

Digital Media Forensics

Michael Allgeier 2000-05-08

Introduction

The area of digital media forensics is not just the art of finding deleted or hidden data; it is also the understanding of the underlying technologies behind the various tools used and the ability to present scientifically valid information. Digital media forensics is a growing science that governmental agencies have long practiced, with the commercial sector not far behind. Many governmental agencies are far ahead of most companies when it comes to searching, seizing, and analyzing information systems and the proper accountability of digital evidence. With secrets and lives to lose if sensitive information were released to the wrong people, the reasons behind their expertise are understood. The ability to identify the person(s) responsible for the compromise or theft and means of transmittal is paramount for further protection and control of sensitive information. Many companies are now focusing on the problem of industrial espionage and the control of proprietary information. Current economic espionage estimations indicate US companies lose over 50 billion dollars each year with the possibility of 150 billion dollars per year lost by the year 2003. Putting an exact dollar amount on the value of lost proprietary information is impossible, but needed to prompt decision makers. Even with encryption, access control and auditing tools, digital media forensics is a key aspect for information security officers.

Overview

For law enforcement digital media forensics used to be limited to a normal printout from a computer. This is the case. The history of digital media forensics started predominantly within governmental agencies and a few dedicated civilian professionals. Most of the government funded methodologies and forensic software were tightly controlled. Many programs remain controlled for use by law enforcement personnel only. On the other hand, some of these dedicated professionals wrote some basic programs for DOS that are still currently in use. Most recent forensic programs are easy to use Graphic User Interface (GUI) software, which can handle many different operating systems and are available to the public. Not that long ago, computer forensics was like the "wild, wild west". There were very few training programs, no certifications of any kind, and most investigators were playing catch-up with technology. Times have changed. There are several structured private and government training programs, recognized certifications, and an increasing number of technologically savvy investigators.

Though there is no singular certification for computer forensics, the International Association for Computer Information Systems (IACIS) is a non-profit organization that offers a widely recognized and comprehensive certification for digital media forensics professionals. Along with other certifications, many US Agencies and private companies now offer excellent training programs. The Department of Defense has a newly formed training program for investigators called the Defense Computer Investigations Training Program (DCITP), DCITP offers DoD investigators and technicians a single computer forensic training program. Companies such as: Mares and Company, LLC; Guidance Software, Inc.; Ontrack; KompuKirk and LostData.Net offer data recovery, software and training for the private sector. The aforementioned companies and organizations are merely examples and should not be considered all encompassing. As operating systems, programs, and technology changes, so will the art of digital media forensics.

Training

Digital media forensics is growing and is an ever-evolving field. Many competent examiners/ investigators comprise the core of this field, though there are some methodologies and personnel that are dangerously on the fringe. A person with only a few thousand dollars can buy enough equipment and software to setup a limited forensics lab. A potential problem exists if the person does not understand the technology and methodology behind the GUI automated forensic software. A defense attorney can easily attack and defeat the credibility of the examiner's knowledge and training (reading the software operating manual does not take the place of training). Fortunately most people in the business are well trained and very knowledgeable. Most forensic examinations yield scientifically valid and useful information. Also, what is not found might be just as useful and important, a seized hard drive not having files which are associated with normal use might indicate secure wiping or manipulation. Always remember that digital media forensics is a scientific tool used for an investigation. The future of digital media forensics depends on examiners and investigators remaining unbiased and adhering to scientifically sound methods. Curiosity coupled with a properly executed examination is key in finding pertinent data associated with the case or investigation.

Formal training sets standards and ensures proven procedures are followed. Security courses can easily be found with common search engines and within the information security field. Security training is normally very expensive, and sorely needed. If a company cannot afford a full time information security officer, it might be wise to find a company that specializes in deploying incident response teams and/or some type of remote security monitoring. It might be cost effective to pay a security company or consultant to design or lock down a preexisting

network, rather than to appear on the news, lose proprietary information, have your credibility crippled, and still have to pay for the security lock down after the fact. Identify shortcomings and plan for training six months out. Training is quickly outdated; it's just the nature of the IT field, especially information security.

Hidden Data

Data may be hidden in many ways, only limited to the imagination. As you may know, when a file is deleted the information remains and only the reference to where that information resides is altered. This is not a preferred method to hide data, for doing so will free the operating system to write to the area. Changing the file extension from a ".doc" to ".dll" might fool an unwitting coworker, but not most computer literate people. You might believe that such simple ideas would never fool you, but what if a person reversed letters in a word. During a physical level search for the word "dog", you may find nothing because the person changed it to "god". Manually searching a floppy diskette cluster by cluster for possible clues might seem plausible until you find yourself with a 30 GB hard drive. Automated forensic tools come in handy, to say the very least. Encryption is an extremely powerful method to hide data, but having encryption software might tip the investigator or examiner to look deeper or ask more questions. Steganography is another powerful and interesting method to hide data. Steganography is the ability to represent data within another area of data, e.g. imbedding a text document inside a digital picture by altering the picture's palette so that it is not visible to the naked eye. The same can be done to many other file formats. There are endless possibilities in how one might hide or disguise data, just remember that if you can make it you can break it, it only takes time.

Laptops and On-line Forensics

With the increase of telecommuting and use of laptops, the instances of theft are on the rise. Many companies are turning to mobile security solutions that will not only encrypt the data but when decrypted, will protect it from viruses and prying eyes from the Internet. When, not if, a laptop is stolen or lost, a damage assessment and investigation is conducted. Hopefully the computer is recovered at some point, and at that time forensics will help identify what files were accessed and at what times. Forensics could also help identify the thief. Another growing area in data forensics is the tracking down of web server vandals. After an instance of web defacement, normally most evidence is lost when the web server is re-built and placed back into operation. It is the responsibility of the incident response team to react and investigate, but with little original forensic data to go on, they rely heavily on log analysis. It should be plain

to see that proper logging and auditing is essential along with the cooperation of the ISPs.

Evidence

What is evidence? Simply put, evidence is anything that can show proof. A good rule to follow is even if you don't think the information would ever go to court, treat it as evidence anyway. Evidence can be entire computer systems, on-line data, hard drives, floppy diskettes, tapes, CD ROMs, hand held electronic organizers, MP3 players, written notes, or just about anything when it comes down to it. Knowing what to take is dependent upon what is relevant to the investigation and what is authorized. Properly written security policies are essential building blocks for all information security officers. There are several free resources available such as CERT.org, National Institute of Standards and Technology (NIST), and infosyssec.net; you might also want to pass it through your legal department. In addition to the legal issues surrounding obtaining evidence, properly gathering the evidence is no small task. I suggest having an evidence gathering kit specifically for magnetic media. This might be time consuming at first, but a real lifesaver when you're on the job. Some basic items might be: a ledger, chain of custody documents, a camera, tags, envelopes, tape, pens and markers, non-static bags, a small computer tool kit, just to name a few. Before seizing anything, a well focused and thought out plan with identified goals should be first.

Methodologies

Methodologies to digital media forensics may vary depending on the company's procedures, resources, intent, and the media itself. Some of the basic areas are the stand-alone computer, workstations, servers and online media. Stand-alone, workstation and removable media examinations and investigations are fairly straightforward. Servers and online media can at times be challenging to obtain and preserve. Luckily there are some well-trained information security officers in the field, along with several companies that specifically focus on media recovery and full investigations, some examples of and resources are mentioned above. Far too often, key data was never captured because auditing and logging were not turned on. Even if this is the case, there are still areas to gather information; don't forget reviewing the backups and talking to the local system administrators. An Intrusion Detection System (IDS) could save your company money, time and the company's reputation. An IDS isn't strictly for protection from a "hacker" but also from the trusted user. From experience, there is more to fear from the trusted user. There has been some debate and misunderstanding on the placement of an IDS, placing one internal and one external of your firewall will show you who's knocking on your

front door and who has the key. Having one security mechanism in place will not provide proper security, it should be applied to all levels from your gateway back to the desktop. Forensics on a properly secured network is normally simple and straightforward.

Conclusion

The science of digital media forensics has come a long way and, as time passes will become a staple of the corporate information security officer. A general understanding is the first step, the realization of its necessity comes next. As companies respond to the gross losses of proprietary information, forensics will play a larger part in the planning and execution of policy.

This article merely touches on some of the aspects of digital media forensics and does not endorse any security companies, governmental agencies, or products. It is further intended to help identify the information security officer's need for digital media forensics capabilities.

Michael Allgeier is a former electronic warfare analyst and Special Agent. He is currently a Senior Security Engineer with NETSEC specializing in IDS, digital media forensics, investigations, penetration testing, and network security architecture.

Relevant Links

[IACIS](#)

International Association for Computer Information Systems

[Department of Defense Computer Forensics Laboratory](#)

Department of Defense

[Privacy Statement](#)

Copyright 2006, SecurityFocus