Using Computer Forensics to Investigate Employee Data Theft

2017
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>When Employee Data Theft Is Suspected</td>
<td>3</td>
</tr>
<tr>
<td>IP Theft Investigations</td>
<td>4</td>
</tr>
<tr>
<td>Preserving and Analyzing Electronic Evidence</td>
<td>4</td>
</tr>
<tr>
<td>USB Activity Analysis</td>
<td>5</td>
</tr>
<tr>
<td>Files Recently Opened</td>
<td>6</td>
</tr>
<tr>
<td>Cloud Storage</td>
<td>6</td>
</tr>
<tr>
<td>Personal Email Accounts</td>
<td>7</td>
</tr>
<tr>
<td>Internet History Report</td>
<td>7</td>
</tr>
<tr>
<td>Paper Documents</td>
<td>8</td>
</tr>
<tr>
<td>Deliverables and Project Timeframe</td>
<td>8</td>
</tr>
<tr>
<td>Getting Started</td>
<td>8</td>
</tr>
<tr>
<td>Authors</td>
<td>9</td>
</tr>
</tbody>
</table>
Introduction

Over 25 percent of employees steal proprietary data when departing a company or organization.¹ To that end, our experience shows that departing employees have a sense of ownership over the data that they copy. Intellectual property commonly stolen includes customer lists, secret formulas, source code, strategy documents and other trade secrets. The information is often used against the organization when the former employee goes to work for a competitor or decides to start a new company.

When suspicions of employee data theft arise, it is important to engage a computer forensics expert to perform a theft of IP analysis in order to preserve electronic data and uncover important evidence. Using specialized software, the expert can reveal digital footprints such as:

- USB activity
- Files recently opened
- Cloud storage usage
- Files sent to personal email accounts
- Internet activity
- Recently printed documents

The results of the analysis can provide the foundation for legal action such as a temporary restraining order, permanent injunction, subpoena of personal devices, or other litigation to prevent the misappropriation of company data.

When Employee Data Theft Is Suspected

Employee data theft occurs most frequently just prior to, or immediately after, an individual’s termination or resignation from an organization. Telltale signs that an investigation is warranted include unusual activity by the employee, such as:

- Plugging a personal USB thumb drive or hard drive into a computer

• Coming into work at odd hours or establishing remote desktop connections during off-hours
• Transferring large amounts of data on the company network
• Visiting file sharing sites like Dropbox or Google Drive
• Sending emails with attachments to personal accounts

If there are concerns that a departing employee has stolen proprietary data, then it is important to take steps not to delete important electronic evidence located on his or her computer. If the computer is powered on, then leave it on, because important evidence may be stored on the computer’s random access memory and could be deleted if the computer is powered off. Also, ensure the computer cannot be accessed remotely by disconnecting it from the network.

If the computer is already turned off, then place it in secure storage. Furthermore, confirm the employee’s login credentials are disabled or have been changed, but do not let the IT staff reinstall the operating system or reassign the computer to another employee. Such actions could destroy or overwrite any evidence of wrongdoing. Finally, resist the temptation to “take a peek” at what is stored on the computer by turning it on and accessing files because this could alter the data, thereby making the investigation more complex.

If the suspected employee had a company-issued cell phone, then place it in secure storage as well. Smartphones hold an abundance of useful information such as text messages, emails, call logs, internet activity and more. The simple act of resetting the phone, however, can permanently destroy this data.

IP Theft Investigations

Preserving and Analyzing Electronic Evidence
The first step in a theft of IP investigation is to forensically preserve the data on the employee’s device(s). The computer forensics expert will create chain of custody documentation, photograph the hardware, and verify the integrity of the preserved data, among other things. These steps ensure that the electronic evidence will be admissible in court.
Once the data is preserved, the next step in the investigation is to perform an analysis to identify software and artifacts that may be indicative of IP theft. These areas on a typical Windows installation include:

- USB activity
- Files recently opened or deleted
- Cloud storage
- Personal email accounts
- Internet history report
- Printed documents

**USB Activity Analysis**

Many of today's USB devices, such as thumb drives and external hard drives, have enough storage capacity to save an entire copy of a user's hard drive. As such, they are one of the most common tools used to steal data. The good news is that using a USB device leaves behind a trail of digital evidence that can prove invaluable to an investigation.

Analyzing a user’s USB activity can reveal several key facts regarding what was connected to the computer and when. In most cases, forensic experts can determine the serial number and/or brand of the USB device, as well as the first and last time the device was connected to the computer. In some instances, they may also be able to verify each time a specific USB device was connected.

Oftentimes, the analysis will reveal that an external USB hard drive or flash drive was connected for the first time during an employee's last week of employment. While most analyses reveal a new USB connection, it is also possible that a device used throughout the
duration of the suspect’s employment was never returned. A device such as this would likely contain numerous documents and files that were related to the employee’s day-to-day activities and could contain value to a competitor. If it is a requirement that employees return company-owned USB drives at the end of their employment, forensic experts have the ability to verify whether or not that policy was upheld.

Files Recently Opened

While confirming that a USB device was connected to a computer is significant, it is even more important to know what files were accessed and potentially transferred to the device. The Microsoft Windows operating system creates various artifacts when a user opens a file or folder. These artifacts indicate what was opened, when it was opened and where it was opened from. A classic red flag is if the employee was opening files during the last week of employment that were not related to the work being performing during that time.

Another consideration is the organization’s data access policy. If data access restrictions are not in place, then the employee may be able to access company files unrelated to current work that are stored on the network. The existence of these artifacts when combined with a USB activity timeline can indicate a high probability that data was copied off the system.

Lastly, the artifacts can also contain specific information about where the file existed. If a file was opened from a USB drive, the artifact will indicate this, providing factual evidence that the suspect is in possession of a USB drive that contains specific files. For example, combining a USB analysis and files recently opened analysis could show that on October 7, 2016, at 7:22:08 a.m., a non-company-issued SanDisk thumb drive with serial number 851450 was plugged into the computer for the first time and a file titled “Client Contact List.xlsx” was opened.

Cloud Storage

If the analysis shows that certain files were accessed but no USB activity was detected, the next step in the investigation is to identify evidence that a cloud storage provider such as Dropbox, Google Drive or Microsoft OneDrive was accessed. The purpose of these applications is to share and sync data across multiple computers. For example, Dropbox may
have been surreptitiously installed on the employee’s work computer as well as his or her home computer. Consequently, the simple act of syncing a company file to Dropbox will instantaneously also make that file available on the employee’s home computer.

The good news is that cloud storage applications often have corresponding log files and databases that record what files the user accesses and what activities are performed. These logs can signify files have been uploaded to the cloud in the past even if they have already been deleted from the shared folder. Some of these applications even save deleted data in a separate “hidden” folder on the computer itself that users typically are not aware of. As a result, a theft of IP analysis may show that Dropbox was installed on the user’s work computer and that early in the morning on October 7, 2016, fifty files were deleted and the “hidden” folder reveals these were company files.

**Personal Email Accounts**

Some individuals may use their company email to send attachments to their personal email account such as Yahoo or Gmail. In these cases, forensic experts are able to perform a preservation of the employee’s work email to identify and document the evidence of misconduct.

**Internet History Report**

An Internet history report can be generated that shows, inter alia, recent Internet searches, web sites and pages visited, cookies from websites, and Internet downloads that occurred. Such information is helpful in establishing what an individual thought was important or even their state of mind. For example, analysts have discovered that individuals have searched on how to delete data or copy data surreptitiously and that they reviewed websites that were in essence “how to manuals” to perform certain deleterious acts.
**Paper Documents**

Finally, individuals who are a little less aware of more modern techniques to copy data will simply print the documents they wish to take out the door. In these cases, forensic experts are able to determine the last known print date of Microsoft Office documents.

**Deliverables and Project Timeframe**

The turnaround time for a theft of IP analysis performed by JURINNOV, LLC is typically one week. Our clients receive multiple, easy to understand deliverables in the form of spreadsheets, html reports, and written reports containing the findings of the analysis. Our forensic experts also spend time with our clientele either over the phone or in person to discuss the reports in detail so that they know exactly what a report contains and the assumptions and opinions of the forensic expert. If necessary, our experts also provide depositions or expert witness testimony regarding the authenticity of the evidence and their findings.

**Getting Started**

If suspicions of employee data theft arise, it is important to take precautions to prevent the misappropriation of sensitive company data. To get started, call 1-877-840-4357 or email sales@jurinnov.com to discuss how our computer forensics team can help with the investigation.
Authors
Timothy M. Opsitnick, President, JURINNOV, LLC, Joseph M. Anguilano, Director of Operations, and Trevor B. Tucker, Forensic Analyst. JURINNOV, LLC, a wholly-owned subsidiary of Technology Concepts & Design, Inc. (TCDI), is a technology company that provides cybersecurity and eDiscovery services. Cybersecurity consulting includes investigating accidental or malicious data breaches as well as providing security strategies and assessments to prevent such occurrences. eDiscovery consulting includes computer forensic investigations and ASP ESI hosting. JURINNOV news and information is available at www.jurinnov.com.

For over 25 years, TCDI has been providing technology solutions through partnerships with large corporations and law firms. These solutions include advanced litigation support software and services for electronic discovery, hosted review and production, and large-scale litigation case file management. TCDI news and information is available at www.tcdi.com.