

Incident Response and System Auditing Tool

ProDiscover Incident Response enables you to quickly and thoroughly examine a live system operating anywhere on your network. When used as part of an incident response procedure or as part of a routine system audit, ProDiscover *Incident Response* enables you to determine if that system has been compromised and allows you to gather the evidence needed to prove it.

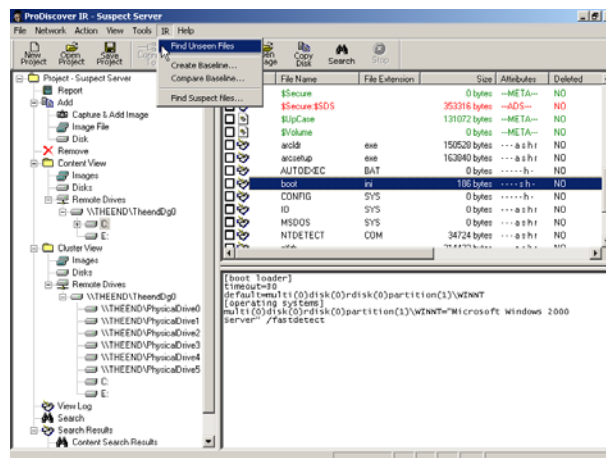
Features and Benefits

- Quickly verify if your system has been compromised without taking the system down.
- Analyze remote systems over the network eliminating the need to hire expensive staff or travel to remote locations.
- Utilizes remote agent to access suspect system disk at the sector level, revealing all files even if suspect system has been compromised by Trojan or rootkit.
- Create a bit-stream image of the target system disk and physical memory to preserve evidence and restore the system quickly.
- Image shadow copy of remote system disk.
- Remote image copy may be sent out local system port or to a network storage location to improve image capture performance.
- Search entire disk, including unallocated space, slack space, Windows NT/2000/XP Alternate Data Streams, and even HPA section (patent pending), for complete system integrity.
- Powerful search capability using key words or regular expressions.
- Create index of image to allow for nearly instantaneous searches.
- Automatically create and record MD5, SHA1, or SHA256 hashes of evidence files to prove data authenticity and integrity.
- Capture volatile state information such as open ports with connected IP addresses, route tables, ARP cache, logged-on users, etc. to investigate an incident.
- Capture image of BIOS/CMOS memory to find compromises.
- 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.
- Find files and processes that are being cloaked by rootkits.
- Create system baseline for comparison to uncover altered files.
- Utilize Perl scripts to automate investigation tasks.
- Utilize user provided or National Drug Intelligence Center Hashkeeper hash sets to verify integrity of all system 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.
- Maintains multi-tool compatibility by reading and writing images in the pervasive UNIX[®] dd format and reading images in E01 format.
- Support for VMware to run a captured image.
- Remote agent may be preinstalled or pushed out, installed, and run remotely in normal or Stealth mode (with System Administrator privileges) to avoid detection.
- Linux boot disk provided to image systems without removing hard disk drive.
- User selectable 256 bit AES or Twofish encryption protects data transfers and remote system access.
- 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.

If you suspect that your system has been compromised or if you perform regular system audits, you need to thoroughly examine systems without taking them down. ProDiscover *Incident Response* will enable you to quickly, and with certainty, determine the integrity

of your system while it is still on-line, performing its normal operations.

ProDiscover *Incident Response* utilizes an agent that runs on the suspect system to read the disk and RAM memory at the bit level. This enables ProDiscover *Incident Response* to work around the suspect system's o/s and examine all files, even if they are hidden by a Trojan or rootkit. It also prevents any valuable metadata, such as last time accessed, from being altered. ProDiscover *Incident Response* can search the system for over 1000 known Trojans or rootkits. And, to insure the integrity of the o/s, ProDiscover *Incident Response* can examine all files and compare their hash signature to the signatures of known good files from a user provided baseline or from the National Drug Intelligence Center Hashkeeper database. ProDiscover *Incident Response* allows system administrators to be sure that they uncover any compromised files in the least intrusive manner.



If the system has been compromised, ProDiscover *Incident Response* allows the system administrator to make a bit stream image of the disk and memory and capture system volatile state information for later analysis so that the system may be restored to proper working order to get it back on-line quickly. The off-line analysis of the data is easy and allows evidentiary quality data to be provided to law enforcement agencies.

ProDiscover 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 *Incident Response* is licensed to be installed on up to three workstations for one concurrent user. The PDServer[™] 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 *Incident Response*.