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).

**Where does the relevant data reside? Cloud? PC? Laptop? Network?**

Select the sources you need to collect from.

**Use a tool specifically engineered to collect ESI**—it will ensure that the collection is defensible.

**Connect to the sources that are relevant.**

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-responsive ESI.**

**Use a tool specifically engineered to collect ESI**—it will ensure that the collection is defensible.

**Connect to the sources that are relevant.**

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-responsive 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:

- **Be read only so that the data cannot be spoliated**
- **All collected data must be pristine**
- **Detailed audit logs of all collections actions**

**Preserve the pristine container so that it can be produced if the data is ever challenged.**

If data needs to be further processed or reviewed simply ingest a copy of the container into your preferred litigation tool.

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

**GOAL**

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