# 

13:24:32.192571 , 1:24pm 32.192571second

192.51.100.15.52444 > 203.0.113.2.domain

source address(computer's IP) > DNS server IP

"A?" in the log indicates that the DNS request is asking for the IP address (IPv4) associated with the domain name "[www.yummyrecipesforme.com](http://www.yummyrecipesforme.com)".

# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | |
| --- | --- |
| The UDP protocol reveals that there is issue contacting the DNS server  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message “udp port 53 unreachable”  The port noted in the error message is used for DNS protocol traffic , indicating that this is an issue with the DNS server.  The most likely issue is that the DNS server is not responding, | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred at 1:24PM.  The IT team became aware of the incident when the customers notified the organization that they received the message “ destination port unreachable” when they attempted to visit the website yummyrecipesforme.com.  The actions taken by the IT department to investigate the incident are conducting packet sniffing test using tcpdump.  Key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.) is DNS port 53 was unreachable .  A likely cause of the incident is that the DNS server is down or the port 53 is blocked by firewall. |