CHAPTER 11

Looking Ahead: Challenges and Concerns

Information in This Chapter:

- Standards and Controls
- Cloud Forensics
- Solid State Drives
- Speed of Change

INTRODUCTION

Digital forensics is still in its infancy. It is very much a work in progress given its relatively short existence as well as the rapid rate of technological change. This work in progress status is likely to carry on for quite some time. This situation results in many challenges and controversies that the legal and forensic communities must wrestle with. The challenges are many. One such challenge is wrestling with emerging and potentially "game changing" technology. Another is reaching a consensus with the forensic science community at large, particularly when it comes to established best practices.

Digital forensics is causing a massive collision if you will, between two seemingly unyielding forces: the legal system and forensic communities that operate at a relatively slow and deliberate pace versus the blinding speed of technology. Neither is built for speed. There are good reasons for that. The stakes are far too high to admit forensic evidence that hasn't been proven reliable. This proven reliability takes time and can't be achieved over night.

Two technologies, cloud computing and solid state hard drives, present "game changing" challenges. As it stands, digital evidence in either of these environments could very well be unrecoverable for either technical or legal reasons (or both). These technologies are in use today and represent a problem to which there is no easy answer. How all of these challenges will be met has yet to be seen.

The Basics of Digital Forensics. DOI: 10.1016/B978-1-59749-661-2.00011-5

STANDARDS AND CONTROLS

Standards and controls are a fundamental part of scientific analysis, including forensic science. A **standard** is "a prepared sample that has known properties that is used as a control during forensic analyses" (Barbara, 2007).

A **control** is defined as "a test performed in parallel with experimental samples that is designed to demonstrate that a procedure is working correctly and the results are valid" (Barbara, 2007). In essence, a control is simply a sample that provides a known result.

That may hold true for serology, chemistry, toxicology, and the like, but its relevance to digital forensics is a matter of dispute. More traditional forensic scientists are taking the stance that standards and controls are essential for all forensic disciplines, including digital and multimedia forensics. One of the major digital forensic bodies, the Scientific Working Group on Digital Evidence (SWGDE), is taking the exact opposite position. The controversy began with an article on Forensicmag.com in 2007 by John Barbara. In the article, Barbara raised the issue of standards and controls in digital forensics. He is a Crime Laboratory Analyst Supervisor with the Florida Department of Law Enforcement (FDLE). He is also an ASCLD/LAB inspector and has been since 1993. In the article he laid out his case citing the mandatory use of standards and controls in every other forensic discipline. He argued that the use of standards and controls is necessary to prove that the tests were performed in a scientific manner and that quality assurance measures were followed.

In the end, closely following these established scientific practices ensures that any results gained are accurate, reliable, and repeatable. He further argued that without the use of standards and controls, it would be "extremely difficult or impossible to scientifically assess the validity of the results obtained from the analysis of the physical evidence" (Barbara, 2007). Finally, he raised the admissibility standards required by the *Daubert* case.

In *Daubert*, the court said that when considering the admissibility of any scientific evidence, the focus should be on the principles and methodology and not on the conclusions that they generate.

The Scientific Working Group on Digital Evidence (SWGDE) doesn't agree. Their position is that standards are being used in digital forensics, but controls are "not applicable in the computer forensics sub-discipline" (Scientific Working Group on Digital Evidence, 2008).

SWGDE's position centers on false positives. They say that false positives do not exist in computer forensics. Tools and processes may miss evidence, but they will never find evidence that doesn't exist. The main objective of any digital forensic examination, says SWGDE, is to find data relating to criminal activity that already exists. Therefore, there is no real value to the analysis or the results.

They conclude by saying that "validation, data integrity (through hashing), and performance verification" are a more appropriate solution than the traditional

use of standards and controls (Scientific Working Group on Digital Evidence, 2008).

SWGDE agrees, saying "New technology, typically proprietary in nature, emerges daily. As these new technologies emerge, new solutions and techniques are needed to understand and examine evidence. Comprehensive understanding and validated techniques need to move swiftly from the research community to the examiner community" (Scientific Working Group on Digital Evidence, 2008).

CLOUD FORENSICS (FINDING/IDENTIFYING POTENTIAL EVIDENCE STORED IN THE CLOUD)

Cloud computing is a hot topic in information technology. The many benefits it brings are undeniable and not lost on organizations across the globe. As such, it's being widely adopted. The cloud, however, is a double-edged sword, and a sharp one at that. With its many benefits come major challenges from both forensic and legal perspectives.

What Is Cloud Computing?

There are many definitions of **cloud computing** from which to choose. TechTarget describes cloud computing as "a general term for anything that involves delivering hosted services over the Internet" (TechTarget, 2007). These hosted services generally fall into a few different categories including:

- Infrastructure as a Service (IaaS).
- Software as a Service (SaaS).
- Platform as a Service (Paas).

The term "cloud computing" is derived from the "cloud" symbol that is normally used in network diagrams to represent the Internet.

The National Institute of Standards and Technology (NIST) provides a more complex definition. They define the cloud this way: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011).

Not all clouds are the same. There are **private clouds** and public clouds. **Public clouds** sell services on the open market. Technology behemoths such as Microsoft (Azure), Amazon (Amazon Web Services), Rackspace, and Google are just some of the major players in the cloud market. These **Cloud Service Providers,** or **CSPs,** can have data centers scattered around the world.

The cloud model relies heavily on virtualization and redundancy. TechTarget defines virtualization this way: "**Virtualization** is the creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device or network resources" (TechTarget, 2000).

ADDITIONAL RESOURCES

Public Clouds

To get a closer look at how public cloud services are sold and managed, visit some of these providers.

http://www.microsoft.com/en-us/cloud/default.aspx?fbid=XBzeu9E4wgy
http://aws.amazon.com/
http://www.rackspace.com/cloud/

The Benefits of the Cloud

Recognizing the many benefits of the cloud, companies and other organizations are flocking there in droves. They are seeking both the convenience and cost savings this computing model offers. The ability to essentially "dial-up" computing resources as needed is hard not to like. With the cloud, an organization's infrastructure can expand and contract as needed. From a cost perspective, this approach can save a significant amount of money. Companies can save on much of the initial investment for network hardware and software.

Having the data or services replicated in more than one data center provides redundancy. The redundant nature of the cloud ensures that the user's files and/or applications are safe and available whenever they need them. Should one center or its connectivity go down, the second should be able to respond.

Cloud Forensics and Legal Concerns

The cloud may be a dream come true for those in business and information technology, but it represents a nightmare for those who deal with digital evidence. The primary challenges are twofold, one technical and the other legal. Technically, the cloud is without question not a forensically friendly environment, especially when compared to the relatively cozy confines of magnetic drives. Pulling deleted data from traditional drives has long been a staple of digital forensics. The cloud will likely be putting that to an end. Deleted files on a magnetic drive remain on the disk until they are overwritten. In the cloud, when a file is deleted the mapping is removed immediately, usually within a matter of seconds. This means that there is no remote access to the deleted data. As is the case with magnetic drives, that space is now available and will likely be overwritten in the cloud (Ruan, Carthy, Kechadi, & Crosbie, 2011).

There is an alarming lack of established forensic tools and procedures for acquiring and analyzing digital evidence in the cloud. Current tools and methodologies are largely ineffective in this environment. Much more research needs to be done.

ALERT!

Cloud Persistence—Dropbox

As many challenges as cloud functionality presents, in certain instances it can work in our favor. For example, Dropbox saves all deleted files (by default) for thirty days.

Dropbox's "Pack-Rat" service can keep data indefinitely (with the Pack-Rat add on). Granted, you will need a subpoena or search warrant to get to it, but the fact that it could be available is nice to know (Dropbox, 2011).

Legally, dealing with multiple jurisdictions can significantly frustrate efforts to get to the relevant data in the first place. As we've seen, CSPs can have their data centers located almost anywhere in the world. Legal requirements and procedures can vary, and vary considerably from country to country, and from jurisdiction to jurisdiction. This problem compounds exponentially if the data have crossed international boundaries.

Regulation could assist in mitigating this issue. It could help by mandating that CSPs operate in such a way that facilitates the preservation and recovery of potentially relevant data. Service Level Agreements, or SLAs, can also make a difference. An SLA is a written agreement between a customer and a provider. The SLA spells out in great detail what support and services the customer will get from the provider. As part of that agreement, the customer can require certain assurances regarding information security and how digital evidence will be preserved and collected should that ever become necessary. From a customer's perspective, this is an important detail that shouldn't be overlooked. This is particularly true in organizations where litigation is likely. Having this arrangement in place can be very beneficial to the forensic examiner, especially as opposed to starting from scratch with no protocols, procedures, or relationships in place.

SOLID STATE DRIVES (SSD)

Magnetic drives have been a mainstay in personal computers for years. Forensically, they afford examiners the ability to recover significant amounts of user-deleted data. Those days, it appears, may very well be coming to an end. These traditional magnetic drives are being replaced more and more. Welcome to the era of solid state hard drives (SSD).

How Solid State Drives Store Data

Traditional magnetic drives have multiple moving parts including the platters and the actuator arm (that moves the read/write head). As the name implies, solid state drives do not. SSDs are somewhat similar to RAM and USB thumb drives, storing data in tiny transistors. Unlike RAM, SSDs are nonvolatile and can store data even without power. In order to keep the charge over long periods of time, without power, SSD transistors employ an additional gate (called a floating gate), which is used to contain the charge (Bell & Boddington, 2010).

If you recall from Chapter 2, magnetic drives break the storage space up into smaller units. These units include sectors, clusters, and tracks. SSDs also separate the storage space into smaller units. The base units are called blocks and are normally 512 KB in size. Blocks are then subdivided into even smaller units called pages. Each page is typically 4 KB in size.

Wear is a concern with SSDs. Each block can only withstand a certain number of writes. Some estimates put that number somewhere between one thousand and ten thousand times. Given this limitation, you would want the drive to avoid writing to the same block over and over. Writing to the same space repeatedly will cause it to wear out faster than others. Manufacturers solved the issue by instituting a **wear leveling** process performed by the SSD.

MORE ADVANCED

File Translation Layer

On a solid state drive, the computer thinks the data are stored in one location, while in reality they are physically located in another. An SSD drive uses a File Translation Layer to ensure that the computer isn't writing to the same block over and over. If the SSD detects this is occurring, it will "translate" the new writes to a less used location (Bell & Boddington, 2010).

Magnetic drives have the ability to instantly overwrite data to any sector that's labeled as unallocated. SSDs do not. Each transistor must be "reset" (erased) before it can be reused. This reset process slows down the drive. To speed things up, SSD manufacturers have configured the drive's controller to automatically reset unused portions of the drive. This process is known as **Garbage Collection.**

The Problem: Taking out the Trash

Solid state drives have a mind of their own. Many drives initiate the Garbage Collection routine completely on their own, without any prompting by the computer at all.

This is both problematic and troubling from the perspective of the forensic analyst. First, verifying the integrity of the evidence becomes extremely difficult and jeopardizes its admissibility in court. Second, there is the automated destruction of potentially relevant data on the drive. If the Garbage Collection routine is run during or after its acquisition, validation becomes exponentially more difficult because the hash values won't match.

Today, we routinely use cryptographic hashing algorithms, such as MD5 or SHA1, to take the "digital finger print" or "digital DNA" of a hard drive. We can then retake the "fingerprint" of our clone at any time and compare it with the "fingerprint" of the original. They should match exactly, verifying the integrity of the evidence (Bell & Boddington, 2010).

SPEED OF CHANGE

You may have noticed that the speed of technological change is a recurring theme throughout this book. Its impact is truly significant and felt across both the digital forensics and legal communities. It also impacts the organizations that rely on the results such as law enforcement and private companies. Take case backlogs, for example. In most if not all laboratories there is a significant backlog of cases including those involving digital evidence. Change contributes to this backlog by slowing down the examination process. Take an updated application such as a chat client. There can be major differences in where and how the software stores the artifacts examiners need to locate and analyze. Artifacts that may have been written to the registry in a previous version are now held exclusively in RAM and disappear when the machine is powered down.

Examiners presented with this situation will have to attempt to find a proven solution from others in the digital forensics community. Failing that, the examiner may have to conduct the research on their own and validate the results. This takes time. Message boards (such as the one for HTCIA members) and e-mail lists are worth their weight in gold in these circumstances. They provide a ready channel for communication and problem solving.

ADDITIONAL RESOURCES

Twitter

Twitter can be a great resource for digital forensic professionals. It can alert you to new techniques, research articles, court decisions, news, and more. There are many individuals and companies that share a great deal of news and information pertaining directly to digital forensics. Today we are bombarded with information, some good and some bad. Following well known, established entities on Twitter can help reduce the "noise" and help keep you current. This is one tool that can help you deal with the speed of change. These are just a sampling of the people and companies worth following.

Digital Forensics

Vendors/Organizations	Individuals
@AccessDataGroup	@robtlee
@EnCase	@jtrajewski
@sansforensics	@girlunallocated
@DFMag	@keydet89
@HTCIA	@codeslack
@MFITraining	@4n6woman
@cellebrite USA	@AppleExaminer
@syngress	@chadtilbury
	@hal_pomeranz
	@4cast
	@CyberCrime101

(*Continued*)

(*Continued*)

Electronic Discovery

Vendors/Organizations	Individuals
@DiscoverTERIS	@sharonnelsonesq
@EDDUpdate	@RalphLosey
@e_discoverynews@KrollOntrack	@EUdiscovery@InfoGovernance
@Clearwell	@ComplexD
@PosseList	

SUMMARY

Digital forensics faces many tests on the road ahead. The blinding speed of technology, new game-changing technologies such as cloud computing and solid state hard drives, and disagreements with established forensic disciplines, just to name a few. The constant, relenting pace of technology hits the DF community hard as it fights to keep pace. The speed of change affects the legal system as well. The system itself is not "built for speed" in general and certainly not for the speed of technology. The end result is that in certain situations, previously tried-and-tested tools and protocols will be ineffective. The research, development, and testing needed to solve the problem takes time.

Delivering services over the Web, cloud computing's bread and butter, represents a major shift away from the computing model that the world has grown accustomed to. Remote applications, hardware, platforms, and infrastructure have a great many benefits; reduced costs and elasticity are just two. Behind the scenes, the cloud relies heavily on virtualization and redundancy. The massive data centers used to deliver public cloud services are likely to be widely dispersed, residing in multiple states or even different countries. Meeting the legal requirements to gain access to this data can take an astronomical amount of time. It's entirely possible that by the time the legal burden is met, the evidence in question may no longer exist.

Solid state hard drives are another game-changing technology that must be addressed. These devices may serve the same function as our familiar magnetic drives, but they certainly don't act like them. The storage method they use, tiny charged transistors, must be "reset" before being written to. This process slows down the drive, impacting performance. To mitigate the slowdown, drive makers have built in a process known as Garbage Collection. This process begins this reset process in only minutes. This procedure destroys data on the drive in such a way that current tools and techniques cannot recover it.

Digital evidence and its associated forensic processes are sometimes radically different from other, established disciplines. Bedrock forensic practices such

as the use of standards and controls are found to be meaningless to some in the digital forensics community. Those opposed say that unlike serology and toxicology, it simply isn't possible to get a false positive result from a digital forensic examination. The tool, they say, may miss some evidence, but it will never find evidence that wasn't already there.

These are just a few of the significant challenges faced by front-line practitioners. There is much work to be done if these challenges will be met.

References

Bell, Graeme B., Boddington, Richard (December 2010). *Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?* Journal of Digital Forensics, Security and Law.

Mell, P., & Grance, T. (2011, January). *The NIST Definition of Cloud Computing.* Retrieved October 9, 2011, from: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

Microsoft Corporation. (n.d.). *IPv6.* Retrieved September 17, 2011, from: http://technet.microsoft.com/en-us/network/bb530961.aspx

Ruan, K., Baggili, I., Carthy, J., & Kechadi, T. (n.d.). *Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability: A Preliminary Analysis.* Dublin, Ireland: University College Dublin.

Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). *Cloud Forensics: An Overview.* Dublin, Ireland: IBM Ireland Ltd.

TechTarget. (2007, December). *Cloud Computing.* Retrieved October 11, 2011, from: http://searchcloudcomputing.techtarget.com/definition/cloud-computing