

EMAIL ARCHIVING FOR A GOVERNMENT INVESTIGATION

A DIGITAL FORENSICS CASE STUDY

THE SITUATION

As part of an investigation conducted by the Department of Justice (DOJ), Innovative Driven 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. The data set was missing significant portions of or entire email accounts and had six-years of deleted 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 DOJ'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 SOLUTION

The missing data was determined to be the result of a revision in the client's data retention policy. All data prior to this revision was stored on a previous Exchange Vault that was kept offline. 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 to reduce costs. ID had to completely rebuild and configure the Exchange Vault, made possible by the extensive experience the ID's forensic experts have with these tools.

THE RESULT

Six-years of missing data, email communication, and user accounts were effectively restored and rebuilt into a format that could be extracted for review. 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.



\$20k+

in cost savings working
with ID forensic experts