

## Remote Computer Forensic Tool for Internal Investigations

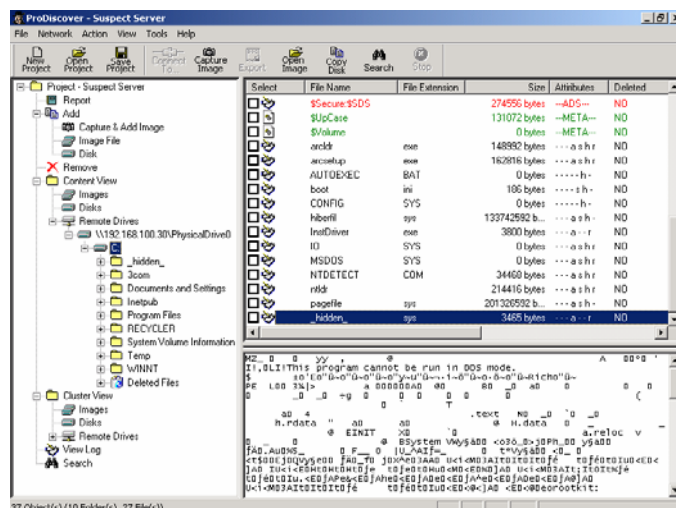
**ProDiscover Investigator** is a powerful computer forensic tool that enables corporate security professionals to remotely investigate the disk and memory contents of systems throughout your network to check for illegal activity or for compliance to company policy and to gather evidence for potential use in legal proceedings.

### Features and Benefits

- Speed investigations and save travel costs by forensically examining live systems throughout your network.
- Utilizes remote agent to read suspect disk at bit level, enabling you to examine all the contents of the suspect disk, including HPA and Windows NT/2000 Alternate Data streams.
- Remote agent may be pushed out, installed, and run remotely in Stealth mode (with System Administrator privileges) to avoid detection.
- All data transferred over the network may be protected with 256 bit AES or Twofish encryption.
- Preview and search suspect files to find evidence quickly and without altering any data or metadata.
- Automatically creates and records MD5 or SHA1 hashes of evidence files to prove data integrity.
- Image live memory and entire suspect disk, including hidden HPA section (patent pending), for further analysis.
- Maintains multi-tool compatibility by reading and writing images in the pervasive UNIX<sup>®</sup> dd format.
- 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 graphics thumbnail viewer and registry viewer.
- Utilize Perl scripts to automate investigation tasks.
- Extracts EXIF information from JPEG files to identify file creators.
- Linux boot disk provided to image systems without removing hard disk drive.
- 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 Investigator** is a key tool for effective internal investigations. It is not possible to hide data from ProDiscover as it reads the disk at the sector level, circumventing the standard file system. This allows ProDiscover to recover deleted files, look in slack data and even the HPA section of disk as well as examine Windows Alternate Data Streams. This unique approach also allows you to examine the files without altering any valuable metadata such as last time accessed. ProDiscover Investigator will not alter any data on the disk - period!

ProDiscover Investigator lets you capture and image of the RAM memory of a suspect system to search for passwords that may give you access to encrypted areas on the disk. Or you can search through the entire disk for keywords and phrases with full Boolean capability to find the data you want. You can use the hash comparison capability to find known illegal files or to weed out known standard operating system files utilizing data provided by the National Drug Intelligence Center in their Hashkeeper database. ProDiscover Investigator'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 Investigator.



ProDiscover Investigator 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.

### ProDiscover Console System Requirements

- Windows 2000/2003/XP
- 1.2 GHz or higher Pentium-compatible CPU
- 256 MB RAM (512 MB recommended)
- 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 Investigator is licensed to be installed on up to three workstations for one concurrent user. The PDServer<sup>™</sup> Remote Agent and Linux boot disk are licensed to operate on an unlimited number of systems. Site, Enterprise, and Source licenses are also available for ProDiscover Investigator.