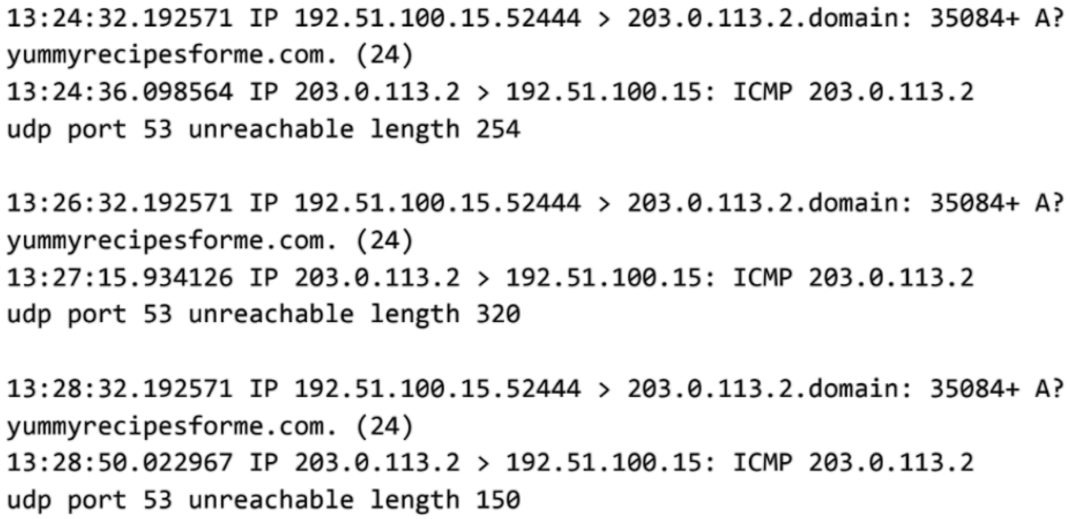
Cybersecurity Incident Report:
Network Traffic Analysis



```
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.

As part of DNS protocol, UDP protocol was used to attempt contact with DNS server to retrieve IP address of yummyrecipesforme.com (IP: 203.0.113.2). ICMP protocol responded with an error message, indicating issues contacting the DNS server. Error message displayed “udp port 53 unreachable.” Since port 53 is associated with DNS protocol traffic, the issue must be with the DNS server. Also, plus sign after query ID number 35084 indicates flags with UDP message and “A?” symbol indicates flags with performing DNS protocol operation, where an A record maps a domain name to an IP address. This may be caused by a DoS attack against the DNS server.

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

The incident occurred today at 1:24 pm, (log files indicate 1:24 pm, 32.192571 seconds). Customers notified the organization that they received the message “destination port unreachable” when they attempted to visit the website yummyrecipesforme.com. We conducted packet sniffing tests using tcpdump. In the resulting log file, we found “DNS port 53 was unreachable.” Next steps to take is to identify whether the DNS server is down (e.g. by DoS attack) or traffic to port 53 is blocked by firewall.