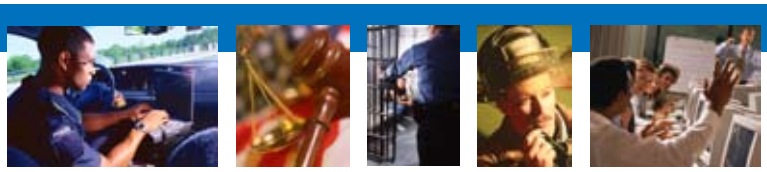

October 2007

Methods for Capturing Volatile Data

By Steven Bolt CISSP, A+, Network +
Computer Training Specialist
and
Earl Door EnCE, Network+
Computer Training Specialist

As crime scenes increasingly involve investigating home networks, it is becoming more and more necessary for law enforcement investigators to consider capturing the volatile data on a running computer when seizing it for forensic analysis.[1]

Computers require that a certain amount of computer memory called **random access memory** (RAM) be used by the operating system and its applications when the computer is in operation. The computer utilizes this RAM to write the current processes it is using as a form of a virtual clipboard. The information is there for immediate reference and use by the process. This type of data is called **volatile data** because it simply goes away and is irretrievable when the computer is off.[2]

The current trends in off-the-shelf computers include, at the very least, 512 megabytes (MB) of RAM with 1 gigabyte (GB) of RAM quickly becoming the new standard. Wikipedia defines RAM as:

> *"Random access memory (usually known by its acronym, RAM) is a type of data storage used in computers. It takes the form of integrated circuits that allow the stored data to be accessed in any order – that is, at random and without the physical movement of the storage medium or a physical reading head.* ***RAM is a volatile memory, as the information or instructions stored in it will be lost if the power is switched off****."*[3]

In order to document what applications were running on a computer, past practice in incident response involved viewing the monitor and recording the running applications viewable on the desktop. But this practice falls far short of documenting the running system. Noting what information displays on the screen or simply "pulling the plug" does not consider or document all the processes running on a system. In fact, pulling the plug on a running computer results in the loss of

---

[1] This guide provides step-by-step instructions for acquiring the RAM of a running system using three specific tools. This is a companion document to *Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community,* by Todd Shipley, CFE, CFCE, and Henry R. Reeve, Esq., published by SEARCH in 2006, which provides a high-level policy look at this topic. The 2006 primer is available for download at **http://www.search.org/files/pdf/CollectEvidenceRunComputer.pdf**.

[2] *Collecting Evidence from a Running Computer* at p. 5.

[3] Source: **http://en.wikipedia.org/wiki/RAM**.

this volatile data, which may contain valuable evidence. The running processes resident in RAM may include Trojan Horses, chat logs, alternate data streams and viruses, as well as network information, including attached storage devices. The existence of this volatile data strongly suggests that the past practice of pulling the plug needs to be reconsidered.

Investigators must consider the *least intrusive* methods in order to gather as much information about a running system as possible. This guide will shed some light on a few tools that can be used to assist the digital investigative community in its efforts to recognize the potential of volatile data and to safely capture it for further analysis.

Helix

Helix is a live CD that is a heavily modified version of Knoppix; both are bootable Linux distributions that reside solely on the CD. They are each fully functioning operating systems with all the bells and whistles that entails. Helix has been modified to meet the needs of the forensic examiner and field technician. It is comprised of two sides: A bootable side and a live Windows side. This guide addresses using the live Windows side to capture the RAM of a system being investigated.

The Helix CD is comprised of a multitude of tools, and the CD is available free of charge from e-fense™, Inc. at **http://www.e-fense.com/helix/index.php**. Drew Fahey, a Denver-based computer forensics and security specialist with e-fense, has pulled these tools together and placed them on the CD to assist investigators. Many of these tools assist in the automation of gathering information on a running system, and investigators should consider using them. **Note**: Using the Windows side of Helix *does* make changes to the targeted system. In light of evidence collection, investigators need to be aware of these changes, which include Dynamic Link Library (DLL) additions and registry entries.

Helix provides a system snapshot function that enables users to take an image of the running system and copy that information to removable media such as a USB hard drive or thumb drive. The system snapshot is located on the live side. Simply insert the CD and if the **autorun** feature is enabled, the following screen should appear (Figure 1).

Figure 1. Helix warning page

This first popup window warns that this tool is being used on a live system and will make changes to that system. The contact information for e-Fense.com is also listed. If the autorun feature is not enabled, navigate to the CD/DVD ROM drive and select the **helix.exe** file to run the application.

Select **Accept** and the application moves forward to the tools pages. The main tools page (Figure 2) provides several options for pulling information from a running system.

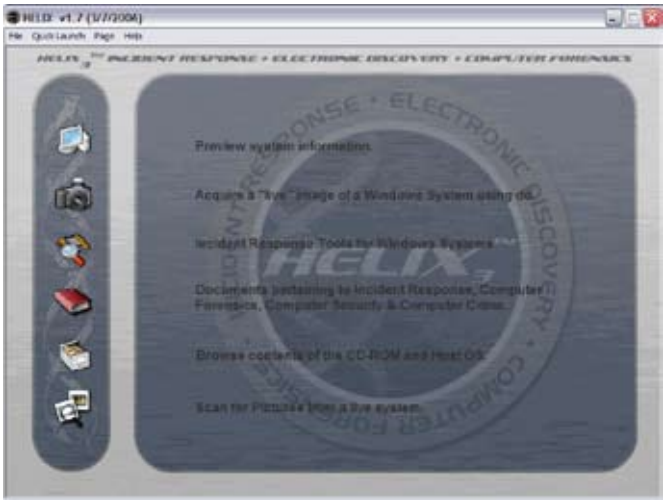

Figure 2. Main tools page

Each of the tools is located down the left-hand side of the window, and offers several options that can be explored. Included under the **documentation icon** is the complete manual for Helix, which provides detailed descriptions of each tool and the functionality of Helix. All digital investigators are encouraged to read, at the very least, the first 90 pages of the manual, which details the live side of the Helix tool.

For the retrieval of RAM, use the **camera icon**, which includes the tool that can provide a dd image of a running Windows system.

Figure 3: Live Acquisition page

The Live Acquisition page (Figure 3) provides several options for capturing a snapshot of the system, which can include the RAM. The **Source** drop-down menu provides the option to choose which information to capture. In this example, the system contains approximately 2 GB of system RAM. Click the arrow and all recognized attached physical and logical drives will display. In this case, the RAM, or physical memory has been selected.

Location options allow users to specify where they want the system snapshot, as well as the name of the image, to be sent or stored. The two selections are for an attached or shared drive, which would include USB attached storage or the NetCat option, which allows an on-scene investigator to push the system snapshot to a NetCat listener system. NetCat listener systems can be located at the investigator's office, or at a regional computer forensics lab. The system has to have a NetCat listener up and running, which is another tool located on the Helix CD (Figure 4). If NetCat is selected, the IP address of the listener system, as well as the port, must be specified by the on-scene investigator. Firewall and other security measures would have to be taken into consideration if NetCat were to be utilized.

Figure 4: NetCat

The **dd** options allow users to specify block size and offer the ability to split the image into multiple files to meet the capacity of the equipment they have brought to the scene. By default, the **conv:** window is set to **noerror**, which tells the dd image to continue to acquire and to not stop if there is an error in the image file.

Once all parameters have been selected and set, select **Acquire**. Two pop ups will provide user notices, one displaying the dd command and asking if it is OK to run, the other providing instructions on pasting the command in the command shell (Figures 5 and 6).

Figure 5: Warning notice

Figure 6: Notice regarding paste to clipboard

A forensic command shell will be launched that consists of trusted binaries (Figure 7). Trusted binaries are commands that are run from the CD and are shown as a command shell or command window. These commands are to ensure that the image being created has not been compromised by a root kit and that the commands being run are not, in fact, running commands behind the scene.

Once the command shell is launched, right-click and select **paste** to paste the commands into the command shell. Pressing the **Enter** button runs the command and sends the dd image to the specified storage location.

Figure 7: Command shell with trusted binaries from clipboard

Once the command runs and finishes, three files should be located in the specified location:

- The first is **filename.dd**; the file contains the image (and the filename is whatever name the user specified it to be).
- The second is a file called **filename.dd.md5**, which is a file that contains the MD5 checksum of the image file.
- Lastly, **audit.log** is a file that contains the command and the output of the program.

After the user is finished and if the user is ready to close the application, Helix will launch a popup window and ask if the user wants a .PDF log file. This log file shows all the tools the user ran while in the Windows system and the results of those tools.

RAMDump.bat

A customized batch file from GMG Systems is available that allows an incident responder to dump the RAM of a running system. Batch files are simply lines of code that are read by MS DOS and executed. In this case, the code tells the system to dump the contents of its RAM to the location from which the batch file was launched. This file is a customized version of the UNIX dd command; it has been customized to run on a Windows machine to extract the targeted physical memory.

This tool consists of several files that must be placed in folders and saved onto a portable drive. The user should place these files on a USB thumb or portable drive. Keep in mind that the portable drive will work faster than the thumb drive. It is recommended that users create a folder on their portable drive titled RAM Dump or some other easily recognized name. Then, transfer the necessary files to that folder location. Once the transfer of files is completed, the folder subdirectories should appear like the following images (Figures 8, 9 and 10):

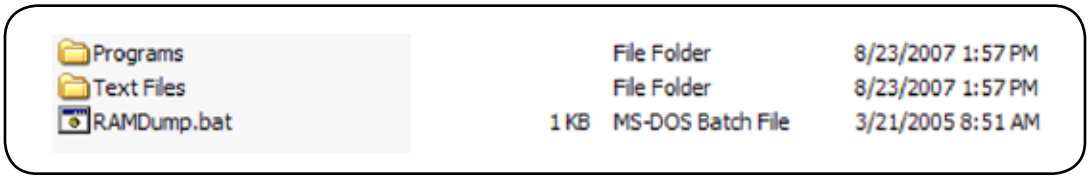

Figure 8: Files and folders for the RAMDump batch file

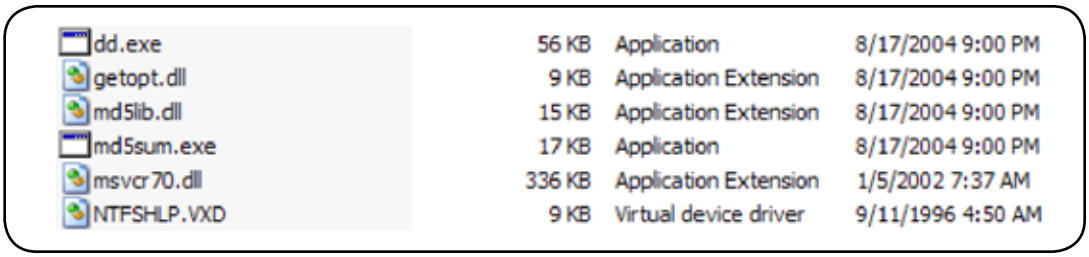

Figure 9: Files that should be under "Programs"

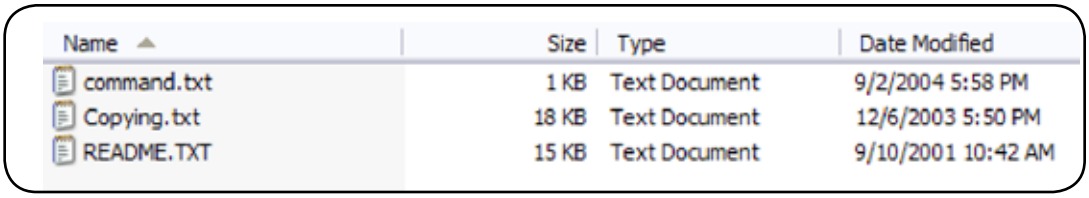

Figure 10: Text files under "Text Files"

Figure 8 shows the folders and the Batch file that comprise this tool. Figure 9, depicts what files should be located under "Programs." The user should ensure that the files are all present and that they have the appropriate extensions. And lastly, the user should read all the text files that are located in the **text** folder. All these files must be present in order for this tool to work properly.

Using the tool is quite simple. While on-scene, the user needs to plug in the portable drive containing this RAM Dump utility to the suspect's computer. This will make changes to the system, but remember the concern here is about the *least intrusive* methods to collect as much evidence as possible. Once the drive is attached and the system confirms the drive recognition, navigate to the RAM Dump folder. Finally, simply double-click on the **RAMDump.bat** file to launch the tool. The command shell that is launched notifies the user that the script will dump the RAM of the system (Figure 11). Keep in mind that depending upon the amount of RAM, this may take some time.

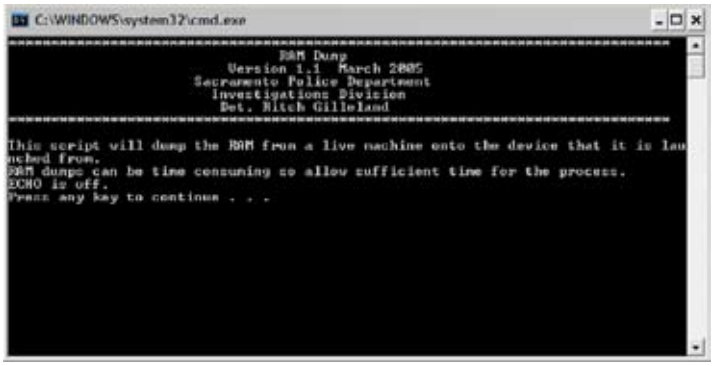

Figure 11: Notice from RAMDump script

The script runs and the user is notified of the progress (Figure 12). Once completed, there should be two more files located within the RAM Dump folder.

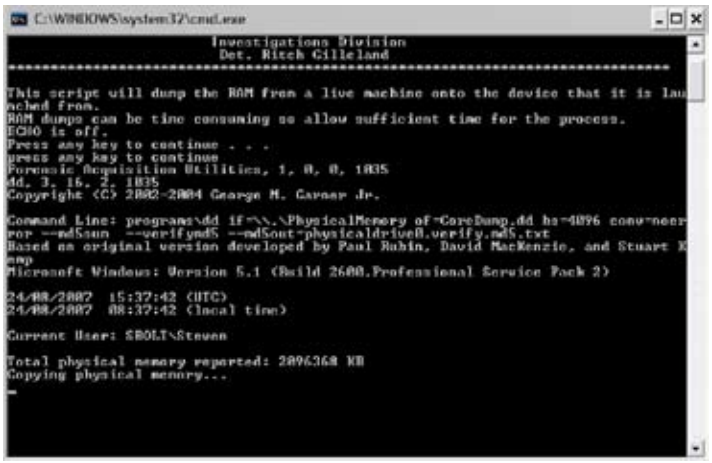

Figure 12: Running the script

These two new files (see Figure 13) are **CoreDump.dd**, which is the raw dd image of the RAM memory. The second file is **physicaldrive0.verify.md5.txt,** which is an MD5 hash of the acquired RAM memory. This particular file is taken after the RAM Dump is acquired for verification purposes.

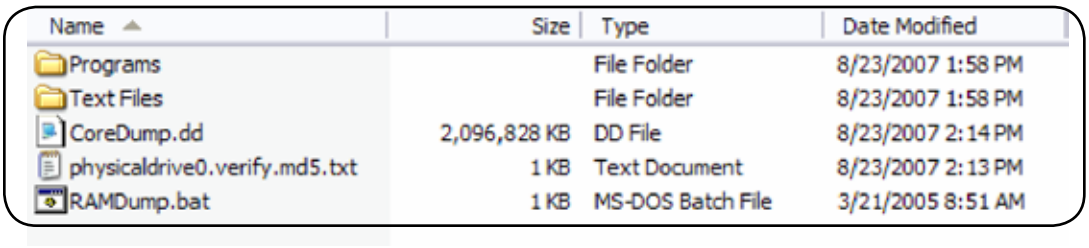

Figure 13: The two new files

The raw dd image can then be imported into a commercial forensic application such as EnCase from Guidance software, FTK from Access Data or some other such application. Once the dd image has been imported into an application, the parsing can begin, which may be used to complement the full forensic on the powered-down computer system.

Process Explorer from SysInternals

Thus far, two tools have been presented that show how a user may take a snapshot of the physical memory, or RAM, of a running system. These two methods extract a raw dd image that requires a secondary tool or application to read the information.

Process Explorer from Sysinternals, now a subsidiary of Microsoft, provides a method for digital investigators to capture the running processes of a live system. Be aware that this tool, as well as the other two mentioned earlier, makes changes to the live system. Care should be taken to weigh the potential value of these tools and the information gained against the potential legal challenges.

Process Explorer is one of many free tools that can be downloaded at **http://www.microsoft.com/technet/sysinternals/default.mspx**. There are many tools located on this site and users are further encouraged to research each for they all provide many useful functions.

From the Process Explorer Web site:

> *"Ever wondered which program has a particular file or directory open? Now you can find out. Process Explorer shows you information about which handles and DLLs processes have opened or loaded… The Process Explorer display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in: if it is in handle mode you'll see the handles that the process selected in the top window has opened; if Process Explorer is in DLL mode you'll see the DLLs and memory-mapped files that the process has loaded. Process Explorer also has a powerful search capability that will quickly show you which processes have particular handles opened or DLLs loaded."*

Investigators should have this tool in their tool box and perhaps already loaded onto their USB drives for on-scene seizure and investigation. To launch this utility, navigate to its location and double-click the .exe file. This launches the application and immediately begins to gather the information (Figure 14).

Figure 14: The two windows of Process Explorer

These windows show the processes that are running, the identified company name that has signed the application, as well as much more information. Process Explorer can be thought of as the Microsoft Task Manager on steroids. Process Explorer provides all the functionality of Task Manager, plus much more. For the purposes of this guide, the main function of interest is the ability to view the currently running processes, as well as the ability to save this information as a text file.

Conclusion

The amount of physical memory, or RAM, continues to increase in off-the-shelf computer systems. Manufacturers continue to meet the market demands as consumers continue to strive for more memory for their multimedia and multitasking needs. Digital investigators need to be aware that simply pulling the plug on a system loses RAM, which may contain evidence. Once the plug has been pulled, that data has been lost forever. Additional steps must been taken to secure the RAM memory and to preserve the evidence that may be contained therein.

Some of these collection steps and tools have been detailed within this guide, and it is meant as an introductory document only. Investigators are encouraged to research this topic more in order to become more proficient with these tools, as well as to be well informed in this matter so that they are able to articulate their actions in a legal setting.

Selected References

Brown, Christopher L.T., *Computer Evidence Collection & Preservation* (Hingham, MA: Charles River Media, 2006). Available at **http://www.delmarlearning.com/charlesriver/**.

Carrier, Brian, *File System Forensic Analysis* (Boston, MA: Addison-Wesley Professional, 2005). Available at **http://www.awprofessional.com/bookstore/product.asp?isbn=0321268172&rl=1**.

e-fense™, Inc., *Helix Live CD-ROM*. Available at **http://www.e-fense.com/helix/**.

Garner, George M. Jr., *Forensic Acquisition Utilities* (August 17, 2004). Available at **http://users.erols.com/gmgarner/forensics/**.

Mandia, Kevin, and Chris Prosise, *Incident Response: Investigating Computer Crime* (Berkeley, CA: Osborne/McGraw Hill, 2001). Available at **http://books.mcgraw-hill.com/getbook.php?isbn=0072194510&template=osborne**.

This report was prepared by the Training Services staff of SEARCH, The National Consortium for Justice Information and Statistics, under funding from the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.