



What We Do

Evidence Collection Tools

The IXimager application is designed for advanced computer forensics professionals. It enables a user to quickly and efficiently create an exact, forensically exact, duplicate of an entire target machine (an "image") in an encrypted ASB format, the only encrypted forensics product made. It provides the ability to boot and image machines based on virtually any hardware and software combination, or operating system in use.

Fusus is a live Windows application which allows a user to create a forensically sound physical or filesystem images without software installations on the target machines.

Data Review and Analysis Tools

Ilook is a desktop application designed for advanced computer forensics professionals. It enables a user to process, review and analyze digital media; Ilook, Fusus, or IXimager evidence files; VMware VMDK virtual disks; or other legacy image formats.

IVault is a review tool for non-technical users such as case investigators, case reviewers, or attorneys. These users can review evidence with a minimum of training, and no specialized understanding of the details of computer forensics. IVault is produced in a virtual server and standalone version giving flexibility and connectivity to any customer of data mining.

IlookPI and IVault provide advanced features such as indexing and searching, and multi format file viewers to enable investigators to execute the quickest and most comprehensive analysis of the evidence possible.

Collaboration and Data Protection

Many members of the law enforcement community today, even skilled professional forensics specialists, lack an effective mechanism for secure electronic sharing of evidence files. As a result, they are forced to copy evidence files to physical storage media, and hand-deliver or mail that storage media to fellow team members. IXimager and Fusus both produce encrypted image formats which can be examined in IlookPI without prior decryption. Additionally, IlookPI provides two types of system images that can be created directly from a mapped image of any system at hand or of a physical device separately.

Unique to this field, the investigator now can generate and distribute critical evidence or

ediscovery results for review using IVault's encrypted evidence stores. The use of IVault allows the evidence, whatever the nature, to remain encrypted, and to be viewed on an IVault system without leaving retrievable traces on the reviewer's system or otherwise contaminating the review machine or infiltrating it with harmful processes that are part of the evidence itself under examination. There is an immediate safe harbor of the data and the use of the process automatically creates a protected "legal hold" environment within the science of computer forensics.