



A No-Nonsense Guide to File Collections

**Learn a Few Simple Steps which Prevent Spoliation, Incomplete Productions
and Increase Potential Evidence**

By Jon Rowe, CCE
Certified Computer Examiner
President

Pinpoint Labs
Jon.rowe@pinpointlabs.com
www.pinpointlabs.com

Incomplete and undocumented electronic discovery collections occur every day and the results are costly to both the client and their legal counsel. In the typical litigation, clients expect their attorneys to guide them through the entire process. After all, litigation is what attorneys do for a living. In fact litigation is a burden to clients in that it is both costly and distracts client personnel from the client's core business. Few would argue that the failure to properly advise a client as to how a file cabinet of documents should be handled in a litigation is potential malpractice. Now that most documents are electronic and the file cabinets are computer networks, the failure to properly advise a client as to how electronic data should be handled in a litigation is potential malpractice in the form of spoliation and missing evidence.

Advising clients about proper file collection methods must be considered from the beginning of each case. Using processes and applications which preserve and verify collected electronic files with minimal impact on client systems is critical. Without these, creating defensible and verifiable electronic discovery productions and evidence authentication is difficult, if not impossible.

Common Problems Related to Electronic File Collections

Normally, a discovery request is created and the corporate IT department or other client employee copies relevant files or directories to disc or USB drive. From the client's perspective, this is the least costly way to collect data. It can be, however, the most costly way in the long run. The integrity of files collected from corporate servers and client machines are in jeopardy because many electronic document collections are completed using tools which lack the ability to confirm results and properly document the process.

Attorneys need to advise clients as to proper collection techniques. While not every case warrants a full third party forensic collection, every case does warrant a defensible and verifiable electronic data collection process. Discussion as to when a full third party forensic collection is needed is beyond the scope of this article but the possible need must be considered before the decision is made to move forward with a different class of collection.

Incomplete File Collections

Many file collection projects take many hours or days and contain hundreds of thousands, if not millions, of files. The software used to copy and burn files often lacks a verification process, therefore files that are skipped, partially copied, or corrupt go unnoticed.

Incomplete and corrupted file collections pose an unseen danger, as reviewers may never know that a relevant file was unavailable or unsearchable. The best way to ensure that all relevant files identified are properly copied and delivered without error includes:

- Hash verification for every file
- Log incomplete copies, files in use or skipped files
- Maintain descriptive error logs
- Proactive error reporting and feedback
- Verification (chain of custody) log

Recommending that clients use file collection methods with the above options helps ensure all electronically produced files are intact and available for review.

Client System Modification

Current collection efforts should include using applications and processes which preserve the native states on servers and individual client PC's. However, many file collection utilities require an installation on corporate systems, which can introduce multiple obstacles:

- Corporate IT policies may prevent installing new software without prior approval
- Transferring software licenses between systems may require purchasing multiple copies or contacting the developer
- Collection software may not have all file dependencies on target computer

File collection software should ideally be portable and run without installation. The 'zero footprint' software option preserves the native state of the servers and client machines.

Inconsistent Results

When attorneys and their support staff are not involved in recommendations or implementing best practices for file collections (or fail to even know what the best practices are), the quality of the file productions can suffer and client claims for malpractice can result. When individuals responsible for file collections are not familiar with adequate collection tools, they may resort to file copy utilities that do not include verification or they do not know how to set the options.

Common copy utilities have dozens of options which, if not used in the right combination, can cause a number of errors. Additionally, there can be a higher likelihood of errors if multiple parties attempt to replicate the same settings.

It is important to ensure that file collections are consistent across multiple projects. Using intuitive tools that require minimal end user interaction is preferred.

Avoid Common Collection Problems

As a result of these crippling issues, a new breed of collection software was developed. You can learn more about SafeCopy 2.0 and Pinpoint Labs at www.pinpointlabs.com. Pinpoint Labs focuses on forensically sound tools related to preservation, collection and filtering. Pinpoint Labs applications are intuitive, affordable and address common litigation support needs.

SafeCopy 2.0 Mobile Edition

SafeCopy 2.0 Mobile Edition is a portable file collection software that runs from U3 compatible flash drives, eliminating the need to install the software on servers or client machines. SafeCopy 2.0 was designed to overcome the daily issues encountered during active file collections.

What is U3? U3 is a standalone application environment that allows users to install and run software directly from a USB device. SafeCopy 2 Mobile Edition is perfect for file collection, acquisition, or even in-house use when you need the freedom to use SafeCopy 2.0 wherever you choose.

Recommend SafeCopy 2.0 Mobile Edition

You have discovered your client needs to collect and copy documents located in network directories or from a client system. Providing SafeCopy 2.0 Mobile Edition or recommending that your client obtains a copy ensures they are using a production level collection tool that addresses the basic collection issues identified in this paper.

SafeCopy 2.0 Mobile Edition allows your client to easily select multiple

source directories, documents the process, confirms the results, and allows them to easily move the software from one computer to the next without installing software on the client systems. SafeCopy 2.0 Mobile Edition will provide you a chain of custody and error report for any files that could not be collected.

EXCUSE ME, WHAT'S YOUR ADMIN PASSWORD?

When a vendor is called on site to collect files, they may bring a laptop to run their collection software. Normally, they would need an administrative password to logon to your client's network and copy the appropriate files. Unfortunately, getting administrator rights and mapping locations and file shares takes additional time and often becomes a challenge.

If your vendor is using SafeCopy 2.0 Mobile Edition, they can use an existing system where a USB port is available, is already logged in and has access to the requested directories and files. Using existing systems will put your client at ease and reduce the collection time.

Summary

Many recognize that preserving, verifying, and documenting electronic discovery collections not only confirms relevant files are acquired, it helps legal departments avoid spoliation and demonstrates to their clients they are implementing best practices. As inside counsel, general counsel, and corporate IT departments learn more about litigation readiness, it becomes more important that their partnering legal departments keep abreast of the changes and are the ones leading the way.

Being proactive and recommending the proper methods and tools for ESI (Electronically Stored Information) collections will ensure consistent results and provide a "heads-up" on

any issues encountered. Many legal departments and service providers rely on SafeCopy 2.0 from Pinpoint Labs for active file collections because collections results are confirmed, incomplete jobs are immediately reported, and the process is thoroughly documented.

PURCHASE SAFECOPY 2.0 MOBILE

(http://www.pinpointlabs.com/software/safecopy2me/atl_purchase.php)

SAFECOPY 2.0 FREE EVALUATION

(http://www.pinpointlabs.com/software/safecopy2me/atl_download.php)

About Pinpoint Labs

Pinpoint Labs was founded by Jon Rowe and James Beasley, who are Certified Computer Examiners and members of The International Society of Forensic Computer Examiners. Their experience includes 15 years of litigation support and more than two decades in software development.