

Computer Forensic Tool for Law Enforcement

ProDiscover Forensics is a powerful computer security tool that enables computer professionals to find all the data on a computer disk while protecting evidence and creating evidentiary quality reports for use in legal proceedings.

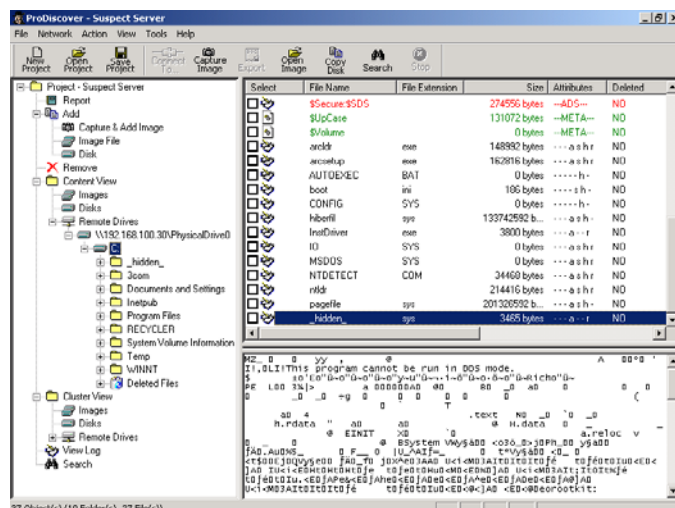
Features and Benefits

- Create Bit-Stream copy of disk to be analyzed, including hidden HPA section (patent pending), to keep original evidence safe.
- Search files or entire disk including slack space, HPA section, and Windows NT/2000/XP Alternate Data Streams for complete disk forensic analysis.
- Preview all files, even if hidden or deleted, without altering data on disk, including file Metadata.
- Maintain multi-tool compatibility by reading and writing images in the pervasive UNIX[®] dd format and reading images in E01 format.
- Powerful search capability using key words or regular expressions.
- Create index of image to allow for nearly instantaneous searches.
- Support for VMware to run a captured image.
- Examine and cross reference data at the file or cluster level to insure nothing is hidden, even in slack space.
- Automatically generate and record MD5, SHA1 or SHA256 hashes to prove data integrity.
- Utilize user provided or National Drug Intelligence Center Hashkeeper database information to positively identify files.
- Examine FAT12, FAT16, FAT 32 and all NTFS file systems including Dynamic Disk and Software RAID for maximum flexibility.
- Examine Sun Solaris UFS file system and Linux ext2 / ext3 file systems.
- Integrated thumbnail graphics, internet history, event log file, and registry viewers to facilitate investigation process.
- Integrated viewer to examine .pst / .ost and .dbx e-mail files.
- Utilize Perl scripts to automate investigation tasks.
- Extracts EXIF information from JPEG files to identify file creators.
- Automated report generation in XML format saves time, improves accuracy and compatibility.
- GUI interface and integrated help function assure quick start and ease of use.
- Designed to NIST Disk Imaging Tool Specification 3.1.6 to insure high quality.

ProDiscover Forensics is a key tool for effective computer forensic analysis. It is not possible to hide data from ProDiscover Forensics as it reads the disk at the sector level. This least intrusive approach also allows you to examine the files without altering any valuable metadata such as last time accessed. ProDiscover Forensics will not alter any data on the disk - period! ProDiscover Forensics can recover deleted files, examine slack space and access Windows Alternate Data Streams.

ProDiscover can even dynamically allow you to preview, search and image the Hardware Protected Area (HPA) of the disk utilizing a patent pending process.

ProDiscover Forensics lets you search through the entire disk for keywords, regular expressions, and phrases with full Boolean search capability to find the data you want. You can use the hash comparison capability to find known illegal files or to weed out known good files such as standard operating system files by utilizing the included data from National Drug Intelligence Center in their Hashkeeper database. ProDiscover Forensics's powerful search capability is fast and flexible, allowing you to search for words or phrases anywhere on the disk, including the slack space. The extensive on-line help capability and easy to use GUI interface allow you to quickly start using ProDiscover Forensics.



ProDiscover Forensics automatically creates evidentiary quality reports needed to document your results, complete with every file and hash signature where evidence was found. This saves time and prevents errors which might compromise your case.

Forensic Console System Requirements

- Windows 2000/2003/XP/Vista
- 1.2 GHz or higher Pentium-compatible CPU
- 2 GB RAM
- 500 MB available hard-disk space
- CD-ROM or DVD-ROM drive
- VGA or higher resolution monitor
- Keyboard and Mouse (or compatible pointing device)

License

ProDiscover Forensics is licensed to be installed on up to three workstations for one concurrent user. Site, Enterprise and Source licenses are also available for ProDiscover Forensics.