Summary

After analyzing the data presented from the tcpdump log, there was a trend found in the data. The tcpdump log starts at 13:24 and ends at 13:28 meaning that it tried to reach its destination via DNS 3 times which resulted in port 53 being unreachable. The query number 35084+ A also shows issues with the DNS and protocols. Furthermore, the ICMP error response message regarding port 53 supports that the DNS server is not responding. Due to that error the assumption is hard to ignore when the flags are with the outgoing UDP message and domain name retrieval.

```
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
```

Step 3: Provide a summary of the problem found in the tcpdump log

Identify trends in the data. Assess which protocol is producing the error message from the DNS server for the yummyrecipesforme.com website. Recall that one of the ports that is displayed repeatedly is port 53, commonly used for DNS.

In your analysis:

- Include a brief summary of the tcpdump log analysis and identify which protocols were used for the network traffic.
- Provide a few details about what was indicated in the log.
- Interpret the issues found in the log.

Record your responses in part one of the cybersecurity incident report.