Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
Incident occurs at 1.23 pm.There was problem in loading website yummyrecipesforme.com, on Initial investigation it was detected that DNS server was unable to fulfill request from client to load website.By analyzing network traffic through TCPdump analyzer it was found that UDP protocol port 53 which is assigned duty to fulfill queries related to Domain Name Resolution is not listening

Part 2: Explain your analysis of the data and provide one solution to implement
On analysis of data it is clear that UDP port 53 which is responsible for fulfilling Domain Name Resolution requests from clients is not listening to queries. In terms of risk, a minor cause of the problem can be that Firewall is blocking queries. The major cause of the problem can be a type of Denial of Service (DoS) attack known as DNS Flooding in which DNS ports are flooded with data packets to get the server down. If problem occurs due to misconfiguration of firewall then we need to reconfigure firewall to continue services I case of successful DoS attack, we need to temporarily use TCP port 53 (though it may not be supported by all DNS client) and simultaneously have to deploy DDoS mitigation services to block unwanted traffic on the DNS port.After successfully resolving problem we need Digital Forensics to understand how attack was carried out, to avoid such incident in future