Live Data Acquisition:
The New Default Standard for Capturing ESI?

By David Greetham, National Director of Forensics,
Legal Enterprise Solutions
Over the last quarter century, legal requirements have increased the prevalence of and reliance upon computer forensics. Meanwhile, use of information technology has intensified—with data volumes growing exponentially. For many years, the computer forensics community has established and followed predefined collection standards. Today, forensic imaging remains the foundation for all computer forensics, and is critical when having data admitted as evidence in courts and tribunals worldwide. Consequently, it is more important than ever to identify and utilize the most effective and defensible imaging methods available, while remaining cognizant of any cost concerns that clients may have.

Imaging Methods for Data Acquisition

Recent amendments to the Federal Rules of Civil Procedure (FRCP) have changed the guidelines for discovery—including ESI. These amendments can result in significant costs for parties in civil litigation. During discovery, ESI on desktop and laptop computers (“workstations”) is generally gathered in one of two ways: on-site imaging or remote live imaging. On-site imaging can be performed with the computer on or off but usually incurs hourly time and travel expenses for forensics technicians. By contrast, remote imaging is typically performed “live”—with a workstation turned on—and is typically charged at a flat rate per device.

Workstations typically contain a wealth of ESI. While servers (combined with the efficiency of the RAID technology typically used) quickly overwrite old data, workstations can in theory retain records of every file ever created (assuming the data has not been overwritten with new data). In a modern Microsoft Windows system, a workstation’s master file table (MFT) functions as its “index” to all of its files. When a user deletes a file, the MFT removes the pointer to that file, but until overwritten with new data, the source data is still present on the workstation. Through forensic imaging, all past and present files—including those deleted by the user—can be captured as long as the data has not been overwritten with new data. Forensic imaging also captures metadata (“data about the data”), which can be vitally important to an investigation.

For workstations, on-site acquisition of ESI is a standard process. A chain of custody form is completed for the equipment being imaged. The data custodian or technician shuts down the workstation before the technician removes the hard drive, creates a forensic image, validates the process and then reinstalls the hard drive into the computer. Finally, the technician turns on the workstation to verify it is in working order prior to leaving.

Live computer forensic imaging, which is performed while a desktop or laptop workstation is on, offers some important advantages over the more traditional static imaging, which is performed after a workstation is shut down. Live acquisition of electronically stored information (ESI), allows for the collection of the contents of random access memory (RAM); generally defeats hardware and software encryption; eliminates the need to shut down workstations and take them offline; and supports time and cost savings for investigators as well as end clients. Despite these advantages, questions have persisted around the validity of ESI collected through live acquisition. In this article, Ricoh Legal explores the validity of these questions and discusses potential advantages of live acquisitions.
With a remote imaging process (using Remlox™, for example), computer users—the data custodians—can facilitate the creation of their own forensic images. A tamper-resistant package is sent to the custodian, who then attaches an encrypted hard drive to the computer. The remote live imaging tool runs, with no input required on the part of the custodian. The tool creates a full and complete forensic image of the hard drive while the system is on. It also performs an electronic audit of the computer system—recording a range of information, such as the make, model and serial number of the system; the make, model and serial number of the hard drive; user details; domain details; number of drives connected and other pertinent information. After the custodian completes the provided chain-of-custody paperwork, he or she uses a pre-addressed package to return the encrypted hard drive to the forensic lab.

In this example, remote live imaging offers three important advantages compared to traditional on-site imaging:

• Captures ESI in an expeditious, convenient and cost-effective manner
• Enables imaging of random access memory (RAM)
• Can defeat or bypass most encryption

Speed, Convenience and Cost-Effectiveness
 Few would argue that a remote approach to live imaging is the clear winner when it comes to cost and time efficiency. Compared with deploying forensic experts to perform imaging on site, the remote process is fast, secure and convenient. Data custodians can facilitate the live imaging process at their convenience, such as after hours or while on the road. Further, when a forensic image needs to be created quickly, scheduling and deploying a technician simply may not be feasible at short notice. Since remote live imaging can be deployed and completed within 24 hours, it is the clear choice when time is of the essence.

Random Access Memory
By definition, the contents of RAM are dynamic and temporary. With live imaging, an image of RAM can be captured. With a static approach, this volatile data is lost when the system is shut down. Yet, the contents of RAM can be a rich source of potentially important ESI. Indeed, an article published by DFI News outlines nine of the most common artifacts that can be found in RAM:

• Past and current network connections—including the remote IP address and port number used in network connections
• A list of processes that were running at the time of RAM capture—information that can provide important insights about how the system was being used
• User names and passwords
• Loaded Dynamically Linked Libraries (DLL)
• Contents of an open window—including any keystrokes into Webmail, an e-mail client, values into a form field and an IM chat client and chat sessions (including participants)
• Open registry keys for a process, which can be crucial to identifying registry keys associated with a malicious process
• Open files for a process
• Unpacked/decrypted versions of a program
• Evidence of memory-resident malware—an increasingly prevalent type of malware that lives only in a system’s memory

Live imaging can seamlessly capture all of this ESI, providing a complete picture of how the system has been used. Static imaging could also capture the contents of RAM—as long as it is feasible to use compressed air to cryogenically freeze RAM chips before shutting down the system, removing RAM chips and then placing them into a specialized reader. While such an approach is technically possible, it probably is not desirable from a time or resource standpoint. Thus, although not every case will require the contents of RAM to be imaged, live imaging is the clear choice for those that do, or for those where the full scope of requirements may not yet be known.

Source: http://www.dfinews.com/article/memory-forensics-where-start?page=0,1
Defeating or Bypassing Hardware and Software Encryption

By definition, live imaging generally defeats encryption—an increasingly common practice due to security risks and regulatory requirements. Encrypted hard drives and encryption software are more affordable—and more in demand—than ever before. Organizations are using this technology to protect sensitive information, thereby addressing regulatory requirements and reducing the risk of costly and embarrassing security breaches.

What would be the point in creating a static image of a fully encrypted hard drive? After all, the image collected will be inaccessible to the forensic examiner. The examiner could try to persuade IT administrators to share their decryption codes, but it is highly unlikely that these confidential decryption keys would be shared. By contrast, live forensic imaging generally bypasses encrypted hard drives and encryption software simply because the user has already logged on and begun to use the workstation with pre-authorized credentials—placing the target ESI in an unencrypted state.

As noted in The Impact of Full Disk Encryption on Digital Forensics, “Encryption is one of the strongest protection measures against unauthorized access to data. The need for securing data on hard drives has led to an increase in the use of strong encryption. Until recently, forensic examiners could recover digital evidence from computers despite the use of encryption. However, the integration of encryption into operating systems, specifically full disk encryption (FDE), is making recovery of digital evidence more difficult. Today, a forensics examiner may encounter a full disk encryption interface prior to the machine booting, preventing access to any data unless the necessary credentials are supplied. If these credentials are not available, forensic examiners may have to acquire a forensic image of a live system while the contents are in an unencrypted state.”

FOUR TESTS PERFORMED

Vestige Ltd. chose two operating systems for the analysis: Microsoft Windows XP Service Pack 3 installed on a 40GB SATA drive hosted on a Sony Vaio PCV-R572G desktop and Microsoft Windows 7 Ultimate installed on a 160GB SATA drive and also hosted on a Sony Vaio PCV-R572G desktop. The lab conducted four tests:

TEST 1. The Microsoft Windows XP system was shut down with the command “shutdown -s -t 0”. The “-s” option directed the computer to shut down and not restart. The “-t 0” option directed the computer to shut down immediately. The command was executed on 9/1/2011 at 2:23:00 Eastern. Upon completion of the shutdown process, the hard drive was removed. The hard drive was then connected to a forensic analysis machine through a Tableau IDE/SATA bridge (model T35e) in order to write block the data. The hard drive was then analyzed using Encase v6.18 for evidence of changes to files or the Windows registry.

TEST 2. The Microsoft Windows XP computer was left running. A USB hard drive containing RemloX v3.1 was attached to the computer’s USB port. Process Monitor (Procmon) v2.96 was executed for the purpose of tracking actions performed by the computer. Procmon, a Microsoft application, is an advanced monitoring tool for Microsoft Windows that shows real-time file system, Registry and process/thread activity. The RemloX™ application was then executed. RemloX™ created a full and complete forensic image of the host hard drive at the physical level onto the connected USB drive. The Procmon logs were then analyzed for evidence of changes to files or the Windows registry.

TEST 3. The Microsoft Windows 7 system was shut down with the command “shutdown -s -t 0”. Again, the “-s” option directed the computer to shut down and not restart and the “-t 0” option directed the computer to shut down immediately. The command was executed on 9/2/2011 at 9:32:00 Eastern. Upon completion of the shutdown process, the hard drive was removed. The hard drive was then connected to a forensic analysis machine through a Tableau IDE/SATA bridge (model T35e) in order to write block the data. The hard drive was then analyzed using Encase v6.18 for evidence of changes to files or the Windows registry.

TEST 4. For the fourth test, The Microsoft Windows 7 system was left running. A USB hard drive containing RemloX™ v3.1 was attached to the computer’s USB port. Procmon was again executed for the purpose of tracking actions performed by the computer. The RemloX™ application was then executed. RemloX™ created a forensic image onto the connected USB drive. The Procmon logs were then analyzed for evidence of change to files or the Windows registry.

Concerns Surrounding Forensic Soundness
Traditional static imaging has been through extensive verification processes and has met certification requirements. Consequently, it is universally and scientifically accepted as an accurate and effective method to forensically acquire ESI. By contrast, questions have persisted about the forensic soundness of live imaging: “Purists argue that forensic acquisitions should not alter the original evidence source in any way. However, traditional forensic disciplines such as DNA analysis show that the measure of forensic soundness does not require the original to be left unaltered. When samples of biological material are collected, the process generally scrapes or smears the original evidence. Forensic analysis of the evidentiary sample alters the sample even more because DNA tests are destructive. Despite the changes that occur during preservation and processing, these methods are considered forensically sound and DNA evidence is regularly submitted as evidence.”

Ricoh Forensics commissioned a study by a third-party lab to compare changes made during the shutdown process to create a static acquisition and those made during a live acquisition. Specifically, the study was intended to identify and then compare changes made to files or the Microsoft Windows Registry between both a live acquisition and the more traditional method of static acquisition in which the computer must be shut down.

Key Findings
The third-party lab conducted a series of tests (see “Four Tests Performed”), which produced the following results:

<table>
<thead>
<tr>
<th>Operating system:</th>
<th>Static Imaging (changes recorded during computer shut down process)</th>
<th>Live Imaging Using Remlox™v3.1 (changes recorded while computers were running)*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft Windows XP Service Pack 3</strong>&lt;br&gt;<strong>Hardware:</strong> 40GB SATA drive hosted on a Sony Vaio PCV-RS72G desktop</td>
<td>Changes to files on the hard drive&lt;br&gt;30 files created or modified</td>
<td>Changes to Microsoft Windows Registry&lt;br&gt;23 registry keys modified&lt;br&gt;16 files created or modified&lt;br&gt;1 registry key modified</td>
</tr>
<tr>
<td><strong>Microsoft Windows 7 Ultimate</strong>&lt;br&gt;<strong>Hardware:</strong> 160GB SATA drive hosted on a Sony Vaio PCV-RS72G desktop</td>
<td>91 files created or modified&lt;br&gt;21 registry keys modified&lt;br&gt;46 files created or modified&lt;br&gt;No changes to registry keys</td>
<td></td>
</tr>
</tbody>
</table>

*Note: In both cases of live imaging, there may be an additional change to the computer from the insertion of the USB device on which the Remlox™ application resides. This change would depend on whether or not the computer being imaged had previously interfaced with that particular USB device. Any changes would be the typical changes made to the Microsoft Windows Registry for the insertion of a new USB device, as well as changes to the setupapi.log (or setupapi.dev.log) and any drivers that might need to be installed (rare in the case of USB devices).
Full details are available in Vestige Ltd’s report, Live Forensic Imaging, Using Remlox™. The study’s conclusion underscores the forensic soundness of live imaging:

“The evidence clearly demonstrates that running Remlox™ (a live forensic imaging application) at the physical level has minimal effect on file changes. Comparing the change in the data on a hard drive from the Remlox™ operation versus the change in the data on a hard drive when issuing the shutdown command, the results demonstrated that the shutdown command on a Microsoft Windows XP system or Microsoft Windows 7 system results in more changes to files and the Registry than utilizing the Remlox™ imaging process” (emphasis added).

Summary
Despite the beliefs and skepticism of the more “traditional” forensic examiners, the third-party lab tests deliver scientific proof that live imaging can be an effective way to gather ESI. In fact, these tests show that live imaging of workstations may be considered more forensically sound—making fewer changes to workstations than when the workstations are shut down prior to creating a static image.

When the forensic examiner is provided with a workstation that is already shut down and powered off, a static image would clearly remain the method of choice. However, in circumstances where a workstation is on and the user is logged on, a live image should be considered the most effective and least invasive method to be used. Further, it provides the RAM and encryption advantages described in this article.

ABOUT THE AUTHOR
David A. Greetham, CFE, is National Director of Forensics, Legal Enterprise Solutions for Ricoh Americas Corporation. He is retained by law firms and corporations as a consulting and testifying expert in the area of Computer Forensics. He has performed investigations and provided consulting services relative to electronic evidence in large scale litigations involving up to 12,000 custodians. He has overseen the litigation process through the entire data life span, from pre-litigation consulting, data collection, data culling, preparation of data for attorney review, to providing expert testimony. Additionally, David has been responsible for forensic examinations of computer systems and other electronic storage media involved in theft of trade secrets, Internet misuse, harassment, murder, kidnapping, fraud and alleged spoliation.

David has testified as a forensic expert on many occasions both nationally and internationally. He is a frequent speaker for Bar Associations continuing legal education (CLE) events, and industry associations. A Licensed Private Investigator with the States of Texas and Florida, David is also a member of the High Technology Crime Network (HTCN) and the Association of Certified Fraud Examiners (ACFE).