Solving Email Archiving Challenges for a Government Investigation

Digital Forensics – Case Study & Analysis

Innovative Discovery, LLC

Context

As part of an investigation conducted by the Department of Justice, Innovative Discovery, LLC ("ID") collected active and archived data from email accounts of more than 500 users over the course of eight months. Users consisted of both current and former employees, from various departments within the organization, and located throughout the United States.

Challenges

- Missing significant portions of, or entire email accounts
- Extent of deleted/removed data spans over 6-years
- Lack of archiving application support
- Department of Justice investigation deadline

Collection Process

During the initial collection process, ID's Forensic Experts identified multiple users whose partial or entire email accounts could not be located within the Exchange Vault provided and immediately informed the Client. After working with the Client's IT department and consulting with the archiving application support team, ID concluded that the Exchange Vault was missing 6 years of data. If the missing data and email accounts from this gap could not be located and restored, the Client would be left without an adequate response to the Department of Justice's investigation and could face possible fines and/or sanctions. Furthermore, the restoration process would need to be completed in timeframe that would not delay or negatively impact the entire investigation.

The missing data was determined to be the result of a revision in the Client's data retention policy, which is maintained by the IT department. All data prior to this revision was stored on a previous Exchange Vault that was kept offline. In spite of this, according to both the Client's records and the IT department's maintenance logs the previous Exchange Vault did not exist. Therefore, the initial collection conducted by ID's Forensic Experts was incomplete, as it consisted only of the active data, current Exchange Vault, and Live Email Exchange. A second collection would need to be conducted on all data that was archived prior to the revised retention policy.

ID concluded that in order to access the 6-years of missing data, the entire offline Exchange Vault would need to be restored. However, the support/maintenance licensing had been cancelled by the Client in an effort to reduce costs, an occurrence becoming more common as companies strive to control their technology-related expenses. Consequently, ID had to completely rebuild and configure the Exchange Vault without any assistance from the archiving tool support team. ID's extensive experience with these tools enables our Forensic Experts to act as solution providers when technical support from the archiving application is unavailable.

Six-years of missing data, email communication, and user accounts were effectively restored and rebuilt into a format that could be extracted for review of any relevant documents that may be required by the Department of Justice.

The Client averted any possibility of sanctions or incurring legal fines and penalties due to ID's successful restoration – all while saving over $200,000 when compared to the cost of technical support from the archiving application.