

# *Introduction to Using ProDiscover<sup>®</sup> for Computer Forensics Investigations*

Christopher L. T. Brown, CISSP  
Technology Pathways, Founder & CTO  
[clbrown@techpathways.com](mailto:clbrown@techpathways.com)  
619-435-0906 / 888-894-5500 x111

Copyright © 2004, Technology Pathways, LLC

# Purpose of this Presentation

- Review the basic principles of computer forensics
- Provide attendees an understanding basic methodologies used in computer forensics disk image processing
- Introduce attendees to evidence *Collection, Analysis and Case Management using ProDiscover<sup>®</sup>*

# ProDiscover® Architecture & Product Family

# Tools For The Process

- The ProDiscover<sup>®</sup> family of products are designed to support the forensics process for specific markets
  - ProDiscover<sup>®</sup> – for Windows
  - ProDiscover<sup>®</sup> – Forensics
  - ProDiscover<sup>®</sup> – Investigator
  - ProDiscover<sup>®</sup> – 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<sup>®</sup> 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, SUN Solaris UFS on SPARC and X86 Platforms, LINUX Ext2/3

# Independent Validation (1)

- ProDiscover® has been utilized by professionals to find and present evidence for civil and criminal proceedings
- An Independent Review of Forensic Tools was recently published by Mark Scott on the SANS web site validating the ProDiscover imaging process  
<http://www.sans.org/rr/special/forensicimaging.php>

# Independent Validation (2)

- The Dartmouth Institute for Security Technology Studies report Law Enforcement Tools and Technologies for Investigating Cyber Attacks - Gap Analysis Report ranks ProDiscover® as meeting the greatest number of needs for Preliminary Investigation and Data Collection.
- [http://www.ists.dartmouth.edu/TAG/gap\\_analysis.htm](http://www.ists.dartmouth.edu/TAG/gap_analysis.htm)

# Independent Validation (3)

- Digital Investigations Journal Vol. 1 No. 4 (December, 2004)  
*<http://www.compseconline.com/digitalinvestigation>*
  - *Remote Forensics'*, by Philip Sealey
  - *Tool review - remote forensic preservation and examination tools*, by Eoghan Casey & Aaron Stanley
- Network Computing Magazine (December 2004)  
*<http://www.networkcomputing.com/>*
  - *Network Forensic Tools - Elementary, My Dear Watson*, by Marisa Mack

# Installing ProDiscover®

# Supported Platforms (1)

- ProDiscover Console tested on:  
Win98SE, W2K, XP and Server2003
- Processor and Memory needs based on case. Tested with 128 MB and 1.2 GHz  
Recommend much more for today's searches and case needs

## Supported Platforms (2)

- ProDiscover Remote Agents for:
  - Sun Solaris X86
  - Sun Solaris SPARC
  - Windows 98 SE/W2K/XP/2003
  - LINUX
- Remote HPA Removal driver supported for:
  - W2K/XP/2003

# Installation

- Installation Process
  - Auto Run
  - Setup.exe
  - ProDiscoverRelease<version><edition>.exe
- Internet connection **NOT** needed
- **NO** dongle needed

# Post Installation (1)

- Licensing
  - Uses licensing file with company information
    - ProDiscover<edition>.vpl
    - Example: ProDiscoverLR.vpl
  - By default ProDiscover includes a temporary license file that will fully activate ProDiscover for 5 uses
  - To fully activate ProDiscover simply copy your companies license file (delivered by email) over the temporary license file in the default installation directory

# Post Installation (2)

- TCP/IP Performance
  - ProDiscover IN/IR Only
  - Reboot for Performance Registry Entries to take effect

# Post Installation (3)

- PARemove.sys Driver
  - Not required to run
  - Allows access to disks HPA
  - Found in the \Driver directory under the default installation directory
  - Readme.txt file contains step-by-step directions for installation

# Directory (Folder) Structure

- ProDiscover installs to the following folder by default:  
“C:\Program Files\Technology Pathways\ProDiscover\”
- Subdirectories include:
  - **Driver**
  - **Hash Sets**
  - **Linux Boot Disk**
  - **ProScript - Documentation/Examples/Output/UserScripts**
  - **Remote Agent – Scripts/Windows/Solaris/Linux** (*IR/IN only*)
  - **Sample Images**
  - **Sample Pics**
  - **Search Term Sets**

# ProDiscover Projects

- When using ProDiscover<sup>®</sup> 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.dsX)

# 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
- An XML schema description file can be found in the default installation directory
  - ProjectFileSchema.xsd

# Starting ProDiscover<sup>®</sup>

- At program launch ProDiscover<sup>®</sup> 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<sup>®</sup> 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

# Imaging Methodology

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

# 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<sup>®</sup> supports imaging local drives in several ways:
  - Disk-to-disk image (test booting)
  - Disk-to-image file (faster searches, disk geometry)
    - PD Format or Convert to “dd”
    - \*.eve, \*.cmp, \*.pdg, \*.pds, \*.dd
  - Image file-to-disk (restore an image)
- Disk can be accessed via:
  - IDE Bus
  - USB-IDE Converters
  - Network (LAN/WAN) with (ProDiscover<sup>®</sup> IR/IN)

# Many Ways to Image

- Hand Held Forensic Imagers
  - ICS – SoloForensics (Solo III)
  - LogiCube – SF-5000/MD5
  - My Key DiskCopy
- Unix “dd” Command
  - ProDiscover<sup>®</sup> supports reading dd images
  - ProDiscover<sup>®</sup> supports original imaging in dd format or converting ProDiscover<sup>®</sup> image format to dd image format for use in other forensics tools

# Demo Collecting an Image

# Live Imaging & Analysis with ProDiscover<sup>®</sup> *IR*

# Why Live Enabled Disk Forensics

- Pervasive use of networks
- Least intrusive (evidence dynamics)
- Long term investigations
- Remote artifact extraction
- Cross-over preview & imaging

# Live Imaging & Analysis

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

# Benefits of Live/Remote Forensics

- Allows for remote **Preview** of Live systems without taking them off line
- Allows for remote **Imaging** of live systems without taking them off line
- LINUX Remote Agent on a LINUX boot disk  
Allows for imaging of “system-at-rest”. Great for Notebook imaging through a cross-over cable

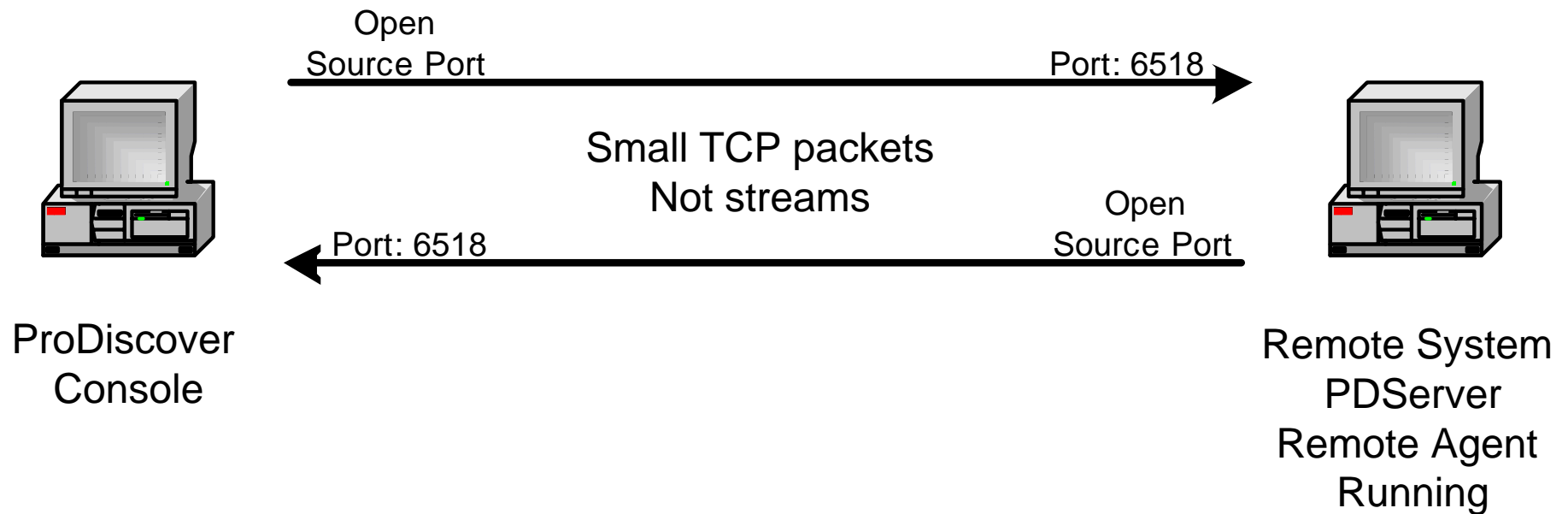
# Creating Remote Agent (1)

- Windows
  - Windows Remote Agent CD Included
  - Tools Menu | Create Remote Server Disk (uses pdserver.eve file in \server directory)
  - Burn Files from root of \Server directory
- SUN
  - Burn Files from root of \Server\Sun\platform directory
  - Burn ISO image from same directory

# Creating Remote Agent (2)

- LINUX
  - LINUX Boot CD with remote agent included
  - Burn Files from root of \Server\LINUX\ directory
  - Burn ISO image of remote agent from same directory
  - Burn ISO image of LINUX boot CD with remote agent

# The Remote Connection



# Connection Characteristics (1)

- Data channel encryption
  - Unencrypted (default)
  - 256 Bit AES
  - 256 Bit TwoFish
- Remote Agent Visibility
  - Foreground application (default)
  - Stealth mode option
    - Using scripts, menu option or command line
    - PDServer.exe -S:Password
- Server is read only protecting data

# Connection Characteristics (2)

- Can run as domain user in Windows
- Must be root in UNIX/LINUX
- Configurable port settings for firewall filtering
  - Console set by choosing
    - File | Preferences... | PDServer
  - Remote Agent by Launching from command line
    - PDServer.exe -p:80
- Set remote agent password by command line
  - PDServer.exe -S:password

# Connection Characteristics (3)

- GUIDs (Globally Unique Identifiers) are created for each side of the connection which are sequenced to maintain connection integrity and security
- Session setup is always encrypted regardless of user encryption settings
- Has been used on intercontinental connections through the Internet

# Connection Characteristics (4)

- If a session is determined to be “broken” the it must be reset on one of the following
  - Console - “Network | Release Remote Client”
  - Remote Agent - “Tools | Release Client”

# PDServer™ Rem0te Agent (1)

- All Imaging and Preview functions supported
- Agents for all supported platforms
- HPA functions are supported for all remote disks excluding Win98SE
- Live 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
- GUI menu option and scripts are provided for remote installation and removal
- Scripts require a few files from the Windows NT 4.0 Resource Kit and PSKill.exe from System Internals

# PDServer™ Remote Installation Demo

# IR Menu Functions

- Find Unseen Files
- Find Unseen Processes
- Forensic Baseline and Compare
- Find Suspect Files (hash db compare)
- Process Explorer
- System State (route tables, user info, etc.)
- Open/Connected IP endpoints

# Linux Remote Boot CD (1)

- Created to allow imaging on site of a disk-at-rest through a cross-over cable.
- Linux Boot is based on John Andrews DSL (Damn Small Linux)
  - [www.damnsmalllinux.org](http://www.damnsmalllinux.org)
- DSL was based on Knoppix
  - [www.knoppix.org](http://www.knoppix.org)

# Linux Remote Boot CD (2)

- Technology Pathways further changed DSL to:
  - Ensure no local system disk are mounted (remote agent provides raw read-only access) Knoppix will increment the journal count on journaling file systems with mounting even in read-only
  - Not auto mount a LINUX swap partition as Knoppix will
  - Remove all non-essential GUI and applications
  - Auto-run the PDServer Remote Agent

# Searching Files & Slack Space

# Fast & Accurate Searching

- Just as in data views, ProDiscover<sup>®</sup> offers various approaches to searching:
  - Content level searching
  - Cluster level searching
  - Registry Searching
  - Event Log Searching

# 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<sup>®</sup> 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

# Windows Registry Viewer

# Viewing Windows Registry

- What is the Windows Registry
  - Multi-File
  - Dynamic
  - Static
- Forensic view
- Procedures
  - Right-click on “windows” system dir and choose “Add to Registry Viewer”

# Windows Event Log Viewer

# Viewing Event Log Viewer

- What is the Event Log Viewer
- Forensic view
- Procedures
  - Right-click on “windows” system dir and choose “Add to Event Viewer”

# Reporting & Production

# Automatic Reporting

- Reporting is a key component of any case
- The ProDiscover<sup>®</sup> 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)
  - Files, Clusters, and Registry Keys
- File Signature Mismatches
- Search Results
- Project Notes

# Graphics Specific Data

- Adding EXIF data to reports
- Adding thumbnails to reports
- Auto-loading thumbnails to reports
- Manually adding thumbnails to reports

# 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)

# COMPUTER EVIDENCE

## *Collection & Preservation*

- Teaches investigators how to ensure case integrity when dealing with computer evidence
- Provides a practical resource for collection and preservation that will help ensure legal acceptability
- Covers key areas such as rules of evidence, evidence dynamics, network topologies, collecting volatile data, imaging methodologies, and forensics labs and workstations
- Includes a CD-ROM with shareware and commercial demo software tools as well as document templates, worksheets, and references



Networking & Security Series

CHRISTOPHER L.T. BROWN

# Thank You Questions?

Technology  
Pathways

703 First Street  
Coronado, Ca. 92118

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

[www.TechPathways.com](http://www.TechPathways.com)

[clbrown@TechPathways.com](mailto:clbrown@TechPathways.com)



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