Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Developing a Computer Forensics Team

Efforts to establish sound information assurance programs are rapidly evolving due to increased connectivity, enhanced technology, and the continuous introduction of operating and application systems software. The information assurance practitioner is repeatedly faced with new challenges to keep up with these changes. In parallel, these changes in technology have greatly affected the role of investigators. Law enforcement investigations, civil litigation, private investigation, and corporate investigations are all affe...

Copyright SANS Institute
Author Retains Full Rights

AD
Take control of vulnerability threats Now!
Request a Free Trial
Secunia
Stay Secure

Christine Vecchio-Flaim
Security Essentials Practical
June 2001

Developing a Computer Forensics Team

Overview

Efforts to establish sound information assurance programs are rapidly evolving due to increased connectivity, enhanced technology, and the continuous introduction of operating and application systems software. The information assurance practitioner is repeatedly faced with new challenges to keep up with these changes. In parallel, these changes in technology have greatly affected the role of investigators. Law enforcement investigations, civil litigation, private investigation, and corporate investigations are all affected. Regardless if the situation is a criminal matter, civil matter, or a corporate internal personnel issue, investigators must be cognizant to fact that computers touch every facet of our lives.

The term "forensics" is usually associated with the use of science and technology to investigate and establish facts in criminal or civil courts of law. Computer forensics applies this definition to computer-related evidence. The science of computer forensics is an emerging specialty in the information security industry. There are currently a limited number of experts in the field and there are no formally established standards, criteria, or certification requirements. As the computer forensics specialty matures, these areas will evolve and standards will be set as in all other areas of scientific forensics. Of course, as technology changes, some of the tools and processes will need to change but the basic methodology would stay relatively constant.

Developing a Computer Forensics Team

The size of the forensics team will vary greatly dependent upon the size and the role of the organization. Some organizations may not require more than one or two specialists to effectively meet their needs but larger organizations and law enforcement agencies could require very large teams. Remember it isn't always feasible to conduct forensics in-house. If you have a very sporadic requirement for forensics work or cannot apply the required resources to developing a team, it may make more sense to contract the work out to a forensics services company when the services are needed.

Don't expect to build your team up overnight. Because the computer forensics specialty is fairly new, it can be very difficult to find skilled forensic specialists to develop a team. It may be necessary to find one or two experienced specialists to start. Then, you can bring in other information technology (IT) professionals and get them the training and experience they need under their guidance.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

In a small organization and particularly in the corporate world, it may seem that it would be an easy solution to place individuals with information technology responsibilities in a part-time forensic specialist role. This practice is not advised because the computer forensics specialist should be completely impartial to internal operations and should not have a direct chain of command into the IT organization.

An individual who is interested in becoming a computer forensics specialist should have a strong information technology background. This is an essential and fundamental requirement. The individual must have a thorough understand of how different operating systems, applications, and hardware effect information systems. It is also important that the individual has a good comprehension of investigative techniques, methodologies, and standards. Finally, the individual should be properly trained in the computer forensics specialty, using a variety of tools and techniques for a wide range of potential situations. It is rare that a specialist will be able to rely on one set of tools for all situations.

When performing computer forensics, the forensics specialist must remember the basics of any type of investigative forensics work. Proper planning, documentation, chain of custody, and the rules of evidence still apply and must be diligently followed. It is imperative that the individual stringently applies these methodologies to their forensic work. The forensic specialist must keep in mind that the average person may not fully understand the methods and techniques used to obtain the evidence, and as a result a judge, or a jury, or a corporate attorney may question the results of their investigation. In addition, the forensic specialist must be able to effectively document and report the findings of their investigation. Proper documentation is essential and must be capable of standing up to scrutiny. Additionally, the specialist must be able to effectively report their procedures and findings in layman's terms. The specialist may also be required to give testimony and endure extensive examination and cross- examination. The computer forensics specialist must have excellent written and oral communication skills. Finally, it is essential that the computer forensics specialist remain impartial, with no predisposed presumption of guilt or innocence.

There are some excellent resources for training available to the aspiring forensics specialist. The following are just a few of the training resources available.

New Technologies Incorporated (NTI) http://www.forensics-intl.com

System Administration, Networking, and Security (SANS) Institute http://www.sans.org

Kroll Worldwide http://www.krollworldwide.com/training/courses.cfm

Utica College Economic Crime Management Undergraduate and Graduate Degree Programs http://www.utica.edu/CriminalJusticeECI.asp

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Preparing the Lab

As you build your team, you should begin to acquire the tools and equipment that will be needed to conduct a variety of forensic examinations. This step will require a great deal of planning and resources.

The forensics team should conduct a thorough analysis of what types of operating systems, hardware, and environments, they will be expected to analyze. This will determine what tools and equipment will be required to conduct their examinations. Keep in mind that the examiners will likely need a variety of different tools to effectively perform their work.

The team should have a secure laboratory to perform their examinations, store tools and equipment, and properly secure evidence gathered during their examinations. A good forensics workstation for the lab will be required. Your team may also require portable forensic equipment for field analysis.

The equipment and tools required for forensics examinations can be very costly. Properly equipped forensic workstations can cost well over $7000 each and software tools can cost several thousands of dollars for each license. Some tools are offered to law enforcement agencies for reduced prices, or free when combined with paid training classes. You will need to check with the different vendors to see what they offer.

Once you have your equipment and tools in place, use them to practice. Each tool works differently and may even behave differently from system to system. The forensic specialist should practice on a variety of platforms and equipment to ensure they understand the nuances of their tools. This is the time to determine the strengths and weaknesses of the various tools and find the best solutions for each situation.

The following is a list of some of the standard tools and equipment currently available. It is not completely inclusive and new tools are always being developed.

@stake http://www.@state.com

@stake provides password auditing and recovery application called LOphtCrack. The latest version of LOphtCrack is LC3.

Columbia Data Products http://www.cdp.com/

SnapBack Forensics Version offers Forensic Backup, Investigation, Restoration, Tools & Utilities.

DIBS USA, Inc. http://www.computer-forensics.com/
Forensic Workstations, Portable Evidence Recovery Units

Digital Intelligence Incorporated – http://www.digitalintel.com

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Offers a variety of forensic software tools including, FRED, DRIVESPY, IMAGE, PART, and PDBLOCK.

Fred Cohen & Associates – http://www.all.net
Provides a tool called ForensiX, which is a comprehensive Digital Forensic Analysis Package.

Forensic Computers http://www.forensic-computers.com/
Forensic Computers offers a full range of Forensic Lab and Portable Workstations

Guidance Software http://www.guidancesoftware.com/

Guidance Software is the make of EnCase. EnCase is a comprehensive tool that provides non-invasive acquisition and analysis to document, recover, and preserve forensic evidence. Guidance Software also offers electronic hard disk drive write-blocking hardware

New Technologies Incorporated (NTI) http://www.forensics-intl.com/

NTI offers many different forensic tools including SafeBack, CRCMD5, DiskSearch 32, DiskSig, DM, FileCNVT, FileList, FILTER, GetFree, GetSlack, NTAView, NTI-DOC, Ptable, Seized, ShowFL, and TextSearch Plus. NTI also has password cracking utilities. Some of these utilities are only available to law enforcement agencies. Check out the site for a complete description of the tools and their availability.

The Coroners Toolkit (TCT) http://www.fish.com/forensics

The Coroners Toolkit is a collection of programs that can be used for an analysis of a UNIX system after break-in. This set of tools is freeware and was developed by Dan Farmer and Wiese Venema

Techniques and Methodologies

Prior to commencing your first computer forensics investigation, your team should have a written methodology for the performing the analysis. This methodology should address the basic fundamental procedures that will be performed for every investigation. The specific tools may differ from case to case, but the methodology should remain the same unless there are specific documented reasons for making modifications.

Planning is essential and should be the first step in each case. What type of system do you anticipate? What is the environment? Is a warrant required? How will you obtain access? How

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

will you secure the environment? Do you have the right forensic specialist selected for the task at hand? How many specialists do you need? Is your toolkit prepared? Safe transportation? How will you document the environment? Do you need a team of specialists?

The next step in a forensic investigation is to secure the environment. This step ensures against tampering with evidence or putting yourself in a potentially dangerous situation. The steps necessary to secure the environment will vary greatly depending upon the environment. Your planning should have addressed this so you should be prepared.

Before performing any analysis, it is essential that you document the scene. This is the "entrance scene". What do you see when you walk in the office door where the workstation is plugged in or open the trunk to retrieve the laptop? Videotaping can be a very effective resource for this step in the process. By utilizing a video camera, still camera, or at a minimal hand sketches, you can recreate the scene. In addition to the photographic image, you should also document the scene in notes. These notes should include all equipment, peripherals, and media including serial/model numbers and any other pertinent information that accurately depicts the scene.

Secure the evidence. Is the system running or turned off? What is your next step? Will you do a system shut down or power down via an abrupt unplug of the machine? Your steps may vary based upon the situation, the system, or its operating system. Regardless of which method you utilize, it should be documented. Keep in mind that the system should be shut down as quickly as possible. This is necessary to deter against the potential of destructive processes running in the system background.

The system should now be appropriately labeled, and readied for safe transport. Remember to document all steps in the custody chain. Once the system or media is in your custody, it should never be left unsecured.

Transport the evidence if possible to the lab environment that you have established. In some cases this will not be possible and you will need to utilize a mobile toolkit to complete the analysis. Regardless, document your actions and be prepared to defend your methodology.

Regardless of the tools that you use, you should never work off of the original media that you intend to analyze. A cardinal rule in computer forensics is that the original media should remain untouched and unaltered. Always make a bit stream image backup disk of the media that you intend to analyze, better yet make two image disks. Lock up the original and a copy. By doing so, if you make an error analyzing the first copy, you still have another to work with and still leave the original media intact and unaltered.

Begin the evaluation. An evaluation consists of numerous processes that are necessary to perform a thorough analysis of the media. The specific progression of these steps may be dependent upon the forensic tools that you are using. These steps may include the following processes:

- Documenting System Date and Time
- Mathematical Data Authentication

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Key Word Searches
- Evaluating Swap Files, File Slack, and Unallocated Space
- Identifying File, Program, and Storage Anomalies

Each forensic tool has a different method for reporting the results. In most cases, it will be up to the forensic specialist to develop an easy to understand, and accurate account of the examination and the associated results. The format of this report can vary greatly dependent upon the audience it is intended for.

Finally, the forensic specialist must be prepared to explain and possibly defend each step in the forensic process and should always be prepared to testify in court if necessary. If a standard methodology has been used in the examination process, the examiner will look far more credible in the courtroom.

Summary

Computers are interwoven into society and will increasingly be used as a tool for criminals. Computers can be used by: a kidnapper to write a ransom note, a pedophile to market child pornography, or a serial killer to stalk or geographically map out their next victim. In all of these cases a properly trained computer forensics specialist could utilize their skills to acquire the necessary evidence against the perpetrator.

Acquiring and analyzing computer evidence properly and effectively is a complex process requiring a significant amount of planning, resources, and technical expertise. Every organization needs to assess their own needs to determine whether they will utilize an in-house computer forensics team or contract with a forensics specialist as needed.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References

Web References

Alphabetical List of Computer Forensic Products, Timberline Technologies
URL: http://www.timberlinetechnologies.com/products/forensics.html

Jack Champlain, "Computer Forensics Investigation"
URL: http://www.acuia.org/article_of_the_year/2000_article.html

Thomas Rude CISSP, "Evidence Seizure Methodology for Computer Forensics"
URL: http://www.crazytrain.com/seizure.html

James O. Holley, Security Magazine "Computer Forensics in the New Millenium", September 1999
URL: http://www.scmagazine.com/scmagazine/1999_09/survey/survey.html

New Technologies Inc. "Computer Evidence Processing Steps"
URL: http://www.forensics-intl.com/evidguid.html

Print References:

Illena Armstrong, Security Magazine "Computer Forensics, Tracking Down the Clues", April 2001

Matt Villano, CIO Magazine " I.T. Autopsy", March, 2001

© SANS Institute 2001, Author retains full rights

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**