

Windows Forensics

***fo-ren-sics* (P)** Pronunciation Key (f-rnsks, -zks)
n. (used with a sing. verb)

The use of science and technology to investigate and establish facts in criminal or civil courts of law

Forensics is a topic that has captured recent public interest. From DNA evidence in the O.J. Simpson trial to bullet fragment analysis in the Washington, D.C., sniper trials, the basic concepts of forensics have become more familiar to the American people now more than ever.

Fictional television programs such as *CSI: Crime Scene Investigation* and *Cold Case* showcase forensic science, and docudramas such as *New Detectives* and *Forensic Files* focus on cases in which forensic evidence has led to or supported a prosecution. Both types of shows highlight the glamorous side of forensics, the discovery of the proverbial smoking gun, which ultimately leads to a successful arrest and prosecution. They do not do justice to the weeks and months of effort that go into the identification, acquisition, and analysis of the evidence by a team of dedicated, highly trained analysts. It makes for good television to show the comparison of two hair follicles under a microscope; the audience is much less interested in the days spent combing through a vehicle inch-by-inch to find and catalog those follicles. Similarly, in the world of computer investigation, it makes for better drama to show a graphical *phone trace* tracking a dial-up user located around the globe than to show the days spent acquiring and hashing a hard drive and the meticulous preparation of the evidence report.

Computer forensics applies the same scientific principles as other forensics fields to the identification, acquisition, and analysis of digital evidence. With the advent of the Internet, both network and system forensics are becoming

increasingly interrelated. The digital evidence sought by an analyst might reside on any number of devices, including personal digital assistants (PDAs), USB pen drives, digital cameras, and cell phones. Additionally, all modern operating systems are network capable, and it is rare to find standalone PCs with no external connections, providing further evidence on routers, servers, firewalls, and proxys. The field of computer forensics encompasses both system forensics and network forensics, and an understanding of both is required to conduct a thorough investigation.

The Corporate Computer Forensic Analyst

Unlike most analysts in the field of criminal forensics, practitioners of computer forensics are not always working for or with law enforcement agencies. The demand for skilled computer forensic analysts in the corporate world exceeds the supply, and experienced analysts are highly sought-after. In addition to supporting law enforcement, a computer forensic analyst might be called upon to:

- Recover files intentionally deleted by a disgruntled employee.
- Determine the root cause of a computer compromise.
- Track down the author of a threatening email.
- Investigate unauthorized copying and intellectual property theft.
- Obtain evidence an employee viewed inappropriate material.
- Refute or support claims of overtime hours worked.

The end goal of an analyst working in a corporation might vary greatly from that of an individual working for or with a law enforcement agency. In the corporate world, the ultimate goal is to protect the company's interests, not to prosecute all potential offenders. For example, if an isolated brochureware website in a remote subsidiary is defaced and no sensitive information is involved, the corporate goals are likely as follows:

1. Identify the cause of the defacement.
2. Restore the site as quickly as possible.
3. Prevent future occurrences.

For most companies, it makes no fiscal sense to track down and prosecute the offender if there is no appreciable loss and reoccurrence can be prevented. If, however, an insider is found transmitting intellectual property to a competitor, the company may very well be interested in both civil and criminal proceedings.

Regardless of the final outcome of an individual investigation, the computer forensic analyst might not know whether his work will be presented in court for weeks, months, or even years after the initial incident. Therefore, he must take the same precautions as law enforcement officials in safeguarding the integrity of the investigation and must always work under the assumption that the results of the analysis will be presented in a court of law at some point. At the same time, the corporate analyst has an array of specialized tools at her disposal and is able to use them to her advantage in investigations. Although the typical computer incident response team (CIRT) in a company does not generally carry Luminol or fingerprint-gathering equipment in their response kits, a corporate CIRT may already have administrative rights (or the ability to obtain them) on corporate assets as well as the ability to search and seize company-owned equipment without the need for a warrant.

NOTE Although computer data stored on a corporate asset and created using corporate systems is generally considered company property in the United States, it is not considered such in many other countries. The French Supreme Court ruled in the case of *Nikon France v. Frederic Onos* that a company was explicitly prohibited from viewing the personal emails or files of an employee, even if created with and stored on company-owned equipment.

Not everyone is cut out for the world of computer forensics. The work requires detail-oriented individuals who are willing to document everything they do. At the same time, analysts must think creatively and respond quickly and effectively to the unique situations that they face in the field. A typical CIRT includes executive management, public relations, corporate security, legal, and IT subject matter experts. For this reason, the analyst must communicate effectively both orally and in writing. In addition to being able to perform the technical tasks associated with the job, the analyst must successfully explain evidence to a variety of audiences, each with vastly different backgrounds.

One question that must be asked when hiring and training analysts is this: “Would I be comfortable with this person testifying on the company’s behalf in court?” Individuals who are new to the field must be mentored and supervised appropriately, and a clean criminal history is a necessity. Convicted hackers need not apply.

Windows Forensics

To date, much of the literature and tools have focused on Unix/Linux-based forensic analysis. The Unix/Linux (*nix) environment provides many capabilities not natively present on the Windows platform, including the ability to

mount drives as read-only, perform complex regular expression queries on content, and obtain easy hardware-level drive access (as opposed to partition-level). No good forensic analyst discounts the value of the tools available on a platform such as Linux, and all would do well to become familiar with these tools; indeed, this book directly references several Windows ports of decades-old *nix tools as well as Cygwin-based tools. Any complete forensics lab has at least one Linux environment either native or running through a virtual machine product such as VMWare. Additionally, a large number of today's top analysts are specialists in these environments, and they will continue to be critical to forensic analysis.

TIP Cygwin is a Linux-like environment for Windows operating systems. Many commands useful in forensic analysis like `strings` and `grep` are included in the distribution. VMWare Workstation from EMC and Virtual PC 2004 from Microsoft are essential forensics tools for the loading of disk images as well as the analysis of forensic information.

Despite the historical grounding of computer forensics in the *nix world, the Windows environment is ubiquitous in many organizations today. Depending on whom you ask, Windows penetration ranges from 85 percent to 97 percent of all computer-based operating system installations in the United States. Even the low-end figures illustrate that Windows remains the dominant operating system by a large margin and the one that analysts are most likely to encounter in a corporate setting. As Windows usage has grown, so has the support for Windows-based forensic tools and techniques. Companies such as Guidance Software and NewTechInfosystems (NTI) produce Windows-based forensic suites, and Sysinternals produces support tools that are invaluable assets in any toolbox. Also, capabilities not generally present in the *nix world such as remote drive acquisition (at the hardware level) are being introduced and changing the dynamics of forensic response.

NOTE Onestat quotes Windows penetration in the United States as 97.5 percent (www.onestat.com/html/aboutus_pressbox10.html). IDC shows Windows as having 85 percent of client sales in 2004 (news.com.com/2100-1001-243527.html?legacy=cnet)—amplified by the fact that many Linux clients aren't purchased. *LinuxWorld* disputes the numbers (www.linuxworld.com/story/32648.htm) and moves by companies like IBM to Linux may change the statistics as well.

At the same time, new challenges are being presented to the forensic analyst. Encrypted File System (EFS), SYSKEY, and products like Microsoft Passport assist in providing increased security for the Windows environment, but they can make the job of the forensic analyst more difficult. The specifics of these tech-

nologies as well as everything from Windows file systems to Internet Explorer history files are currently relevant to most corporate investigators, but no comprehensive single source for this information is currently available. For the corporate investigator, this means having to cobble together information from numerous sources and apply *nix techniques to the Windows environment.

By providing a Windows-focused guide in terms of the target machines as well as the analysis tools, this book endeavors to provide *nix experts with the detailed workings of the Windows operating systems that pertain to forensic analysis. It also aims to provide solid grounding for Windows experts looking to break into the exciting and challenging world of computer forensics.

Not all investigations return the expected results. Investigating anomalous behavior can lead to unexpected findings (possibly the best example being

CASE STUDY: THE MYSTERY TYPIST

One afternoon my security team received an email message from our IT help desk. Attached was the re-created transcript of a user conversation and an unusual Microsoft Word document. The transcript was along the lines of the following:

User: Someone broke into my computer and is typing odd messages to me when I use Microsoft Word.

Help Desk: What type of messages, sir?

User: Meaningless phrases, but I think he has a camera trained on me.

Help Desk: Why do you think he has a camera trained on you, sir?

User: He only types the messages when I'm in Word, and sometimes he types things related to phone conversations I'm having.

Help Desk: Is it happening right now?

User: Yes. He's typing things about our conversation right now. Should I hang up the phone?

Help Desk: Save the document and send us a copy. We'll call security and have them come by.

When we opened the attached document, it appeared to be a standard memo with random phrases inserted, including pieces of the user's side from the previous conversation. An investigator was sent down to talk with the user and analyze the machine.

Faced with a likely lack of stored evidence (the user had saved only the one document we already had), the investigator tried to see whether she could reproduce the problem. She opened several documents, typed miscellaneous messages, recorded all incoming and outgoing network traffic, and found nothing unusual. A secondary search of running processes and an anti-virus and anti-spyware check likewise turned up nothing.

(continued)

CASE STUDY: THE MYSTERY TYPIST (continued)

After spending several hours analyzing and monitoring the user's laptop, the investigator called the user in to attempt to duplicate more precisely his actions. The user began typing in Microsoft Word, and no extraneous words appeared. After a few moments, the user began to get frustrated and used several expletives, which did appear on the screen. At that point, the investigator realized it was not actually a security breach; the user had accidentally turned on Windows voice recognition and every time he made a phone call, the mystery typist re-appeared!

Cliff Stoll's *Cuckoo's Egg*). One unusual-sounding referral from our help desk illustrates this and highlights a potential pitfall for investigators.

People, Processes, and Tools

In order to build a competent computer forensic capability within an organization, the initial focus must be on people, followed by process and tools. Many organizations looking to build competency in the computer forensics space reverse these priorities, spending large sums of money on enterprise-class software and lab hardware. When the hardware is in place, existing staff begin to develop processes around using their newly purchased tools. The tail wags the dog! Finally, companies begin to search for individuals who are certified in or experienced with the tool suite purchased to round out their capabilities.

The more effective way to build forensic capability is to start with people. The first step should be hiring an experienced examiner to mentor existing staff, bring in supplementary staff, and develop sound forensic procedures. To find a qualified individual, one must do the following:

- Go to a trusted source in information security and ask for recommendations on good people.
- Look to reputable organizations, including Infragard and the High Technology Crime Investigation Association (HTCIA) for pools of knowledgeable individuals as these groups have performed background/reference validation on members.
- Hire individuals with direct investigative experience.
- Evaluate certifications such as CISSP, CISA, SANS, and EnCase carefully.
- Approach candidates as if they were taking the witness stand in court, asking yourself whether they will hold up to judicial scrutiny as experts.

When the successful candidate is empowered in the role of running a CSIRT, the first order of business is to develop an investigative policy and associated procedures. At a minimum, the policy should address the following:

- Who is empowered to investigate and under what circumstances?
- What oversight is needed to approve investigations?
- How is the investigation run cross-functionally?
- What scenarios and circumstances warrant an investigation?
- How are the results of investigations processed, and how are disciplinary procedures carried out?

Policy dictates the operational structure, roles and responsibilities of the team, and the scope of its investigations. Procedures can then be developed for the individual aspects of an investigation, dictating who performs specific investigative actions, what steps must be taken for common procedures, and how these steps are validated. Common procedures involve the following:

- Evidence handling and chain of custody
- Forensic acquisition or duplication
- Communication of incidents
- Common analysis activities (mailfile, file system, logfiles, and so on)
- Terms of engagement for bringing in other parties
- Retention procedures for evidence

Many good sources can be shamelessly plundered for their expertise, including NIST and CERT. After the procedures have been adopted and tested, tools can then be purchased or acquired to fill the gaps or enhance the procedures.

The tools mentioned throughout this book vary greatly in cost, and the capabilities do not always merit the price tag. Since I am talking about Windows forensics, analysts need solid laptops and desktops for performing analysis — nothing fancy, but a decent amount of memory and the latest processor will pay for themselves in time savings when they are most needed, during an actual investigation. Secondly, a good tape backup unit, DVD-R drive, and lots of disk space are needed. One may begin using freely available tools, replacing them as necessary with more expensive toolsets. At a minimum, you will need:

- An acquisition tool to perform forensic duplications
- An analysis tool to search hard drives
- Basic text search and manipulations tools
- A data integrity verification tool

TIP Depending on your organization's specific policies, machines confiscated during investigations can become future lab machines.

For a barebones starter kit, free versions of dd can be used for the duplication of files (with netcat for remote duplication and data transfer). WinHex makes an excellent, inexpensive general-purpose drive analysis tool, and Windows ports of common *nix string manipulation utilities (grep, strings, cat, less, and so on) can be used for more complex file search and manipulation operations. Finally, the md5sum program provides data integrity verification. Placed in capable hands, these basic tools will yield a much better cost/benefit ratio than a full implementation of EnCase Enterprise, custom-built forensic computers, and single-purpose specialty tools in the hands of partially trained individuals.

Computer Forensics: Today and Tomorrow

The field of computer forensics is quickly maturing. Certification programs from organizations like SANS and Guidance train individuals in computer forensic analysis. Forensic-specific software packages are no longer restricted to the ad-hoc task-specific software built by enthusiasts. Complete packages such as EnCase, the NTI suite, and The Coroners Toolkit (TCT) offer support and court-proven solutions for the computer forensic analyst. Organizations such as the Infragard partnership between industry and the Federal Bureau of Investigation (FBI) and HTCIA consist of computer security professionals sharing knowledge and practical experience in the field. Research into computer forensics is being performed and taught at universities, including Carnegie-Mellon, the University of California at Berkeley, and Penn State. Literature on most aspects of computer forensics is widely available, including influential texts such as Eoghan Casey's *Digital Evidence and Computer Crime* and Kruse & Heiser's *Computer Forensics: Incident Response Essentials*.

Many of the tools, techniques, and practices in the field of computer forensics are still emerging, and the exponential growth of digital information ensures that the field will remain new and interesting for the foreseeable future. Although much effort goes into performing computer forensic investi-

gations, the moment that you uncover a file that a user thought he had deleted or find evidence confirming that a suspect sent harassing messages is incredibly rewarding and fulfilling.

Additional Resources

Refer to the following list for additional resources:

Access Data — Forensic Toolkit

www.accessdata.com/Product04_Overview.htm?ProductNum=04

Computer Emergency Response Team (CERT)

www.cert.org

Cygwin Linux-like Environment

www.cygwin.org

Guidance Software (makers of EnCase)

www.encase.com

Infragard

www.infragard.net

High Tech Crime Investigation Association

www.htcia.org

Microsoft Virtual PC

www.microsoft.com/windows/virtualpc/default.mspx

NTI (makers of SafeBack)

www.forensics-intl.com

NIST Computer Security Division

csrc.nist.gov

SANS

www.sans.org

SysInternals

www.sysinternals.com

VMWare

www.vmware.com

WinHex

www.winhex.com

