

## Incident Response and System Auditing Tool

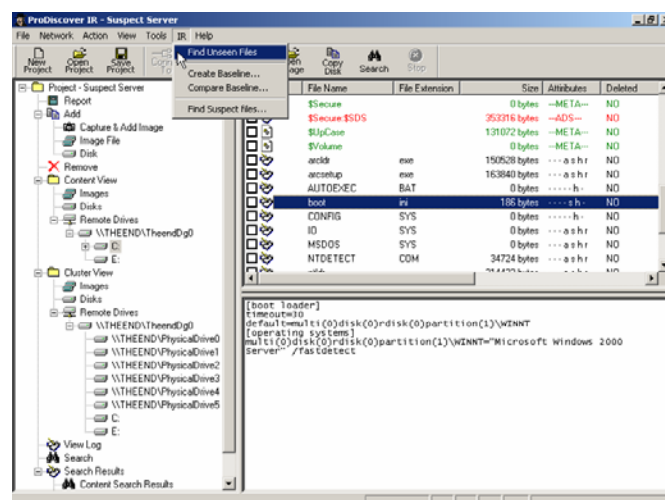
**ProDiscover Incident Response** enables you to quickly and thoroughly examine a live system operating anywhere on your network. When used as part of an incident response procedure or as part of a routine system audit, ProDiscover *Incident Response* enables you to determine if that system has been 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.
- Access suspect system disk at the sector level, revealing all files even if suspect system has been compromised by Trojan or rootkit.
- 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.
- Create a bit-stream copy of the compromised system disk and memory to enable you to quickly restore the system without losing valuable evidence.
- Capture volatile state information such as open ports with connected IP addresses, route tables, ARP cache, logged-on users, etc. to investigate an incident.
- Integrated process explorer and registry viewer.
- Find files and processes that cannot be seen by suspect system O/S.
- Create system baseline for later comparison to uncover altered files.
- Utilize Perl scripts to automate investigation tasks.
- Utilize user provided or National Drug Intelligence Center Hashkeeper database information to positively identify 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.
- 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.
- 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 your network 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
- 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 *Incident Response* is licensed to be installed on up to three workstations for one concurrent user. The PDServe™ 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*.