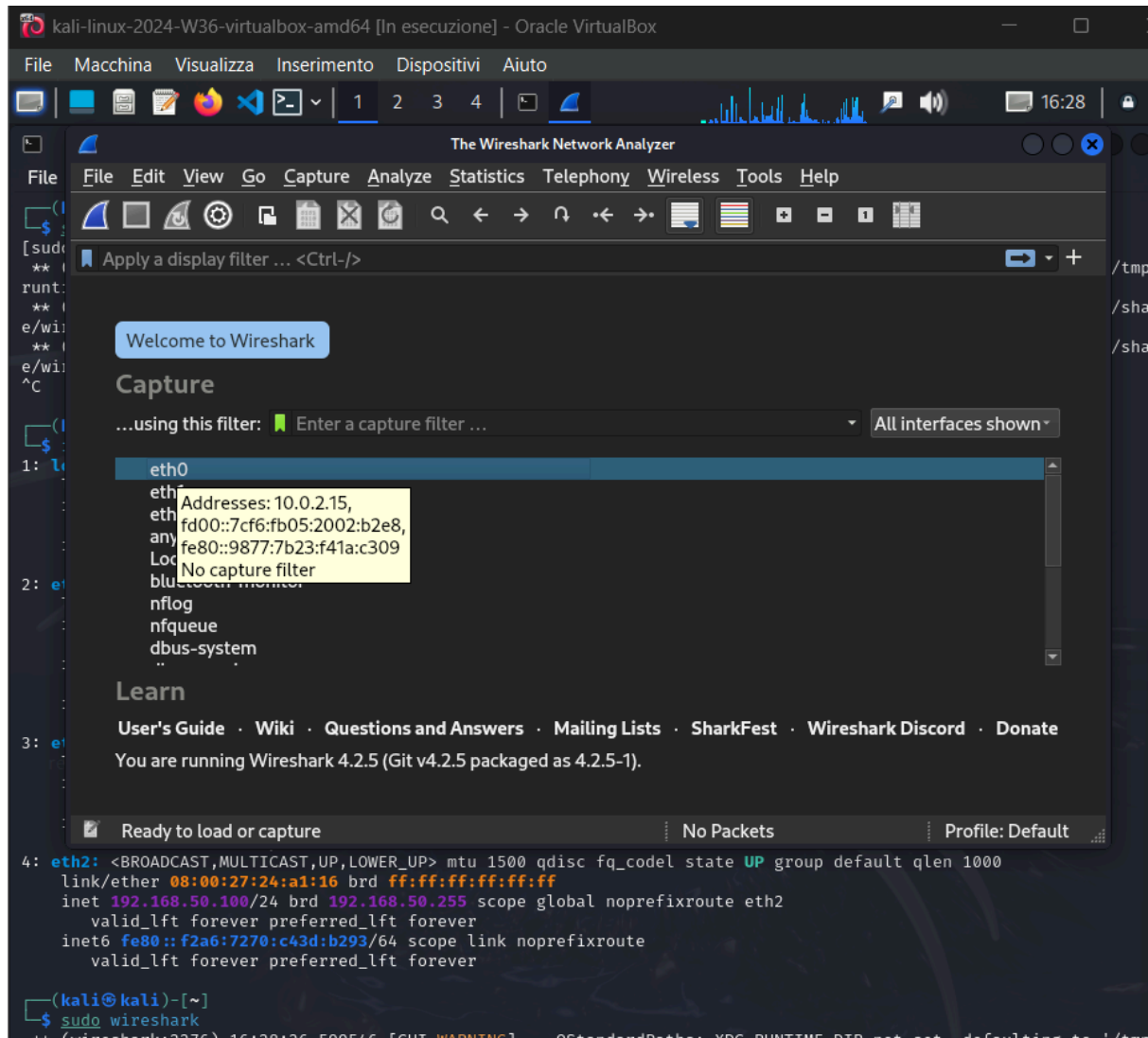
Configurazione delle interfacce di rete

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:14:ae:9f brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 86330sec preferred_lft 86330sec
    inet6 fd00::7cf6:fb05:2002:b2e8/64 scope global dynamic noprefixroute
        valid_lft 86331sec preferred_lft 14331sec
    inet6 fe80::9877:7b23:f41a:c309/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:64:f1:e4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute eth1
        valid_lft 530sec preferred_lft 530sec
    inet6 fe80::eac5:d2c5:e2c6:bb72/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:24:a1:16 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth2
        valid_lft forever preferred_lft forever
    inet6 fe80::f2a6:7270:c43d:b293/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Il comando `ip a` è stato utilizzato per elencare tutte le interfacce di rete disponibili sul sistema Kali Linux. Tra queste, è stata identificata l'interfaccia `eth0` con l'indirizzo IP `10.0.2.15`, che sarà utilizzata per catturare il traffico.

Passaggio 2: Avvio di Wireshark

Avvio e selezione dell'interfaccia



Wireshark è stato avviato con privilegi di root utilizzando il comando `sudo wireshark`.

Nella schermata iniziale, è stata selezionata l'interfaccia di rete `eth0`, in quanto utilizzata per la connessione.

Passaggio 3: Cattura del traffico DNS

Generazione del traffico DNS

```

(kali㉿kali)-[~]
-$ nslookup google.com
Server: 10.0.2.3
Address: 10.0.2.3#53
Non-authoritative answer:
Name: google.com
Address: 216.58.204.238
Name: google.com
Address: 2a00:1450:4002:411::200e

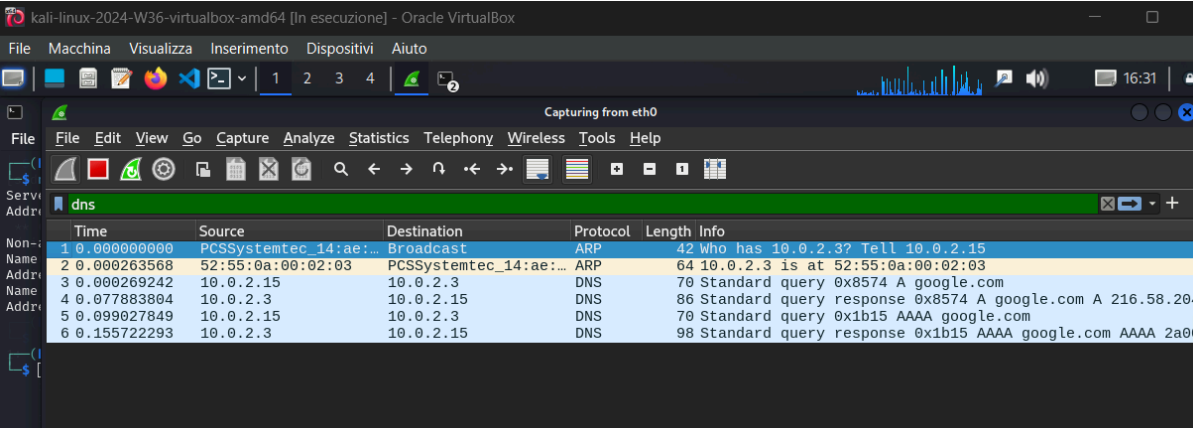
```

Per generare traffico DNS, è stato utilizzato il comando:

```
nslookup google.com
```

Questo ha prodotto una richiesta DNS per il dominio **google.com**, come evidenziato nel terminale (Screenshot 3).

Interruzione della cattura



Time	Source	Destination	Protocol	Length	Info
1.0.000000000	PCSSystemtec_14:ae:...	Broadcast	ARP	42	who has 10.0.2.3? Tell 10.0.2.15
2.0.000263568	52:55:0a:00:02:03	PCSSystemtec_14:ae:...	ARP	64	10.0.2.3 is at 52:55:0a:00:02:03
3.0.000269242	10.0.2.15	10.0.2.3	DNS	70	Standard query 0x8574 A google.com
4.0.077883804	10.0.2.3	10.0.2.15	DNS	86	Standard query response 0x8574 A google.com A 216.58.204.238
5.0.099027849	10.0.2.15	10.0.2.3	DNS	70	Standard query 0x1b15 AAAA google.com
6.0.155722293	10.0.2.3	10.0.2.15	DNS	98	Standard query response 0x1b15 AAAA google.com AAAA 2a00:1450:4002:411::200e

Dopo aver generato traffico sufficiente, la cattura è stata interrotta. I pacchetti DNS catturati sono stati filtrati utilizzando il filtro **dns** in Wireshark.

Passaggio 4: Analisi delle query DNS

Dettaglio della query

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PCSSystemtec_14:ae:...	Broadcast	ARP	42	Who has 10.0.2.3? Tell 10.0.2.15
2	0.000263568	52:55:0a:00:02:03	PCSSystemtec_14:ae:...	ARP	64	10.0.2.3 is at 52:55:0a:00:02:03
3	0.000269242	10.0.2.15	10.0.2.3	DNS	70	Standard query 0x8574 A google.com
4	0.077883804	10.0.2.3	10.0.2.15	DNS	86	Standard query response 0x8574 A google.com A 216.58.204.238
5	0.099027849	10.0.2.15	10.0.2.3	DNS	70	Standard query 0x1b15 AAAA google.com
6	0.155722293	10.0.2.3	10.0.2.15	DNS	98	Standard query response 0x1b15 AAAA google.com AAAA 2a00:1450

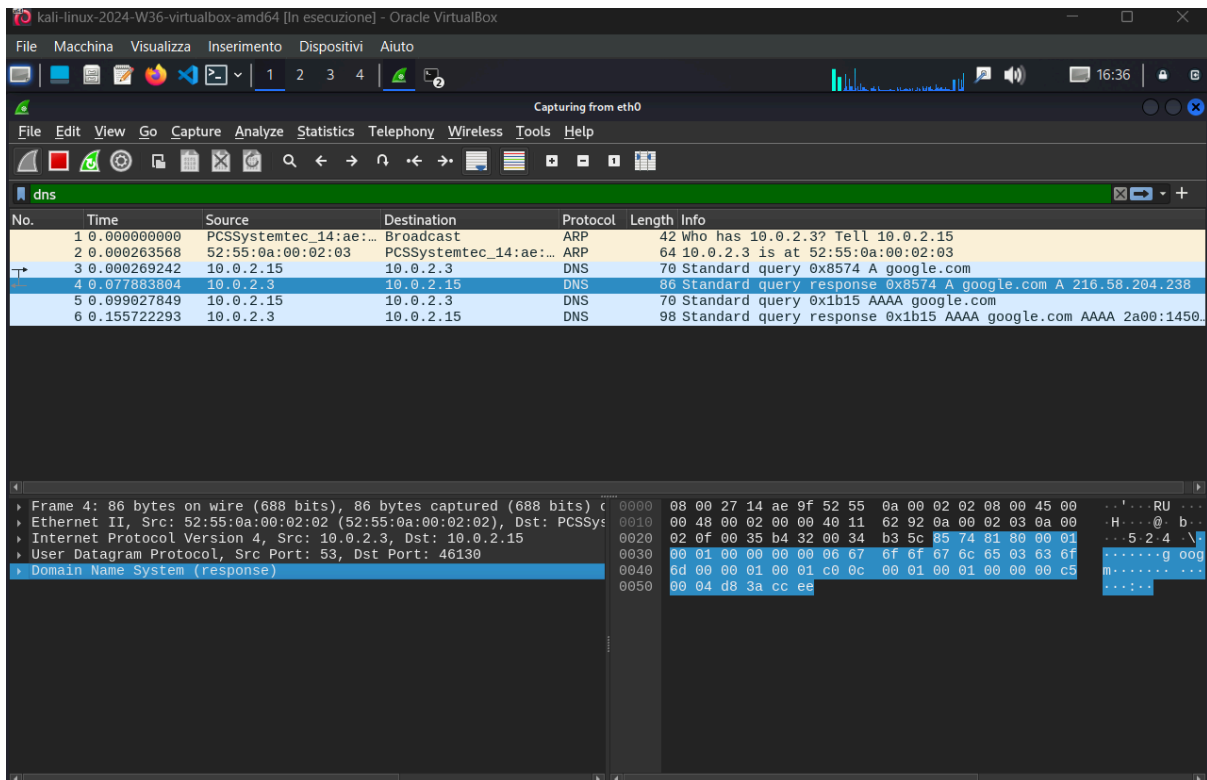
Frame 3: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on	0000	52 55 0a 00 02 03 08 00 27 14 ae 9f 08 00 45 00	RU
Ethernet II, Src: PCSSystemtec_14:ae:9f (08:00:27:14:ae:9f), Dst: 52:55:0a:00:02:03	0010	00 38 7e a7 00 00 40 11 e3 fc 0a 00 02 0f 0a 00	.8~...@. ...
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3	0020	02 03 b4 32 00 35 00 24 18 47 85 74 01 00 00 01	..2.5\$.G
User Datagram Protocol, Src Port: 46130, Dst Port: 53	0030	00 00 00 00 00 00 06 67 6f 6f 67 6c 65 03 63 6fg ood
Domain Name System (query)	0040	6d 00 00 01 00 01	m.....

Una delle query DNS catturate è stata selezionata. Come mostrato nel dettaglio del pacchetto, la query ha richiesto un record di tipo **A** per il dominio **google.com**.

- **Transaction ID:** Identifica univocamente la richiesta.
- **Flags:** Indicano che si tratta di una query standard.
- **Questions:** Contiene il dominio richiesto (**google.com**) e il tipo di record (**A**).

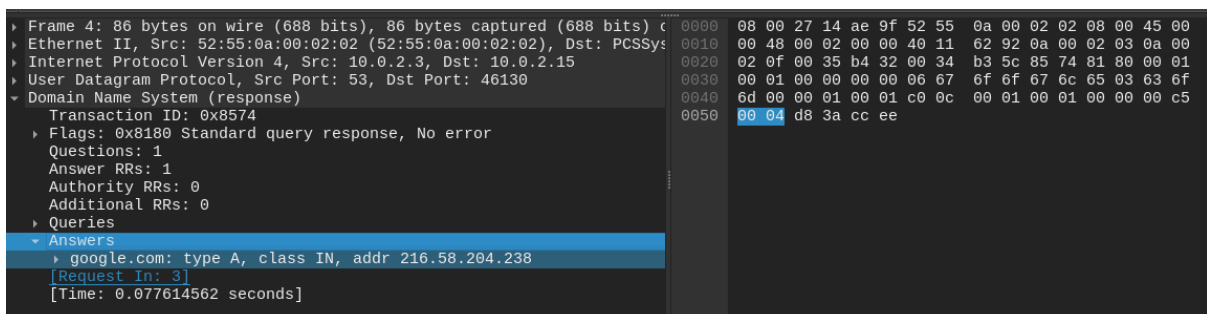
Passaggio 5: Analisi delle risposte DNS

Dettaglio della risposta



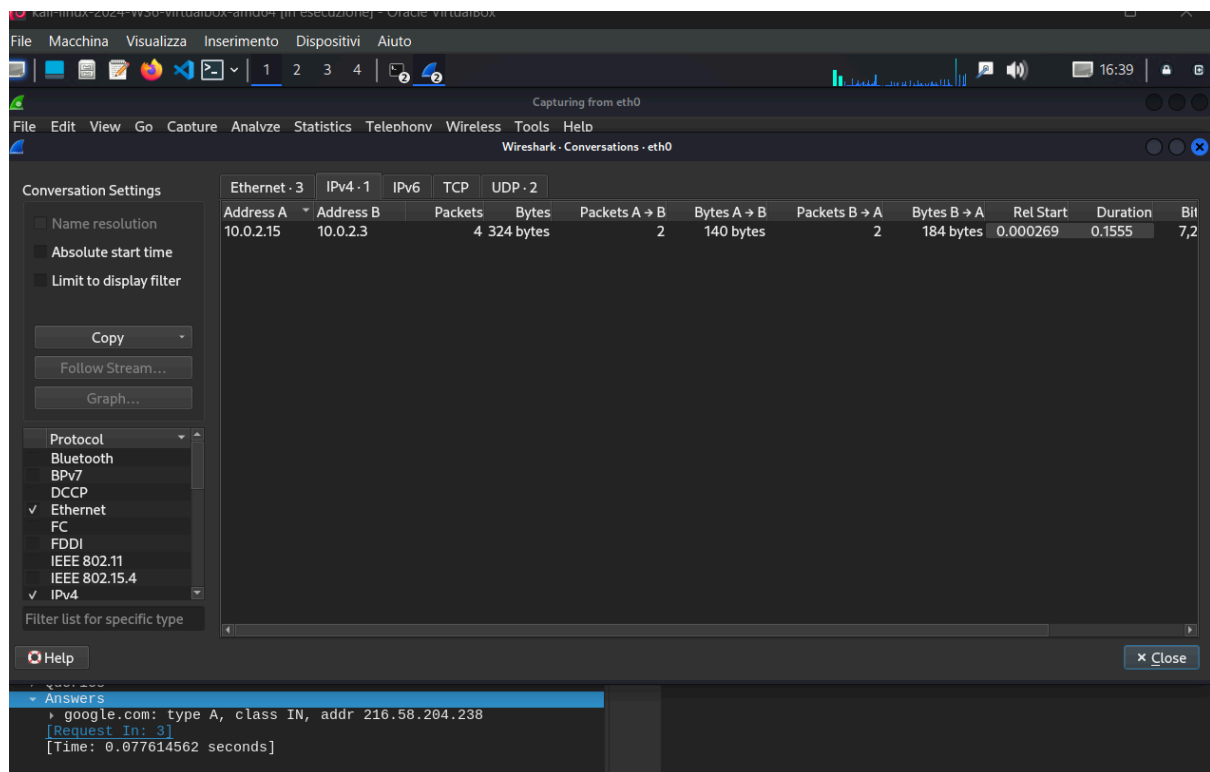
Il pacchetto di risposta corrispondente è stato analizzato. La risposta contiene un record di tipo **A** che associa il dominio **google.com** all'indirizzo IP 216.58.204.238.

- **Answers:** Indica il tipo di record (**A**), la classe (**IN**) e l'indirizzo restituito.



Passaggio 6: Statistiche sul traffico

Statistiche delle conversazioni



Le statistiche delle conversazioni DNS sono state visualizzate tramite il menu **Statistics > Conversations**. Questo ha mostrato il numero di pacchetti e byte scambiati tra il client (10.0.2.15) e il server DNS (10.0.2.3), come visibile nello Screenshot .

Conclusioni

Il laboratorio ha consentito di:

1. Catturare correttamente il traffico DNS utilizzando Wireshark.
2. Analizzare una query DNS, identificandone i dettagli come il tipo di record richiesto e il dominio.
3. Esplorare una risposta DNS, comprendendo il mapping tra dominio e indirizzo IP.
4. Visualizzare le statistiche delle conversazioni per una panoramica quantitativa del traffico analizzato.

Gli screenshot forniti documentano ogni passaggio richiesto dalla traccia, completando il laboratorio con successo.