Cybersecurity Incident Report:

Network Traffic Analysis

Part 1: Provide a summary of the problem found in the tcpdump log
The tcdump log captures network traffic related to an attempt to resolve the domain yummyrecipesforme.com The protocols involved are **UDP** (User Datagram Protocol) for DNS queries and **ICMP** (Internet Control Message Protocol) for error messages. The log shows repeated attempts to perform a DNS lookup, each followed by an ICMP "udp port 53 unreachable" error.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The repeated ICMP errors suggest a consistent problem with the DNS server's ability to respond to DNS queries on UDP port 53. This could be due to a service outage, firewall blocking UDP traffic on port 53, or a misconfiguration on the DNS server. The fact that the errors are ICMP messages, originating from the DNS server itself, indicates that the server is active, but the DNS service is not.