

White Paper

Automated Digital Evidence Collection and Publishing: Reduce Investigation Time and Costs

May 2011

Automated Digital Evidence Collection and Publishing

I. Digital evidence is a rapidly growing challenge

The world of digital evidence analysis is in the midst of dramatic changes. In the last decade, it has become much easier to create, access, view and share digital information over the Internet. The cost of storing a gigabyte of data has decreased over 2.7 million times in the past 30 years and will continue to fall. Experts predict that the cost per GB will be less than \$0.01 in 2020¹. This means it is becoming even easier for criminals to access, store and distribute illegal content at a low cost and with a ready-made, web-based distribution channel.

The amount of digital data that floods forensic workflows places a great deal of pressure on time and resources. There is a gap between the volume of seized evidence and the capabilities to manually process it, and one case can bog down an entire forensic lab. Law enforcement agencies must improve current processes and obtain new solutions to not only meet these current challenges, but to accommodate future data growth.

II. Digital evidence processing: How one case can bog down the whole lab

FBI 2009 Report:

- 1,756 terabytes of data processed
- 58,609 pieces of digital media
- 21,810 CDs and DVDs

Digital forensic officers encounter cases that involve illegal content downloaded and stored from the internet, such as pornographic crimes. Much of the evidence seized in these cases enters forensic labs in the form of optical media: CDs, DVDs and Blu-ray Discs™ (BD). After a warrant has been issued, investigators may enter a suspect's home to collect every optical disc that has been created, bought or stored. Whether it resembles music, a movie or obviously contains illegal content, every disc is confiscated and brought back to the lab for analysis—a typical case brings in around 50 or more discs. The frequency of these crimes plus the sheer volume of discs creates a large and unmanageable seized evidence backlog. One digital lab may have 8-9 months' worth of discs sitting on the shelves, waiting to be processed and analyzed.

Time and resource costs

Two main issues arise during digital evidence analysis. First, the amount of time it takes to process the evidentiary discs is overwhelming. Because the majority of these tasks are completed manually, it takes an examiner at least 30 minutes to process a single disc. In a typical 50-disc case, it could take an examiner over 25 hours to process all seized digital media. Second, there is often a lack of adequate personnel and resources to complete comprehensive evidence processing in a timely manner. Analysis tasks may overflow to multiple departments, and manual evidence processing takes officers away from their vital duties. As a result, disc evidence backlogs continue to grow while cases go unsolved.

¹ Carlson, B. (2010). "Speeding the Digital Forensics Process". Retrieved from <http://www.forensicmag.com>

Automated Digital Evidence Collection and Publishing

Temporary fixes

In order to deal with time and resource challenges, many forensic labs incorporate temporary fixes. For instance, a large quantity of evidentiary discs obtained in a case may be split between several examiners. Or, instead of processing all discs involved in a case, officers will stop the examination once they have captured enough evidence to prove the suspect guilty. If there are damaged or hard to read discs— a frequent occurrence in computer crimes—officers will avoid manually investigating these discs in order to save time.

While these temporary fixes may reduce the time and resources required for digital evidence examination, they further compound the problem. Once discs are split between separate examiners, irregularities inevitably arise in how the discs are processed and how reports are created. And when examinations stop because enough discs have been processed to prosecute criminals, or the media is too damaged, the potential of finding illegal content or identifying victims linked to a suspect is significantly reduced. Cases can be compromised.

Digital data continues to grow

Considering that the total storage capacity for all digital storage devices shipped into the home could reach 650 exabytes annually by 2013², the issues surrounding digital evidence seizure and backlog are not going away; more digital data stored in tighter, smaller spaces will inevitably call for more digital evidence analysis processing. Digital data growth issues concern examiners, investigators and prosecutors alike. How will agencies continue to meet the resulting evidence management challenges?

Exabyte:

A unit of information or computer storage equal to 10^{18} bytes.

III. The solution: Automated Digital Evidence Processing and Distribution

In recent years, digital evidence software has gotten smarter. Leading software tools have incorporated advanced techniques that automate the arduous tasks associated with reviewing and analyzing criminal digital data. Digital evidence workflows are increasingly being established around these software tools. Expending time and money on new systems and adapting workflows that veer away from these tools is not an optimal solution. A smart technology model that plugs directly into existing workflows, such as Automated Digital Evidence Collection and Publishing, is a more effective long-term solution.

² Carlson, B. (2010). "Speeding the Digital Forensics Process". Retrieved from <http://www.forensicmag.com>

Automated Digital Evidence Collection and Publishing

An Automated Digital Evidence Processing and Distribution solution is a optical disc-centric system that:

- Streamlines digital evidence workflow and automates the evidence ingestion process
- Closes the gap between the time required to process digital evidence discs and the limited number of available personnel and resources
- Significantly decreases lab/investigation time and resource costs
- Provides a secure, standardized, disc-centric evidence archive and distribution asset that is prepared for digital data growth

Typical digital evidence workflow:

- 1) Create an authentic mirror image or 'forensic backup' of the data
- 2) Preview data and scan discs to capture all evidence
- 3) Export digital data for distribution and potential use in litigation
- 4) Create a content report detailing found evidence
- 5) Create an archive of the data that complies with requirements

Task automation reduces costs

When Automated Digital Evidence Processing and Distribution plugs into an existing lab workflow, the five essential tasks of evidence processing—usually performed manually by personnel—are now fully automated.

After ingesting the discs, the system works with software tools to create an image of the discs' contents, and then scans the data to capture evidence. After the data has been catalogued, a report is automatically created that details all found evidence, including file and whole disc hash values. Examiners can review data and intervene when necessary by taking further action on suspect discs, and captured evidence can be automatically exported to optical media for secure distribution and long-term archiving.

Because the solution is automatic and disc-centric, it speeds up ingestion time, allowing all discs in a case (CDs, DVDs and BDs) to be examined and reducing overwhelming backlogs of seized evidence. Officers no longer have to stop processing discs after a certain amount of evidence has been obtained—a major temporary fix employed by many agencies. With Automated Digital Evidence Processing and Distribution, more evidence is processed in less time without acquiring additional resources, and personnel can focus on more crucial tasks.

Evidence distribution asset preserves the chain of custody

After disc evidence has been processed, an Automated Digital Evidence Processing and Distribution system provides a secure, efficient and disc-centric distribution asset—an advantage that is missing in many digital evidence workflows. Optical discs are highly compatible; everybody in the chain of command from officers to legal counsel has technology to read CDs and DVDs.

Optical media is also a highly secure, court-approved form of evidential storage. Password protection and encryption can be enabled to ensure that only authorized parties are able to read the contents of the disc. Plus, optical media is the only form of digital data storage that has enough space on its surface for labeling, clearly identifying the contents within and eliminating the need to scan hard disk systems for data. With

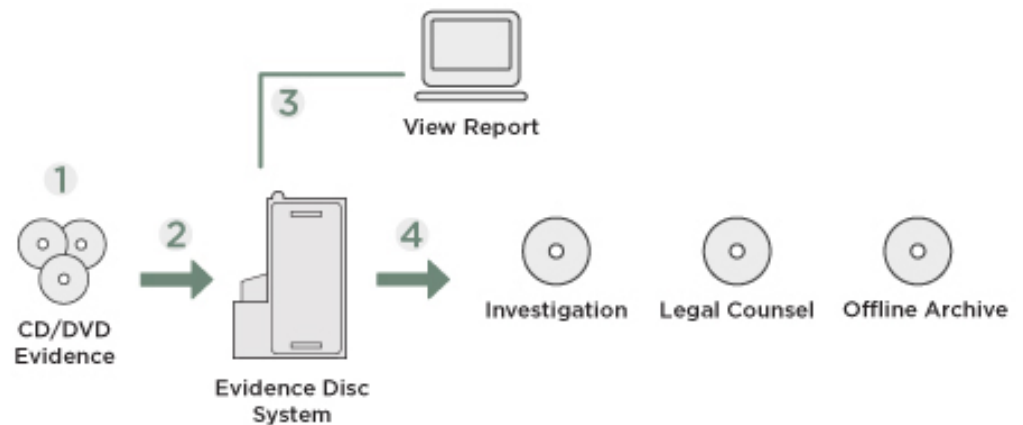
Automated Digital Evidence Collection and Publishing

an automated, disc-centric solution, agencies have a smart method of storing and distributing highly sensitive digital evidence while preserving the chain of custody.

IV. EDS – A successful model for Automated Digital Evidence Processing and Distribution

Rimage's Evidence Disc System (EDS) is an illustrative model of an Automated Digital Evidence Processing and Distribution solution, enabling agencies to perform more effective evidence processing in less time.

For example, with manual methods, an agency that has 5 cases per month with 50 discs per case could have 125 hours of examination time on their hands (30 minutes per disc). By automating examination tasks with the EDS solution, that agency can reduce their examination time by 100 hours. Personnel have a simple learning curve because the system plugs directly into their existing workflow. Here's how it works:



1. Investigators collect CDs, DVDs and BDs from a crime scene.
2. EDS solution ingests all discs and creates a content report, including hash values (can be done overnight).
3. Investigators review the report and take further action on suspect discs.
4. Evidence can be exported to process the case and support prosecution in court.

Automated Digital Evidence Collection and Publishing

Benefits of the EDS solution: Efficient evidence archiving

Optical discs and hard drives are the most realistic options for exporting and storing digital evidence, but the use of hard drives brings up a few issues. First, there is the chain of custody. Strict policies have to be in place to limit access to forensic images stored on drives and ensure that images from separate cases do not commingle. Second, the maintenance of hard disk space can be costly, prompting agencies to limit the amount of evidence that they analyze and store.

Because the EDS solution automatically exports digital data to optical discs that are inherently ready for secure offline archive, officers no longer have to determine which evidence they should and should not export. All found evidence can be cleanly stored and organized on the discs, and the disc surface can be clearly labeled to enable quick and easy accessibility plus enhanced traceability.



The need to spend additional costs on upgrading existing or acquiring new hard disk space is eliminated; one dual-layer DVD can house up to 8.5 GB data, and one dual-layer BD contains up to 50 GB of storage space. And optical disc's secure nature allows intuitive access rules to be enabled, even as discs change hands throughout the chain of custody.

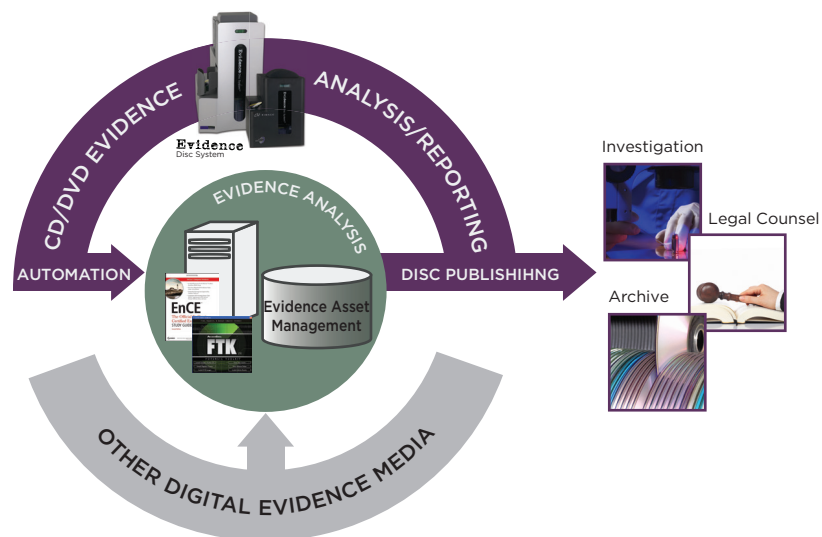
Increased analysis accuracy

The EDS solution includes advanced technology to process and gather content from hard-to-read or damaged discs, drastically decreasing the amount of time required to process imperfect discs and increasing analysis accuracy, without additional time and costs. Every disc in a case can be processed and catalogued, including hash values, and officers can review all evidence regardless of bad disc sectors. The ability to process more data means that the evidence against a suspect grows, and adding more data to the central database strengthens future cases against repeat offenders.

Automated Digital Evidence Collection and Publishing

Solution for multiple evidence targets

Beyond ingesting digital evidence stored on CD/DVD/BD, an automated EDS solution has the ability to export and standardize data captured on disparate evidence targets, such as smart phones, tablets and portable hard drives. If a case brings in one or ten different seized digital devices, labs can export data from each device to an affordable, portable and secure form of optical media for evidence distribution and archive.



V. Conclusion: Evolve with digital data

Agencies have been challenged by the rapid growth of digital media. Traditional digital evidence analysis methods struggle to keep pace with current changes. As illicit data continues to be easily stored in formats like smart phones and tablets, and as hard drive storage capacities become even larger, forensic officers will encounter greater amounts of digital evidence in each computer crime case.

As these technological advancements continue, forensic labs need to innovate by adopting digital-focused knowledge and procedures to manage the growing flood of data without spending excessive time and money. Incorporating an Automated Digital Evidence Processing and Distribution system into an existing digital evidence workflow is a smart and efficient method for handling current case loads and backlogs as well as preparing for future advancements. A solution like the EDS system enables agencies to evolve with digital evidence while saving time and money.

White Paper

Automated Digital Evidence Collection and Publishing: Reduce Investigation Time and Costs

May 2011

©2011 Rimage Corporation. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Rimage is a registered trademark of the Rimage Corporation. All other brand or product names are trademarks of their respective owners and are used without intention of infringement.