

Computer Forensics; Collection, Analysis and Case Management using ProDiscover[®]

Christopher L. T. Brown, CISSP
Technology Pathways, Founder & CTO
clbrown@techpathways.com
619-435-0906 / 888-894-5500

Copyright © 2003, Technology Pathways, LLC

Purpose of this Presentation

- Provide attendees an understanding of how the ProDiscover[®] family of products support the computer forensics process
- Introduce attendees to evidence *Collection, Analysis and Case Management* using ProDiscover[®]

Presenter: Christopher L. T. Brown

- Over 20 Years Industry Experience
- Various (ISC)², Microsoft, CITRIX, CompTIA and CISCO certifications
- Consultant, Developer, Author
- UCSD Extension Information Security Instructor and Certificate Board Member
- HTCIA Board, InfraGard Member

Founder & CTO



Technology
Pathways

**Security
Products and Services
for
Corporate, Legal, and
Government**

Agenda

- Product Architecture and Process Support
- Collecting an Evidence Image
- Network Imaging & Analysis with ProDiscover[®] IR
- Filtering Non-interesting Files
- Searching Files & Slack Space
- File Cluster Cross-referencing
- Reporting & Production

Product Architecture and Process Support

The Process

- Collection
- Preservation
- Filtering & Identification
- Presentation

Tools For The Process

- The ProDiscover[®] family of products are designed to support the forensics process for specific markets
 - ProDiscover[®] – Forensics (DFT)
 - ProDiscover[®] – Incident Response (IR)
 - More to come...
- Basic features and UI are common to all family tools
- Customized functionality in each tool to suit the user

ProDiscover[®] Core Architecture

- Read the disk at the sector level in a Read-Only mode
- Perform all display and functions through it's own trusted, read-only file system
- Currently supports all versions of FAT and NTFS including Dynamic Disk, Software RAID and Volume Sets

Getting Started

- Installation Process
 - Supports systems with/without internet connection
 - Licensing steps outlined in Quick Start Guide, Readme.rtf and Help File
 - Backup “LSERVRC” File

Beginning A Project

- When using ProDiscover[®] each case is referred to as a "Project"
- The project file is a file name with the file extension "DFT" (project.dft)
- Each project file contains information about the project which can include multiple disks and images
- Search results are maintained in (project.dsr)

Project File

- All exported project reports are created from the project file and search results file
- Project files are maintained in XML format to allow for greater flexibility in automated data extraction for use in other applications
- At program launch ProDiscover[®] allows the user to:
 - Create a new project
 - Open an existing project

Demo Creating & Saving a New Project, UI and Help

Working on a Live Disk (*Preview Operations*)

Preview Operations

- ProDiscover[®] allows investigators to add disks directly to a project for:
 - Previewing a disk in the field
 - Full analysis of disk-to-disk images
- All program functionality is supported while previewing disk

Demo Disk Preview

Collecting an Evidence Image

Forensics Imaging Methodology

- Bit-Stream Image (not file copy, ghost, xcopy, etc...)
- Why?
 - You want the slack space
 - To recover deleted files
 - Unrecoverable file fragments

Forensics Imaging Methodology (2)

- Hardware Write-Blocked
 - Non-forensic software may write to the drive/image
 - OS may write to the drive/image

NIST (National Institute of Standards & Technology) Disk Imaging Tool specifications

Imaging Support

- ProDiscover[®] supports imaging local drives in several ways:
 - Disk-to-disk image (test booting)
 - Disk-to-image file (faster searches, disk geometry)
 - *Image files are compressible*
 - Image file-to-disk (restore an image)
- Disk can be accessed via:
 - IDE Bus
 - USB-IDE Converters
 - Network (LAN/WAN) with (ProDiscover[®] IR)

Many Ways to Image

- Hand Held Forensic Imagers
 - ICS – SoloForensics
 - LogiCube – SF-5000
- Unix “dd” Command
 - ProDiscover[®] supports reading dd images
 - ProDiscover[®] supports converting ProDiscover[®] image format to dd image format for use in other forensics tools

The ATA Hardware Protected Area (HPA)

- Created in ATA 4 spec to allow manufactures to hide diagnostic & recovery tools
- Allows a disk to *Hide* an area of the disk for non-os use
- BIOS nor the OS see the hidden area
- Most imaging methods do not detect the presence of an HPA
- FirstWare and AREA-51 allow consumers to use HPA to hide data

HPA Support

- Removal is difficult and normally destroys access to the HPA's file system (HPA becomes unallocated disk space)
- ProDiscover[®] can non-destructively look inside the HPA and image or extract any files from within
- HPA white paper available

Demo Collecting an Image

Network Imaging & Analysis with ProDiscover[®] *IR*

Network Imaging & Analysis

- ProDiscover[®] *IR* was designed in a client/server model
- ProDiscover[®] - Console or *Client*
 - Main application functionality
- PDServer[™] - Server or *Network Agent*
 - Run on remote system to allow ProDiscover[®] client access to disk

PDServer™ Remote Agent

- Offers choice of clear and TwoFish encrypted data channel
- Provides “Stealth mode” for covert imaging and analysis of live systems (*requires one-step installation*)
- Configurable port settings for firewall filtering
- Server is read only protecting data
- Must be an administrator equivalent to run

PDServer™ Rem0te Agent (2)

- All Imaging and Preview functions supported
- Runs on all supported platforms and Windows XP Series
- HPA functions are supported for all remote disks excluding Win98SE
- Network Images are sometimes referred to as a “smear” since bits on the original may change during imaging

Pushing PDServer™ Out

- The need to push agent and support files to systems in remote locations
- Scripts are provided for remote installation and removal
- Requires a few files from the Windows NT 4.0 Resource Kit and PSKill.exe from System Internals

PDServer™ Remote Installation Demo

Filtering Non-interesting Files

Reducing Search & Analysis Time

- Limiting the search base
- The average Windows 2000 system will contain around 20,000 files
- Many of these files are of no interest
 - Operating system files
 - Application files

Known Goods

- File hash comparisons are considered the best practice for filtering out known files
 - SHA1 (newer and gaining popularity)
 - MD5 (most widely used)
- Many organizations keep their own file hash databases for these comparisons
- Option for “No-Hash” speeds up index creation (can hash indexed files later)

Hash Databases

- NDIC (National Drug Intelligence Center)
 - HashKeeper – Limited availability
- NIST (National Institute of Standards and Technology)
 - National Software Reference Library (NSRL) Reference Data Set (RDS)
 - \$ 90.00 annual subscription (quarterly releases)
 - <http://www.nist.gov/srd/dblist.htm>

Known Bads

- ProDiscover includes a database set of "*Known-bad*" hash values:
 - Currently over 400 Windows/Linux Trojans and Rootkits
 - SHA1 and MD5 hashes
 - Hashkeeper format

Filtering by Hash Set

- Both NDIC's Hashkeeper and NIST's database allow hashes to be extracted into flat (*.hsh) files
- ProDiscover[®] will read hash sets dumped to the hashkeeper format allowing users to:
 - Find files based on hash
 - Filter files based on hash
 - Hide files based on hash

Demo Hash Filtering

Searching Files & Slack Space

Fast & Accurate Searching

- Just as in data views, ProDiscover[®] offers two approaches to searching:
 - Content level searching
 - Partition or Directory...
 - Cluster level searching
 - Partition & Physical Drive

Content level searching

- Searches the viewable file system (deleted files included)
- Does not search boot sector, unallocated and slack space
- Provides the ability to search only in files marked "selected"
- Provides the ability to mark "selected" all returned files
- Case Sensitive, Whole Word, ASCII and HEX options
- Much faster than entire disk bit level searches

Cluster level searching

- Searches the entire disk at the bit level
- Includes boot sector, unallocated and slack space (everything)
- Offers the option to return the resulting search cluster contents to a single or multiple files
- Case Sensitive, Whole Word, ASCII and HEX options
- Slower than content level searching

Tips on Searching

- Search for unique strings:
 - Misspellings
 - Phrases rather than words
 - Trial searches for known values
 - Whole word searches are helpful

FAT Search Test Set

- A search string test set and image from the Computer Forensics Tool Testing List Server
- Image contains 12 unique strings placed in files, slack, fragmented clusters, etc.
- Intended to test tool capabilities
- Very few tools found all 12 unique strings
- ProDiscover[®] found them all!

FAT Search Test Set can be found at

[http://www.cerias.purdue.edu/homes/
carrier/forensics/tests/test2/desc.html](http://www.cerias.purdue.edu/homes/carrier/forensics/tests/test2/desc.html)

Searching Demo

File Cluster Cross-referencing

Switching Views

- Often it is helpful to switch between content view and cluster view
- Some investigations require the lowest level of analysis and reconstruction
- ProDiscover[®] offers the facilities to quickly switch views

Finding a Files Clusters

- ProDiscover[®] allows users to easily find the clusters a file resides in by right-clicking on the file
- Helps manually inspect file slack and neighboring clusters

Finding a Clusters Files

- ProDiscover[®] allows users to easily find what file a cluster belongs to by right-clicking on the cluster
- Helps to quickly locate files from the cluster view
- Helps to identify orphaned file fragments

Cluster Xref Demo

Reporting & Production

Automatic Reporting

- Reporting is a key component of any case
- The ProDiscover[®] report is automatically generated as the case progresses

Report Categories Include:

- Project Name, Number & Description
- Images & Disk added to the project
- Extracted Registry Data
- Evidence of Interest (selected files)
- File Signature Mismatches
- Search Results
- Project Notes

Managing Report Contents

- While working a project the report contents can be managed using the “Action | Clear Report” menu item
- Options include:
 - Evidence of Interest
 - Search Results
 - File Signature Mismatch
 - OS Info (registry extraction)

Exporting the Report

- Reports are not currently directly editable, but can be exported in RTF or TXT
- TIP: Users can create HTML report by opening RTF files in Word and Saving as HTML format
- TIP: Project Reports are embedded in the Project file (.dft) which are in XML format. Change the file extension to .xml and open in MS Excel for easy sorting of evidence

Exporting Evidence Files

- Any single file can be exported/recovered by right-clicking the file and choosing “**recover**”
- Batch processing available for all files marked “**selected**”
- Files can be “**bates**” numbered in the copy process (white paper available)

Thank You Questions?

Technology
Pathways

703 First Street
Coronado, Ca. 92118

Phone: 888-894-5500
FAX: 619-435-0465

www.TechPathways.com

clbrown@TechPathways.com



**Are your
tools
keeping
pace with
the
criminals?**