



## Forensic Milestones

Much of what is now called computer forensics had its beginnings in the early versions of ILook, prior to the first general restricted user release of Version 7.0 in 2000. The release of ILook Version 2, in 1996, to a restricted, localized user base, marked a milestone in LEO computer forensics. However, early user base restrictions on ILook distribution precluded general public knowledge of the product's rich developmental history. Historically, Perlustro's primary goal has been to provide the most thorough and selective tools for salvaging any type of data; i.e., recovering and viewing files and artifacts not found by any other product; or recovering virtualized objects and folders.

Our commitment to providing the most capable forensics tools resulted in 42 releases of Version 7, prior to the release of the new .NET-based Version 8 in March 2004. Until 2008, ILook Version 8 was the only base version in release during 48 months of distribution. During that period there were 19 releases made to facilitate capability and correct bugs and errors within the application base - including 9 external tools. The ongoing development and refinement of ILook to meet the growing and changing demands of its user base has culminated in the creation of the most recent version, ILookPI. This revolutionary product is designed to deliver groundbreaking results, in the most clear and comprehensive form, and with virtually no user interaction required with the application or data in order to achieve positive investigative results.

The limitations noted above, also prevented public knowledge of the many capabilities of IXimager Version 2. Among its many features, IXimager holds the ability to image Apple systems, a feature that has existed throughout its distribution, but was virtually unknown because it was limited even to its own user base.

Below is a list of ILook "firsts in the field", which preceded the release of ILook Version 7.0. As a group, these features and functions made data reduction a fundamental element in the forensics process and, for the first time ever, allowed many in law enforcement, intelligence and the military to conduct investigations of computer systems within a Windows Environment.

### **ILook "Firsts in the Field"**

#### **Version 2**

- Implemented Apple Mac partition recognition.
- Implemented NTFS uncompressed named stream support and beta compressed named stream support.

#### **Version 3**

- LINUX Ext2 filesystem driver implemented.
- Mac HFS filesystem driver implemented.

- Mac HFS+ filesystem driver implemented.
- Added support for Mac HFS format floppy disks.

## Version 4

- Access Control List (ACL) interpretation for NTFS4 & NTFS5 file systems.
- ILook can now map Linux logical partition images & detects and maps Linux partitions via the Partition Probe function.
- Added custom file signature extraction to Salvage function.
- Added 17 popular word processing and spreadsheet file formats to the Salvage function.

## Version 5

- CRC32, MD5 and SHA1 hashing available from all partition, folder and file objects.
- ILook can import a variety of European and US law enforcement hash set formats for ILook's hash analysis functions.
- Negative hash analysis implemented which can exclude large amounts of known files from an investigation.
- Positive hash analysis implemented which can highlight known files regardless of their location or name.
- ILook can generate hash sets from any group of files on any filesystem available to the machine that ILook is running on.
- Ext3FS driver implemented (journaling variant of Ext2FS).
- SCO Sys V AFS filesystem driver implemented.
- SCO Sys V AFS filesystem driver implemented.
- SCO Sys V HTFS filesystem driver implemented.
- Can now export hash results from image data into an ILook format hash list.
- Investigator can specify that .JPG and .GIF salvage will use file trailers as stop points instead of 'n' number of sectors.

## Version 6

- WinNT and Win2k direct device investigation facility. Directly examine floppy disks and hard drives instead of via an image.
- Image directly accessed devices (via BIOS), useful for producing working image sets (with MD5 or SHA1 verification)
- Win9x direct floppy investigation facility. Directly examine floppy disks instead of via an image.
- Integrated thumbnail picture viewer and picture viewer - displays all common graphic formats.
- Support for VMWare Virtual Volume (DSK) image format.
- File deconstructors for IE v4 & v5 History files (INDEX.DAT).
- File deconstructor for Netscape history files (HST).
- File deconstructors for Outlook Express index (IDX) and mailbox (MBX) files.
- File deconstructor for Netscape cache database (FAT.DB).
- File deconstructors for Outlook Express v5 mail and usenet message stores (DBX).
- Base64 and UUE ripper functions to decode unsegmented email and usenet attachments.
- File and folder level elimination filter, allows an investigator to exclude groups of files which have been eliminated
- Conversion function which converts any supported image set to ILook's native compressed image format.
- Image hash function provides MD5 or SHA1 hash of any image set defined to ILook.
- ILook's IE cache deconstructor now supports cookie and history store formats.
- Rewrote Salvage Inline function, now recovers any given file type and not just GIFs, JPGs and BMPs.

