



DISCOVERY

VeHARVEST™ ESI COLLECTION PROCESS

TECHNICAL PROCESS DESCRIPTION

VeHARVEST is made up of several modules that run concurrently on the target network to identify, filter for criteria, and ultimately capture files that must be quarantined and reviewed for relevance in a litigation matter.



Connecting the application to the client's network

VeHARVEST is a server based application that is run from a server provided by Visual Evidence. The **VeHARVEST** server is connected to the client's network on an open port provided by the Client. The application employs the use of an open source Linux based tool called CIFS (Common Interface File System) to attach to the client's network file system and interact with the system in a read only manner.

Using this technology it is possible to connect multiple **VeHARVEST** servers at one time to increase the processing throughput. The limitation on how many servers may be used is bound by the client's network bandwidth.

Prior to an engagement Visual Evidence provides a bandwidth test program for the client to perform on their network. This applet is provided by Visual Evidence on a CD and can be easily installed by the client. The test results will assist in determining the bandwidth available to perform the network harvesting. From these results time estimates regarding collection and segregation can also be calculated.

Crawling the network for ESI

Using a proprietary script employing a low level system IO library wrapped in a C#, .Net application, a snapshot of the target machine or machines directory structure is captured. The results of this interaction with the system are recorded in a MySQL database. As soon as the initial inserts are made into the database, a second process is initiated. This process sends a request to retrieve all metadata located in the target directory.

- Server Collection of ESI
- Alternative to Back-up Tape Restoration
- Cost Effective
- Time Efficient
- Court Sanctioned

This process also is a proprietary script employing a low level system IO library wrapped in a C#, .Net application. The metadata that is retrieved at this stage is:

1. File Name
2. Create Date
3. Modify Date
4. Access Date
5. File Size

Harvesting of Desired ESI

At this point a third process is launched to initiate the harvesting of files. If there is a date range filter as part of the criteria matching, it is employed at this juncture to limit the files that will require subsequent text review.

All files that meet the date range and prescribed criteria are retrieved and copied using a DCFLDD forensic file imaging utility to the **VeHARVEST** server. At this point the MD5 and SHA1 file hash checksums are calculated and stored in the **VeSHARE™** DB. As the hash is collected it is compared against hash total already harvested and duplicates are discarded: however, the file metadata and location information are retained. Once the file has been harvested, a mime detection applet is engaged to assist in determining the native format of the file. Those files that are detected to be archive type (compressed) are extracted and the extracted files are processed as regular files. If a file type cannot be identified, or if the file type registers as an image type file, it is maintained from further review.

At this time all files determined to be e-mail type archive files are converted to RFC822 compliant. These e-mail types files include .pst, .nsf, .dbx, .mbx, and .mbox. Ost file types are harvested for later extraction.

As the e-mail files are converted to RFC822 compliant files, any attachments are processed in the same manner as regular files.

After the ESI population has been normalized, regular expression term matching is engaged upon the ESI population. All files that match the provided word or phrase criteria are immediately quarantined for further review. Files that do not match the criteria are cleansed from the **VeHARVEST** database.



VISUAL EVIDENCE / E-DISCOVERY LLC

THE CRITTENDEN BUILDING 1382 WEST NINTH STREET SUITE 400 CLEVELAND, OH 44113
PH 216.241.3443 800.310.0981 FX 216.615.4920 WWW.VEVIDENCE.COM