ZAPPROVED™

The Path To
A Forensically Sound Collection

edited by: Sarah Thompson

START

Many people erroneously assume that a forensic image is the only way to have a forensically sound collection that will stand up to scrutiny in court. Not only is that untrue, but it can lead to costly overcollection of electronically stored data (ESI).

IDENTIFY

1. Where does the relevant data reside? Cloud? PC? Laptop? Network?
2. Select the sources you need to collect from.

COLLECT

1. Use a tool specifically engineered to collect ESI—it will ensure that the collection is defensible.
2. Connect to the sources that are relevant.
3. Filter the data so that you only get what you need, no more no less.

   Select folders rather than drives

   DeNIST, dedupe, and use date-range filters to reduce the data set of non-responisve ESI

Once Data is collected, the data needs to be preserved in a forensically sound container in order to maintain defensibility. To be defensible the container must have the following:

SECURE

1. Be read only so that the data cannot be spoliated
2. All collected data must be pristine
   - Data unchanged by the collection process to preserve potential evidence
   - Restored file and system metadata as it was pre-collection
   - File & folder structure preserved as it was on the original source
3. Detailed audit logs of all collections actions
   - What was and wasn't collected and why
   - Who collected the data and when
   - The details about the source collected from
   - The Hash value of all files collected

PRESERVE

1. Preserve the pristine container so that it can be produced if the data is ever challenged.
2. If data needs to be further processed or reviewed simply ingest a copy of the container into your preferred litigation tool.

GOAL

A forensically sound and defensible collection that you know will stand up to scrutiny.

GLOSSARY

DEDUPE
Remove files that are exact duplicates.

DENIST
Remove files that are known non-discoverable file types like system files.

HASHES
An alphanumeric value associated with a file or email that changes if the item is altered in any way. Used to prove that a file has not been altered in any way. There are different hashing methodologies: MD5, SHA1 or SHA 256. (We use MD5)

FORENSIC IMAGE
A complete copy of a hard drive that is forensically sound and includes all data on the drive including unallocated and slack space.

FORENSICALLY SOUND
A method of collection that is defensible in court because you can prove the data has not been altered.

LIVE FILES
Files that are available thru the operating system.

METADATA
Attributes of a file or email such as date created, last modified, last accessed, etc.

RESPONSIVE ESI
Electronically stored information that is relevant to a litigation matter or inquiry.

SOURCE
Location of documents (OneDrive, DropBox, email, computers, network, remote laptops etc...)