Exemplary Evidence

Working Titles: Exciting New Advances in Theft of Intellectual Property Investigations

Caption/Teaser: Are you concerned your company's intellectual property or proprietary data may have been misappropriated or otherwise lost or shared with unauthorized parties? Creating a timeline of events is a key requirement for securing a successful outcome. Focusing on relevant evidence artifacts is critical to ensure the investigation moves forward smoothly. And determining where documents were saved and identifying with whom they were shared are important tasks to build your case and prove intent.

Authors: John J. Carney, Esq., Chief Technology Officer
Kevin V. Bluml, Chief Computer Forensic Examiner
Carney Forensics, www.carneyforensics.com

Are you concerned your company's intellectual property or proprietary data may have been misappropriated or otherwise lost or shared with unauthorized parties, intentionally or negligently? Typically, IP theft occurs shortly before or after the employee tenders their employment termination notice. Creating a timeline of events is a key requirement for securing a successful outcome.

One of the biggest challenges during an IP theft investigation is narrowing down the vast amount of document, email, and message evidence residing on computers, phones, and online cloud accounts. Focusing on relevant evidence artifacts is critical to ensure the investigation moves forward smoothly. Determining where documents were saved and identifying with whom they were shared are important tasks to build your case and prove intent.

Three Scenarios for Proving Intellectual Property Theft

Documents must be copied or sent somewhere to make unauthorized use of them. This can be done in a variety of ways from simple printing of documents and taking the paper copies to copying the documents to several devices or storage options including, but not limited to:

- USB removable storage devices such as thumb/flash drives that easily slip into a pocket or purse, to larger removable disk drives commonly used for backups
- Emailing the documents to a personal email account, or a competitor's email address
- "Cloud" or online storage accounts such as Dropbox, Google Drive, Microsoft OneDrive and many others

Let's look at what we can determine from each of the above scenarios.

Removable Storage Devices

One of the most common ways documents are taken or misappropriated today is by removable storage devices. Most computers do a good job of tracking the use of removable devices, especially the first and most recent time a device is connected to the computer. Information such as the actual or a virtual serial number of the device is recorded along with known manufacturer data such as the name and model number, when it was attached to the computer, and what drive letter was assigned. Other metadata that may be available includes file names and original locations of files, the location documents were copied (on the removable device), the size and date and time stamps associated with the original document and its copy.

Any device can contain data, and not just the data you might expect. A camera could have an email file on it. A music player could have photos or documents on it. A phone could store any type of data from documents, pictures, spreadsheets, emails, to AutoCAD drawings. Anything digital can reside on most any device. Even file names can be misleading or intentionally hiding something. Who would expect an email file to be called "hello.txt" or a confidential business spreadsheet to be called "ourhouse.jpg"? Changing the name of the file does not change the data in the file, but it does change a specific date and time stamp that could be helpful in creating a timeline.

If a removable device is found to have been connected to a former employee's computer on his or her last day in the office, it's probably a cause for concern. If the device can be recovered, it is straightforward to determine if the device recovered is the actual device at issue and then to identify which documents reside on the device.

For example, if you see an executive connected a USB backup device to his or her computer on the last day in the office and you find evidence that shows a file called “FullBackup.bkf” was on that device, you will most likely want to consult with your internal counsel. Hint; FullBackup.bkf is a common name for, you guessed it, a full backup of the computer to which it is attached.

Email Accounts

Email is ubiquitous and used by nearly everyone these days particularly in the business world. Its widespread use makes it a prime avenue for data theft, often without the realization of the many ways that email is tracked and audited.

Businesses should have robust tools and practices in place to constantly track and document any email activity, especially email to or from external email addresses. Auditing should be enabled and routinely backed up to allow extended look-back if needed. In Microsoft Office 365 for example, default auditing is only retained for 90 days. This limited amount of time can be problematic if an issue is not discovered soon enough to be examined while logs are still available.

There are several Data Loss Prevention (DLP) options available that can help prevent or at least alert staff to potential proprietary data loss via email. Determine the most at-risk data and develop rules or criteria that can be checked against any outgoing email to help stop this theft or inadvertent loss of important data. Simple checks for identifiers like Social Security numbers, credit or debit card numbers, driver’s licenses, medical ID numbers, or passports are other examples to watch.

DLP solutions can even check more broadly for emails with attachments, or specific types of attachments such as Excel spreadsheets or Zip files. DLP can also check for or limit destination addresses. For example, is there any business reason to send emails to a Gmail or Hotmail or Yahoo email address? (There may be, but it is something to consider.)

Investigating Deleted Email

Typical business email systems will usually contain an email server that does the bulk of the work regarding sending and receiving email messages and the related artifacts. This server will be one of the primary places to look for evidence. This will include logs, potential drafts of messages, copies of the actual messages and potentially any replies or responses to the messages, or even failure notices if there was a problem with the original message.

Deleted email may be recoverable depending on the specific circumstances and the type of email system. Server based email is usually backed up regularly so if backups exist, the email may be on one or more backups. Also, if setup properly, email servers can be configured to require an email to be backed up prior to allowing any deletion of the message. Even if the email was deleted, it is very similar to regular files in that the data itself may still be there even if it is not readily visible to the normal user.

As part of an ongoing investigation or if you have reason to be concerned about email message deletion, another option may be available to help limit that concern. Using Microsoft Office 365 as an example, within that system, administrators can implement legal hold functionality that will prevent the user from deleting or otherwise tampering with any current or future email messages or activity.

Email can also be found on the user’s local system either due to the way it was configured or to allow “offline” viewing of email (useful for times when either out of the office or away from a stable network for example, on a plane). Also, if the recipients of the message of concern are known and cooperative, you may obtain a copy of the message from them, either voluntarily or via legal means such as a subpoena or document request.

If the email of concern went to a large online email provider like Google or Microsoft, it may also be possible to request copies of the email from them via subpoena or a preservation order. This same idea can be used if the email went to another company. Odds are good that their email system still has evidence of the email activity, at least in logs, even if the email itself is no longer readily available.

Cloud Service Accounts

The best and simplest explanation we have heard for “Cloud” services and what it means is “someone else’s computer”.

Evidence of Cloud service use is usually apparent. The specific web site with some associated history of recent activity or the cloud application may be found on the computer. Logs of what was recently done with that service may exist either on the subject computer or the cloud service provider’s systems. Other artifacts may exist within the computer that show recent activity or files involved with the service. There is often a folder structure with associated files for the cloud service

on the local computer. With the appropriate authority or permission, a forensic collection of the actual cloud account at issue is possible. The service provider may also provide other artifacts or evidence of recent or historical activity on the subject account. The account holder's cooperation is needed for the cloud service provider to inform a third party. An appropriate legal request such as a subpoena or preservation order may be used.

Starting the Investigation

When an investigation is warranted, often the first thought goes to how to quickly and cost effectively it can be performed.

It is common to think that handling things in-house will be the most cost-effective way to accomplish the investigation, especially if you have an investigative team already in place.

The biggest caveat with that plan is that it will succeed only if the team has the proper training and tools needed to perform the highly technical and process critical investigation in a forensically sound manner.

Digital forensics is a highly specialized field, one with new forms of evidence to recover and new methods and tools to do it. Think of the number of updates that occur with a computer system, sometimes dozens of changes in a month or even more often. Or, a cell phone with new models coming out regularly besides the monthly updates, as just a couple examples. Each new update or version of new software brings new challenges, potentially new artifacts to learn about and recover, even new logs or data locations that must be understood to take advantage of the plethora of information that must be analyzed.

The First Commandment of Electronic Evidence

The first of the ten commandments of electronic evidence by Sharon D. Nelson, Esq. and John W. Simek of Sensei Enterprises, Inc. states, "Thou shalt not stomp all over the evidence." As digital forensics experts they opine, "When computer forensics specialists get together and swap war stories, one recurrent theme is the unbelievable number of times that clients have fouled themselves up by trampling electronic evidence. Typically, as soon as a potential legal matter is recognized, a law firm or corporation authorizes someone from its IT department to 'look through' the evidence. Unbeknownst to them, while their IT staff is busy finding golden nuggets of evidence, they are also changing the dates and times of the files they are accessing and possibly altering information that indicates which user ID did what. While it may not entirely discredit the case, you have now given fodder to opposing counsel at the very least – and you will have to spend more money on the forensic examination because unraveling dates and times and explaining 'the stomping' effect is now part of the examiner's job."

Nelson and Simek conclude with this sage advice for clients and lawyers, "It is a very foolish client that contaminates evidence by having in-house folks look at it – from a judge's point of view, the client has a vested interest in that evidence. Far more credible is an initial, independent forensic examination by a certified third party."

Next month Exemplary Evidence will explore mobile device forensic approaches to reversing wrongful convictions. It will focus on how mobile evidence is the new DNA in post-conviction criminal defense litigation.