EPICODE

Cyber Security & Ethical Hacking
Laboratorio giorno 3 – Cisco CyberOps

Esplorazione del Traffico DNS

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.

Istruzioni

Parte 1: Catturare il Traffico DNS

Passo 1: Scaricare e installare Wireshark.

a. Scaricare l'ultima versione stabile di Wireshark da www.wireshark.org. Scegliere la versione software necessaria in base all'architettura e al sistema operativo del PC. In alternativa potete usare kali.

b. Seguire le istruzioni a schermo per installare Wireshark. Se viene richiesto di installare USBPcap, **NON** installare USBPcap per la normale cattura del traffico. USBPcap è sperimentale e potrebbe causare problemi USB sul PC. Questo passaggio non è necessario se avete optato per kali.

Passo 2: Catturare il traffico DNS.

a. Avviare Wireshark. Selezionare un'interfaccia attiva con traffico per la cattura dei pacchetti.

b. Pulire la cache DNS (non necessario se avete optato per kali).

1) In Windows, inserire ipconfig /flushdns nel Prompt dei Comandi.

2) Per la maggior parte delle distribuzioni Linux, una delle seguenti utility viene utilizzata per la 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 caching DNS della tua distribuzione Linux.

(i) Identificare l'utility utilizzata nella tua distribuzione Linux controllando lo stato:
Systemd-Resolved: **systemctl status systemd-resolved.service**
DNSMasq: **systemctl status dnsmasq.service**
NSCD: **systemctl status nscd.service**

(ii) Se stai usando systemd-resolved, inserisci `**systemd-resolve --flush-caches**` per pulire la cache per Systemd-Resolved prima di riavviare il servizio. I seguenti comandi riavviano il servizio associato usando 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, inserire sudo killall -HUP mDNSResponder per p.ulire la cache DNS nel Terminale. Eseguire una ricerca su internet per i comandi per pulire la cache DNS per un OS più vecchio

c. A un prompt dei comandi o terminale, digitare nslookup per entrare in modalità interattiva.

d. Inserire il nome di dominio di un sito web. Il nome di dominio www.cisco.com è usato in questo esempio.

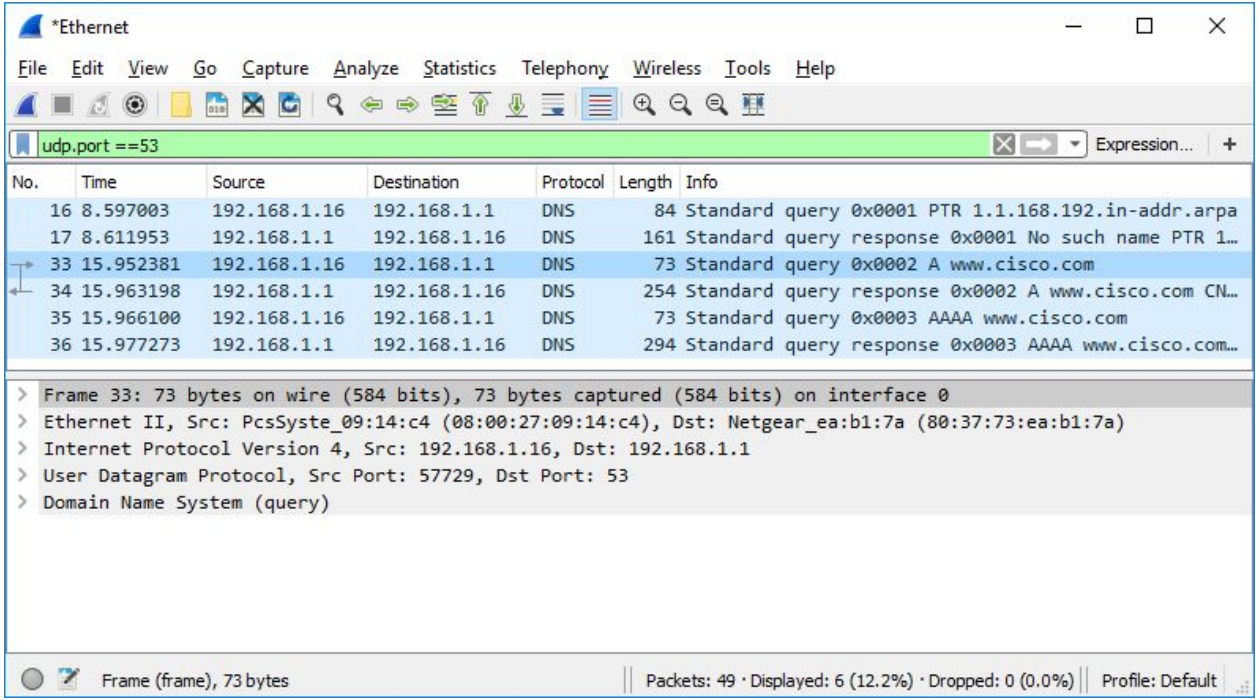
e. Digitare exit quando finito. Chiudere il prompt dei comandi.

f. Fare clic su Stop capturing packets (Interrompi cattura pacchetti) per fermare la cattura di Wireshark.

Parte 2: Esplorare il Traffico delle Query DNS

a. Osservare il traffico catturato nel riquadro Elenco Pacchetti (Packet List) di Wireshark. Inserire udp.port == 53 nella casella del filtro e fare clic sulla freccia (o premere invio) per visualizzare solo i pacchetti DNS.

Nota: Gli screenshot forniti sono solo esempi. Il tuo output potrebbe essere leggermente diverso.



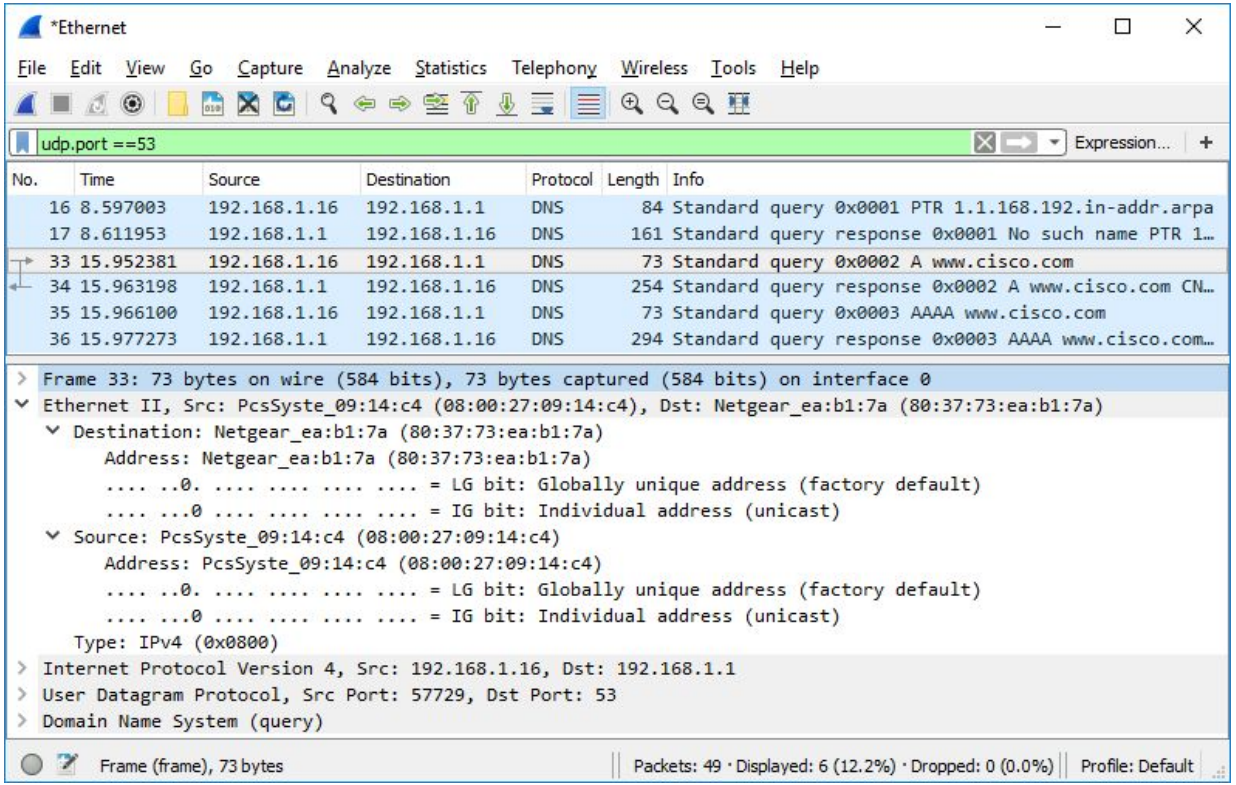
b. Selezionare il pacchetto DNS che contiene Standard query e A www.cisco.com nella colonna Info.

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

d. Espandere Ethernet II per visualizzare i dettagli. Osservare i campi di origine e destinazione.

Quali sono gli indirizzi MAC di origine e destinazione?

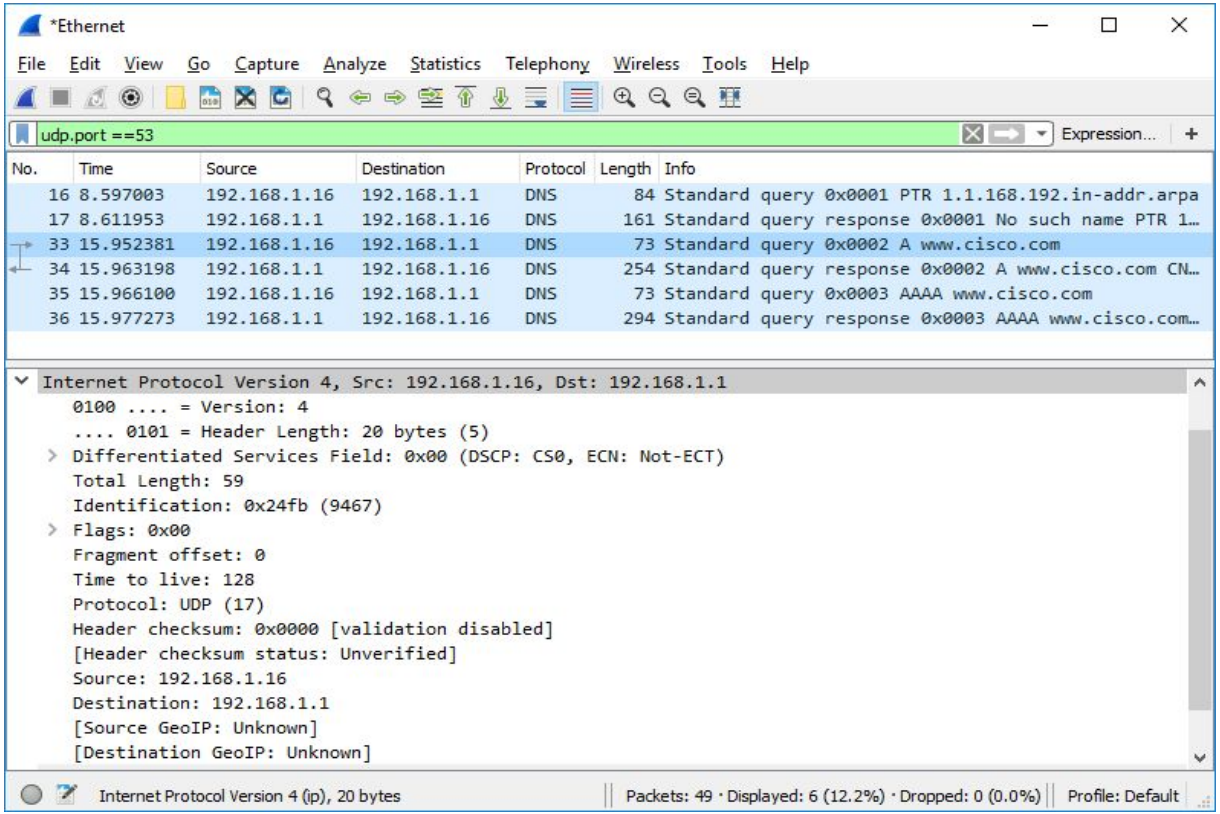
A quali interfacce di rete sono associati questi indirizzi MAC?

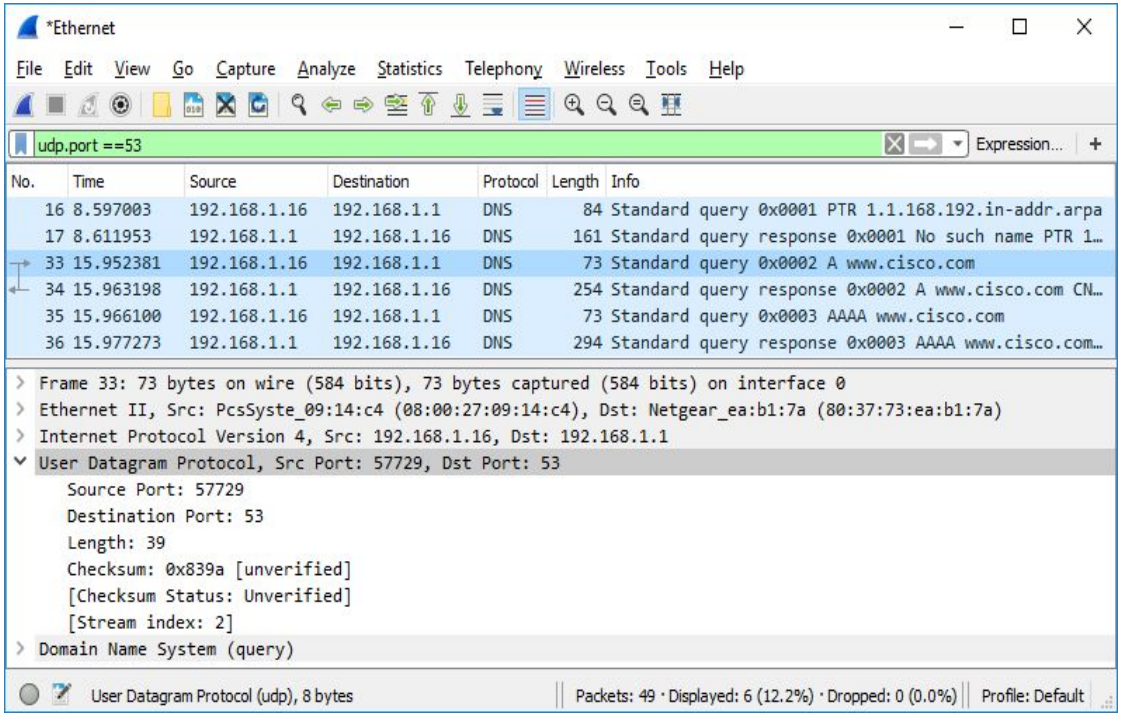


e. Espandere Internet Protocol Version 4. Osservare gli indirizzi IPv4 di origine e destinazione.

Quali sono gli indirizzi IP di origine e destinazione?

A quali interfacce di rete sono associati questi indirizzi IP?





f. Espandere User Datagram Protocol (UDP). Osservare le porte di origine e destinazione.

Quali sono le porte di origine e destinazione?

Qual è il numero di porta DNS predefinito?

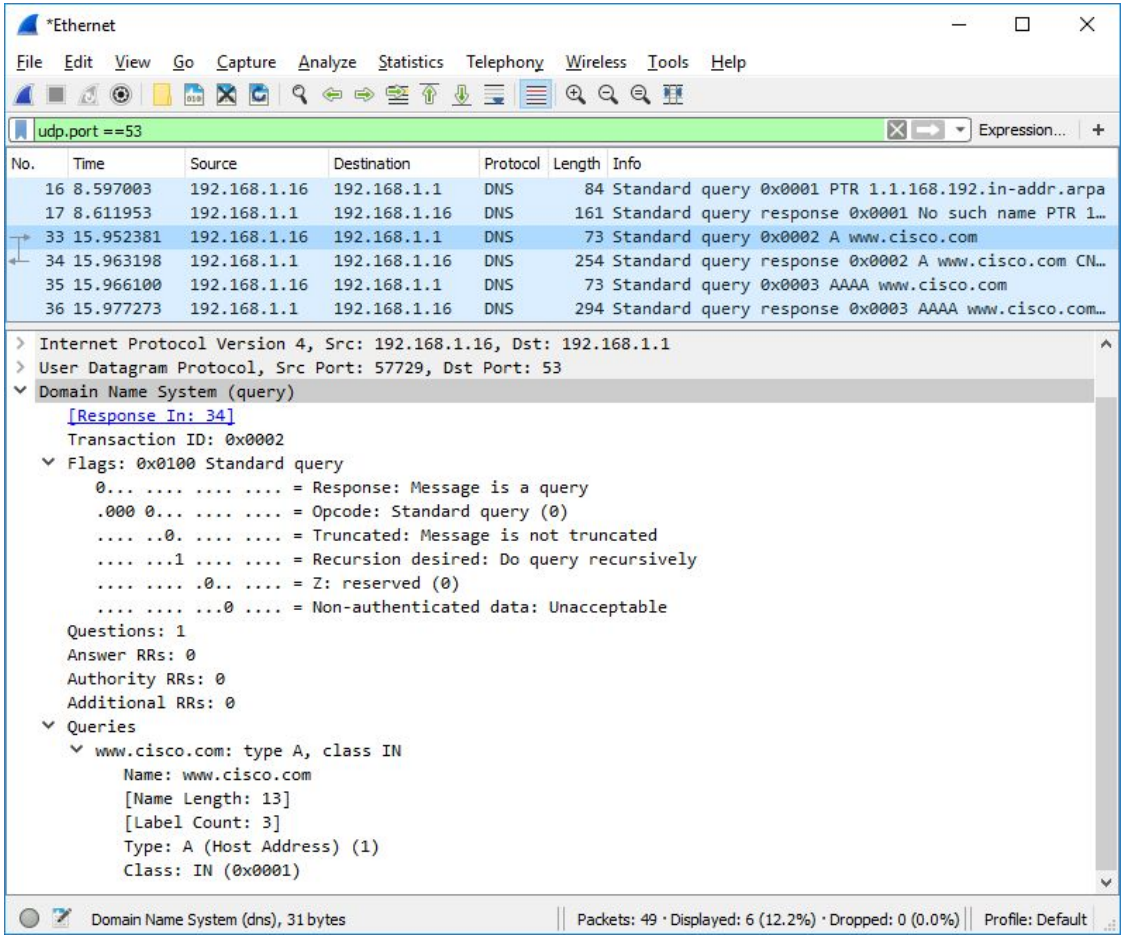
g. Determinare l'indirizzo IP e MAC del PC.

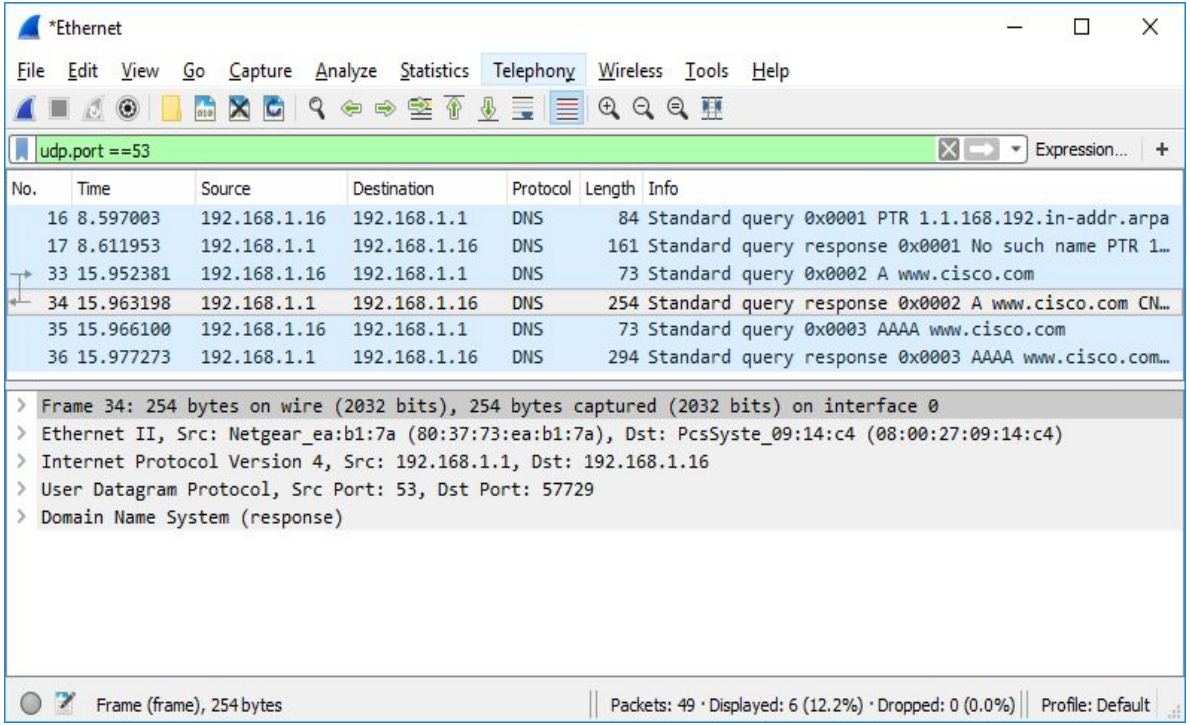
1. In un prompt dei comandi di Windows, inserire arp –a e ipconfig /all per registrare gli indirizzi MAC e IP del PC.
2. Per PC Linux e macOS, inserire ifconfig o ip address in un terminale.

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

h. Espandere Domain Name System (query) nel riquadro Dettagli Pacchetto. Quindi espandere Flags e Queries.

i. Osservare i risultati. Il flag è impostato per eseguire la query ricorsivamente per interrogare l'indirizzo IP di www.cisco.com





Parte 3: Esplorare il Traffico delle Risposte DNS

a. Selezionare il corrispondente pacchetto DNS di risposta che ha Standard query response e A www.cisco.com nella colonna Info

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

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

b. Espandere Domain Name System (response). Quindi espandere Flags, Queries, e Answers.

c. Osservare i risultati.

Il server DNS può fare query ricorsive?

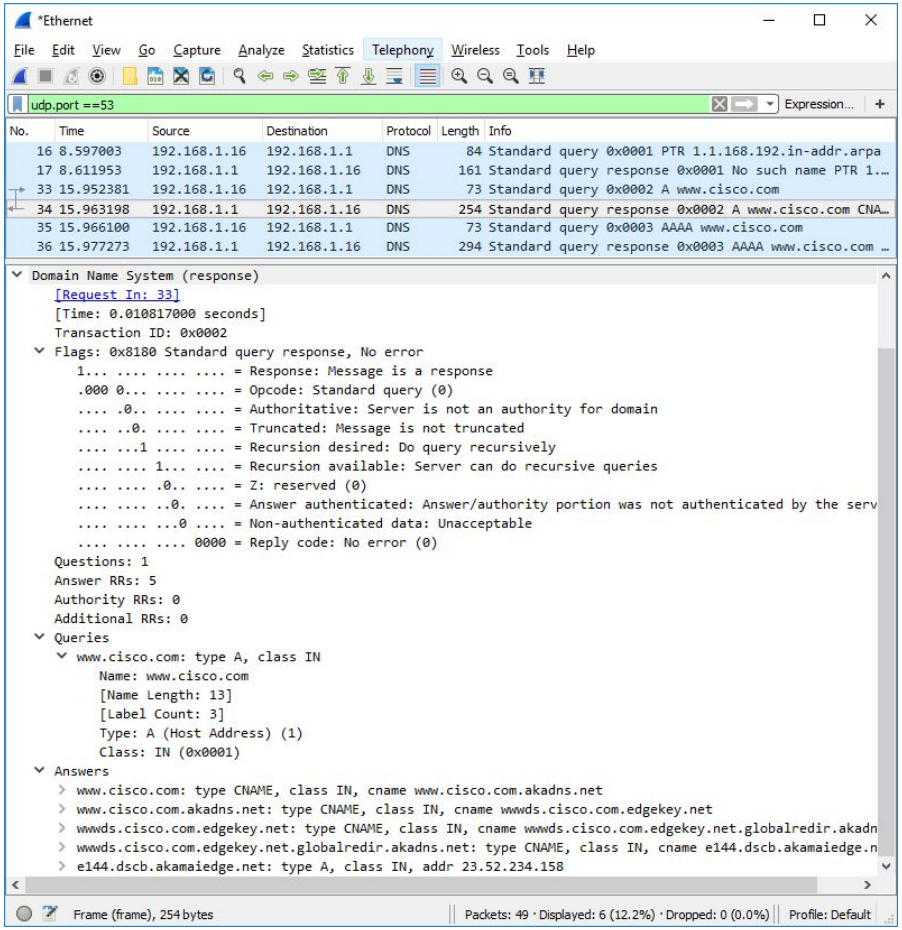
d. Osservare i record CNAME e A nei dettagli delle Risposte (Answers).

Come si confrontano i risultati con quelli di nslookup?

Riflessione

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

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



EPICODE

Roma | Milano | Berlino

business@epicode.com