PRATICA S11L3

Esplorazione del Traffico DNS

Risorse Richieste

1 PC con accesso a internet e Wireshark installato

Obiettivi

- Parte 1: Catturare il Traffico DNS
- Parte 2: Esplorare il Traffico delle Query DNS
- Parte 3: Esplorare il Traffico delle Risposte DNS

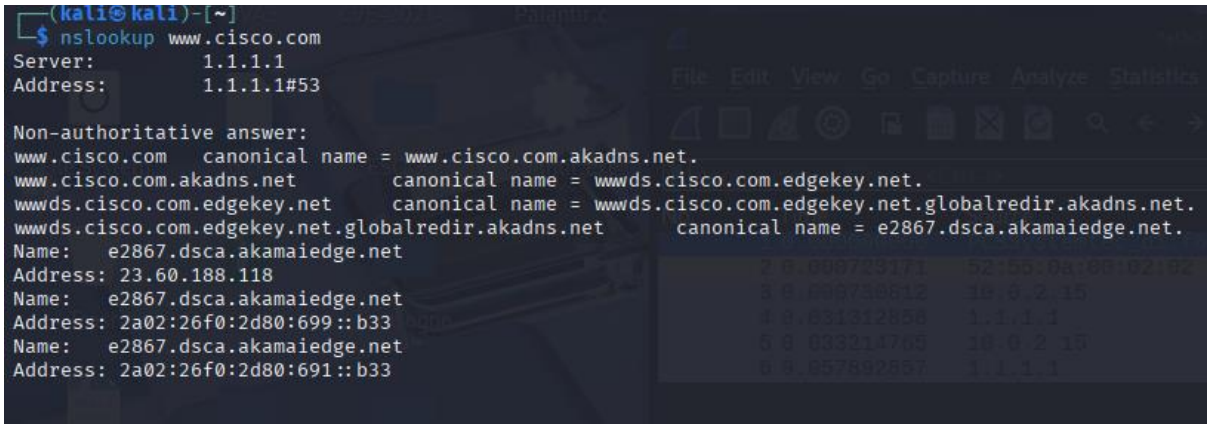
Contesto / Scenario

Wireshark è uno strumento open source per la cattura e l'analisi dei pacchetti. Wireshark fornisce una scomposizione dettagliata dello stack dei protocolli di rete. Wireshark permette di filtrare il traffico per la risoluzione dei problemi di rete, investigare problemi di sicurezza e analizzare i protocolli di rete. Poiché Wireshark permette di visualizzare i dettagli dei pacchetti, può essere usato come strumento di ricognizione da un attaccante.

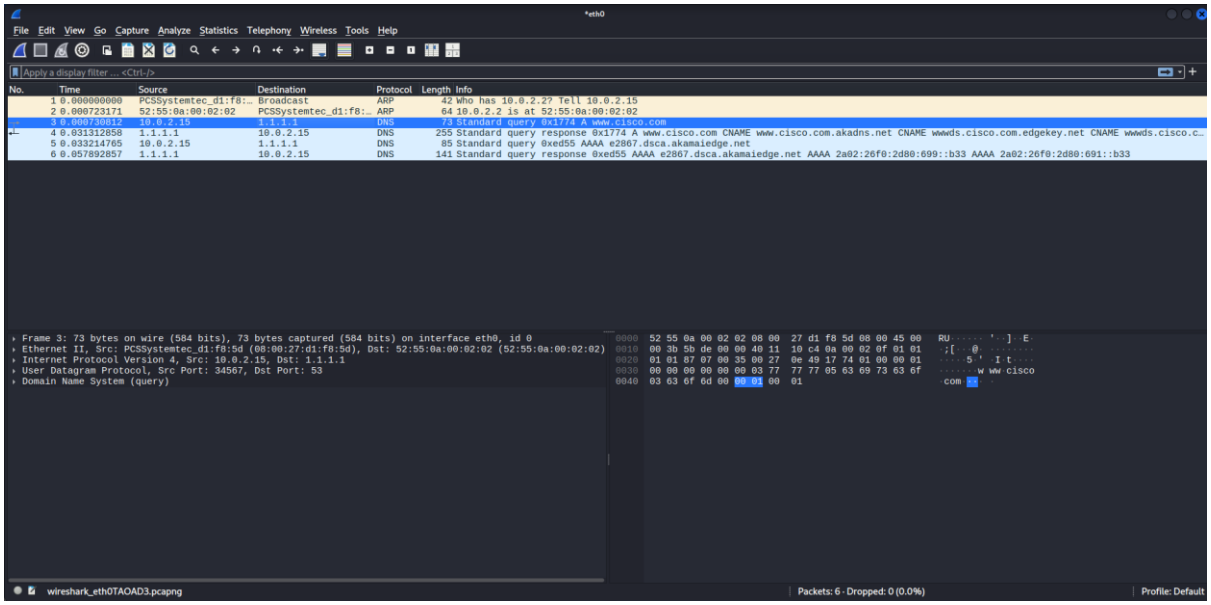
In questo laboratorio, installerai Wireshark e lo userai per filtrare i pacchetti DNS e visualizzare i dettagli sia dei pacchetti di query DNS che di quelli di risposta.

Catturare il traffico DNS

- **Avvio Wireshark** Apro Wireshark sul mio sistema.
- **Scelgo l'interfaccia giusta** Seleziono **eth0**, la mia interfaccia di rete attiva, che mostra traffico in tempo reale. È quella che userò per la cattura.
- **Avvio la cattura** Clicco su "Start capturing packets" per iniziare la registrazione del traffico.
- **Interrogo il DNS via terminale** Apro il terminale e digito `nslookup` per entrare in modalità interattiva.
- **Eseguo la richiesta DNS** Inserisco il nome di dominio che voglio analizzare. In questo caso uso `www.cisco.com` come esempio.



- **Chiudo la sessione** Digito `exit` per uscire da nslookup e chiudo il terminale.
- **Termino la cattura in Wireshark** Torno su Wireshark e clicco su "Stop capturing packets" per interrompere la registrazione.



Esplorare il Traffico delle Query DNS

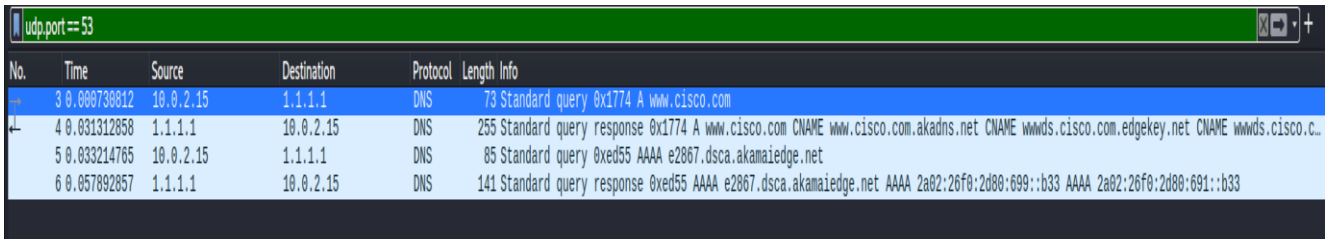
Dopo aver catturato il traffico sull'interfaccia **eth0**, osservo i pacchetti nel riquadro **Packet List** di Wireshark.

Per isolare solo quelli relativi al protocollo DNS, inserisco il filtro:

- udp.port == 53

nella barra dei filtri in alto. Premo **Invio** (oppure clicco sulla freccia accanto) per applicarlo.

A questo punto, Wireshark mostra esclusivamente i pacchetti UDP diretti alla porta 53, cioè quelli usati per le richieste e risposte DNS.



Dopo aver applicato il filtro `udp.port == 53`, scorro l'elenco dei pacchetti nel riquadro **Packet List** e seleziono quello che, nella colonna **Info**, mostra:

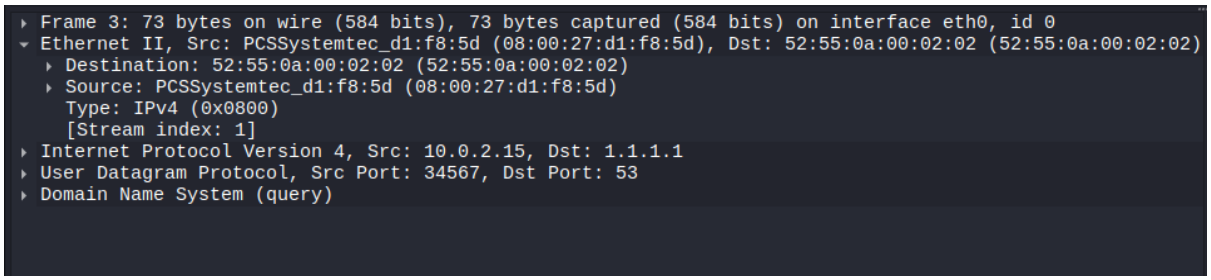
- Standard query 0x1774 A www.cisco.com

Una volta selezionato, passo al riquadro **Packet Details** per analizzarne la struttura.

Osservo che il pacchetto è composto da:

- **Ethernet II**
- **Internet Protocol Version 4 (IPv4)**
- **User Datagram Protocol (UDP)**
- **Domain Name System (query)**

Espando la sezione **Ethernet II** per visualizzare i dettagli a livello di collegamento. Qui esamino attentamente i campi **Source** e **Destination**, che indicano rispettivamente l'indirizzo MAC del mittente e del destinatario.



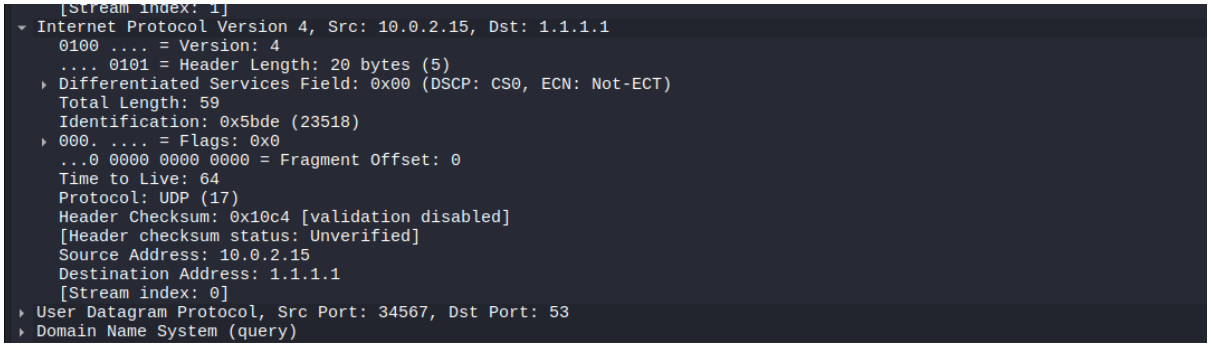
- **Quali sono gli indirizzi MAC di origine e destinazione?**
  Nel dettaglio del pacchetto, sotto la sezione **Ethernet II**, osservo i campi relativi agli indirizzi MAC. L'indirizzo **MAC di origine** è `08:00:27:d1:f8:5d`, mentre quello **di destinazione** è `52:55:0a:00:02:02`. Questi identificano rispettivamente il dispositivo mittente e quello ricevente a livello di collegamento.
- **A quali interfacce di rete sono associati questi indirizzi MAC?**
  Il **MAC di origine** è `08:00:27:d1:f8:5d`, associato alla mia interfaccia di rete **eth0**, da cui è partita la richiesta. Il **MAC di destinazione** è `52:55:0a:00:02:02`, appartenente al server DNS che ha ricevuto la query e inviato la risposta.

Nel riquadro **Packet Details** di Wireshark, espando la sezione **Internet Protocol Version 4 (IPv4)** per analizzare il livello di rete.

Qui osservo due campi fondamentali:

- **Source**: l'indirizzo IPv4 del mittente del pacchetto
- **Destination**: l'indirizzo IPv4 del destinatario

Questi valori mi permettono di capire da dove proviene il pacchetto e verso quale host è diretto. Nel contesto della mia analisi DNS, l'IP sorgente corrisponde al mio sistema (o al resolver DNS), mentre l'IP di destinazione è quello del server DNS interrogato.



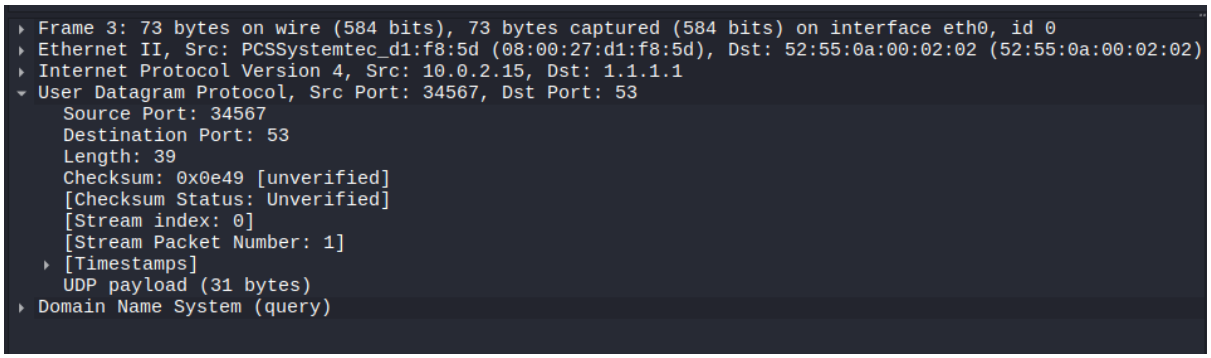
- **Quali sono gli indirizzi IP di origine e destinazione?**
  Nel dettaglio del pacchetto, sotto la sezione **IPv4**, leggo chiaramente gli indirizzi coinvolti nella comunicazione. L'indirizzo **IP di origine** è `10.0.2.15`, cioè il mio sistema locale. L'indirizzo **IP di destinazione** è `1.1.1.1`, il server DNS che ho interrogato.
- **A quali interfacce di rete sono associati questi indirizzi IP?**
  L'indirizzo **IP di origine** è associato alla mia interfaccia di rete **eth0**, che ha generato la richiesta. L'indirizzo **IP di destinazione**, invece, è legato all'interfaccia del server remoto che ha risposto. Questo mi conferma che il pacchetto è partito dalla mia macchina attraverso **eth0** ed è stato ricevuto correttamente dal destinatario.

Nel riquadro **Packet Details**, espando la sezione **User Datagram Protocol (UDP)** per esaminare i dettagli del livello di trasporto.

Qui osservo due campi fondamentali:

- **Source Port**: la porta di origine, da cui è partito il pacchetto
- **Destination Port**: la porta di destinazione, verso cui è diretto

Nel mio caso, la porta di origine è assegnata dinamicamente dal mio sistema, mentre la porta di destinazione è la **53**, utilizzata per il servizio DNS.



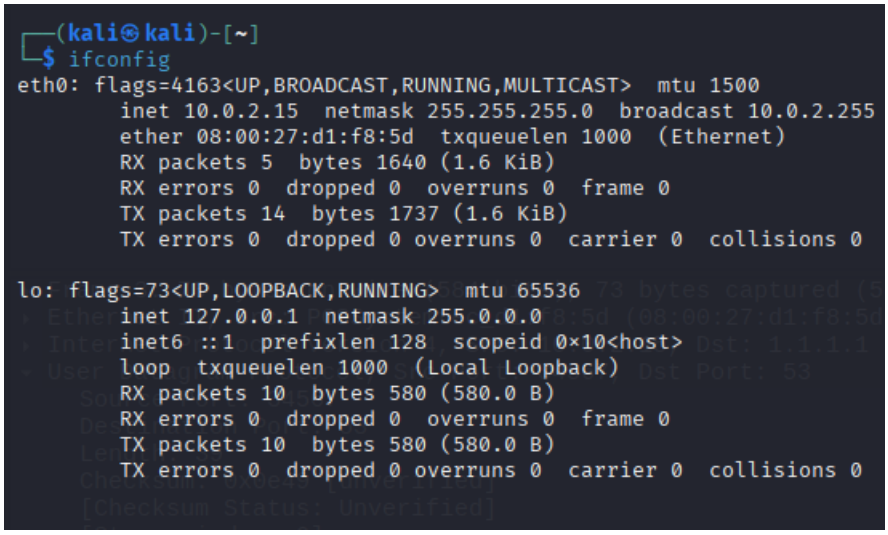
- **Quali sono le porte di origine e destinazione?**

noto che la **porta di origine** è 34567, assegnata dinamicamente dal mio sistema per questa richiesta. La **porta di destinazione**, invece, è la 53, riservata al servizio **DNS**.

- **Qual è il numero di porta DNS predefinito?**
  La porta **predefinita per il DNS** è la **53**, ed è ufficialmente riservata al servizio **Domain Name System**. È su questa porta che il mio sistema invia e riceve le richieste di risoluzione dei nomi, sia in fase di interrogazione che di risposta, utilizzando il protocollo UDP o TCP a seconda del tipo di scambio.

Apro il terminale e digito uno dei seguenti comandi per visualizzare le informazioni sulle interfacce di rete del mio sistema:

- ifconfig



- **Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC. Qual è la tua osservazione?**

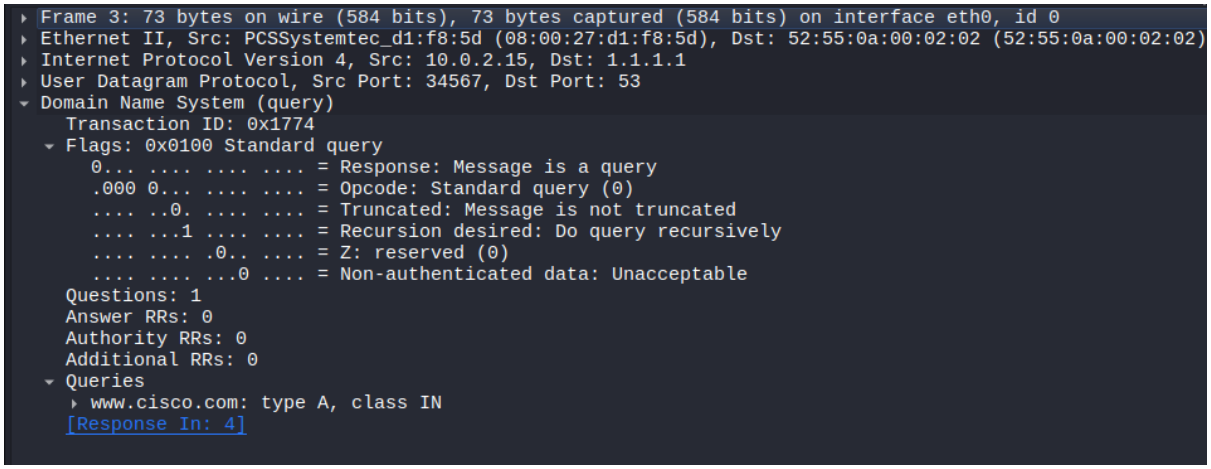
  Gli indirizzi **IP** e **MAC di origine** che ho rilevato nel pacchetto analizzato con Wireshark corrispondono esattamente a quelli assegnati alla mia interfaccia di rete **eth0**. Questo mi conferma che la richiesta è partita direttamente dal mio sistema, attraverso quella specifica interfaccia.

Nel riquadro **Packet Details**, espando la sezione **Domain Name System (query)** per esaminare il contenuto della richiesta DNS.

Procedo quindi ad aprire le sottosezioni **Flags** e **Queries**.

- Nei **Flags**, noto che il bit "Recursion Desired" è attivo: questo significa che ho richiesto al server DNS di eseguire la risoluzione in modalità **ricorsiva**, cioè di interrogare altri server se necessario per ottenere una risposta completa.
- Nella sezione **Queries**, trovo la richiesta specifica: sto cercando l'indirizzo IP associato al nome di dominio www.cisco.com.

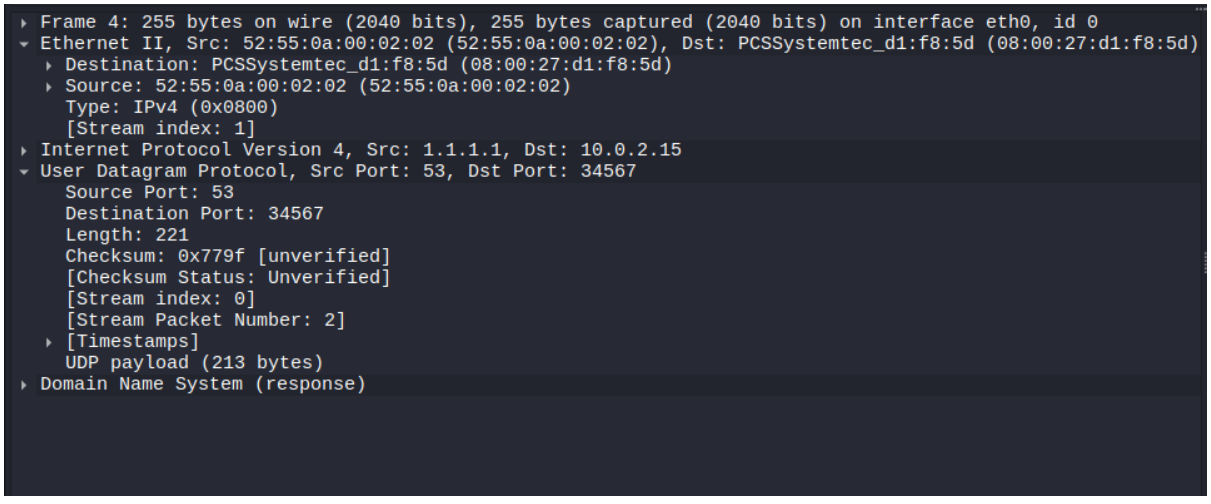
Questa analisi mi conferma che il mio sistema ha inviato una query DNS ricorsiva per risolvere il nome del sito.



Dopo aver analizzato la query DNS, scorro l'elenco dei pacchetti nel riquadro **Packet List** e seleziono quello che, nella colonna **Info**, mostra:

- Standard query response 0x1774 A www.cisco.com

Questo è il pacchetto di **risposta DNS** corrispondente alla mia richiesta.



- **Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione?**
  Nel pacchetto DNS di risposta che ho analizzato con Wireshark, gli indirizzi di origine e destinazione sono ben definiti:

    - L'indirizzo **IP di origine** è `1.1.1.1`, con **MAC** `52:55:0a:00:02:02` e **porta** 53, che identifica il server DNS da cui proviene la risposta.
    - L'indirizzo **IP di destinazione** è `10.0.2.15`, con **MAC** `08:00:27:d1:f8:5d` e **porta** 34567, che corrisponde al mio sistema locale, cioè al client che ha effettuato la richiesta.

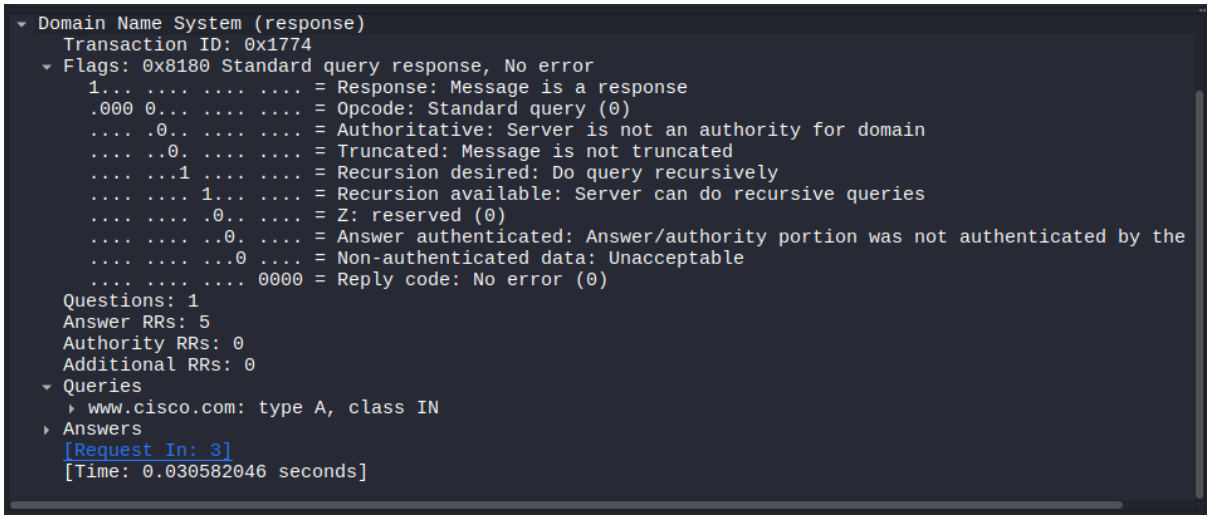
  Questi valori confermano che la risposta DNS è tornata correttamente al mio host attraverso l'interfaccia di rete **eth0**.
- **Come si confrontano con gli indirizzi nei pacchetti di query DNS?**
  Nel pacchetto DNS di **risposta**, noto che gli indirizzi sono **invertiti** rispetto alla **query** originale:
    - L'indirizzo **IP di origine** è ora `1.1.1.1`, con **MAC** `52:55:0a:00:02:02` e **porta** 53, cioè il server DNS che mi sta rispondendo.
    - L'indirizzo **IP di destinazione** è `10.0.2.15`, con **MAC** `08:00:27:d1:f8:5d` e **porta** 34567, cioè il mio sistema locale.

  Questa inversione è normale: il server DNS risponde alla mia richiesta, usando gli stessi indirizzi e porte ma scambiando i ruoli di mittente e destinatario

Nel riquadro **Packet Details**, espando la sezione **Domain Name System (response)** per esaminare la risposta ricevuta dal server DNS.

Procedo quindi ad aprire le sottosezioni:

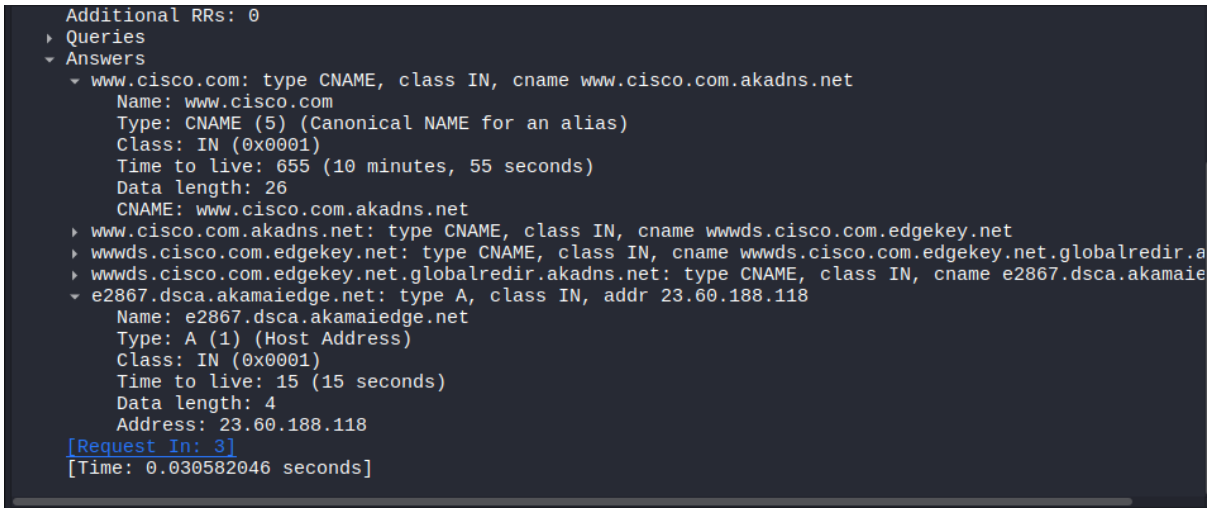
- **Flags**: qui verifico che il bit "Recursion Available" sia attivo, segno che il server ha eseguito la risoluzione ricorsiva come richiesto. Inoltre, il flag "Response" è impostato, confermando che si tratta di una risposta e non di una query.
- **Queries**: trovo la richiesta originale, ovvero la risoluzione del nome `www.cisco.com`.



- **Il server DNS può fare query ricorsive?**

La **query DNS** che ho analizzato è configurata per eseguire la risoluzione in modalità **ricorsiva**. Questo significa che il mio sistema ha richiesto al server DNS non solo di rispondere, ma anche di interrogare altri server se necessario.

Nel riquadro **Packet Details** di Wireshark, espando la sezione **Domain Name System (response)** e poi apro il blocco **Answers** per analizzare i dati restituiti dal server DNS.



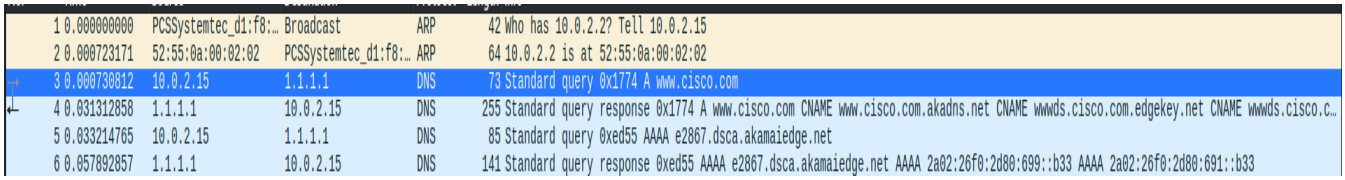
- **Come si confrontano i risultati con quelli di nslookup?**
  Con il comando `nslookup`, ottengo direttamente l'indirizzo **IP associato al dominio**, utile per una verifica rapida della risoluzione DNS. Wireshark, invece, mi permette di andare molto più a fondo: posso analizzare **l'intero pacchetto DNS** inviato dal mio sistema, osservare i **flag**, le **query**, le **risposte**, e verificare ogni dettaglio del protocollo, inclusi **MAC address**, **porte**, e **livelli OSI** coinvolti. In sintesi, `nslookup` mi dà il risultato finale, mentre **Wireshark mi mostra il viaggio completo del pacchetto**.

Riflessione

- **Dai risultati di Wireshark, cos'altro puoi imparare sulla rete quando rimuovi il filtro?**

  Una volta **rimosso il filtro** in Wireshark, noto immediatamente la presenza di pacchetti **ARP** (Address Resolution Protocol). Questa comunicazione è fondamentale: il mio sistema sta cercando di **associare un indirizzo IP a un MAC address** sulla rete locale, per poter inviare correttamente i pacchetti al livello di collegamento.

  L'ARP è il primo passo nel dialogo tra dispositivi: senza di esso, non potrei sapere a quale interfaccia fisica inviare i dati.



1	0.000000000	PCSSystemtec_d1:f8:…	Broadcast	ARP	42 Who has 10.0.2.2? Tell 10.0.2.15
2	0.000723171	52:55:0a:00:02:02	PCSSystemtec_d1:f8:…	ARP	64 10.0.2.2 is at 52:55:0a:00:02:02
3	0.000730812	10.0.2.15	1.1.1.1	DNS	73 Standard query 0x1774 A www.cisco.com
4	0.031312858	1.1.1.1	10.0.2.15	DNS	255 Standard query response 0x1774 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME wwwds.cisco.c…
5	0.033214765	10.0.2.15	1.1.1.1	DNS	85 Standard query 0xed55 AAAA e2867.dsca.akamaiedge.net
6	0.057892857	1.1.1.1	10.0.2.15	DNS	141 Standard query response 0xed55 AAAA e2867.dsca.akamaiedge.net AAAA 2a02:26f0:2d80:699::b33 AAAA 2a02:26f0:2d80:691::b33

- **Come può un attaccante usare Wireshark per compromettere la sicurezza della tua rete?**

  Se un **attaccante** riesce a posizionarsi sulla mia rete locale — ad esempio tramite accesso fisico, Wi-Fi compromesso o una macchina virtuale infiltrata — può usare **Wireshark** per intercettare e analizzare il traffico in transito. Ecco cosa potrebbe fare:

  1. Sniffing dei pacchetti

  L'attaccante può catturare pacchetti non cifrati, come quelli di protocolli HTTP, FTP o DNS, e leggere in chiaro:

  - Credenziali di accesso
  - Cookie di sessione
  - Query DNS (che rivelano i siti visitati)

  2. Raccolta di informazioni

  Analizzando gli indirizzi IP, MAC, porte e protocolli, può mappare:

  - Dispositivi attivi sulla rete
  - Servizi esposti
  - Sistemi operativi e versioni

  Queste informazioni sono preziose per preparare attacchi mirati.

  3. Spoofing e Man-in-the-Middle

  Se riesce a manipolare il traffico (ad esempio con ARP spoofing), può:

  - Intercettare comunicazioni tra dispositivi
  - Iniettare pacchetti malevoli
  - Reindirizzare il traffico verso server controllati

  4. Analisi di vulnerabilità

  Monitorando il traffico, può identificare:

  - Software obsoleti

- Servizi non protetti
- Pattern di comportamento prevedibili