```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

Parte 1: Sintesi del problema riscontrato nel traffico DNS e ICMP

I log del network protocol analyzer indicano che la **porta 53 (UDP)** risulta **irraggiungibile** durante i tentativi di risoluzione del dominio **yummyrecipesforme.com** tramite il server DNS esterno con indirizzo IP **203.0.113.2**.
La porta 53 è normalmente utilizzata per il **traffico DNS**.
Il registro di rete mostra diversi messaggi ICMP "**Destination Unreachable – Port Unreachable**" restituiti dal server DNS.

Questo comportamento può indicare una **configurazione errata del servizio DNS**, una **regola del firewall che blocca il traffico UDP sulla porta 53**, oppure un possibile **tentativo malevolo di interrompere la risoluzione DNS** all'interno della rete.

Parte 2: Analisi dei dati e possibile causa dell'incidente

L'incidente si è verificato intorno alle **13:24 del 10 ottobre 2025**, quando il team IT ha rilevato una serie di errori di risoluzione DNS durante il monitoraggio del traffico di rete.
Il team ha utilizzato lo strumento di analisi **tcpdump** e ha identificato un modello ricorrente di richieste DNS inviate tramite **UDP** dall'indirizzo **192.51.100.15** verso **203.0.113.2**, seguite da messaggi ICMP che indicavano che la **porta UDP 53 era irraggiungibile**.

Il team di sicurezza ha quindi avviato un'indagine per verificare se il **servizio DNS** sul server esterno fosse attivo e correttamente configurato. Sono state inoltre controllate le **impostazioni del firewall e delle ACL** per determinare se il traffico UDP in entrata o in uscita sulla porta 53 fosse bloccato.

I risultati principali mostrano che le richieste DNS venivano costantemente respinte, confermando che il server di destinazione **non accettava traffico DNS su UDP**. Ciò potrebbe essere dovuto a un **malfunzionamento del servizio DNS**, a una **configurazione errata del firewall** o a una **politica di filtraggio di rete** applicata al perimetro.

Il dipartimento IT sospetta che l'incidente possa essere stato causato da una **configurazione errata del server DNS** o da un **blocco del traffico UDP sulla porta 53** imposto da una misura di sicurezza. Sono in corso ulteriori verifiche per determinare se l'evento possa essere collegato a un **tentativo di scansione malevolo** o a un **errore accidentale di configurazione**.