**Catturare il traffico DNS**

**Esplorare il traffico delle query DNS**

**Esplorare il traffico delle risposte DNS**



**Esplorazione del Traffico DNS**

Contesto / Scenario

Wireshark è uno strumento open source di cattura e analisi dei pacchetti. Wireshark fornisce una ripartizione dettagliata dello stack di protocolli di rete. Wireshark consente di filtrare il traffico per la risoluzione dei problemi di rete, investigare problemi di sicurezza e analizzare i protocolli di rete. Poiché Wireshark consente di visualizzare i dettagli dei pacchetti, può essere utilizzato come strumento di ricognizione per un aggressore.

In questo laboratorio installerai Wireshark e lo utilizzerai per filtrare i pacchetti DNS e visualizzare i dettagli dei pacchetti di query e risposta DNS.

**Parte 1: Cattura il traffico DNS**

**Passaggio 1: Scarica e installa Wireshark.**

a. Scarica l'ultima versione stabile di Wireshark da www.wireshark.org . Scegli la versione software di cui hai bisogno in base all'architettura e al sistema operativo del tuo PC.

b. Segui le istruzioni sullo schermo per installare Wireshark. Se ti viene chiesto di installare USBPcap, NON installare USBPcap per la normale cattura del traffico. USBPcap è sperimentale e potrebbe causare problemi USB sul tuo PC.

**Passaggio 2: cattura del traffico DNS.**

a. Avvia Wireshark. Seleziona un'interfaccia attiva con traffico per la cattura dei pacchetti.

b. Cancellare la cache DNS.

1) In Windows, digitare ipconfig /flushdns nel prompt dei comandi.

2) Per la maggior parte delle distribuzioni Linux, una delle seguenti utility viene utilizzata per la memorizzazione nella cache DNS: Systemd -Resolved, DNSMasq e NSCD. Se la tua distribuzione Linux non utilizza una delle utility elencate, esegui una ricerca su Internet per l'utility di memorizzazione nella cache DNS per la tua distribuzione Linux.

(i) Identifica l'utilità utilizzata nella tua distribuzione Linux controllandone lo stato:

Systemd-Resolved: stato systemctl systemd-resolved.service

DNSMasq: stato systemctl dnsmasq.service

NSCD: stato systemctl nscd.service

(ii) Se si utilizza system-resolved, immettere systemd-resolve –flush-caches per svuotare la cache per Systemd-Resolved prima di riavviare il servizio. I seguenti comandi riavviano il servizio associato utilizzando privilegi elevati:

Systemd-Resolved: sudo systemctl restart systemd-resolved.service

DNSMasq: sudo systemctl restart dnsmasq.service

NSCD: sudo systemctl restart nscd.service

3) Per macOS, inserisci sudo killall -HUP mDNSResponder per cancellare la cache DNS nel Terminale. Esegui una ricerca su Internet per i comandi per cancellare la cache DNS per un sistema operativo più vecchio.

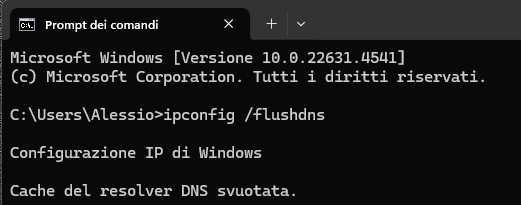
c. Al prompt dei comandi o al terminale, digitare nslookup per accedere alla modalità interattiva.

d. Inserisci il nome di dominio di un sito web. In questo esempio viene utilizzato il nome di dominio www.cisco.com .

e. Digitare exit quando terminato. Chiudere il prompt dei comandi.

f. Fare clic su Interrompi acquisizione pacchetti per interrompere l'acquisizione di Wireshark.

In Windows, inserisci ipconfig /flushdns nel Prompt dei comandi.



- Inserisci il nome di dominio di un sito web. Il nome di dominio è www.cisco.com. Clicca.

- Ferma la cattura dei pacchetti per interrompere la cattura di Wireshark.

- Osserva il traffico catturato nel pannello della lista pacchetti di Wireshark. Inserisci `udp.port == 53` nella casella del filtro e clicca sulla freccia (oppure premi invio) per visualizzare solo i pacchetti DNS.

Parte 2: Esplora il traffico delle query DNS

1. 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.

b. Selezionare il pacchetto DNS contenente la query standard e A www.cisco.com nella colonna Info.

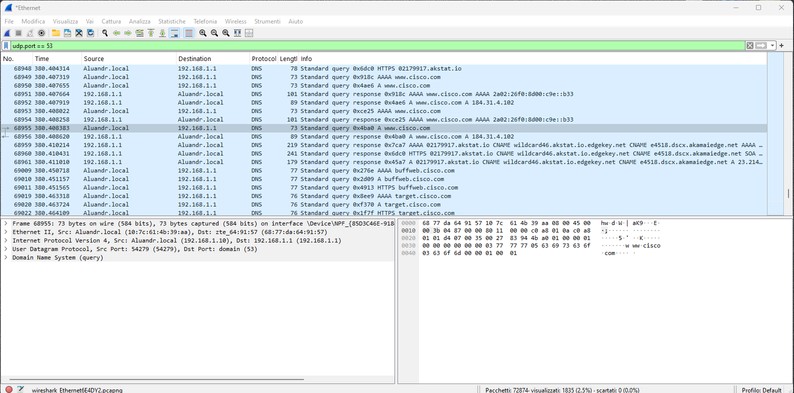
c. Nel riquadro Dettagli pacchetto, notare che questo pacchetto ha Ethernet II, Internet Protocol versione 4, User Datagram Protocol e Domain Name System (query).

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

Quali sono gli indirizzi MAC di origine e di destinazione? A quali interfacce di rete sono associati questi indirizzi MAC?

In questo esempio, l'indirizzo MAC sorgente è associato alla NIC sul PC e l'indirizzo MAC di destinazione è associato al gateway predefinito. Se è presente un server DNS locale, l'indirizzo MAC di destinazione sarebbe l'indirizzo MAC del server DNS locale.

e. Espandi Protocollo Internet versione 4. Osserva gli indirizzi IPv4 di origine e di destinazione.

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

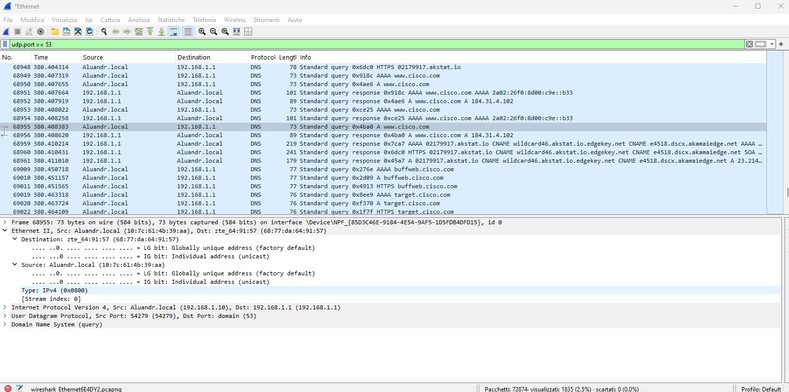
- Inserisci il nome di dominio di un sito web. Il nome di dominio è www.cisco.com. Clicca.

**Esplorare il traffico delle query DNS**

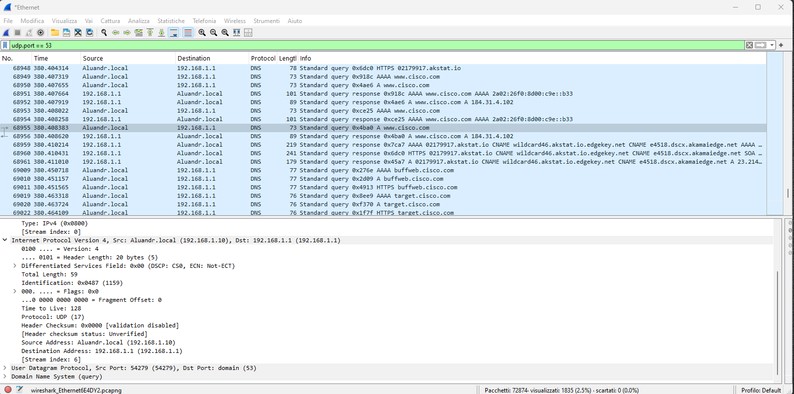
- Ferma la cattura dei pacchetti per interrompere la cattura di Wireshark.

- Osserva il traffico catturato nel pannello della lista pacchetti di Wireshark. Inserisci `udp.port == 53` nella casella del filtro e clicca sulla freccia (oppure premi invio) per visualizzare solo i pacchetti DNS.

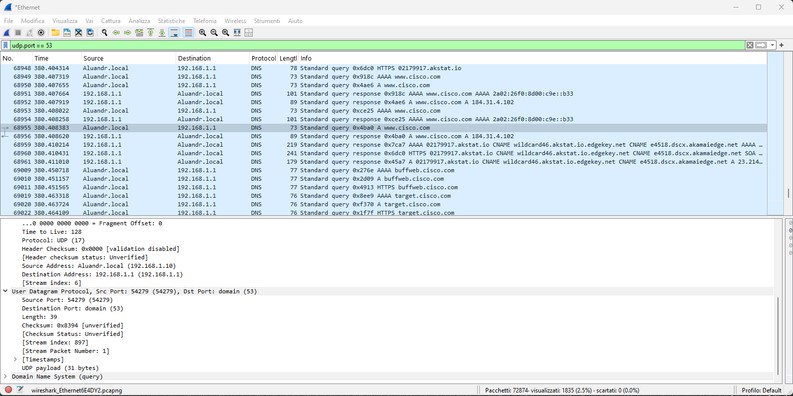
- \*\*Espandi Ethernet II per visualizzare i dettagli. Osserva i campi di origine e destinazione.\*\*



Espandi il Protocollo Internet Versione 4. Osserva gli indirizzi IPv4 di origine e destinazione.

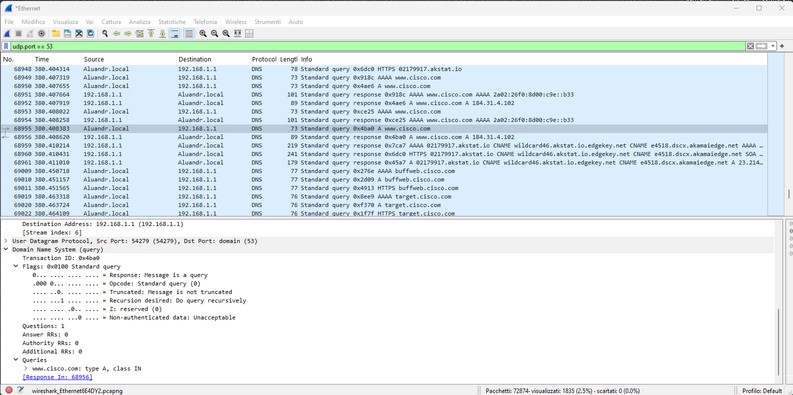


* Espandi il Protocollo Datagramma Utente (UDP). Osserva le porte di origine e destinazione.

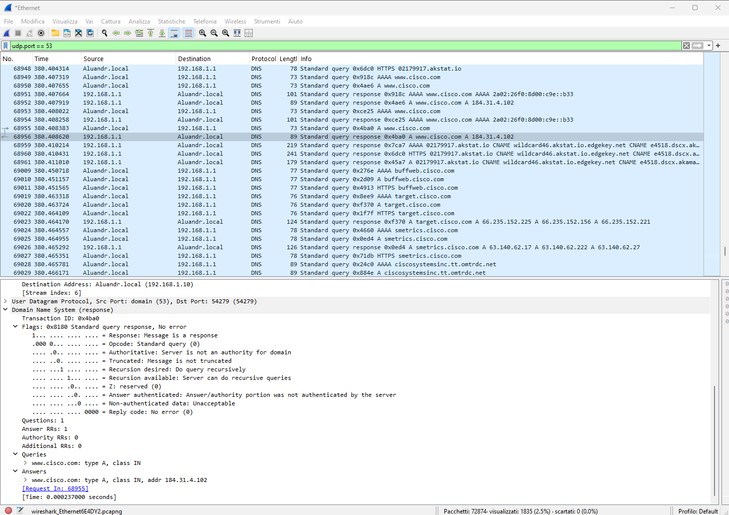


**Esplorare il traffico delle risposte DNS**

Espandi il Domain Name System (query) nel pannello Dettagli pacchetto.Poi espandi le Flags e le Queries.



Seleziona il pacchetto di risposta DNS corrispondente che ha "Standard query response" e "A www.cisco.com" nella colonna delle info



Espandi Domain Name System (response). Poi espandi le Flags, Queries e Answers.

