

```
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
```

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

- The client sent multiple requests (3) via the UDP protocol for a DNS resolution for the website `yummyrecipesforme.com`, indicated by the A?, when trying to reach the website. Each time there was a response to the client, the ICMP protocol was used which is the protocol used when there is an error. The error states “udp port 53 unreachable length –“

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

- Based on the information, the DNS server is down or unable to respond to the request. This is known because port 53 is used for DNS, meaning that the used port for resolving DNS requests is not reachable. More testing would have to be done to see if it's offline, if there was a DoS attack, or a misconfiguration.