Report: Analisi del Traffico DNS con Wireshark

1. Obiettivo del laboratorio

Lo scopo di questa esercitazione è imparare a:
- Catturare e filtrare il traffico DNS generato dal sistema
- Analizzare in dettaglio le query DNS e le risposte DNS
- Rilevare indirizzi MAC, IP e porte UDP
- Comprendere il comportamento del protocollo DNS
- Riflettere sull'utilizzo lecito e potenzialmente illecito di strumenti di sniffing

2. Contesto legale

L'utilizzo di Wireshark per catturare pacchetti è legale solo in contesti autorizzati. In questa attività:
- È stato utilizzato un dispositivo personale (Kali Linux)
- La rete analizzata è sotto il nostro controllo (ambiente locale)
- Le query DNS sono generate consapevolmente da un comando (`nslookup`) verso un dominio pubblico

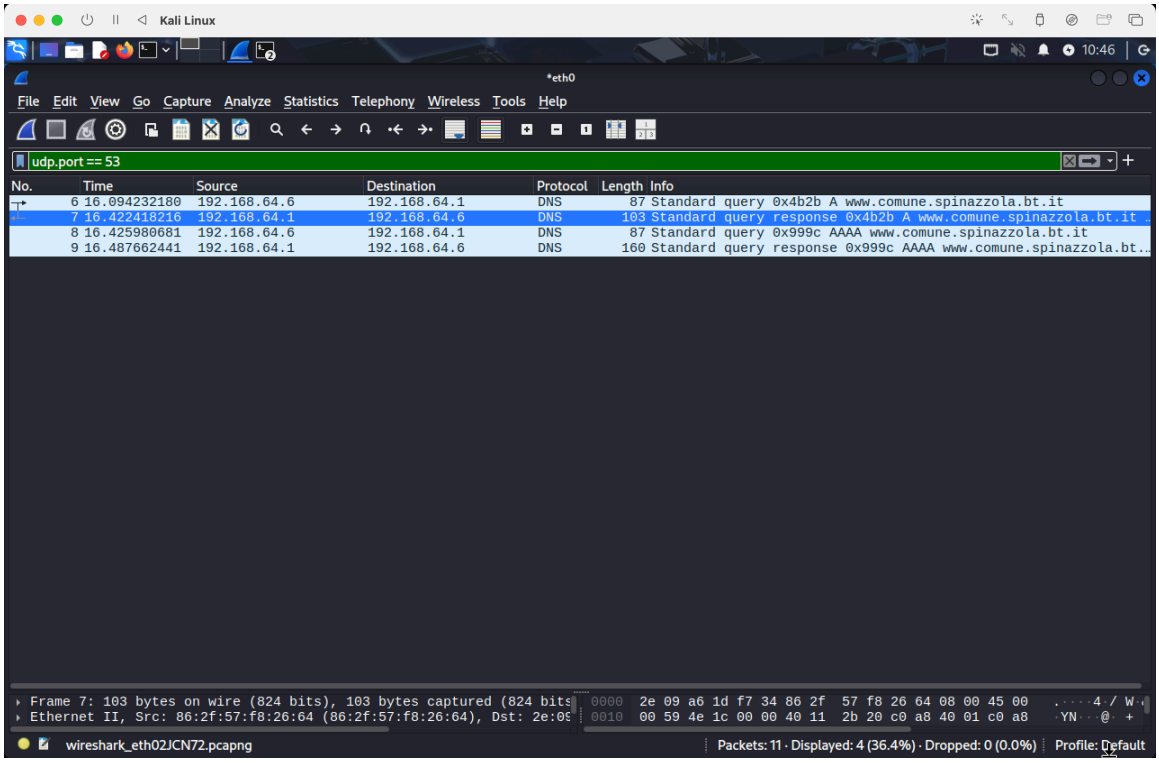
Non è stato intercettato alcun traffico di terzi. L'uso è quindi conforme alle norme legali e deontologiche, e si inquadra in un contesto didattico-laboratoriale.

3. Strumenti e comandi utilizzati

- Software: Wireshark
- Kali Linux (VM)
- Comandi terminale: nslookup www.comune.spinazzola.bt.it
- Interfaccia monitorata: eth0
- Filtro applicato in Wireshark: udp.port == 53

4. Fasi operative

1. Pulizia cache DNS con `sudo systemctl restart systemd-resolved.service`
2. Avvio di Wireshark sull'interfaccia eth0
3. Esecuzione della query DNS con `nslookup www.comune.spinazzola.bt.it`
4. Interruzione della cattura una volta ricevuta la risposta
5. Applicazione del filtro udp.port == 53

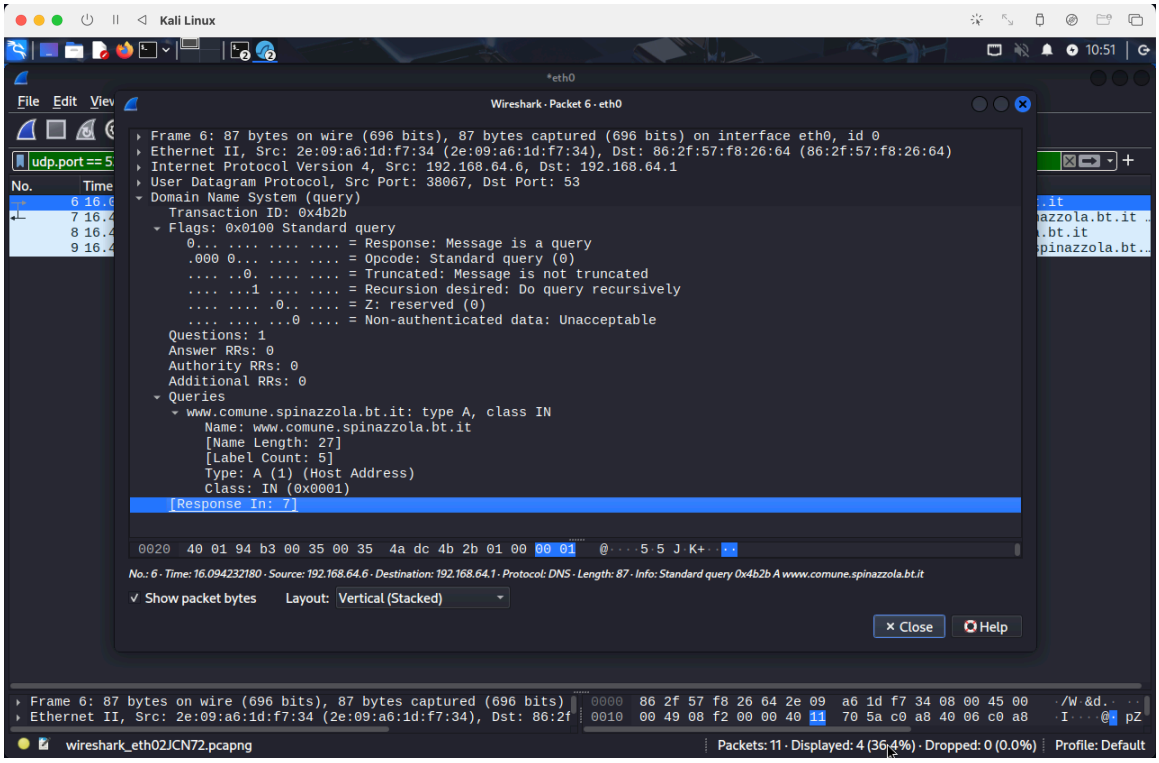


5. Analisi dei pacchetti DNS

Frame 6 – Query DNS

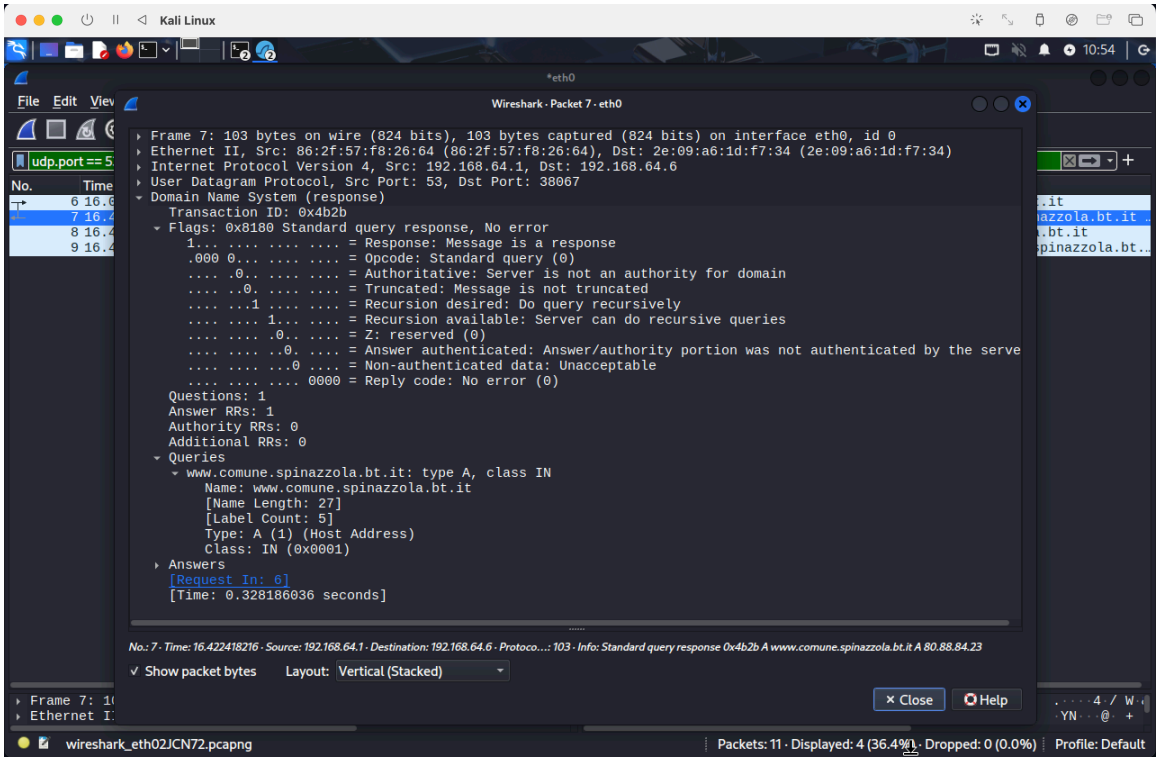
Dominio richiesto: www.comune.spinazzola.bt.it
Tipo: Standard query A
MAC sorgente: 2e:09:a6:1d:f7:34
MAC destinazione: 86:2f:57:f8:26:64

IP sorgente: 192.168.64.6
IP destinazione: 192.168.64.1
Porta sorgente UDP: 38067
Porta destinazione UDP: 53
DNS Flag: Recursion Desired = 1



Frame 7 – Risposta DNS

Tipo: Standard query response A
IP restituito: 80.88.84.23
MAC sorgente: 86:2f:57:f8:26:64
MAC destinazione: 2e:09:a6:1d:f7:34
IP sorgente: 192.168.64.1
IP destinazione: 192.168.64.6
Porta sorgente UDP: 53
Porta destinazione UDP: 38067
DNS Flag: Recursion Available = 1



6. Riflessione e Sicurezza

Osservando i record di risposta DNS, Wireshark mostra dettagli completi della risoluzione del dominio.
Il comando nslookup restituisce lo stesso IP, ma non mostra i flag o l'intero contenuto DNS.

Quando si rimuove il filtro in Wireshark, si osservano altri protocolli (ARP, ICMPv6, MDNS), che forniscono informazioni utili sulla rete.

Un attaccante può usare Wireshark per:
- Osservare i siti visitati (DNS sniffing)
- Identificare IP e MAC della rete
- Attuare spoofing DNS o ARP
- Eseguire attacchi MITM (Man-in-the-Middle)

Wireshark è quindi uno strumento potente ma da utilizzare solo in ambienti controllati.