

ProDiscover Remote Analysis and Imaging Application Note



Introduction

Some of the ProDiscover® family members allow you to analyze and image a live system over your network while that system is on-line, performing its normal operations. All the features available in ProDiscover to analyze and image a local disk are available remotely. Additionally, with the remote forensic capability of ProDiscover, you can image the RAM memory of a remote system, allowing the capture of key passwords and memory only resident malware. This information would be lost if traditional local disk only forensics are employed.

The remote forensic capability can be used to simplify and improve the job of the examiner in many applications. For example:

- Internal Investigations - Investigate any employee without needing to travel to the employee's location.
- Incident Response and System Audits - Search for malware such as Trojans and rootkits (even kernel mode rootkits) on any system in your network.
- Probation Monitoring - Remotely monitor the computer system of individuals on probation to insure compliance.
- Evidence Collection - Collect evidence to provide to authorities without shutting down your vital business systems
- Electronic Discovery - Gather appropriate documents for production from systems throughout your network.

ProDiscover is the affordable alternative to meet your remote analysis and imaging needs. This note contains the information needed to understand how to utilize the remote capability of ProDiscover.

Static Image versus Smear

While you may take a live system off line and stop all processes when using ProDiscover to analyze and image a system, often this is impractical. In cases such as incident response where you are not sure if a system has been compromised, it is costly to shut down critical business applications while you search for malware. Even if you find a compromise, often companies cannot afford to shut down their business systems long enough to gather the evidence required to find and prosecute the offenders. In cases of internal investigations, secrecy is often paramount and you cannot shut down the system of the employee under investigation to perform the investigation. When this is the case, the forensic imaging of a live system creates what is often referred to as a "smear". Smears capture the image while disk I/O processes are still taking place due to other processes running on the system. While this may create some internal inconsistencies in the data, as long as the data being collected is not over-written, this process is perfectly valid in capturing evidence and has been successfully offered as evidence in court cases.

Setting up and running a remote ProDiscover session

There are five steps to completing a remote forensic session. They are:

1. Deploying the PDServer™ remote agent on the target system
2. Launching the PDServer remote agent on the target system
3. Connecting to the PDServer remote agent using the ProDiscover console
4. Performing live analysis and/or imaging
5. Stopping and removing the PDServer remote agent (if desired)

In order to set up and run a remote forensic session using ProDiscover, you will need the PDServer remote agent. This agent needs to be deployed and launched in the target system in order for the ProDiscover console software to connect to it and perform the remote analysis and imaging. The PDServer remote agent reads the data off the target system disk at the hardware sector level and transfers these bits to the ProDiscover console where they are re-built into ProDiscover's internal "read-only" file system for display.

Steps 1&2. Deploying and launching the PDServer remote agent

There are three ways to deploy and launch the PDServer remote agent on the target system, and depending on the method used, the usage rights required on the target system will vary. The following describes each method and the rights needed:

Trusted CD – The PDServer remote agent can be burned to a CD deployed by placing this trusted CD into the target system. This will require physical access to the target machine. The binaries need only user access rights on the target machine and will auto-launch when placed into the CD drive. Loading the PDServer remote agent from a CD or USB pocket flash drive places the agent in memory only and will not alter the disk image of the suspect system.

Pre-Installation – The PDServer remote agent may be pre-installed on all systems that may be of interest. If the PDServer remote agent is pre-installed, it may automatically be launched at system start-up or may be launched only when needed. You may launch the PDServer remote agent locally with only user level access to the system. To launch PDServer remotely, you can use virtually any remote administration tool such as Telnet, Dameware or Hyena. You will typically need system administrator rights on the target system to utilize these remote access tools, and you will need to be able to access the system through any firewalls that may exist between the system running the remote administration tool and the target system.

Pushing out and running remotely – The PDServer remote agent may be pushed out to the target system, installed, and launched from a remote system. (Note, this operation does not need to be performed from the system which is running the ProDiscover console.) To push the PDServer remote agent to the target machine, you will need system administrator rights on the target system. The ProDiscover console provides an integrated ability to push out, install, and launch the remote agent on a target system. Technology Pathways also provides scripts to remotely push out and install and launch the PDServer remote agent on a target system. Pushing out and installing the PDServer remote agent will alter the disk of the target system and therefore, you run the risk of overwriting some evidence. However, given the small size of the remote agent, this may your best alternative for examining a system.

Step 3. Connecting to the PDServer remote agent

Once the PDServer remote agent is running on the remote system, you must connect to it using the ProDiscover console. The system running the ProDiscover console does not need to part of any domain and does not need to be part of the domain of the target system.

To connect to the target system you will first need the IP address or NETBIOS name of the target system. If you run the PDServer remote agent from the Trusted binary CD, it will open a window and provide you the IP address of the target system in the window title bar. Otherwise, you will need to obtain this information from the system administrator.

If there are any firewalls between the ProDiscover console system and the target system, you need an open TCP port, in both directions, through these firewalls. ProDiscover and PDServer are pre-configured to communicate using TCP port 6518. If this port cannot be made available through your network, the port assignment may be changed to any port desired.

To connect to the target system, you start the ProDiscover console software, open an active project file, then use the “Connect to” command in the Network Menu to input the IP address or NETBIOS name.

Step 4. Performing the analysis and imaging

Once connected to the target system, you can image the system using the Capture Image command or if you want to perform a live analysis, you can use the Add Disk command to add a disk from the remote system to the Tree View Menu of the ProDiscover console.

You need only select this new remote disk to begin the live analysis. ProDiscover will then create the file view and cluster view of this remote drive automatically. From then on, this disk is just like any other local disk on the ProDiscover console. You may perform any task on this remote disk as you would on a local disk.

Because remote communications may have delays you may experience a communication time-out during a remote analysis or image process. ProDiscover allows you to adjust the time-out period and number of retries to meet your network conditions.

Step 5. Stopping and removing the PDServer remote agent

Once the remote analysis and imaging is complete, you may remove the PDServer remote agent if desired. If you are running from the Trusted binaries CD, you need only remove the CD from the system. If you have pre-installed the PDServer remote agent, you should use the same administration tool to stop the PDServer as you used to launch it. If you have pushed the PDServer remote agent out to the target system you may use the ProDiscover console’s integrated ability to stop and remove the script or you may use a script supplied by Technology Pathways to kill the process and uninstall the PDServer remote agent.

Running the PDServer Remote Agent in Stealth Mode

If you install the PDServer remote agent on the target system, either via the pre-install or push out methods, you may select to have it run in Stealth Mode. This will prevent the PDServer remote agent from opening any windows or dialog boxes on the target system which would alert a user to its presence. The PDServer task will however be visible by using the Task Manager, but it may be renamed during installation to decrease the chance of being noticed by typical users.

Security Considerations when using the ProDiscover remote capability.

The remote capability for ProDiscover has been designed with security in mind, and Technology Pathways has implemented several security measures to protect you and your systems. These measures include:

Password Protection

The remote agent may be password protected to prevent use by unauthorized personnel. The password is always encrypted during the session establishment process, even if the user chooses not to encrypt the session. To prevent a brute force attack to guess the password, the remote agent will delay an ever increasing amount of time between accepting successive logon attempts.

Encryption

The user may elect to have all communications between the host and remote agent be protected by 256 bit AES or Twofish encryption. Even if the user chooses to not enable encryption on the data, the password is always encrypted.

Secure Communication Protocol

The protocol used to establish and run all sessions to the remote agent employs Global Unique Identifiers (GUID's) to insure no other process can insert packets in the data stream. This insures the remote agent will only communicate to one client per session.

Write Protected Trusted Binaries

The remote agent may be executed from a write protected device such as a CD or floppy so no unauthorized users may alter it.

Digital Signatures

The PDServer.exe file as well as PARemove.sys device driver have both been digitally signed and are verifiable through the Thawte CA (certificate authority). To verify either file, right-click on the file and choose "digital signatures", highlight the signature and choose "details".

Other Safeguards

Should the user elect to pre-install the PDServer remote agent, the code has been designed to be safe. PDServer is not capable of writing anything to the disk so an unauthorized user cannot use it to create back-doors or load malicious code on the system. The PDServer remote agent has been designed to protect against any buffer overflow error conditions and has been tested and found to not be susceptible to any buffer overflow conditions.

Performance Considerations when using ProDiscover remote capability.

The performance of ProDiscover when utilized in a remote configuration is of course mainly dependent on the network utilized. In a LAN environment, the performance will typically be only slightly lower than the performance of ProDiscover used with local disks.

We have tested ProDiscover over several broadband WAN environments. The performance is typically 5x to 10x slower than the LAN environment. We do not recommend the use of narrowband WAN connections with ProDiscover.