Cisco CyberOps 3

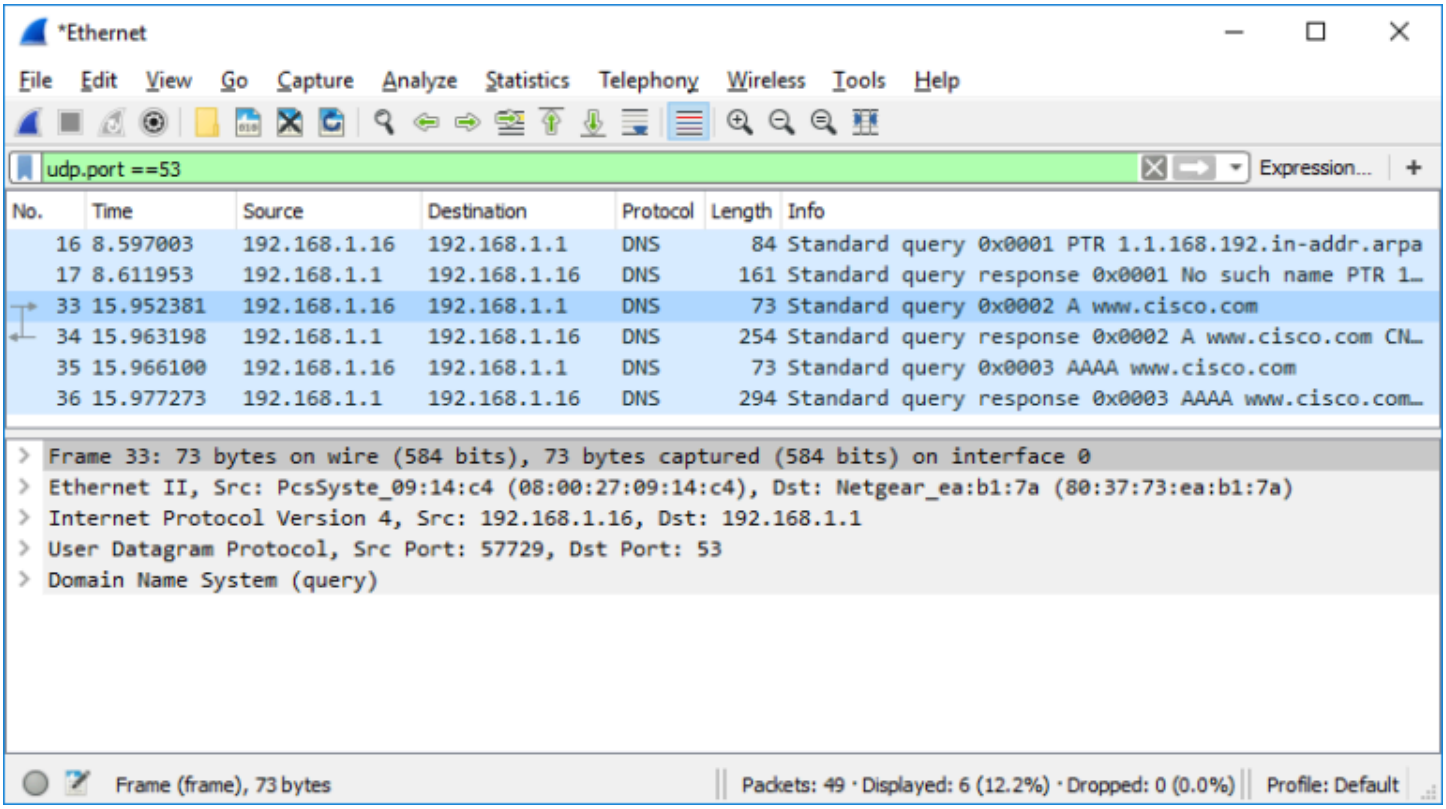
Cattura del traffico DNS

1. **Avvio di Wireshark**
   - Avviare Wireshark e selezionare un’interfaccia di rete attiva per la cattura dei pacchetti.
2. **Svuotare la cache DNS**
   - **Windows**: Aprire il prompt dei comandi ed eseguire:
   - cmd
   - Copia codice
   - ipconfig /flushdns
3. **Generare traffico DNS**
   - Aprire un prompt dei comandi o terminale ed eseguire:
   - cmd
   - Copia codice
   - nslookup www.cisco.com
   - Uscire dalla modalità interattiva di nslookup digitando exit.
4. **Interrompere la cattura dei pacchetti**
   - In Wireshark, fare clic su "Stop" per interrompere la cattura.

Parte 2: Esplora il traffico delle query DNS

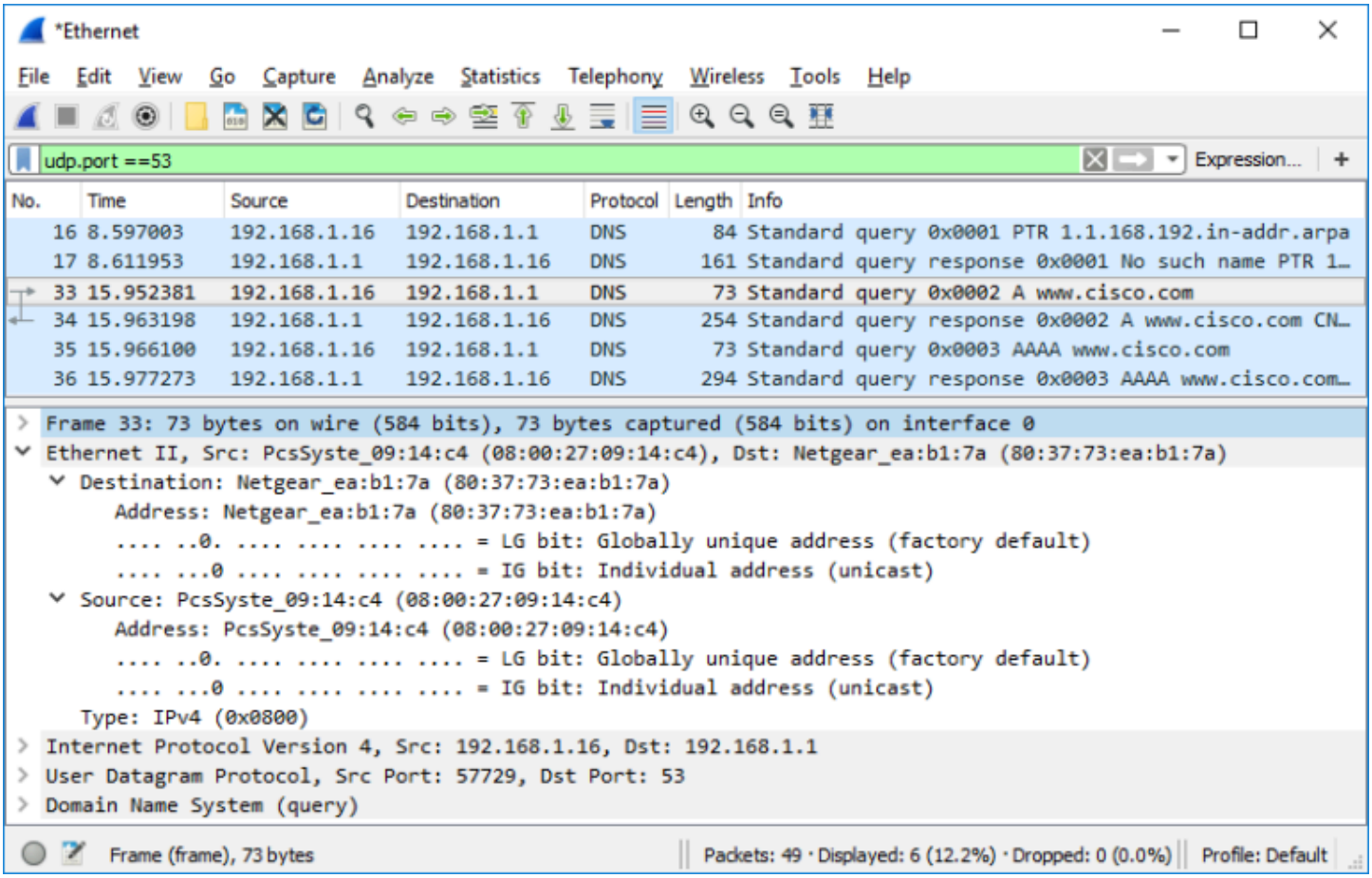
Filtraggio dei pacchetti DNS

1. Inserire il filtro:
2. plaintext
3. Copia codice
4. udp.port == 53
5. Questo mostrerà solo i pacchetti DNS.



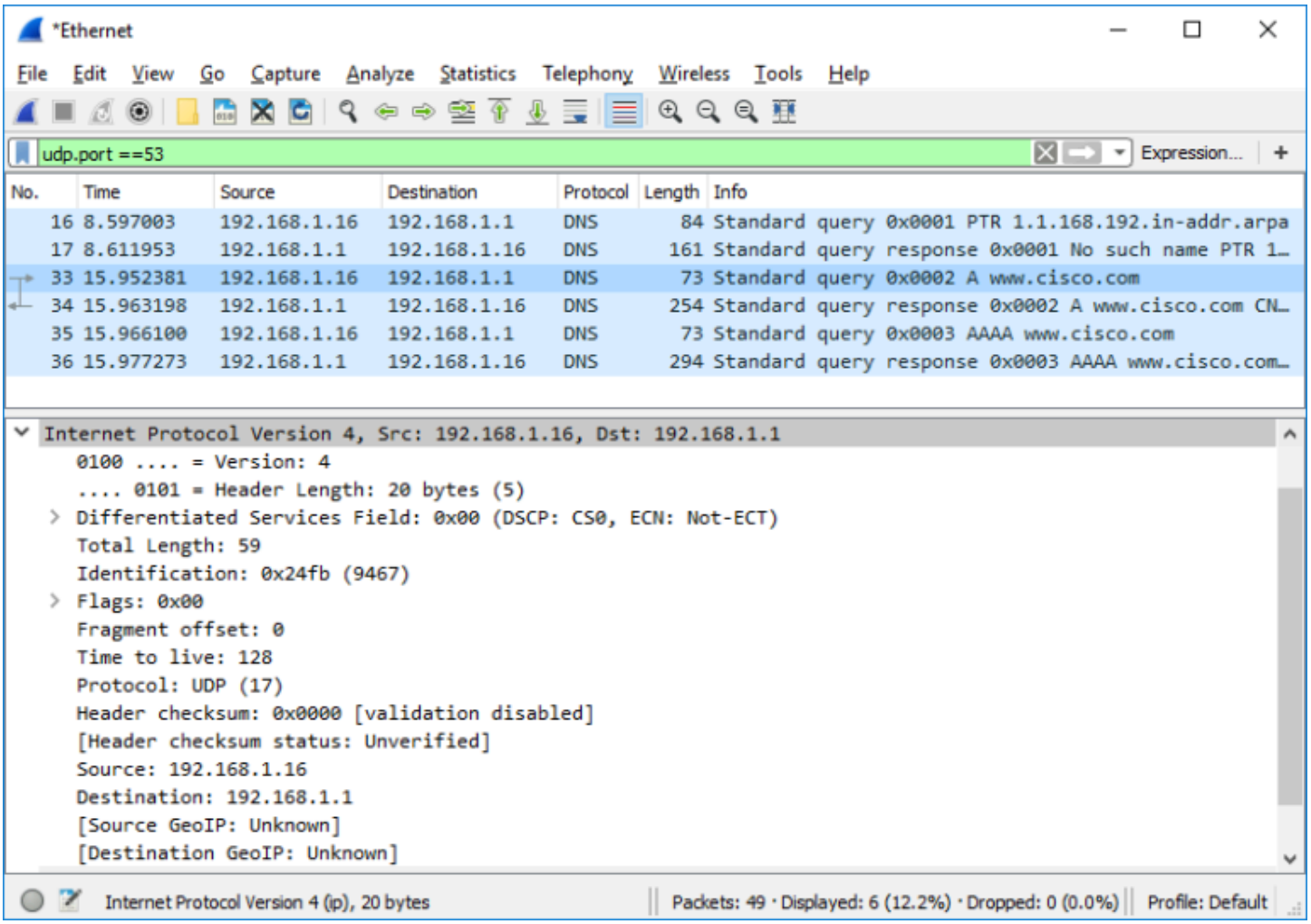
Analisi del pacchetto di query DNS

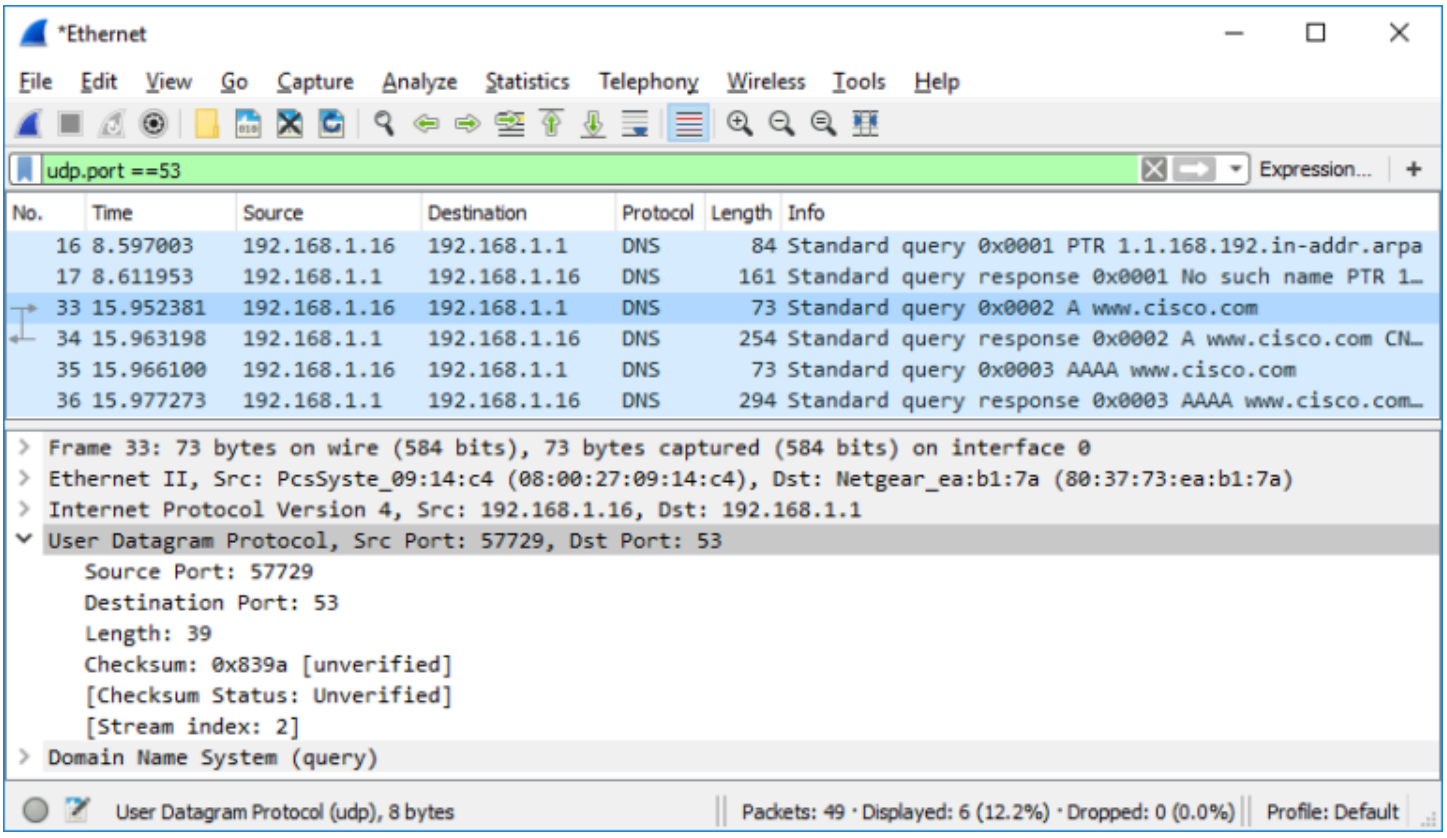
1. **Espansione dei dettagli**:
   - **Ethernet II**: Identificare gli indirizzi MAC di origine (NIC del PC) e di destinazione (gateway o server DNS locale).
   - **IPv4**: Osservare gli indirizzi IP di origine (PC) e di destinazione (gateway o server DNS).
   - **UDP**: Analizzare le porte di origine e destinazione. La porta 53 è quella predefinita per DNS.
2. **Confronto con la configurazione locale**:
   - Utilizzare i comandi:
   - cmd
   - Copia codice
   - arp -a
   - ipconfig /all
   - Confrontare gli indirizzi MAC e IP trovati in Wireshark con quelli registrati dal PC.



Dettagli della query DNS

- Espandere "Domain Name System (query)" per analizzare flag, domande e opzioni.
- Confermare che la query è ricorsiva e richiede l'indirizzo IP per www.cisco.com.





Parte 3: Esplora il traffico di risposta DNS

Analisi del pacchetto di risposta

1. **Confronto indirizzi**:
   - Gli indirizzi MAC e IP di origine/destinazione sono invertiti rispetto al pacchetto di query.
   - Verificare che il numero di porta DNS (53) sia utilizzato nella risposta.
2. **Espansione dei dettagli DNS**:
   - Analizzare i flag e i record (CNAME e A).
   - Verificare che i risultati coincidano con quelli di nslookup.

Riflessione

1. **Osservazione senza filtri**:
   - La rimozione del filtro consente di vedere altri tipi di traffico (es. ARP, DHCP), che possono rivelare informazioni su dispositivi e configurazioni di rete.
2. **Potenziale pericolo**:
   - Un attaccante potrebbe utilizzare Wireshark per intercettare traffico non crittografato e ottenere informazioni sensibili come credenziali o dati personali.

Conclusione

L'utilizzo di strumenti come Wireshark è essenziale per comprendere il funzionamento del traffico di rete, ma è fondamentale garantire che il traffico sensibile sia protetto con crittografia per prevenire intercettazioni da parte di terzi.