EVIDENCE TECHNOLOGY MAGAZINE

The magazine dedicated exclusively to the technology of evidence collection, processing, and preservation
Volume 5, Number 1 • January-February 2007

Death Investigation

SOME OF THE TOPICS IN THIS ISSUE

- Suicide or homicide: Which is it?
- New decomposition research facilities
- How to avoid evidence cross-contamination
- Seven uses of open-source software for the lab

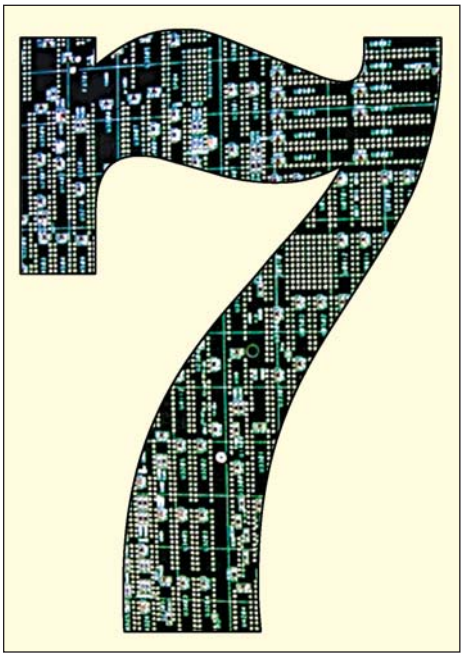
Seven uses of open-source software for the digital forensic lab

Written by Aaron Hughes

YOU WOULD PROBABLY be hard-pressed to find a department anywhere that would state that it has the benefit of full funding. In the law-enforcement community, as in the corporate world, funding for computer and digital-forensics support is often grossly lacking. The joke (and unfortunate reality) is that the coffee budgets are higher than the budgets for digital forensics and response.

Open-source software is often viewed as an opportunity to step outside budgetary constraints. This software is, basically, computer software that is made available at a low cost —or no cost at all—along with the software's source codes, so that users can examine, modify, or improve upon the way it works.

Unfortunately, many people tend to recognize only the financial benefits of open-source software, which is a shame. In addition to potential budget savings, law-enforcement personnel can take advantage of a number of other benefits that are available by using open-source software in the digital forensics lab. Here are just a few examples of those benefits:

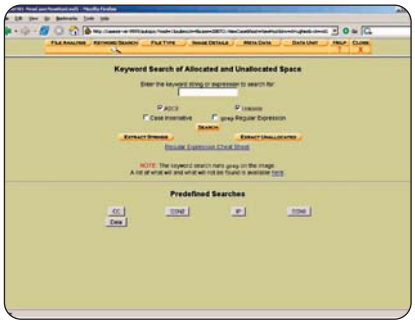


❏ You have the ability to crosscheck commercial software. When working in forensics, it is always of great value to be able to have access to multiple "views" and confirmations of results. Open-source software is a very economical way to view data in a different manner and to double check reported results. A lot of obfuscation software is written with the goal of fooling computer-forensics tools like Guidance Software's EnCase® and AccessData's Forensic Toolkit® (FTK™). The ability to crosscheck results with varying techniques and tools provides a layered view that can be instrumental in detecting obfuscation attempts, as well as in identifying data and patterns that may otherwise be missed.

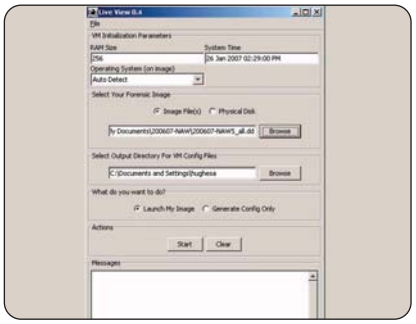
❏ Users can gain an increased understanding of underlying principles. Step away from the automated, opaque, and proprietary functions employed by commercial computer-forensics applications and you will gain a greater understanding of the underlying processes that closed applications are doing "behind the scenes." This will strengthen the abilities of the analyst to understand exactly where to find data that will explain or refute activity on a system or electronic device.

❏ Analysts obtain granular control and flexibility. It is not uncommon to have specific needs for reporting, displaying, or capturing of data that simply cannot be met by a closed tool. Open-source software gives the analyst very granular and modular control over what processing is done and in what manner the data is viewed. This control and flexibility results in an increased capability to convincingly explain or present evidence.

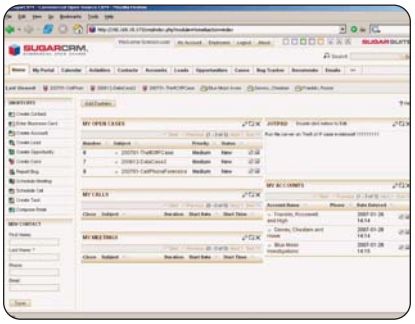
❏ Get the support of thousands of talented individuals who operate with a passion. The open-source forensics community is burgeoning with talented individuals and resources for addressing all kinds of needs in forensics and response. It is important to note that few of these individuals are paid to work



Autopsy, part of The Sleuth Kit, allows for both ascii and unicode searches through allocated and unallocated space. The address: ***http://www.sleuthkit.org****.*



Mounting an image in Live View is both simple and straightforward. The Internet website address for Live View is as follows: ***http://liveview.source.forge.net****.*



Benefit from case, contact, and activity management with SugarCRM: ***http://www.sugarcrm.com/crm/community/sugarcrm-community.html****.*

on the tools that they are presenting to the industry. Don't confuse the unpaid work, however, as the work of an amateur's tinkering; many of these individuals are recognized data-forensics professionals who present these tools and do this work because it is their passion.

- ❑ Lose the "black-box" atmosphere. Granted, there is always a balance between known and accepted closed-source tools and open-source tools. Bear in mind that certain open-source tools have become known and accepted by the industry; the software known as *dd*, for example, was included in testing by the United States Department of Justice's National Institute of Justice and tested out as an acceptable tool for acquisition. The second part of the balance referred to above is unique because with open source the analyst has the ability to "peek under the hood" of the software and understand exactly what the processes are that are being run and utilized—up to and including the very source code that makes the software operate. This can be a legal advantage in that the analyst has the opportunity to verify that the tool actually does exactly what the developers claim.

With a firmly established view of the benefits open source can bring to a data-forensics lab, the next question becomes one of capabilities. For every category of need for a data-forensics lab, there are strong offerings that provide a multitude of capabilities. Here are examples of seven ways that open-source software can be of value:

Open-source use #1: Case Management

One of the best applications for case management is an open-source tool that is used for customer-relations management (CRM). The tool is known as *SugarCRM*. The software comes in two different versions: one that is hosted by the SugarCRM servers and involves a per-month fee, and a second that is hosted on internal servers. The internally hosted option is recomended, since external exposure of lab work is not considered desirable.

SugarCRM allows an analyst to build case lists that can then be used to track specific users, documents, activities, and historical notes. The interface is easily configurable and has a high degree of customization. Best of all, the administrator can strictly control user access and viewing, as well as logging. With the open-source version, there is no per-user cost that you would typically incur with commercial applications.

In addition to these uses, SugarCRM can be utilized to send and receive case-related e-mails so that all communication is maintained in a single location. As mentioned above, one of the advantages to open source is the ability to "peek under the hood." With SugarCRM, the database structure is not proprietary—so it is possible to build a bridge application to tie in third-party applications.

Internet links to the open-source software mentioned in this article

NIJ testing of dd
http://www.ojp.usdoj.gov/nij/topics/ecrime/cftt.htm

SugarCRM
http://www.sugarcrm.com/crm/community/sugarcrm-community.html

dd
http://en.wikipedia.org/wiki/Dd_(Unix)

dd_rescue
http://freshmeat.net/projects/ddrescue/

The Sleuth Kit (TSK)
http://www.sleuthkit.org/

Foremost
http://foremost.sourceforge.net/

Stegdetect
http://freshmeat.net/projects/stegdetect/

Ophcrack
http://ophcrack.sourceforge.net/

John the Ripper
http://www.openwall.com/john/

OpenOffice
http://www.openoffice.org/

Vmware Player
http://www.vmware.com/products/player/

Live View
http://liveview.sourceforge.net/

Open-source use #2: Acquisition

The reigning champ of open-source acquisition is *dd*. This flexible UNIX-based program can be used for low-level copying as well as a variety of unique functions and conversion capabilities. Because dd is so ubiquitous, most commercial forensics applications (such as EnCase, Paraben®, and ProDiscover® Forensics) will directly mount and analyze a dd image.

In addition to dd, there is another program called *dd_rescue* that will not only make byte-for-byte images, but is useful in situations where a drive is damaged. Even when there are sector errors, dd_rescue will continue to try to pull data off of disks. In situations where the data cannot be read from a damaged sector, dd_rescue will log the sector and the problem to a log file and then continue to operate on the next sector.

Demonstrating through proper handling that evidence has not been altered in any way is a must. Two programs, *md5sum* and *sha1sum*, can hash individual files, entire disk images, and even entire directory structures.

Open-source use #3: Analysis

The Sleuth Kit (*TSK*) is a set of command-line tools that are related to *The Coroner's Toolkit* (*TCT*). There is a front-end graphical interface to the command-line tools, called *Autopsy*, that will greatly speed up your general analysis tasks and make image mounting and management a breeze. When simplicity is desired, the *TSK/Autopsy* combination provides a more generic case management than SugarCRM. The activity logs that are generated by this powerful combination are very detailed and useful, regardless of the management and reporting software used. In addition to generic mounting and management, The Sleuth Kit is very useful in recovering strings from unallocated and allocated space in both ASCII and Unicode. Viewing directory structures, deleted files, and timelines of activity is also easily done with The Sleuth Kit.

What if a disk has been formatted or the partition has been destroyed and recovery of files without benefit of partitions is required? There is a program called *Foremost* that was developed by the United States Air Force Office of Special Investigations and The Center for Information Systems Security Studies and Research. This powerful program can be used to carve data files directly from disk, dd image, SafeBack, EnCase, and other sources. The configuration and command-line operation is fairly simple and operation of the program is quick and efficient.

Open-source use #4: Miscellaneous tools of interest

The open-source forensics community has done great work on some specialty tools that can be particularly useful to law-enforcement agencies. Steganography is the technique of hiding one piece of information within another. For example, a document might be encrypted and interlaced within an image that remains perfectly viewable as an image. While still not common, steganography is increasing in usage, and analysts should have something in their toolkit to address this. *Stegdetect* is a tool that was developed to detect the use of steganography specifically within images. It can also be used in conjunction with *Stegbreak* in order to break specific encryption and steganographic methods.

Individuals in forensic laboratories might want to consider incorporating open-source software in their day-to-day working environment.

Along with the ability to detect and view steganography usage, analysts often find it useful to be able to crack system passwords. Two of the most useful applications approach the problem of password cracking from very different angles. *Ophcrack* is a password cracker that uses rainbow tables to crack passwords. Rainbow tables are essentially pre-calculated and generated password tables that present passwords in the most likely order that they will occur. This method can allow very fast recovery of Windows passwords and, in the case of the rainbow tables that come with Ophcrack, a 90% success rate. Ophcrack comes as a standalone program or as a bootable disk.

Another application called *John the Ripper* takes a slightly different approach to password cracking. In a situation where the rainbow tables are not successful, John will run dictionary and brute-force attacks against the password hashes on a system. The system does not need to be booted and running in order for this to occur.

Open-source use #5: Operating systems, support software

While there are some very impressive capabilities presented through the use of open-source software, this benefit extends to the operating system as well.

Bear in mind that we are referring specifically to building a data-forensics network, not migrating an entire department to Linux, which could lead to higher administrative costs despite the savings on licensing.

In the data-forensics lab, Linux can be used very effectively in place of Microsoft operating systems, saving hundreds or potentially thousands of dollars in licensing while at the same time providing an ideal platform for the needs of a data-forensics lab. A perfect example of support-software savings would be in switching the lab to using *OpenOffice* rather than Microsoft Office. All the compatibility with Microsoft Office exists with OpenOffice without the high license fees—and you also get a PDF distiller.

Open-source use #6: Virtual platforms

Although it is not exactly open source, it is worthy to note that VMware has released their free *VMware Player* that can be used to run pre-made virtual systems. Many of these virtual-build systems are free or very low cost and can allow a user to run a virtual Linux or BSD environment on a Windows platform—giving the user access to both worlds.

There is also work being done on a Java-based platform that will take an image created by dd and run it in a VMware virtualized environment in a forensically sound manner. *Live View* is an invaluable tool that allows the analyst to perform non-destructive analysis and is developed by Carnegie Mellon's CERT®. Live View was designed to run the image in a forensically sound manner, while allowing the analyst to interact with the environment. With such a tool, obviously, care should be taken with regards to potentially infected systems.

Open-source use #7: Mobile acquisition and analysis

Most modern laptops come with some licensed version of Windows and a decently sized hard drive. With modern distributions of Linux, resizing a laptop's partitions is fairly easy and painless—and by doing this, you can dual boot a laptop between an already licensed version of Windows and a distribution of Linux—again affording access to both worlds. All of the software named above will run just fine on a laptop as well as a full desk system.

It is clear that there are significant budgetary benefits that come with using open-source software into a data forensics lab. When coupled with the other intangible benefits and then added to the significant capability that open-source offerings bring, it is clear that the individuals on the staff of any organization would do themselves a favor by taking some time to decide *when*—not *if*—to incorporate open source in their environment.

About the Author:
Aaron Hughes is a certified information systems security professional (CISSP) with IAC SecureTech in Houston, Texas. He can be reached by e-mail at:
hughesa@iacsecuretech.com