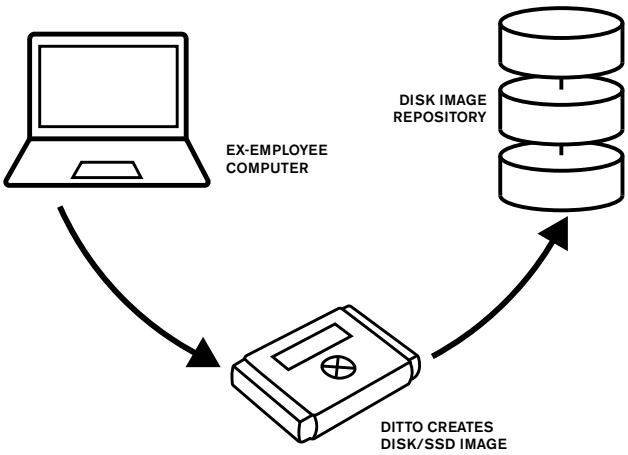
WiebeTech
by CRU

Creating an Inventory of Former Employee Computer Data

Ditto® Forensic FieldStation:

- Low-cost solution for creating images of ex-employee computer drives
- Simple, fast, forensically sound workflow
- Assists with information retention policies and e-discovery



The growth of electronic data has been explosive, as we all know, and the impacts on organizational policy for data retention are many. In 2006, the Federal Rules of Civil Procedure were revised to reflect the challenges posed during discovery by electronic information. As a result, organizations are under explicit rules that make it necessary to preserve information in its various electronic formats and make that information available when asked to do so.

Similarly, there is an expectation and responsibility for organizations–and government law enforcement, too–to preserve electronic information when a criminal case is anticipated, pending, or under way.

To help them comply with local and federal laws, organizations have developed electronic information retention and disposal policies that are designed to balance thoroughness of retention with not placing an undue burden on the organization.

These policies need to include retention of information that was under the control of employees who leave the organization. Should a lawsuit or criminal investigation arise, organizations will

want ready access to files, email, and other electronic data. Organizations should take care when letting ex-employees keep laptops; letting data walk out the door may well have consequences. Regardless of the terms of departure, organizations should be systematic and thorough when collecting information during the exit process.

ENTER THE DITTO FORENSIC FIELDSTATION

One global cybersecurity company has incorporated the CRU WiebeTech Ditto Forensic FieldStation in its mission to systematically retain information from departing employees, regardless of the cause of termination. This US-based company has over 3,000 employees located in offices in major US cities and in many countries in the Asia-Pacific/Japan and EMEA regions.

In response to the requirements stemming from proprietary information being used in violation of non-disclosure agreements, from actual and possible litigation, as well as compliance and regulatory requirements, the company created a process for acquiring hard drive/SSD images as employees leave the company. These drive images are stored in one of seven regional databases that accompany desktop solution centers located around the world.

While it may be possible to search backups of employee computers for necessary information, having obtained a forensically sound disk image ensures that the company can attest to the validity of the data presented for examination.

SIMPLE ACQUISITION LEADS TO LONG-TERM PROTECTION

When an employee leaves the company, his or her computer is returned to the regional desktop support center, where the support center staff follows a straightforward process to acquire and store the computer's disk image:

- An IT technician attaches the computer to a Ditto Forensic FieldStation, which is designed specifically for quickly imaging drives and providing options for simultaneously storing a hashed forensic image to both network and local storage volumes.
- Using the Ditto QuickStart feature, which enables the technician to start the Ditto imager the same way every time, the ex-employee's computer is put into iSCSI mode so the image can be efficiently stored on a volume located on the regional server. When the image has been created, Ditto automatically names the file with the investigator name and case number.
- The technician records the case number in a SharePoint image inventory database, creating a new record associated with the employee. The company now can easily and quickly find the disk image should the need arise.

The disk image is now available to be searched for e-discovery purposes via any of the popular software packages. Some forensic and e-discovery software applications also provide the ability to forensically obtain disk images, though a representative of the cybersecurity company explained that when the IT staff has more than a handful of computers to image, software solutions are unwieldy and inefficient—not to mention incredibly expensive.

WHY DITTO?

The cybersecurity company chose Ditto because of its superior performance, browser-based user interface, free lifetime feature updates, and far superior cost of ownership. Each support site costs about $3,000 for the Ditto unit and additional hardware – compared to software licensing costs of well over six figures per year. In addition, this workflow, combined with the ease of use of the Ditto imager, can be performed by employees who do not have specialized digital forensics training, offering even further savings and efficiency to an organization.

The networked Ditto Forensic FieldStation allows digital investigations to be conducted locally or in another country via VPN. The Ditto Logical Imaging feature provides the ability to discover and forensically image individual files, or a user-selectable collection of files, from hard drives and the NFS and Samba (SMB) network file systems found in corporate and other environments.

The cost-effective Ditto Forensic FieldStation is a valuable tool for any digital investigator to have.

For more information, visit cru-inc.com/ditto. To try a live, online Ditto unit, visit the Ditto Demo site at dittodemo.cru-inc.com.

Founded in 1986, CRU® is a pioneer in devices for data mobility, data security, encryption, and digital investigation. The popular remote/network operable CRU WiebeTech Ditto Forensic FieldStation is used by prominent Federal agencies, law enforcement agencies of all sizes, military organizations, and corporations around the world.

For more information,
visit the CRU web site.

cru-inc.com
sales@cru-inc.com