ESERCIZIO: Laboratorio - Esplorazione del Traffico DNS

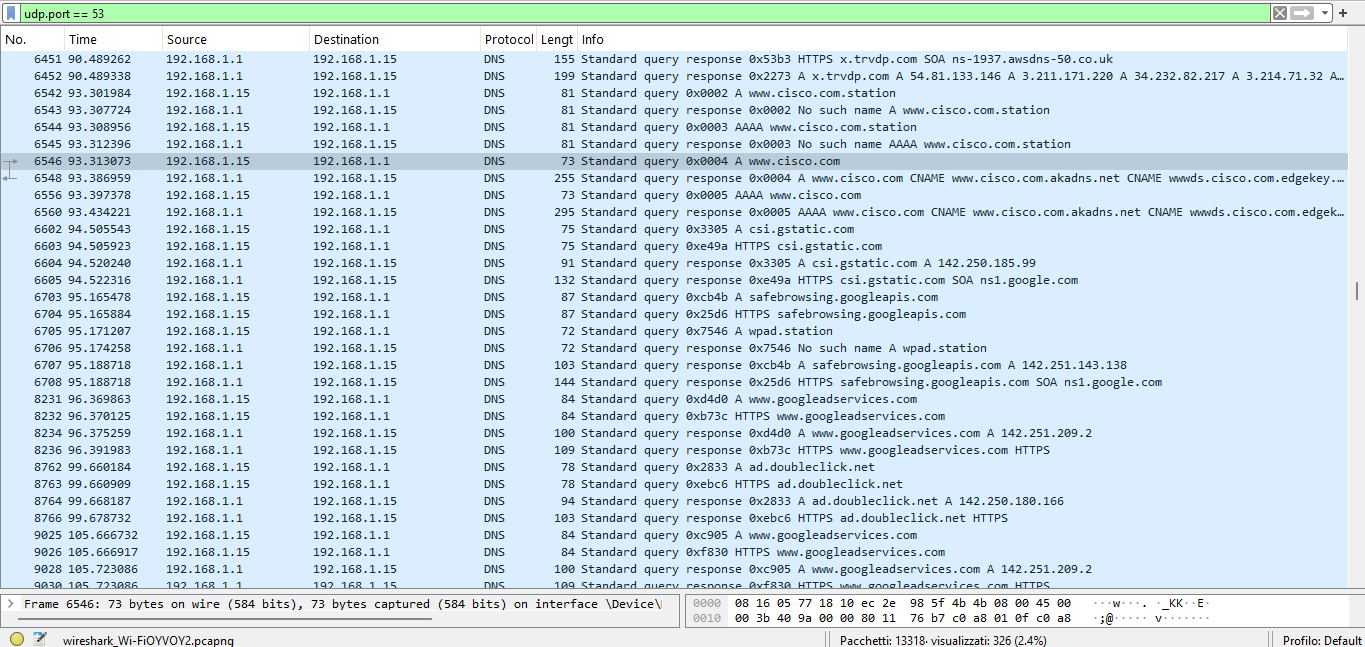
In questo laboratorio, completa i seguenti obiettivi:

● Catturare il traffico DNS

● Esplorare il traffico delle query DNS

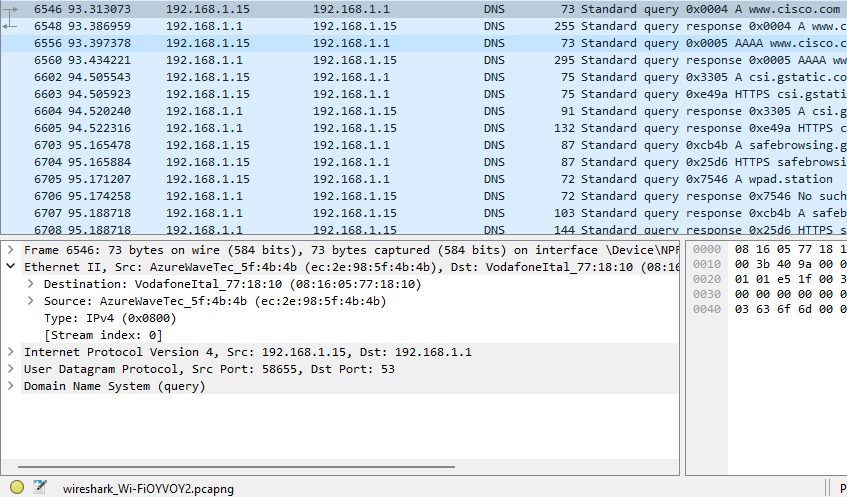
● Esplorare il traffico delle risposte DNS

L’esercizio l’ho svolto su windows, usando il *prompt dei comand*i e *wireshark* (avviato prima ancora di usare il cmd)*.* Il traffico DNS l’ho catturato cancellando la cache. Ho usato il comando ***ipconfig /flushdns***nel cmd di windows. Dopodichè sono andato avanti digitando ***nslookup*,** per accedere alla modalità interattiva. Qui come dominio ho usato *ww.cisco.com* e una volta terminato sono uscito. Da qui in poi ho usato solo wireshark e come prima cosa ho inserito ***udp.port == 53*** nella casella dei filtri, per visualizzare solo i pacchetti DNS.



Ho selezionato il pacchetto DNS contenente la query standard con nome del dominio inserito in precedenza, per visualizzare i vari dati di rete.

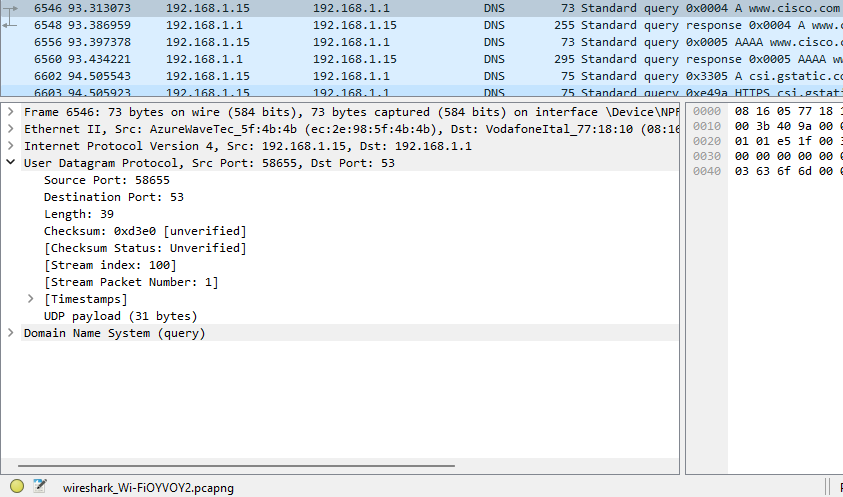
**ETHERNET**

****

(In questo screen mi sono dimenticato di espandere le voci *Destination* e *Source*)

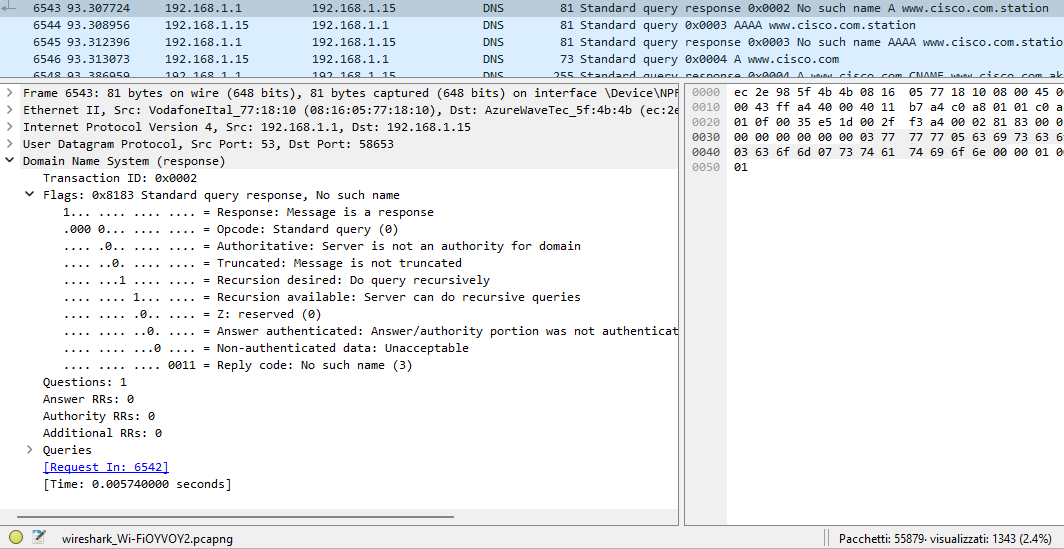
In questo esempio, l'indirizzo MAC sorgente è associato alla NIC sul PC e l'indirizzo MAC di destinazione è associato al gateway predefinito. Se è presente un server DNS locale, l'indirizzo MAC di destinazione sarebbe l'indirizzo MAC del server DNS locale.

**PROTOCOLLO USER DATAGRAM**



Il numero della porta di origine è 58655 e la porta di destinazione è 53, che è il numero di porta DNS predefinito.

**RISPOSTA QUERY STANDARD (flag)**



L'IP sorgente, l'indirizzo MAC e il numero di porta nel pacchetto di query sono ora indirizzi di destinazione. L'IP destinazione, l'indirizzo MAC e il numero di porta nel pacchetto di query sono ora indirizzi di origine.