

# Analisi del Traffico DNS - Report Professionale

**Autore:** Maikol Nosenzo

**Data:** 24 September 2025

## Executive Summary

Questo report presenta un'analisi del traffico DNS catturato con Wireshark. Sono riportati gli indirizzi MAC e IP di origine e destinazione, le porte coinvolte, il confronto tra query e response DNS, e osservazioni sulla rete (tra cui traffico ARP).

### 1. Ethernet — Indirizzi MAC

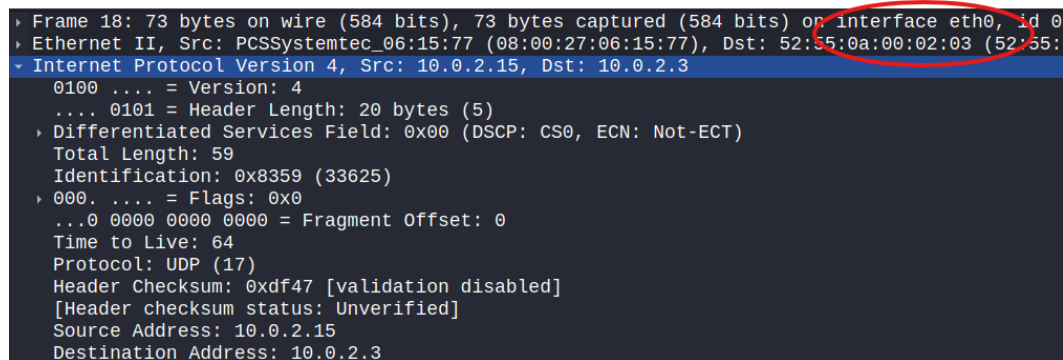
Indirizzo MAC di origine: 08:00:27:06:15:77 (host locale)

Indirizzo MAC di destinazione: 52:55:0a:00:02:03 (server/DNS)

Osservazioni:

- Gli indirizzi MAC sono associati all'interfaccia di rete utilizzata per la cattura (eth0).
- Le comunicazioni mostrano l'inversione degli endpoint tra query e response (come atteso): l'originatore della query diventa destinatario nella response e viceversa.

Figura 1 — Esempio di pacchetto (cattura Wireshark):



```
Frame 18: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_06:15:77 (08:00:27:06:15:77), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 59
  Identification: 0x8359 (33625)
  000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0xdf47 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.0.2.15
  Destination Address: 10.0.2.3
```

### 2. Rete IP — Indirizzi IPv4

Indirizzo IP di origine: 10.0.2.15 (host locale)

Indirizzo IP di destinazione: 10.0.2.3 (server DNS)

Gli indirizzi IP corrispondono all'interfaccia eth0 del sistema che ha effettuato la cattura. Questo conferma che la sorgente delle query è il PC locale e che il server DNS risponde alle richieste.

### 3. Porte — Source & Destination

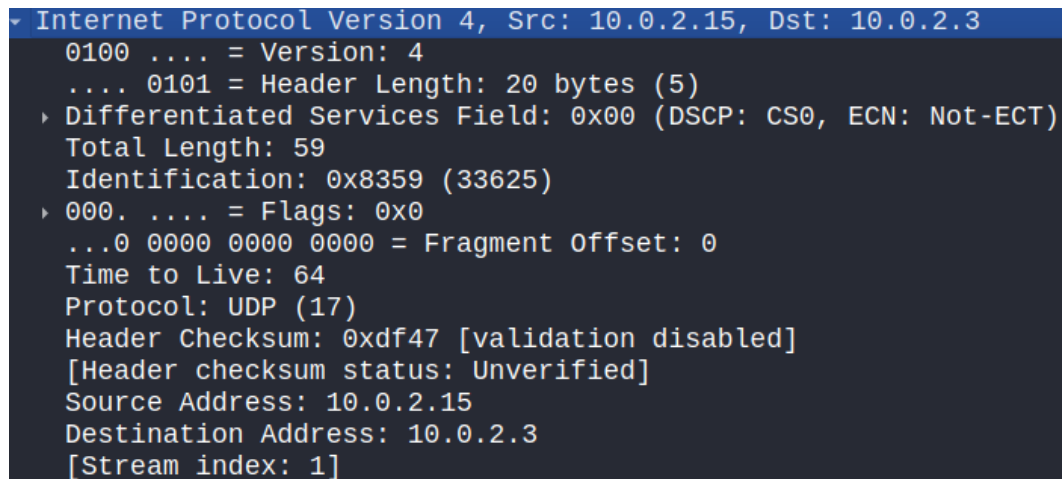
Porta di origine (host): 41758

Porta di destinazione (server DNS): 53

Porta DNS predefinita: 53

Nota: la porta sorgente è una porta effimera scelta dal sistema operativo per la query; il server risponde sempre sulla porta 53 come previsto dal protocollo DNS.

Figura 2 — DNS Query / Response (dettaglio):



```
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 59
  Identification: 0x8359 (33625)
  ▸ 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0xdf47 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.0.2.15
  Destination Address: 10.0.2.3
  [Stream index: 1]
```

#### 4. DNS — Query & Response

Confronto tra query e response:

- Nei pacchetti di query l'host 10.0.2.15 invia richieste al server 10.0.2.3 (porta 53).
- Nelle response si osserva l'inversione degli endpoint: il server 10.0.2.3 invia la risposta a 10.0.2.15.
- Gli indirizzi MAC nei pacchetti mostrano lo stesso comportamento di inversione tra origine e destinazione.

Il server DNS è configurato per eseguire query ricorsive (secondo l'analisi presente nel materiale).

#### 5. Confronto con nslookup

Wireshark fornisce una vista dettagliata di ogni pacchetto scambiato (inclusi header e payload), mentre nslookup restituisce esclusivamente l'esito della risoluzione DNS. Entrambi gli strumenti sono complementari: Wireshark per l'analisi forense/packet-level, nslookup per verifiche funzionali della risoluzione.

#### 6. Analisi ARP e Osservazioni

Rimuovendo il filtro DNS dalla cattura si osservano numerosi pacchetti ARP: richieste 'Who has 10.0.2.X? Tell 10.0.2.15'. Questi pacchetti indicano la mappatura IP→MAC in corso sulla rete locale e sono inviati in broadcast. Le risposte ARP consentono ai dispositivi di popolare la tabella ARP e stabilire comunicazioni a livello Ethernet.

Figura 3 — Esempio di pacchetti ARP osservati:

```

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 n
... ..0... .. = Non-authenticated data: Unacceptable
... ..0000 = Reply code: No error (0)

```

## 7. Implicazioni per la Sicurezza

Un attaccante con accesso alla rete e capacità di sniffing può raccogliere informazioni sensibili se il traffico non è cifrato. In particolare:

- Password e dati trasmessi in chiaro (HTTP, FTP, ecc.) possono essere intercettati.
- È possibile eseguire attacchi Man-in-the-Middle combinando ARP spoofing e sniffing.

Raccomandazioni:

- Utilizzare protocolli cifrati (HTTPS, SSH, TLS) per proteggere i dati in transito.
- Segmentare la rete e limitare l'accesso alle VLAN di management.
- Abilitare DNS-over-TLS o DNS-over-HTTPS dove possibile per proteggere le query DNS.

## 8. Conclusione

La cattura Wireshark analizzata mostra traffico DNS standard tra il client (10.0.2.15) e il server DNS (10.0.2.3). Le osservazioni tratte confermano il corretto funzionamento della risoluzione DNS e mettono in evidenza alcune considerazioni operative e di sicurezza che dovrebbero essere adottate per migliorare la postura di difesa della rete.

## **Allegato: Note originali (domande e risposte)**

S11L3

Osservare i campi di origine e destinazione.

Quali sono gli indirizzi MAC di origine e destinazione?

52:55:0a:00:02:03 destinazione, 08:00:27:06:15:77 source

A quali interfacce di rete sono associati questi indirizzi MAC?

Gli indirizzi MAC sono associati all'interfaccia di rete utilizzata per la cattura dei pacchetti. Avendo catturato i pacchetti tramite una connessione internet, l'interfaccia di rete è eth0.

Osservare gli indirizzi IPv4 di origine e destinazione

Quali sono gli indirizzi IP di origine e destinazione?

L'indirizzo IP di origine è 10.0.2.15, mentre l'indirizzo IP di destinazione è 10.0.2.3

A quali interfacce di rete sono associati questi indirizzi IP?

Gli indirizzi IP sono associati all'interfaccia di rete eth0

Osservare le porte di origine e destinazione

Quali sono le porte di origine e destinazione?

La porta di origine è 41758. La porta di destinazione è 53

Qual è il numero di porta DNS predefinito?

Il numero predefinito di porta DNS è 53

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

L'indirizzo IP e MAC che abbiamo trovato su Wireshark combacia perfettamente a quelli del mio PC.

Abbiamo catturato il traffico del nostro PC tramite Wireshark

Esplorare il Traffico delle Risposte DNS

Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione?

L'indirizzo MAC di origine è 52:55:0a:00:02:02 mentre quello di destinazione è 08:00:27:06:15:77

L'indirizzo IP di origine è 10.0.2.3, mentre quello di destinazione è 10.0.2.15

La porta di origine è 53, mentre quella di destinazione è 41758

Come si confrontano con gli indirizzi nei pacchetti di query DNS?

Confrontato la query dns e la query response, ci accorgiamo che gli indirizzi di destinazione e origine si invertono

Il server DNS può fare query ricorsive?

Sì, il server DNS può fare query ricorsive

Come si confrontano i risultati con quelli di nslookup?

Confrontando i risultati di Wireshark e nslookup, possiamo notare che Wireshark fornisce una visione dettagliata di tutto il traffico di rete e permette di ispezionare ogni singolo pacchetto, anche di altri protocolli.

Nslookup si limita a risolvere i nomi di dominio in indirizzi IP, restituendo solo l'esito della query DNS

Riflessione

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

Togliendo il filtro possiamo notare molte cose interessanti, come ad esempio numerosi pacchetti ARP che chiedono "Who has 10.0.2.4? Tell 10.0.2.15" Queste richieste indicano che i dispositivi stanno cercando di mappare gli IP ai MAC corrispondenti. I pacchetti ARP sono tutti

broadcast, il che significa che le richieste vengono inviate a tutti i dispositivi sulla rete per scoprire chi possiede l'IP in questione.

Alcuni pacchetti ARP contengono risposte, che rivelano gli indirizzi MAC associati agli indirizzi IP. Ciò significa che i dispositivi sulla rete stanno aggiornando la loro tabella ARP con le informazioni corrette sugli indirizzi MAC.

Tramite queste informazioni possiamo imparare alcune cose della rete, come ad esempio:

Topologia di rete, attività sulla rete e/o presenza di dispositivi

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

Un attaccante può usare Wireshark principalmente per intercettare e analizzare il traffico di rete al fine di ottenere informazioni sensibili. Wireshark è uno sniffer, il che significa che cattura i dati che passano attraverso una rete. Per compromettere una rete, un attaccante non usa Wireshark per l'attacco stesso, ma come strumento di ricognizione e analisi.

Un attaccante può utilizzare Wireshark in diverse fasi di un attacco:

Ricognizione e acquisizione di informazioni: un attaccante può usare Wireshark per analizzare il traffico di rete e individuare i sistemi attivi, i servizi in esecuzione, gli indirizzi IP e i protocolli utilizzati. Questa fase è cruciale per pianificare attacchi mirati.

Cattura di dati sensibili: può usare Wireshark per catturare pacchetti di dati non crittografati. Questo include password, nomi utente, cookie di sessione, e-mail e altri dati che viaggiano in chiaro.

Analisi di vulnerabilità: analizzando il traffico, può identificare protocolli insicuri, come HTTP o FTP, e sfruttare queste debolezze per ottenere accesso non autorizzato o per eseguire attacchi Man-in-the-Middle.

Decodifica e analisi post-attacco: dopo aver catturato i pacchetti, l'attaccante può usare le funzionalità di decodifica di Wireshark per interpretare i dati grezzi e estrarre informazioni utili. Questo può includere la ricostruzione di file trasferiti o la lettura di messaggi di chat.