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.

Computer Forensic Legal Standards and Equipment

This paper addresses an issue of increasing importance to companies in this modern era. Computer Incident Response Teams (CIRTs), network security, and intellectual property (IP) security are growing in importance and are becoming many companies' top priority in this age of increased security conscious commerce. The topic of this document focuses on the CIRT aspect of security conscious commerce, but in a less familiar role. This less familiar role of CIRT is the function of investigations and more specifically, the ro...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Name: Damian Tsoutsouris

Version 1.2f (GSEC)

Title: C

Introduction

This paper addresses an issue of increasing importance to companies in this modern era. Computer Incident Response Teams (CIRTs), network security, and intellectual property (IP) security are growing in importance and are becoming many companies' top priority in this age of increased security conscious commerce. The topic of this document focuses on the CIRT aspect of security conscious commerce, but in a less familiar role. This less familiar role of CIRT is the function of investigations and more specifically, the role of computer forensics as part of a company's arsenal in the war on network/resource abuse and intellectual property theft. This document is not designed to provide a specific checklist of <u>everything</u> that a CIRT must have, or provide expert knowledge of all laws related to the handling of evidence. It does however seek to provide the reader with some of the basic considerations and tools available to make a CIRT or corporate investigator effective in gathering, preserving and analyzing computer evidence.

Concept

When someone mentions Computer Incident Response Team, the image of anti-hackers comes to mind for many, and indeed this is a major role if not the only role for many CIRTs. Their primary job is to be called on in the event of an intrusion on the company network, discovery that crucial information property has been compromised, or perhaps to be called upon when a virus or worm is wrecking havoc on the network. At that point of detection, the CIRT typically comes in and attempts to fix the problems, and configure the system to prevent such future attacks. However, a recently discovered and less publicized role for a CIRT is the aspect of computer forensics. The crucial role of computer forensics for CIRTs stems from the common fact that current or former employees initiate a significant portion of intellectual property theft and corporate network abuse.[1] While the threat of an outsider perpetrating such crimes is reduced drastically by lack of knowledge of the infrastructure of the company, disgruntled or greedy employees have easy access to the network and have intimate knowledge of where to go for information and can often easily gain access to intellectual property. Indeed, it is often crucial to an employees' job to have such easy access, and typically the only constraint placed on them is the trust that the company

[1] Davis

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

grants them to adhere to corporate policies and laws on distribution of such information.

Implications

As defined by Judd Robbins, a computer crimes specialist and investigator, *"Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence*."[2] The key here is "potential legal evidence." The data obtained by a CIRT or a related investigator must be able to hold up under the scrutiny of a court of law to be useful. An investigator must keep in mind and assume that any and all evidence discovered, which implicates an individual as guilty of a crime, will end up in court and be subject to intense analysis and scrutiny by the defense counsel. If these legal standards are not met and proper procedures are not followed, the evidence will be portrayed as tainted and/or unreliable, which will create added challenges in convincing the judge and jury that the evidence is a trustworthy factor to be considered in weighing guilt or innocence of the offender. The lack of proper procedures in handling evidence could, of course, also result in some or all of the evidence being ruled inadmissible in court. The effects of this are obvious in that not only is the corporation embarrassed by such an event of evidentiary mishandling and incompetence, but also the chance of being paid restitution or recouping any of their loss is now out of the question.

Opposite of the above scenario, if the evidence gathered against an individual is professionally executed and exceptionally convincing by present legal standards, the case will, in most instances, not even make it to court. The defending counsel will see a solid case presented before them implicating their client and usually attempt to settle things quietly. This has several bonuses for the company. The obvious advantage to settling the case is the reduced expense for all parties involved. If the case is airtight, the company is in a better position to seek full restitution. Unless of course, the defendant, even when presented with solid evidence, would rather go to court, pay trial costs for an attorney, risk being found guilty, have to pay full restitution, have his/her image tarnished, and perhaps even go to jail. Nevertheless, most sane defendants with even mediocre legal counsel will opt to quietly settle restitution and avoid the shame and expense of public court when presented with strong and legally reliable evidence.

A plus of settling out of court for a public company is the ability to avert a potential public relations 'black eye' and the possible embarrassment that could result from information disclosed at a public trial. For stock holders of a public company, the concerns with an employee being able to steal crucial intellectual property, embezzle thousands of dollars, or traffic child pornography using a company's assets, are likely "What kind of people does this company hire, and what measures are they taking to protect our investment?" A trial is simply an emotionally convoluted and final option that any corporation will want to avoid at all costs.

---

[2] Robbins

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

In addition to stock investors and analysts, many companies involved in consulting or joint projects with other companies run the risk of a devalued reputation among competitors if information of employee misconduct is put on display through a public trial. The fact is that companies working on joint projects will not want to share inside knowledge of their company structure and access to facilities and IP when one of those companies has a history of IP theft and embezzlement among its employees. The economic considerations of such a predicament are obvious as these companies would seek business elsewhere. The fact is that many corporations would rather let an offender get off completely free of prosecution rather than take it to court. It simply isn't worth the time, effort, money and indignity. Thus, obtaining and maintaining evidence in line with current legal standards is essential not only to justice, but is essential for company productivity, reliability and financial efficiency.

Policies and Procedures

An example of a practical application of computer forensics would be if "Company X" suspects that one of its employees is viewing child pornography on a company computer, it might request that investigators seize and analyze this computer for evidence of this alleged crime. The investigator has several tasks ahead of him/her and must follow certain procedures to ensure that the evidence is solid and will hold up in court. The basic criteria, which must exist in order for this to occur, are as follows:

1. *"No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer.*[3]
2. *Extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage.*[4]
3. *A continuing chain of custody is established and maintained".*[5]
4. *All procedures and findings are thoroughly documented.*[6]

Perhaps these points seem straightforward initially, but how does one accomplish these tasks? What kind of equipment and tools are necessary? What kind of training is available and required in order for a CIRT to be able to perform at this level?

The first rule of evidence, listed above, addresses the issue of acquiring data without corrupting it in anyway. Using the previous child pornography example, the first thing necessary in this case is to make a backup. An investigator should never do anything to the subject drive before backing it up. This means not even turning the

[3] Robbins.
[4] Id.
[5] Id.
[6] Anderson.

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

computer on! As a computer goes through its boot sequence crucial data can be erased such as file slack or swap files.[7]

The actual data mining will never take place on the target computer, as this would violate the first rule. Therefore this backup must be an exact duplicate of the subject computer. This duplicate is also known as a clone or bit-stream backup. Creating an exact duplicate means that the subject drive needs to be copied (cloned) sector-by-sector to a target drive as opposed to making a file copy. What sector-by-sector means, is that the tool used to make a clone must be able to copy the actual physical disk, not just the files. This is crucial because the clone will also include the free space of the subject disk as well as deleted files and slack space. Going into a detailed description of drive structure is beyond the scope of this paper, so it will only be briefly touched upon.

Slack space is, essentially, the end of a file to the end of its cluster, while free space is the room on the disk that is not being occupied by a file. When a file is deleted, it is essentially marked as free space, but the data therein is not actually erased. Being marked as free space means that the cluster, which that data occupied, is now free to be written over with a new file.[8] If nothing else is written to this cluster, then the original deleted file is still there, though not accessible through normal means such as windows explorer or a command prompt. However, the data is still there and using the proper tools discussed below it will be copied over to the clone drive, and therefore, will be accessible using the proper forensic utilities. This is important for obvious reasons, as it will enable the investigator to see what the suspect offender has deleted from their computer, and these files may come into play as crucial evidence.

So, how does one perform such a backup? Simply copying the files over doesn't work and will not hold up in court as being forensically sound evidence. Some software tools, which perform such tasks to standard, are Guidance Software's' Encase and New Technologies Inc.'s (NTI) Safeback. They accomplish the cloning process as described above. These tools have also been proven to meet the rigorous legal standards of our court systems are used by numerous law enforcement agencies as well as corporations.[9] Training on these tools is essential and is available through the vendors. Training usually consists of approximately a week of disk structure, data mining, rules of evidence, other aspects of computer forensic basics, and how that particular vendors software tools are used to accomplish these tasks. Understanding the basics of computer forensics is crucial for any CIRT. Without the knowledge of disk structure and the capabilities of these tools, the potential of corrupting evidence is almost certain.

Another tool, which is a hardware/software combination and has proven to be very effective is the Forensic Solitaire, manufactured by Logicube. This device (pictured below) is capable of achieving the forensic quality bit-stream backup. What separates it from some of the other tools is that it is very easy to use. It has been designed for use

---

[7] New Technologies Inc.
[8] Cole & Kolde

[9] Logicube & Guidance Software

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

by criminal investigators, who are often not computer experts, and therefore the training time on it is minimal. It has help desk support and is very easy to trouble shoot even for non-technical people. The Solitaire is definitely a tool that any CIRT addressing these types of issues will want as part of their arsenal. Another advantage point to be made about the Solitaire is that it clones subject drives extremely fast. The vendor boasts of cloning speeds in excess of 975 MB per minute.[10] I have used this device on numerous cases and have yet to attain quite that speed, but transfer rates of well over 800MB per minute are the norm! This speed is crucial since hard drives are now exceeding 20GB for laptops and 100GB for PCs. And remember these devices copy the entire drive, not just the files, so speed on these sized drives is crucial for an efficient investigation. Trying to clone a 20GB drive image through the parallel or USB port to a tape drive could take literally an entire working day, whereas the Solitaire device can accomplish this task in less than an hour. The Solitaire also has accessories available such as the "clone card" which enables the forensic expert to clone a laptop hard drive through the PCM/CIA slot in cases where the hard drive is inaccessible. This process is a little slower, but I have still averaged around 100 MB per minute using this method. Another positive aspect of this tool is that it conducts a CRC-32 check at the end of the cloning process.[11] This essentially checks and confirms that the clone is in fact an exact replica of the subject drive. Verifying that an exact clone has been made is crucial in order to qualify for the conditions established in the first rule of preserving evidence.

Once the clone has been made the investigator can now utilize the other tools in his/her arsenal to data mine the drive for evidence while not having to worry about corrupting the original evidence. If the clone is destroyed or corrupted a new one can easily be created.

Another point, which needs to be addressed, is that the media on which the clone is being copied to needs to be free of any and all previous data and viruses. Antivirus tools should be run on the potential clone and then a secure delete program should be run to ensure that data from previous investigations or uses is not on the disk. Any leftover data on the disk would corrupt the new image and therefore violate the first rule of evidence. Both NTI and Encase have such tools such as "Disk Scrub" and the Solitaire device can also be configured to automatically and securely erase the target disk before beginning the cloning process. The secure deletion process works by writing over all data on the media with random characters. Each program has its own specific method but they are essentially the same. For example NTIs "Disk Scrub" gives one the option of how many times the disk is to be written over and what characters one wants to use. By default it uses zeros, ones and Ctrl F6 characters to write over the entire disk. These programs do not just write over system files and documents. They write over the disk sector-by-sector. Just like with the cloning process, this sector-by-sector write over is important because it includes the slack and free spaces in the process. The speed of these overwrites depends on how many passes the user wants it

[10] Logicube
[11] Id.

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

to make. My experience using Disk Scrub on 12 GB laptop drives with 3 overwrite passes averages about 5 minutes. So there really is no reason to neglect this crucial step in preserving evidence since it is fast, easy and essential.

The Logicube Forensic Solitaire[12]
http://www.logicube.com/products/solitaire_forensic.html

The second rule addresses the issue of preservation of evidence. Simply put and continuing with the same example, the subject drive is now preserved in a safe place where it cannot be tampered with. Ideally this would be in a secure evidence room. Considerations in making such a room secure include, limited access, motion sensors which security can respond to during off hours, and floor to ceiling walls to prevent someone from crawling through ceiling tiles from an adjacent room. Also evidence should be protected in a secure, and ideally fireproof, locker away from magnetic sources. It should be noted that some cases could take years to prosecute so the long-term preservation of evidence is crucial. In addition to the above steps, making a tape back up of the subject drive in addition to the initial working back up is a very good idea. This allows the investigator to perform forensics on the working backup while having a tape backup for long term secured storage, perhaps offsite, thereby ensuring that the evidence will be preserved even in the event of a catastrophe or additional criminal act.

The third rule of proper evidence handling addresses the chain of custody issues. The notion of chain of custody is meant to ensure that the evidence is always accounted for. Once a computer is seized, a list of who comes in contact with it needs to be kept, and those coming in contact with the evidence should be as few as possible and include only members of the investigative unit or law enforcement. Also such a log should include the details of the evidence (such as model and make of laptop), the dates and times that these people had custody of the evidence as well as what actions they took on it if any. This is meant to prevent the modification of evidence by a third party, which would render it inadmissible in court or subject to negative scrutiny by defense counsel.

[12] Logicube.

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

Any CIRT should have well documented procedures detailing how such a seizure should take place, who should be notified and who should handle the evidence. This is especially important in any large corporation where, for example, a CIRT based in Chicago simply may not be able to fly at a moments notice to London to seize a computer and perform a forensic backup. In this case, perhaps a human resources person or supervisor will be tasked with securing the computer and sending it to the CIRT. This individual needs to have a checklist detailing the required step-by-step process of seizing and securing evidence, since the human resources person or supervisor will most likely lack the requisite expertise. The checklist needs to be extremely basic and designed for a non-technical person in order to ensure success. NTI software has helpful tools for this such as disks that can be inserted into floppy drives to prevent inadvertent booting of the system. If the system is inadvertently booted with this special disk in place, the boot process usually hits the floppy first which displays a message stating that the computer is crucial evidence and should be powered down immediately.

The final step of documentation is simple to follow and crucial to a successful investigation and subsequent successful prosecution. Without it, the best evidence tools and experts will not be able to convince a judge and or jury that the evidence is sound. Once again, the Solitaire comes in handy as it prints a report at the conclusion of the cloning process which details the types of drives used as well as the confirming CRC check, the date of backup and the success of the backup. NTI and Encase also have similar utilities and reports are available in each of these software's tools detailing times, dates and specifics of findings. The more documentation there is, the less likely that human intervention could alter data and corrupt evidence.

Summary

At this point the reader should have a basic understanding of the important role and necessity for well-trained corporate investigators in the area of computer forensics. In addition the key issues of preservation of evidence, chain of custody and documentation of procedures have been explored on a basic level. This gives the reader a good starting point for what needs to be considered when forming a CIRT tasked with such an investigative role, as well as some of the tools and training available to accomplish this crucial and challenging mission.

References

1. Robbins Judd. "An Explanation of Computer Forensics." 5 December 2001.
   URL: http://www.computerforensics.net/forensics.htm

2. Logicube "The Solitaire Forensics." 5 December 2001.
   URL: http://www.logicube.com/products/solitaire_forensic.html

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

3. Guidance Software "Encase." 5 December 2001.
URL: http://www.guidancesoftware.com/html/encase_ver3_overview.html

4. Davis, Richard A. (2001e) "Internet Abuse in the Workplace." 6 December 2001.
URL: http://www.internetaddiction.ca/cyberslacking.htm

5. New Technologies Inc. "Computer Evidence Processing Guidelines." Computer Evidence Processing Steps. 20 April 1999: 1-6.

6. Cole E. & Kolde J. "Disk Imaging." SANS Security Essentials V: Windows Basics 10 August 2001: 5-8.

7. Anderson, Michael R. "Good Documentation Is Essential." Computer Evidence Processing. 1998: 1-2.

© SANS Institute 2001, Author retains full rights

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

Last Updated: May 25th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
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
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 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 San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	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 Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced