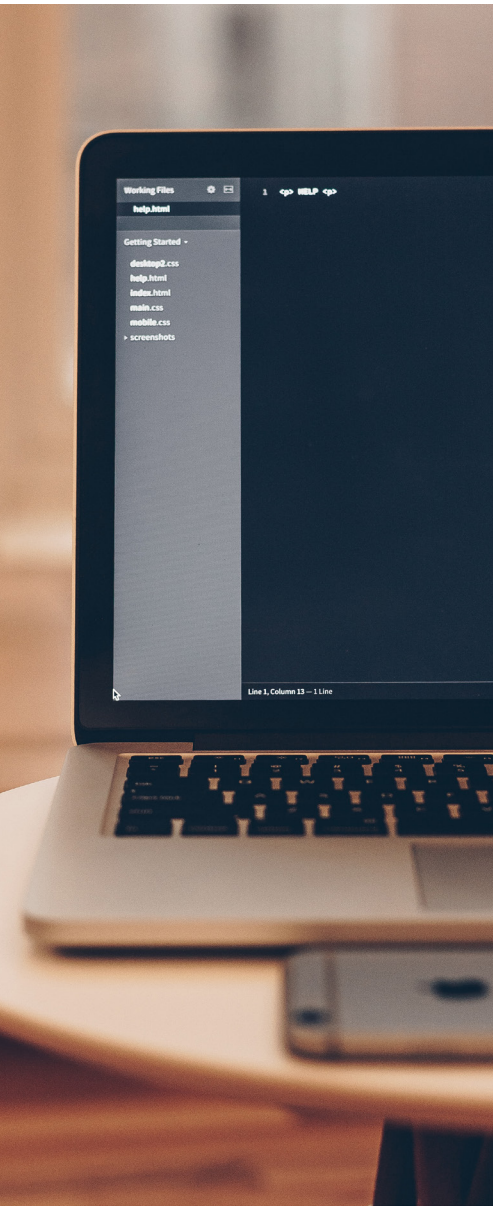
Remote Collections

The proper collection and preservation of your data lay the groundwork for the rest of your legal discovery, but can be difficult to manage. Remote collection is becoming the go-to method in the industry because it saves time and money. ID offers a regulated and technology-agnostic approach to executing remote collection of mobile devices, desktops, laptops, network shares, and email servers. These collections are performed by monitored examiner processes and use a combination of forensically-sound tools and methodologies. In short, ID provides you with flexibility AND a collection you can have confidence in.



ID USES A FOUR-STEP REMOTE COLLECTION PROCESS:

STEP ONE

Once a remote collection request is received, and the scope and limitations are established, ID's forensics department prepares remote collection kits on encrypted USB 3.0 drives. These devices are configured to the specific needs of the client, to include but not limited to: targeted logical collections, physical collections, network share collection, or collections from email repositories and structured data sources.

STEP TWO

After the devices are configured and prepared, they are shipped to the custodians or technical point of contact, along with chain of custody documentation, return instructions, and instructions for contacting and scheduling the collection meeting (if not already scheduled). Once the collection meeting is initiated between the custodian and ID's forensic examiner, the remote collection kit is connected and the forensic examiner will begin the collection process, monitoring it until completion.

STEP THREE

Upon completion of the collection, the examiner verifies the collection and completes the chain of custody documentation with the custodian. The collected data is then encrypted and packaged for shipment back to ID, with shipping labels and information already provided.

STEP FOUR

Finally, when the completed remote collection kits are received by ID, the data is unencrypted, verified again in the forensics lab, and replicated onto backup media. The chain of custody is completed and data is presented to the client for further processing, or stored in evidence until needed.