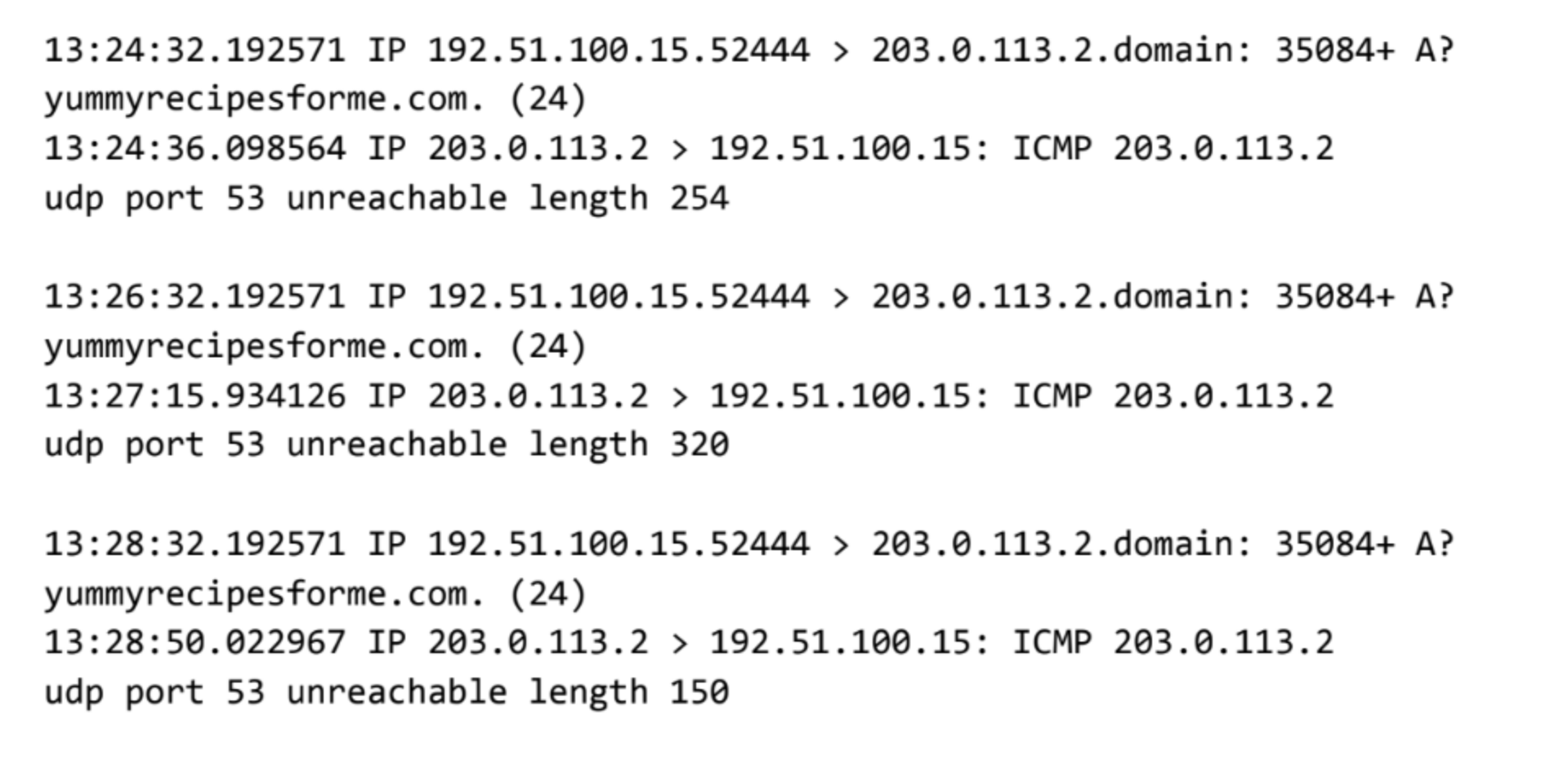
# Cybersecurity Incident Report:

# Network Traffic Analysis



|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The UDP protocol reveals that: port 53 is unreachable  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: 203.0.113.2  The port noted in the error message is used for: DNS, which converts domain names to IP adresses  The most likely issue is: DNS server is not responding to requests |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: at 13:24 when some users tried to access the website  Explain how the IT team became aware of the incident: the users reported that they received the message “destination port unreachable” when attempted to visit the website yummyrecipesforme.com  Explain the actions taken by the IT department to investigate the incident: We conducted packed sniffing actions using tcpdump.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): We found that DNS port 53 is unreachable.  Note a likely cause of the incident: DNS might be down due to a DDoS or a internal problem. |
|  |