Cyber Security 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: The website is unreachable
This is based on the results of the network analysis which show that the ICMP echo reply returned the error message: Port 443 unreachable.
The port noted in the error message is used for: HTTPS traffic (443)
The most likely issue is: a web server, firewall configuration, or a malicious attack.

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

Time incident occurred: [Insert Time] on [Insert Date] in this case, we are doing this activity on October 19th at 10 AM (assuming the HR experienced it at 10 am today)
Explain how the IT team became aware of the incident: The HR team reported that they could not reach the background check web portal.
Explain the actions taken by the IT department to investigate the incident: The IT team ran tests using a network protocol analyzer tool (tcpdump) to capture and analyze ICMP traffic.
Note key findings of the IT department's investigation: The investigation mentions unusual ICMP traffic behavior, error messages in ICMP echo replies, port 443 in accessibility, and further checks to be conducted on the firewall configuration and the web server.
Note a likely cause of the incident: The HR department, in collaboration with the network security team, suspects that a new hire may have initiated an attack to crash the background check website. This can only be confirmed once the system administrator checks the firewall and web server configuration. Until then, the new hire remains an active suspect.