



Global Digital Forensics

Case Study – Digital Forensics

Case Type – Internal Corporate Fraud

Environment – Complex Multi-Location Network and Desktop

Industry – Banking

Scenario:

A large accounting firm was hired to audit certain activities by officers of a medium size, publicly traded bank (the “Bank”). During the investigation, the auditors needed to examine several computer systems used by certain Bank employees. GDF’s digital forensic examiners were immediately dispatched and sent in to arrange for the formal investigation of those systems to search for corroborating evidence in support of the audit team’s suspicions and findings.

Background Information:

In the previous two years, the Bank had gone through a series of transitions, culminating in a new Board of Directors and, because of new regulations in the financial industry, an independent Auditing Committee. The Auditing Committee charged certain officers of the Bank with engaging in suspect activities related to particular Bank expenses that were either hidden or “lost” from the purview of the normal Bank’s accounting practices. In order to stay compliant and to remedy what may have been “bad apples” in the organization, the Bank’s Auditing Committee required the Board to hire an independent accounting firm to review those issues and present a formal report to the Bank. The accounting firm knew that one of the best ways to get to the true facts at the root of those issues was by performing a thorough examination of the Bank’s digital assets. Since the Bank had in place a host of disparate and complicated IT systems, and because of the immense time pressure to solve those issues before the Bank was to release its next mandatory financial statement, a concise but thorough plan for reviewing those digital assets was needed. Complicating matters further was the fact that certain systems run by the Bank’s IT department had been recently changed and many logs and historical records regarding pertinent information were non-existent. There was an enormous volume of paper documents that the accounting firm was reviewing and needed to validate and review those documents against information gleaned from the digital examination as well. Because of the Bank’s size and market capitalization, it did not allocate surplus funds for this type of situation and cost factors were in the forefront, but could not guide the investigation on any substantive level for fear of bias and a lack of diligence.

GDF Involvement:

The accounting firm retained GDF to perform examinations of the Bank’s digital assets as necessary to uncover information that potentially would help the Bank make an ultimate decision regarding how it should proceed with the employees and Bank officers suspected in the wrongdoing.

GDF Findings:

GDF focused its initial examination on particular desktop and network systems used by the suspect employees. Its examiners performed digital forensic analyses on those systems while simultaneously examining data supplied directly from the Bank’s IT department regarding internal network and Internet related activity of those suspect employees. Through those examinations, GDF created lists of particular areas of interest based upon the issues related to the overall investigation and catalogued those lists to further detail certain documents and fragments of data referencing suspicious Internet activity. Using that collected information, the accounting firm was able to corroborate particular aspects of their investigation to conclude that certain Bank officers did in fact do what they were suspected of doing from the beginning. Moreover, GDF also uncovered certain activities of the suspect employees that the auditors did not suspect, but which nevertheless, played an important role in the overall investigation and the final outcome.

Outcome:

Using the digital artifacts GDF collected in a forensically sound manner from the systems it investigated, the Bank’s Auditing Committee was in a better position to find that certain Bank employees had violated Bank policy and possibly certain federal regulations regarding actions by officers of public corporations. The Auditing Committee, together with the Bank’s Board of Directors, was able to terminate the accused employees and also to negotiate settlement agreements favorable to the Bank with those employees, including reducing certain benefits and severance packages owed to them under pre-existing employment agreements. In the end, the Bank saved an enormous amount of money and time by having the digital evidence to use in finalizing the issues related to the investigation and was able to make important deadlines with regards to certain SEC filings.

Global Digital Forensics

Phone 1-800-868-8189 or 727-287-6000