A Series of Electronic Forensics Papers

by

Dr. Henry B. Wolfe

Published in

Computers & Security

ISSN: 0167-4048

Volume 22, Numbers 1-8

Computer forenics

Dr. Henry B. Wolfe

Associate Professor
Computer Security & Forensics
Information Science
Department
School of Business
University of Otago
Corner of Clyde & Union Streets
P.O. Box 56
Dunedin
New Zealand

Tel: (+64 3) 479-8141
Fax: (+64 3) 479-8311
Email: hwolfe@infoscience.otago.ac.nz

Introduction

Computer forensics has been around for a while, but is fast becoming a specialized and accepted (in a court of law) investigative technique with its own tools and legal precedents that validate the discipline. It is a computing profession dedicated to finding the truth. That sounds very altruistic, but any good forensics person with any kind of ethics does only that: finds the truth. It is not in our domain to assign guilt or innocence but rather to find facts in the form of electronic evidence that can be presented in a coherent way so that others may weigh that evidence and then assign guilt or innocence where appropriate.

The bad guys have been shifting their attention away from armed robbery to computer crime. The payoff is much greater and the probability of ever being caught, much less being prosecuted, is significantly lower. An armed bandit walks into a bank and gets an average of $7000 give or take, is likely to be caught and is likely to be prosecuted and do hard time — two to five years or more. On the other hand, a computer crook can expect to steal $250 000, not be caught and even if he is caught will do minimal time inside — if at all. Many countries currently do not have laws that govern computer related crime.

Most readers do not know any bad guys and believe the stereotype shown on TV and in the movies to be accurate. That typical crook is stupid and always gets caught. It would be a mistake to believe that all bad guys are dumb. Quite the contrary. Many are bright, but the two things most of them do have in common are that they are lazy and lack moral values in sync with the rest of society.

As we all know, the shift to computer-related crime has been swift. Therefore, the need for professionals capable of performing electronic investigations that can produce the necessary evidence to convict continues to grow.

This column will be devoted to revealing the skills, talents, methods, techniques, tricks, and tools that are necessary to gather, analyse and present electronic evidence. We welcome your comments, questions, criticisms and contributions.

Validating electronic forensics

Like any new evidentiary technique electronic forensics too has had to be validated. In the late 19th century, fingerprints had to be proven as valid evidence and have become one of the most valuable trace evidence types in use today. In the 20th century the uniqueness of striations found on fired bullets became a valid method of tying a gun to a specific crime.

The polygraph, for example, has a long and colourful history of being used to distinguish between truth and falsehood, however, this has no basis in science and is therefore, not valid in any court of law. The reason for this is that there has never been a scientifically controlled study that proves conclusively any linkage between physiologic change and truth or falsehood. It has been investigated in 1965, 1976 and again in 1983 by the Office of Technology Assessment (formerly an office of Congress) who concluded: "There is very little research or scientific evidence to establish polygraph validity." Justice Thomas in US vs. Scheffer (No. 96-133 — March 31, 1998) in his opinion stated: "scientific field studies suggest the accuracy rate of the 'control question technique' polygraph is 'little better than could be obtained by the toss of a coin,' that is, 50 percent".

0167-4048/03

Not all evidentiary techniques put forward are or have been accepted. In the US, for example, there was a precedent setting case in 1993 Daubert v. Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579 (1993). That case in America at least, lays out for those who follow, a set of five elements that must be achieved in order for evidence gathered by an unproven technique to be accepted:

1. Whether the theory or technique can be and has been tested.
2. Whether it has been subjected to peer review and publication.
3. The known or potential error.
4. The general acceptance of the theory in the scientific community.
5. Whether the proffered testimony is based upon the expert's special skill.

Other countries will have their own precedents that validate electronic forensics evidence gathering methods. The tools, techniques and methodologies of electronic evidence investigation, gathering and analysis have been tried and proven and are accepted in many countries.

Forensic evidence in computing

The gathering of evidence in a computing environment is not merely copying files from the suspect's computer and printing them out for presentation in a proceeding. While that indeed may be an important part of it, there is data that may be pertinent to such proceedings that is not readily or apparently available through ordinary means. Moreover, accessing and finding such data requires specialised tools and knowledge. This and future columns will introduce to the reader a body of knowledge enabling him/her to become aware of what kinds of information exist on a PC and how to go about gathering and preserving the original data and making certified copies of that evidence.

Exactly where data is stored and how PC operating systems deal with files and reading and writing to disk will be described in detail. Other locations of where information may be stored purposely to avoid discovery will also be detailed and discussed, as will methods and tools for browsing those locations as well as making copies of relevant data that might be found there.

Deliberately disguised information in the form of encrypted, misnamed or steganographically hidden data will also be explained. In certain cases we will be able to decrypt data found to be encrypted and the means to do so will be explained and sources noted. In others we will only be able to flag the disguised data and further action will need to be instituted by a Court of Law — should it be warranted.

Preparation for an electronic investigation

The first thing that usually must be done is to gain access to the target machine, passwords and associated offline storage. This may be accomplished by obtaining a search warrant, civil court order or the consent of the owner. In cases where seizure is required, most forensic investigation will take place in a controlled environment i.e. the forensics laboratory. Only in rare instances will the acquisition of the evidentiary copy be taken in place — outside the lab.

To facilitate the smooth issuing of a search warrant the investigator must avoid electronic jargon and translate into simplified legal terms that which is necessary to obtain the legal documents required to gain access to potential evidence.

Once the necessary permissions have been obtained, a plan should be made. Some seizures are simple enough not to have a plan, however,

Henry B. Wolfe

Henry B. Wolfe has a long computing career spanning more than 43 years. He currently specializes in cryptographic problems where related to forensic investigation, general computer security, surveillance, and electronic forensics teaching these topics to law enforcement (both in New Zealand and internationally) as well as at the graduate level in the University of Otago located in Dunedin, New Zealand where he is an associate professor.

planning ahead of time increases the probability that during the process the investigator will not miss any vital clues or available data.

Every investigator who is required to seize equipment should have a toolkit that contains the appropriate equipment, forms and supplies. To begin with the requisite documentation needs to be present. The first and most important form documents the chain of evidence. The term 'chain of evidence' refers to documenting the identity (description), custody and control of evidence (who was in possession) from the instant when it is collected (by whatever means) through and beyond its final presentation in a court of law. If the chain of evidence is broken, that is, if it is not possible to account for the entire time between seizure and presentation then the evidence could become compromised and, therefore, invalid — unacceptable in a court of law.

Storage of evidence when not in use is normally in a controlled secure vault or lockup of some kind. Electronic media should be stored in a data storage cabinet within that lockup.

Job sheets can be used to manage the various tasks assigned to investigative staff. These identify the case, describe in detail the equipment seized, and provide a history of the various techniques used to extract evidence as well as their results.

The toolkit should also contain an electronic camera. This is used to document the environment where the computer and associated devices, documentation and associated materials are located. Often passwords and cryptographic keys are within the view of the owner to ease remembering these details. The photographs could provide clues to or actual values of keys and passwords. It is also used to document the positioning of the various cables and connections to the computer and other devices. Later this documentation will be used when building a working clone for analysis purposes.

Plenty of rubber gloves should be available (remember that trace evidence often plays a part in electronic evidence gathering, therefore, the same precautions to protect any trace evidence must be taken as for any other evidence). We always wear two pairs of rubber gloves. The reason for two pairs is that there are generally lots of sharp bits that we must handle during a seizure in a computing environment and rubber gloves are susceptible to being torn easily. We do not want to contaminate any trace evidence that might be present and, hopefully, the second pair will remain in tact even if the outer pair is breached.

Finally, the toolkit should contain plenty of labels, coloured pens, tags, evidence bags, plastic ties and coloured tapes. These are used to transport and to identify every item seized and to make it possible to exactly connect the right cable to the exact device that it was connected to at the seizure site when building a clone in the laboratory.

We'll leave it here for now and continue with the seizure process next time. Remember, if you have questions or comments (critical, complimentary or helpful) please do contact us.

The circumstances of seizure

Dr. Henry B. Wolfe

Associate Professor
Computer Security & Forensics
Information Science Department
School of Business
University of Otago
Corner of Clyde & Union Streets
P.O. Box 56
Dunedin
New Zealand

Tel: (+64 3) 479-8141
Fax: (+64 3) 479-8311
Email: hwolfe@infoscience.otago.ac.nz

Introduction

In our last column we discussed the basics of computer forensics, trying to describe a basis for validating evidence captured using well-documented and accepted methods and tools. This is still a very new discipline and precedents are few and perhaps there will be many yet to come before findings based on it are accepted as readily as fingerprint evidence is today. Nevertheless, I believe that electronic forensic evidence gathering will become a commonly used investigative technique of ever increasing importance.

This column is devoted to the process of seizure. On the surface it may seem not all that complex, however, every circumstance is different and therefore so too may be the complexities of any given seizure.

The plan

The first thing that you need to do in the seizure process is to plan the seizure. This requires that you know all you can about the case and the suspect prior to presenting your warrant. It will help you decide what equipment and other materials you will need to bring to the seizure. The planning process does not have to be formal or require a huge expenditure of time and energy; however, it is better to approach the process armed with as much knowledge as you can.

Once the warrant has been secured, the officers in charge will determine the timing of the event. It is not normally necessary for forensic investigators to be sworn officers and therefore our activities are carried out after the scene is secured with possibly some advice or assistance in the way it is secured. It is important to know what you're looking for. In one case that comes to mind, the suspect was arrested elsewhere and a constable was dispatched to the suspect's apartment to pick up the suspect's computer. When he returned he presented the forensics people with a monitor and keyboard. When asked where the rest of the computer was, he said that was all there was. The investigators then visited the suspect's apartment and discovered a complete and working Intel 486 inside a cardboard box in the closet. The only noticeable bits were on one side of the closed cardboard box and they were an air circulation fan, floppy disk slot and various other plug ports (power, serial, parallel, mouse, etc.). The constable didn't see the cardboard box as a computer and wasn't really trained as to what to look for.

The seizure

After the warrant is presented, it is vitally important to separate the suspect/owner from the computer immediately. That is perhaps the most important part of securing the scene. If this is not done, it may be possible for the suspect to initiate a process on the target machine that overwrites the contents of the hard drive. Most likely that is where the majority of any usable evidence will be found. If it is overwritten before the investigator is able to make an evidentiary copy, then the likelihood of recovering any useful evidence from the overwritten hard drive is seriously diminished. It may still be technically possible but at great expense. In most cases, the expenditure may not be able to be justified. The FBI is apparently getting good results using a technique called Second Harmonic Magneto Resistive Microscopy. This makes use of an electron microscope and very specialized software, but it is expensive.

From here on out it is advisable to use a checklist to ensure that every step of the

process is carried out and that these are done in the appropriate sequence. The sequence may be very important in some cases and less so in others, however, following the process will instil good work habits and lessen the chance of forgetting anything or making errors. It also facilitates good documentation along the way.

The interview

Interview the owner/user/suspect (and others involved if there are any) and record everything that is said. It is important to tie the suspect to the machine. Obtain a written statement regarding ownership and use of the equipment from the suspect. This may prove useful later when and if the case is tried. Document all contact and remarks made by any of the accused that are present. Ask for passwords: BIOS, system login, network or ISPs, application files, encryption pass phrases, all user names and accounts for each ISP used, names of all ISPs used, and the location(s) of any offsite data storage used or controlled by the suspect. If the suspect refutes ownership and/or use, then it may be necessary to revert to conventional forensic trace evidence methods i.e. fingerprints, DNA, etc.

During the interview(s) it is important not to forget small devices that the suspect may have on his/her person. There are a number of small storage devices that one could pocket that are capable of significant storage capacity. For example, PCMCIA cards can hold a couple of gigabytes, as can the USB key chain dongles. Micro drives can hold a gigabyte and there are various flash memory devices that can hold many megabytes. Java buttons and rings are very small but are capable of holding passwords, encryption keys and encryption software as well. All of these devices may be relevant to your case but if you do not ask for them or have the subject physically searched to find them or do not recognize their potential for storing important evidence then your case may fail as a result.

Document, document, document

If conventional forensics methods are required, first photograph the scene. A complete set of photos is needed taken in 360 degrees as well as specific photos of both front and back of any computing equipment and any associated equipment. Many investigators prefer to use a digital camera for this purpose for two reasons. First, the images are immediately available and second, the images can be incorporated easily into the final report where appropriate.

After fingerprints, etc. are taken, gather and document all relevant evidence. This would normally be any papers or other documents, documentation of any kind (hardware, network, etc.), software and its documentation, books, sticky notes, photos, floppy disks, CDs, etc. All of this is labelled and bagged in the appropriate containers — static proof bags for magnetic media, evidence bags for materials that require them, paper sacks and cardboard boxes for papers and documentation, etc. As well, all items seized must be described and itemized on an inventory documentation form. Documenting everything may seem tedious and time consuming, but it makes it possible to account for everything when and if that becomes necessary. When the seized property is returned to the owner it is also important to be able to account for each item seized to ensure that it is all returned. Moreover, it begins the 'chain of custody'. This refers to the principle that once seized, everything seized can be shown to be controlled by the seizing organization from the time seized through (and beyond) a trial in a court of law. It must be stored and protected beyond in case the verdict is appealed and the evidence is needed for the appeals process intact as well.

Electronic forensics refers to evidence found on devices other than computers too. Relevant evidence may be found in many other devices, For example digital cameras can potentially hold: images relevant to the case, sound, video,

Henry B. Wolfe

Henry B. Wolfe has a long computing career spanning more than forty-three years. He currently specializes in cryptographic problems where related to forensic investigation, general computer security, surveillance, and electronic forensics, teaching these topics to law enforcement (both in New Zealand and internationally) as well as at the graduate level in the University of Otago, located in Dunedin, New Zealand where he is an associate professor.

time and date stamps for these images. Scanners might have imperfections or marks on the glass that could tie them to specific images involved in the case. Scanner software may still hold an image of the last thing scanned. Photocopiers can potentially hold: user logs, documents, time and date stamps for these documents. Fax machines could hold documents, film cartridges with data on them, phone numbers, and send/receive logs. Answering machines could hold caller IDs, deleted messages, last number called. Cell phones could hold address information, email, phone numbers, text messages, voice messages, appointment calendars, etc. Then there are pagers, PDAs, voice mail devices and others. So you can see that the computer may form only one of many sources of potential electronic evidence.

Once the interviews are complete and the other evidence has been collected and bagged, it is time to deal with the computing gear. The photos are again taken once all of the wires, cables and devices are tagged and labelled. These will provide a picture of how the suspect's computer was physically set up so that in the lab it can be duplicated exactly if necessary. Tagging and labelling also enables the investigator to keep track of everything recorded on the seized inventory form.

It can still go wrong – even if you do it right

There's an anecdote that has been circulating in this profession about doing it all correctly. The suspect was immediately separated from the equipment. He stood passively in one corner of the room away from everything to be seized. Everything was documented in the proper way and stored in the appropriate containers. All was transported to the forensics laboratory. The computer equipment was not on, so no special procedures were necessary. Everything was tagged and labelled and photographed. However, when the suspect's hard drive was connected to a forensics machine and its contents inspected it was found to contain nothing. There was no operating system, software, or data files. In fact it was unreadable. The investigators returned to the suspect's premises to investigate further and after some time discovered a switch under the carpet in the corner of the room where the suspect had stood during the seizure. That switch turned the power on to a degaussing device located inside the doorframe. When the investigators removed the computer from the suspect's apartment all magnetic devices within them were degaussed rendering the contents of hard drives and floppy disks useless.

In most cases an evidentiary copy of the suspect's hard drive(s) is made in the electronic forensics laboratory. This is done using a purpose-built machine designed to physically block the write function of the suspect's hard drive unit being acquired. We'll talk more about that in the next column. In some cases, the investigator may not be able to remove subject computers (for example in the case of an ISP whose livelihood is based on the service provided by their machines). There is a different set of procedures that should be followed in such cases. Usually you are dealing with very large storage capacity hard drives or RAID arrays. In order to acquire an evidentiary copy of such devices, it may be necessary to use specialized acquisition equipment. This might be a very high speed LTO tape unit that in addition to is speed also has a very high capacity storage. Typical LTO tapes can hold in excess of 200 gigabytes. This highlights one aspect of electronic forensics. It is a field that requires many different specialized devices — each with a particular purpose. This equates to money. It is expensive to provide the tools necessary to be in a position to deal with the many different situations encountered.

We'll leave it here for now and continue with the process of acquiring data evidence next time. Remember, if you have questions or comments (critical, complimentary or helpful) please do contact us.

Evidence acquisition

Hank Wolfe

Associate Professor
Computer Forensics & Security
Information Science Dept.
Otago School of Business
University of Otago
Corner of Clyde & Union Streets, P.O. Box 56,
Dunedin, New Zealand
Tel: +64 3 479-8141
Fax: +64 3 479-8311
Email: hwolfe@infoscience.otago.ac.nz

In our last column we discussed the seizure process, stressing the important elements of planning, methodology, interviewing, documentation and thoroughness. The acceptability of evidence gathered will be influenced and possibly accepted or refuted as a result of carrying out the tasks described by these elements in a professional and methodical way. Each step by itself cannot make a successful case, however, any step that is flawed or missed may cause a case to fail.

This column is devoted to the acquisition process. This activity, when done properly, forms the basis for further analysis of data and provides the potential for capturing relevant evidence. The methodologies followed during the acquisition process are critical to the validity of any evidence found. In addition, following a formal plan will ensure that all relevant data is captured for later analysis.

Data acquisition

Let's begin by taking a look at data acquisition. This process may be defined as capturing a complete evidentiary copy of the contents of all discovered storage devices. That means a bit-wise copy using specifically designed tools to accomplish that task. On any hard drive there are many pieces of data that are not specifically tied to a file — for example unallocated space. Using the Windows or DOS copy command to acquire evidentiary data will miss capturing all space that is not currently active as well as other special file types (for example system or hidden files, etc.). The key term here is active. Once a file has been deleted, it has **NOT** been removed from the media — it is **NOT** erased. The only thing that happens is that the first character of the deleted file in the File Allocation Table is changed to a hexadecimal '**E5**'. That character tells the operating system that the space (clusters) associated with that entry is now available for reuse. The data located at the associated address on disk will remain intact until such time as it is completely or partially overwritten. A hint for new players: if you mistakenly delete an important file, because of the way that disk space is managed, it may be possible to recover it. That possibility will be influenced by the amount of time that has elapsed since it was deleted. The probability of a successful undelete diminishes as the amount of time, and therefore usage since the file was deleted, increases.

There are a number of different types of media from which we may capture potentially useful evidence. The obvious devices that everyone immediately thinks of are hard drives, floppy disk and CD. These of course are the primary sources of useful evidence, but there are many other storage devices. Some examples of other devices are magneto-optical disks, USB flash memory dongles, PCMCIA cards, iButtons®, micro hard drives, digital flash, memory sticks and the list grows as does their respective capacities. Most of these have substantial capacity for holding data and some are very small and easily concealed. At the same time, for those that require it, there are specialized readers that can access each type of device. These readers will be (or should be) available in most forensic labs. The problem is usually not the ability to read the particular device; it is the cooperation necessary to find out that one or more has been used by the suspect and then to gain access to them. As mentioned in the previous column, the interview, search and seizure process must take into account the need to discover and seize such devices if the suspect has used them.

Acquisition process

The investigator will have a couple of options available. The preferable option is to seize the suspect's equipment and associated storage media, return it to the laboratory and perform the acquisition in the lab. This allows the investigator to control the environment and process the seized media in the optimal way with specialized equipment readily available — for

Henry B. Wolfe

Henry B. Wolfe has a long computing career spanning more than 43 years. He currently specializes in cryptographic problems where related to forensic investigation, general computer security, surveillance, and electronic forensics teaching these topics to law enforcement (both in New Zealand and internationally) as well as at the graduate level in the University of Otago located in Dunedin, New Zealand where he is an associate professor.

those circumstances where it is needed. It also provides an environment that is less stressful thus reducing potential mistakes caused when people are under pressure, in unfamiliar surroundings, and in a hurry. It is natural to overlook things when you are in a hurry and the laboratory environment helps to reduce that risk.

The second option is to make the evidentiary acquisition on the spot. This may be a requirement based on the type of case. It is likely that capturing an evidentiary copy of an ISP's RAID array will take place on site. In such cases, it may not be reasonable to seize the machine and by so doing, potentially put the ISP out of business. This requires that the investigator be equipped with a portable forensics (field) machine and associated software and hardware tools appropriate to the task. This portable machine can easily be constructed with mostly off the shelf parts; however, there are ready-made forensics systems available for a price (Vogon for example produce such a product).

In either case it is important to ensure that the suspect device being copied is physically write protected. This is important when you get to court and the opposition asks for proof that the contents of the original storage device have not been modified. The second reason is that the last thing any investigator wants to do is overwrite the suspect's hard drive and lose or corrupt any potential evidence. Vogon's forensic machine has this physical protection. Guidance Software produces a product called Blocker that can be incorporated into your locally built forensics machine to provide this capability — and there are others. While various vendors may be mentioned in this series on forensics, it should not be misconstrued as an endorsement of any specific product.

Evidentiary media

An investigator has a number of media onto which the bit-wise copy may be recorded. High-speed tape is one of them. There are three or four formats that could be used. Linear Tape Open (LTO) is a very high-density tape that can record up to 200 gigabytes per tape. It is fast and reliable. Digital Linear Tape (DLT) is another high-speed high-density tape format with a capacity a bit less than LTO. Finally, there is the old reliable inexpensive DAT tape used for standard backup purposes. It is slower and can hold less but is inexpensive. The specific laboratory will have to decide where its priorities lie in the choice of tape format. Speed and capacity has a cost — but it may be warranted based on the volume of cases investigated.

The second media is the use of a hard drive for the capture. This is a fast inexpensive and reusable alternative to tape. Normally, the acquisition is done to an alternative hard drive of the same capacity and later in the laboratory, when more time is available, a CD or DVD copy is made and authenticated for permanent storage. This technique requires an inventory of hard drives of various capacities. If this procedure is used, the target hard drive used to capture the bit-wise copy of the suspect's hard drive must be sanitized **PRIOR** to the procedure. Sanitizing the forensic hard drive is accomplished by doing a bit-wise overwrite of the entire drive so that there is absolutely no residue data remaining on the device. This process can be done quickly and easily using a field or laboratory forensics machine with the appropriate forensics tool, which would normally reside thereon. Additionally, it should be done prior to the investigation of any given case so that the forensics disk is immediately ready for use. However, it is not a good idea to carry out this procedure while a suspect's hard drive is connected to the forensics machine. This happened in a recent case and the suspect's drive was accidentally overwritten as a result. Case closed!! This is a good example of why a set of formal procedures is necessary for forensic work and more important, that all investigators follow them.

Acquisition validation

When making the evidentiary bit-wise copy of the suspect's storage devices, it is vitally important that the copy is validated to ensure that it is a provable bit-by-bit copy of the original. This process makes use of hashing algorithms. A hashing algorithm reads a string of data and from it produces a unique value — a fingerprint of that string of data. That data can be a few characters, a single or multiple files or the contents of an entire hard drive. If so little as a single bit is changed in the string and the identical hashing algorithm is used to create a second hash value of the changed string the two values would be different. There are different hashing algorithms used for forensic purposes — Cyclic Redundancy Check (CRC), Message Digest 5 (MD5), etc. However, all hashing algorithms are not created equal and the assessment of which is best should be left to those in the cryptographic arena most qualified to judge. MD5, created by Ron Rivest, seems to be one of the most commonly used and produces a 128 bit value for each string assessed. Both hash values (of suspect drive and the evidentiary copy of that drive) must match and must be incorporated into the forensics report to demonstrate the successful authentication process. Furthermore, the investigator should be prepared to replicate the process to demonstrate the authenticity of the evidentiary data.

Evidence handling

Once the evidentiary copy is made and validated, it is wise to make and validate another working copy from it. The original should be appropriately identified, labelled and then be lodged in the normal evidence lock-up where it should remain. The working copy can be used to build a clone of the original suspect machine where necessary. This process may not be necessary, however, because the forensic analysis tools available can use the working evidentiary copy to search for specific words or phrases, view graphics files, reconstruct deleted files, analyse time lines and Internet logs and for many other purposes. From this analysis, potential evidence is collected and incorporated into the final investigator's case file and report. Throughout the processes discussed in this column, various activities must be logged and documented.

The possession of the evidence is especially important. The 'chain of evidence' refers to the idea that evidence once captured or seized is never out of the control of the authorities who have captured or seized it and that all usage and access to that evidence has been documented and that **ONLY** authorized personnel have had appropriate access to it for official use. This documentation is vital to every case. In the event that any evidence cannot be tracked, for the entire period between its acquisition and the final appeal (and potentially the statutory period thereafter), a court is likely to exclude the use of that evidence.

The business of Electronic Forensics is complex and comprehensive. These columns are not meant to be all-encompassing training for forensic investigators but rather an introduction to the profession. The objective is to raise the awareness of and interest in the discipline. For those practitioners who read this and reflect that this is incomplete or that doesn't go far enough, please be aware that this is an awareness program designed to raise the profile of the profession. We'll leave it here for now and continue with the analysis phase of the forensic process next time. Remember, if you have questions or comments (critical, complimentary or helpful) please do contact us.

Evidence analysis

Introduction

In our last column we discussed the evidence acquisition process stressing the chain of evidence and the importance of following a documented method. These two issues are important in order to ensure that the evidence captured will be acceptable in a court of law — provided that it is relevant to the case at hand.

This column will be devoted to the analysis process and assumes that the previous steps in the whole evidence gathering process have been correctly followed. Once again, the preceding steps are vital enabling us to pursue the analysis of raw data and to produce the finished relevant evidence.

Where's the evidence?

First we need to describe where evidence may be located on any given system. There are three basic types of data that may also be evidence: open or known data that anyone familiar with computing would know about, unknown or less known data that the average user may not be aware of, and finally, hidden data that has been deliberately disguised or deliberately hidden (or both) in a location where data is not normally located.

Known data is comprised of all visible files including the operating system (Windows or Linux and all their associated files), applications software (Word or Excel or CorelDraw or other user tools and all of their associated files), data files created by one or other of these, and configuration files required by certain software residing on the user system; basically, any file that can be seen by a directory command or Windows Explorer. These files are easily accessible and also have associated with them specific time and date information that may provide relevant time line evidence to your case. In addition, data files created by one or other application tools may contain other relevant evidence associated with your case.

Less known data is comprised of unallocated space, Windows work space, and file slack space. Unallocated space is the non-active disk space that is currently available for use (active space contains files that have not been deleted). This includes space not yet written to and deleted files that may not have been overwritten yet or fragments of deleted files that may have been partially overwritten. When a file has been deleted, it is not removed from the hard drive. The only thing that happens is that the first character of the deleted file name in the File Allocation Table is changed to a hexadecimal 'E5'. This code tells the operating system that the associated clusters are now available for re-use. When the operating system or applications program needs space to store a new or temporary file it looks to the File Allocation Table to find that space then overwrites whatever was there before. Until such time, however, the space contains whatever was there at the time of the deletion.

Slack space refers to the space at the end of a cluster that is not used by the file currently residing in that cluster. The smallest piece of data that can be written to a hard drive is a cluster. Each hard drive has its own cluster size depending on the capacity of that hard drive. Cluster size can vary in multiples of 512 bytes up to 65 536 or more. If a file's actual size is less than the exact cluster size or an exact multiple of the cluster size then at the space not required by the file at the end of the last cluster will contain whatever was there before the current file was written there. This slack space is a useful source of information that the user may think no longer exists on their computer.

The Windows operating system automatically creates its own swap file of 20 megabytes or

Hank Wolfe

Associate Professor
Computer Forensics & Security
Information Science Dept.
Otago School of Business
University of Otago
Corner of Clyde & Union Streets, PO Box 56
Dunedin, New Zealand
Tel: +64 3 479-8141
Fax: +64 3 479-8311
Email: hwolfe@infoscience.otago.ac.nz

Henry B. Wolfe has a long computing career spanning more than 43 years. He currently specializes in cryptographic problems where related to forensic investigation, general computer security, surveillance, and electronic forensics teaching these topics to law enforcement (both in New Zealand and internationally) as well as at the graduate level in the University of Otago located in Dunedin, New Zealand where he is an associate professor.

more. This is used for temporary storage by the operating system and can contain anything that Windows has placed there including passwords, encryption keys and potentially useful other data as well. This file is not normally viewable by Windows Explorer and is automatically hidden by the operating system.

Finally, there is data that has been deliberately hidden or disguised in some way. There are various hiding places on a hard drive. When a hard drive cluster takes more than a given number of reads to access it, the operating system interprets that fact to be an indication that the offending cluster may become unstable. This triggers the movement of the contents of the unstable cluster to another address on the hard drive and the flagging of the unstable cluster as 'bad' (also known as 'bad blocks'). Thereafter, the operating system ignores that flagged space and will not attempt to access it. If the operating system can flag clusters as being bad, so too can any programmer who understands how and so too can he/she gain access to the space flagged as bad. Therefore, bad blocks can be used to hide information that is either in plaintext or that has been encrypted (ciphertext). The space at the end of the partition table is normally never used and neither is the space at the end of the boot sector. These are a few examples of places where data can be hidden — and there are more.

Data can also be hidden within other data. It is possible to hide text within sound files, image files, executable files, as well as other file types. This technique is referred to as steganography and there are many freeware, shareware and proprietary products available to accomplish this sort of task. To the casual viewer carrier files do not appear to have any visible or noticeable indicator that would identify the carrier as being used for steganographic purposes. To provide added privacy, some of these steganographic programs also provide an encryption capability.

That brings us to encryption. Of course, it is possible to encrypt data that is confidential in order to ensure its privacy. In fact, everyone is entitled to do so and without prejudice as to their purpose for doing so. The mere fact that someone chooses to encrypt data should not be used to infer criminal intent. In a future column, we will deal with this subject a little more thoroughly.

As you can see, there are plenty of opportunities for an investigator to find evidence if it exists on a computer system. Our task at hand is to discuss how that might be accomplished.

Analysis tools

In the first instance, the forensic investigator will need purpose built forensic tools to be able to analyse the contents of a suspect's data storage devices. We've already mentioned the acquisition software. Our next set of tools will be used to perform the analysis. The better tools will facilitate the analysis of all or most of the storage contents as outlined above. They will provide for string searches of all or subsets of the storage. Some tools will have overlapping functions. For example EnCase is a fully functional acquisition tool as well as a powerful analytical tool. Other analysis may be performed by specialized tools that have only a single purpose. For example, IsEncrypted is a tool created by Access Data that identifies data files that have been encrypted by applications software that it is programmed to search for. That is its only function. Once the encrypted files have been identified, the investigator can then proceed according to their organizational protocol.

Most forensic investigators have an entire library of tools and over time evolve a particular preference for the main analytic tool as well as the sequence in which they perform the analysis. Some tools are in the public domain and some are not. There is an argument for the

preference of well-known and proven standard tools. It is easier to defend the methodology for one of these in a court of law because most of the initial proving of the tool has been done and that information can be called upon to add credibility to your case. If you have invented your own, you may have to go through a validation process before your evidence is accepted in court. If the evidence is hard to attack, then you attack the methodology for its acquisition, identification, analysis, conclusions drawn, etc. You have to make it credible.

The better major tools are rather expensive and are being continuously updated to accommodate new forensic techniques and improve the way the proven functions perform. Linux has a different set of tools than Windows and Macintosh also has some differences as well. The discussions here may center around the Windows environment because it is the most commonly used operating system, however, be advised that there are specialist tools available for the other platforms as well.

There are a number of specific and generalized forensic tools available. This, however, is not an analysis of available tools and therefore, it is worth mentioning that surfing the Web is a good starting point for those who are interested in procuring such tools. If you are in law enforcement, there are a number of sources available to you that may not be available to the general public (the FBI Forensics Unit for example).

The process

The analysis is usually, by far, the most time consuming part of the whole electronic investigation. It is where you either find something of use to the case or not. In this discipline all of the processes are equally important and each must be done with the most care possible. Failing to be vigilant anywhere along the way may result in the disallowing of valid and relevant evidence when it comes to court.

The process begins with setting up your forensics machine (with all of your analysis tools and reporting tools on it) and making an acquired evidentiary copy accessible to it (not the one in the evidence lock up but another certified copy). Before proceeding, the investigator will have studied the case to set the stage for the analysis — knowing the parameters of the offence and gaining knowledge of as much as possible about the parties and potential evidence that might be found on the suspect's system. Often it is advisable to conduct the analysis in partnership with the forensic analyst and the investigator. The investigator can provide insight into what he/she is looking for and the forensic analyst can provide the efficient means to find relevant information that might be on the system.

If the analysis is done by the forensic analyst alone, knowledge gained by studying the case, should provide some ideas as to what specific keywords or phrases to use to begin the search. However, depending on the type of case, approaches will vary. If the case is about child pornography, then browsing all of the graphic images on the system may be the first step. If the case is about an Internet related offence, then browsing the Internet history files might be the first step. At the opening of the analysis it will be obvious whether the entire system has been encrypted. If it has, then another approach will be taken. There are many different approaches and each has it own sequence of tasks — some will overlap and others will not. Throughout the process the analyst must document all searches and their outcomes as well as note leads that may initiate further searches. When pursuing a complicated case, the last thing you want to do is repeat your work.

We'll leave it here for now and continue with some ideas of how to proceed when you encounter encryption on the suspect's system next time. Remember, if you have questions or comments (critical, complimentary or helpful) please do contact us.

Encountering encryption

Hank Wolfe

Associate Professor, Computer Forensics & Security, Information Science Dept., Otago School of Business, University of Otago, Corner of Clyde & Union Streets, PO Box 56, Dunedin, New Zealand
Tel: +64 3 479-8141
Fax: +64 3 479-8311
Email: hwolfe@infoscience.otago.ac.nz

In our last column we took a look at analysing evidence. There are lots of other issues to consider in the analysis process that, by the nature and brevity of this column were not addressed. However, no one expects that after reading a few narrowly focused columns on electronic forensics to have become an electronic forensics expert or practitioner. There's a bit more to it than that.

This column will raise some of the issues and problems faced by investigators who encounter data encryption as part of a specific investigation. We'll discuss some administrative remedies. Then we'll focus on some other more proactive techniques that can be attempted in the event that the administrative procedures fail to produce results.

The encounter

Cryptography has become more and more widely used over the past 15 or so years. Phil Zimmermann's introduction of Pretty Good Privacy (PGP) in the early 1990s and making it available from the Internet for free probably encouraged cryptographic use by average computer users more than just about any other event. Up until that time, cryptography was pretty much the domain of diplomacy, military and intelligence. Banking, of course, was a big user as well.

We are all entitled to privacy and a number of international declarations and local laws of various countries guarantee the human right to privacy. Using cryptography to protect communications and/or data at rest is one way of protecting that privacy. So, in the first instance, no investigator should make any judgement as to innocence or guilt merely because the suspect has chosen to protect his or her privacy by using data encryption.

In the interview process, every suspect should be asked for any passwords and encryption keys that he/she has used on their computer. With this information, the investigator should be in a position to be able to access the system and all files resident thereon. However, occasionally a suspect may have 'forgotten' to provide these keys and passwords at interview time. Of course, when no interview has been conducted there will also be no key or password information available regarding the seized system(s).

It is not always apparent that encryption has been used. An examination of resident software may produce the first indication that it is being used. That means that every investigator must have a fairly complete list of available cryptographic software and check it against the suspect machine's resident software. It is also important to ensure that encryption software has not been kept offline on a USB pen disk or PCMCIA card alternate storage device or on some other storage device. These devices must also be checked to ensure that encryption software is not stored there.

Some files that are encrypted may be identified with appropriate software for that purpose. For example, AccessData Corp has a product called IsEncrypted that will identify files that are encrypted by certain applications programs. Applications like Word, Excel, PKZip, etc. are known by this product and files that have been encrypted by one of these or more than 20 others will be identified by IsEncrypted. If the keys are not available for these files, AccessData has products that will derive the keys from the encrypted file. These are important tools for dealing with files that have been encrypted using applications software in the known list.

Administrative relief

Once it has been established that encryption has been used the investigator should request the keys from the suspect. In most cases they will cooperate. One excuse that is worth mentioning is when asked of a suspected child pornographer, with a very straight face, claimed that in all of the excitement of the seizure he had forgotten his keys. The court cannot force a suspect to 'remember' something once forgotten, however, if the suspect is not willing to provide the keys, the next step is to seek relief from the court. In some jurisdictions a court will order the suspect to provide their keys. If the keys are not provided the suspect is held in contempt of court and incarcerated until such time as they are willing to cooperate and provide the keys.

In this particular example the court was unwilling to hold the suspect in contempt and the investigators were left to consider other options. They solicited help to 'crack' the code and after hearing that cracking the code was not an option they discussed other options that might produce the required keys. At first it might seem that a rubber hose and/or a cattle prod might be the right tools to produce the necessary results, however, cooler heads prevailed and other alternatives were explored.

What are the alternatives?

Cracking the code is certainly one option. With the common use of strong encryption today, the reality is that a positive outcome, of a brute-force cracking attempt, would not be successful in a timeframe that would make that outcome useful. In other words, cracking the code, unless the code is weak, is just not a realistic option.

We are left with other more oblique options. Most forensic investigators use a dictionary search for potential keys as one alternative. All discrete words and the use count for each on an entire suspect system are written into a file, minus stop words, that is then browsed for likely candidates (stop words, in this instance, are a list of commonly used words that are unlikely to be used as a password or encryption key). It may sound simple or crude, however, this techniques has produced surprisingly good results and is certainly worth trying. Often passwords and encryption keys are left in plaintext somewhere on a suspect system.

Another approach is to make use of available information about the suspect and his or her interests. Sometimes referred to as social engineering, this technique examines the individual's background, interests and whatever is known about them and then tries candidate passwords or encryption keys based on that information. This is a hit and miss strategy, however, most people when creating their passwords and keys want to use something that will be easily remembered by themselves. More often that not, they will use things like their wife's name, daughter's name, son's name, mother's name, boat's name, favorite sport team's name, favorite automobile, etc. It's easy to see the kind of thing to look for. In one case (that happened to involve a police officer) a simple search for his badge number produced a half dozen candidate keys. Each candidate key contained the badge number concatenated with a family member's name. The third one tried was the one.

Reverse engineering also holds some potential. While there may be laws in some jurisdictions that make this avenue illegal, it can produce results if you're not in one of them or if you can get the target encryption software reverse engineered in a jurisdiction where it is not illegal. If an encryption application can be broken, then files that have been encrypted using it may no longer be secure. This is different than 'cracking' the encryption code. This technique takes the software apart to see how it works. There are lots of software producers out there but there are not a lot of cryptanalysts out there. For practical purposes,

Henry B. Wolfe

Henry B. Wolfe has a long computing career spanning more than forty-three years. He currently specializes in cryptographic problems where related to forensic investigation, general computer security, surveillance, and electronic forensics teaching these topics to law enforcement (both in New Zealand and internationally) as well as at the graduate level in the University of Otago located in Dunedin, New Zealand where he is an associate professor.

many encryption product creators are not cryptographers and are making use of public or licensed algorithms by incorporating the cryptographic code within their product. Occasionally, this is done in a way that weakens the potential security that might have otherwise been provided. Within law enforcement circles, this information is circulated and used where appropriate.

Some manufacturers of cryptographic applications also build into their products back-door access in case a client has a problem using the vendor's product. These vendors have been helpful when asked by the appropriately identified parties and may also be a source of a solution to a cryptographic problem.

Surveillance or entrapment?

In other circumstances, the use of surveillance tools may produce the desired results. If an individual is under suspicion and the appropriate warrant is issued, it is possible to install software and/or hardware devices on a suspect's system that will enable the capture of passwords and/or encryption keys. In the child pornography case discussed in this column, a surveillance tool was used. A warrant to execute a surveillance plan was issued. The suspect's computer was returned to him. Before doing so, a surveillance tool was installed on the suspect's machine. Within three hours of the return of the computer, law enforcement had the keys that enabled them to view all that was on the evidentiary copy taken at the initial seizure. This resulted in 19 additional counts on the indictment and more importantly — a conviction. Neither would have been possible without using this technique since the case was stalled and would not have progressed any further.

There are several classes of surveillance tools available that may produce results and they can be divided into two general categories: software and hardware. Some of the hardware tools fall into the category of general surveillance like TEMPEST, bugging, cameras, etc. Those will not be discussed here.

Software surveillance tools work essentially like Back Orifice or NetBus. They are able to monitor activities on a suspect system, record selected data (encrypting it too), and where Internet connection is available, communicate gathered information to a predesignated site. These tools typically need to be installed on a target system either by physical access by an investigator or by other automated means like being incorporated into a virus or Trojan. All activities that the user can perform can be monitored and recorded. If there is a microphone attached to the suspect system, it can be activated and conversations can also be recorded. If a video camera is attached to the suspect system, it can be activated and whatever it sees can be recorded or transmitted (if the Internet link is open). These tools can also capture keystrokes and record them. These are powerful tools that can provide an investigator with a wealth of information and should only be used with appropriate warrants and authorizations. Some examples are STARR, DIRT, and Magic Lantern (currently used by the FBI).

If a system is entirely encrypted beginning at boot up time, then software surveillance tools may not be able to be active in time to capture the encryption keys necessary to gain access to the suspect system. It may not even be possible to install them on a suspect machine. The alternative is to install a keyboard capture device. These are small and unnoticeable and usually plug into the keyboard port between the port and the keyboard cable plug. The device will capture ALL keystrokes when the machine is turned on and has power, storing this data on its internal memory. Different products have different storage capacity — from many thousands to megabytes. This type of device must be physically installed and retrieved. In both cases the investigator is at risk of

discovery. Once again, since this could be defined as an interception device, it is usually subject to being installed with the authority of a warrant only. This technology could be incorporated into a keyboard and the bugged keyboard could be substituted for the suspect's actual keyboard, however, this would take some pre-investigation to find out the exact model of the target keyboard. The target would also have to be photographed to ensure that the replacement looks exactly like the original so that the risk of detection is minimised. In practice after the device has been retrieved, it is installed on an investigator's machine and a key phrase is typed. That initiates a menu program that enables the downloading of captured keystrokes to a text file for later analysis. This tool makes it possible for totally encrypted systems to be opened by virtue of the capturing of the keys as they are typed. Typical keystroke devices are KeyKatch, KeyGhost, etc.

We'll leave it here for now and continue with the reporting aspects of the forensic process next time. Remember, if you have questions or comments (critical, complimentary or helpful) please do contact us.

Presenting the evidence report

Introduction

In our last column we took a look at encountering encrypted evidence. There is some additional information that has come to light since the last column. Hard wired keystroke loggers are available that can be installed within the target's own keyboard. These take about fifteen minutes to install but cannot be detected easily by the person under surveillance. They typically have a capacity to store, using 128 bit encryption, up to two megabytes of keystrokes. This is about 300,000 words or a year's worth of typing. Viewing the log is, after opening a word processor or WordPad, as simple as typing on the modified keyboard a password that you control. This will execute a menu program stored on the device and keystrokes can then be downloaded for analysis. There are other menu options that allow you to manage the storage associated with the surveillance device as well as changing its controlling password.

This column will address some of the important issues encountered when preparing the final report. This is not normally the culmination of the whole process but might be if no evidence of use is found or if the parties come to some legal arrangement (plea bargain, etc.). After the report is presented to and reviewed by the prosecutor/attorney in charge of the case, it may be necessary to actually appear in court as an expert witness and testify as to certain aspects of the forensic process. Every electronic forensics investigator must be prepared for that eventuality and be able to defend all of the processes used to obtain any evidence presented as a result of their work. In some cases they may be required to demonstrate how the evidence was obtained.

The report – some comments

The forensics report brings together information that may be vital to any prosecution or civil case. This report must be written in a clear concise style using terms that most non-technical people will understand. Each page must clearly identify the case to which it applies as well as the total number of pages, which comprise the finished report and the date that it was prepared. This is done to enable the reader to know that they have all of the pertinent information. You may go through several iterations of report preparation and if so, the date will enable clear identification of the latest version. The investigator will be mindful of preparing the report from the initial evidentiary capture stage and, throughout the subsequent processes, be recording the key elements of case history, facts found, interview content, specifics (serial numbers, model number, version number, etc.) about seized computing equipment, ancillary storage and software, experiments and tests performed, as well as highlighting and documenting whatever relevant evidence is found.

Of course, underlying all of these activities will be the chain of custody. This refers to the proposition that evidence once captured/seized must be able to be accounted for from that time onward. All access must be documented and given only to those who are properly authorized. The possession and control of evidence must be thoroughly documented and provably demonstrate that it has not been accessed by anyone that was not authorized to do so. Throughout the investigation, analysis and report preparation, the chain of custody must be provably kept in tact. Any break no matter how short or innocent may render the work and subsequent evidence found and presented to be unacceptable in a court of law.

It is worth mentioning that evidence may prove guilt but that it may also prove innocence. It is never in anyone's interest to approach an investigation with any prejudice or prejudgement in mind – no matter who pays for

Hank Wolfe

Associate Professor, Computer Forensics & Security, Information Science Dept., Otago School of Business, University of Otago, Corner of Clyde & Union Streets, PO Box 56, Dunedin, New Zealand
Tel: +64 3 479-8141
Fax: +64 3 479-8311
Email: hwolfe@infoscience.otago.ac.nz

Henry B. Wolfe

Henry B. Wolfe has a long computing career spanning more than forty-three years. He currently specializes in cryptographic problems where related to forensic investigation, general computer security, surveillance, and electronic forensics teaching these topics to law enforcement (both in New Zealand and internationally) as well as at the graduate level in the University of Otago located in Dunedin, New Zealand where he is an associate professor.

it. Remember, that after technical expertise, the only thing we, as forensic scientists, have to bring to any case is our impartial and untarnished reputation. That, once compromised, can almost never be regained. Our advice and findings can only be of value when there is credibility.

Preparing the report

In the first instance, you must be able to demonstrate that the evidentiary copy captured during the investigative period is a true and accurate representation of the original. That is normally done using a well-established and proven hashing algorithm. MD5 is an accepted standard with the likelihood of collisions (duplicate hash values for different data) to be 264 – an acceptable limit for these purposes. A working copy of the evidentiary version is made and authenticated and that is the data set used for analysis. Since we never (or almost never) use the original evidence thereafter, the evidentiary copy is very important. Much of our analysis will be based on searches, experiments, and viewing of a working version of that copy. A clone of the original seized computer may be produced using the working evidentiary copy. Experiments may also be done using that clone. If any of these experiments or other analysis activities causes the clone or forensics machine to fail or become corrupted, we can always revert to the original evidentiary copy and create another working evidentiary copy from which a clone or forensics machine can be set-up – for further analysis. These are standard best practices and must be documented in the event that any question should arise.

Report content

Every report should contain all of the identification (by case), validation (of data acquisition) and inventory (all things seized) information relevant to the case. In addition it should list the names and dates of all who participated in the interview, acquisition, analysis and report production. It should also contain specific drive geometry, clock settings and other technically specific size and configuration information about each device seized.

The report should contain an explanation of the methods that were used to produce evidence presented as well as document the exact source of that evidence. For example, it may be that fragments of text are relevant to a particular case. The source of those fragments should be identified – the file name and extension as well as other statistical details about that specific file (all related dates, folder names, etc.). There should also be a complete version of the entire file available within a documented index to allow for context reference and assessment.

Images discovered that are relevant to the case must accompany the report – either as a direct part of its content (possible by using some forensic tools - EnCase[1] as an example) or as a part of an appendix. Images, in child pornography cases for example, are often hidden in some way – either by diffusion (hidden within another file – using steganography) or by changing the extension of the image files to make it harder for these files to be identified as image files or by other means. They may also be encrypted. Whatever the ploy used, that fact plus the images need to be incorporated into the report.

The time line of various activities of a given suspect may be plotted by time and date stamps found in files created, modified, or deleted. Other timeline information may also be found in the browser cash and history files. In one case the individual was directed by the court not to use his computer after a certain date. He was an officer of the court and knew the consequences of contempt, however, after doing

[1] EnCase – A product of Guidance Software, 572 East Green Sttreet, Suite 300, Pasadena, California 91101, www.guidancesoftware.com.

a timeline analysis it was discovered that the he had used the machine after the appointed time deleting several hundred files and then defragmenting the hard drive. The defragmenting processing, by its nature, overwrote most of the file space that was deleted. No relevant evidence of any other kind was secured from his machine, however, the fact that he had violated the court order gained him a contempt citation and discredited much of his testimony as well.

Presenting the report

Often cases never go to trial because the evidence obtained is so overwhelming that a plea bargain is reached. These are cases where the electronic evidence discovered is so clear and decisively central to the case that to fight it would only make the lawyers richer. As forensic scientists, we can never be sure that cases we investigate will end with the presentation of our evidence. We must always be prepared to testify and defend our credentials, methods, and tools. Some law enforcement and others use proprietary tools to do their acquisition and analysis. Proprietary tools in some cases may be easier to use or may have a greater breadth of capabilities. However, be aware that using non-standard tools invites an attack by the opposition on those tools. The use of well-established tools and techniques avoids scrutiny of those tools (because its already been done and precedents set) and leaves only process and interpretation open to attack. If these are done carefully with clear documentation any attack will be easier to defend. The lesson here is to avoid the use of proprietary forensic tools.

In many cases, electronic evidence plays only a small part in the overall case and may by itself not swing the verdict one way or the other. In murder cases, for example electronic evidence may point to intent by virtue of content but not by itself prove premeditation. Whatever role we play, evidence discovered and presented must be carefully handled and protected to maintain its integrity (as well as our own integrity too) and usefulness.

We'll leave it here for now and continue with some thoughts and advice about giving testimony as a part of the forensic process next time. Remember, if you have questions or comments (critical, complimentary or helpful) please do contact us.

Forensic evidence testimony — some thoughts

Introduction

In our last column we took a look at presenting the evidence report. This time we will discuss some tips that will help the new player to testify with credibility. The first thing that must be remembered is that any court appearance is an adversarial process. As an independent technical expert you must always be sure to remember that you are neither an advocate nor defender of any position. What you have found during your investigation and analysis should be presented in neutral terms as facts and, unless required, not as opinion. Opinion can more easily be disputed, requiring you to defend your assertion. A good attorney may be able to rattle or confuse witnesses and by doing so can sometimes reduce or negate their testimony.

Who is an expert?

As of the writing of this column, there is to my knowledge, no internationally accepted certification of electronic forensics professionals. This will, no doubt, come in time. There are specific organizations, usually vendors of a product that will certify completion of a successful trainee in the use of their product. This certification contributes to one's credibility but in isolation is not normally enough to constitute international or local recognition as an electronic forensics expert. Law enforcement, in various jurisdictions, has formal training programs that are well established and these offer a good degree of credibility. Credentials provide the Court with a level of confidence that your testimony is based on sound best practice techniques. Because there is no formal accreditation, and no formally recognized standard for investigative techniques and forensics experts are not currently required to be licensed, at this point just about anyone can claim to be an "expert".

Those in law enforcement have their training as an advantage when testifying as an expert witness. However, no matter where you hang your hat, you must be involved with and participate in your community of interest and be able to prove it. This adds to your credibility because it provides a conduit for new ideas, techniques and tools that might otherwise be missed. It also offers an opportunity to talk with others of a similar interest about various problems faced in the course of investigations and analysis. Often, innovative techniques, tools and short cuts emerge and are shared amongst practitioners who participate in these forums. Most forensic breakthroughs are not written about in any formal journal. In fact in some cases, techniques that are found to be successful are deliberately kept confidential to give the "good guys" an edge. So, you just cannot go out and find answers in a forensics journal (I don't think there even is one yet).

Being a professional

When testifying in a court of law, you are being judged in every way. Not only is your testimony being appraised but so too is your demeanour and appearance, the quality of your report and documentation, and the directness and confidence of your answers. All this will influence the level of confidence placed in your testimony by those who witness it. Technical people sometimes do not understand that appearance may raise or lower the value of the evidence they present. You are a professional – look and act like one. The report and documentation that you create for others to see must reflect the highest standard of quality and accuracy. That means that there should be no spelling or grammatical errors within it. It must also be put together in a logical sequence that helps the reader/audience/jury to see and easily understand your evidence.

Hank Wolfe

Associate Professor,
Computer Forensics & Security,
Information Science Dept.,
Otago School of Business,
University of Otago,
Corner of Clyde & Union Streets, PO Box 56,
Dunedin, New Zealand
Tel: +64 3 479-8141
Fax: +64 3 479-8311
Email: hwolfe@infoscience.otago.ac.nz

 0167-4048/03

Henry B. Wolfe

Henry B. Wolfe has a long computing career spanning more than forty-three years. He currently specializes in cryptographic problems where related to forensic investigation, general computer security, surveillance, and electronic forensics teaching these topics to law enforcement (both in New Zealand and internationally) as well as at the graduate level in the University of Otago located in Dunedin, New Zealand where he is an associate professor.

Fear of public speaking

It's been often said, that which is most feared by just about everyone is having to speak in front of an audience. This fear can be explained by a number of factors. First, a courtroom is a new, intimidating and normally unfamiliar audience who, to be sure, are critical of what they hear. Second, we often feel that we have nothing of interest or importance to say. Or that we will say or do something stupid and be ridiculed or discredited. Third, as technical people who almost always control their environment, we have no control of the court proceedings. Forth, cross-examination is, by its nature, adversarial and can be stressful to say the least. Finally, every word is transcribed and becomes a part of the Court record. This in itself may be intimidating.

Why then, do we want to participate in such a forum? Because it is part of the game we're in and one of the most important duties of forensic professionals. Anyone can do the technical work. Being able to explain and defend what has been found and talk in easily understood terms about what it means is a challenge. Every court appearance should be treated as an opportunity to hone and sharpen one's speaking and reporting skills. Those in law enforcement will most likely have no choice about testifying. However, those who have a private practice get to choose their cases. That choice should be made with care and a good knowledge of the attorney(s) that you will be working with. Don't work for a jerk. There's not a deal in this world that you can't walk away from.

Having said that, it should not be considered an oratory contest. Questions asked by the attorney on your side of the case should be known and rehearsed ahead of time. The expert witness should normally not be surprised by any questions put by his/her allied attorney. Testifying means answering questions in a clear, precise and concise manner without volunteering any information that is not necessary to answer the question before you. Every additional piece of information not asked for opens a door for further questioning. This can dilute, confuse or obfuscate the importance of the initial answer.

Often the opposition attorney may attempt to rattle you or to weaken or discredit your testimony by asking questions that are difficult or that question your competence. Be thoughtful in your response and remain steadfast in what you have said but do not ever become argumentative with the cross-examining attorney (or anyone else in the courtroom for that matter). That is a recipe for disaster.

When on the witness stand, you are in view by all who participate in the courtroom drama and in some cases the proceeding is being video taped as well. With that in mind, no matter how restless you may become or, how difficult the questions or, how obnoxious the opposing attorney, never allow yourself to betray your feelings physically. Do not sigh or grimace or fidget or in any other way give away your satisfaction, displeasure or impatience. Remain calm and look it. The reason for this physical control is two-fold. First, you may alert the opposing attorney to a potential weakness in your testimony. Second, you may appear to the jury to be tentative or unsure about your evidence and that could diminish the effectiveness of your evidence and testimony.

Exhibits

It is often necessary to use graphical exhibits to make a piece of evidence clear or more easily understandable. Target your audience. Any exhibit put forward also becomes a part of the record and should be constructed at the highest standard – simplicity and honesty is best. Do not try to make a point by an inaccurate or a misleading graphic. Remember, the impression given by it will be a reflection of your professionalism or at least how that

professionalism and expertise is perceived by the reader/audience/jury. We are NOT advocates. We find the truth and report it. Nothing more.

We often take for granted that everyone knows what we know. With that expectation we often use terms of the art (jargon and acronyms) casually in our conversation. In a courtroom, we cannot assume that anyone knows what we know. Evidence explanations and graphics must be couched in terms that anyone can understand. Do not use graphics unless their use enables the clarification of a complex point of evidence or the clarification of a vital technical issue – leading to an understanding of the evidence presented and/or how it was obtained.

Bringing it all together

Forensic investigators are only as good as their skill and ingenuity coupled with their integrity. It is not the role of the investigator to be an advocate or to "get" anyone. The role is clear. It is to find the truth and report it and testify to it as clearly, concisely and precisely as is humanly possible without the colour of bias. The exception can be seen in law enforcement. Within that community, you're either with us or against us. That ethos and culture has no place within private forensic investigation. Our reputation can only be tarnished if we allow bias, for any reason, to become a part of our work. Finally, the only unique thing that we have to sell is that integrity. Once that is sullied, it may not be able to be recovered. Be forewarned and govern yourself accordingly.

Further reading

An excellent reference for those who have to testify as a forensics expert and want to know more is *A Guide to Forensic Testimony – The Art and Practice of Presenting Testimony as an Expert Technical Witness* by Fred Chris Smith & Rebecca Gurley Bace (ISBN: 0-201-75279-4).

We'll leave it here for now and continue next time with some ideas about setting up an electronic evidence forensics laboratory. Remember, if you have questions or comments (critical, complimentary or helpful) please do contact us.

Setting up an electronic evidence forensics laboratory

Hank Wolfe

Associate Professor, Computer Forensics & Security, Information Science Dept., Otago School of Business, University of Otago, Corner of Clyde & Union Streets, PO Box 56, Dunedin, New Zealand
Tel: +64 3 479-8141
Fax: +64 3 479-8311
Email: hwolfe@infoscience.otago.ac.nz

In our last column we took a look at being an expert witness and giving forensic evidence testimony. An added word of cautionary advice for private practitioners: CHARGE A LOT for expert testimony! If you are involved in a high-profile case that drags on and on and you must testify as an expert witness repeatedly at the whim and caprice of the various attorneys, it could disrupt your private practice and cause potential loss of current and future earnings. Your current case load could be seriously delayed and your credibility for future work may also be damaged. The previous discussion, by nature, was very general, however each jurisdiction has a formal set of directives and guidelines specifically to assist expert witnesses so you must also refer to these for more details.

The following discussion will be focused on setting up an electronic evidence forensics laboratory and the various parts that make up a professional facility. The many parts also include the portable forensics kit(s), which includes documentation forms, evidence bags, tags, labels, etc, as well as portable hardware and associated software for undertaking an evidentiary acquisition on site. Not all such activities may be performed in the lab, but the mobile forensics toolkit must be fully compatible and in sync with the laboratory acquisition equipment and software at all times.

There may be accreditation for such laboratories, depending on the jurisdiction. For example, in the US one such accreditation may be sought from the American Society of Crime Laboratory Directors. If accreditation is possible in your jurisdiction, it may be advisable to explore the criteria for achieving it. While there may be differing views as to the value of accreditation, it is my opinion that having it is one more stone in the foundation of credibility, and therefore it should be viewed in a positive light.

The parts

There are several parts that make up a forensics laboratory. Firstly, there is the physical facility itself. This will be the home base for secure storage of evidentiary materials, for the analysis of captured data, for the operation of cloned systems, for the production of final evidence reports, and for the physical premises where the forensics professional will perform most of their duties and work. So, it is a secure storage facility, an office, an operational laboratory, and a production facility all rolled into one.

It should also have a separate interview facility or office where interviews and/or collaborative investigative procedures can be carried out without disturbing any ongoing technical or forensic work. Normally an investigating officer or attorney with an in-depth knowledge of the case will have queries that can be answered more effectively in collaboration with the forensic investigator. The forensics professional will, in real-time, perform specific analysis and/or search actions to find the answer to questions posed by the investigating officer or attorney.

Physical requirements

Physical floor space will be dictated by the size of the group that will occupy it. The space should be in a secure location or contain appropriate measures that will stop unauthorized access to the premises. It should have an adjacent and secure walk-in lock-up vault that can keep intruders from gaining access to its contents as well as protect the contents from fire/heat, smoke, water, and electromagnetic emanations (and should generally not be near radio equipment). The

Computers & Security Vol 22, No 8 0167-4048/03

seized equipment, as well as official certified evidentiary copies of seized data, will be stored in this vault and, with the appropriate enforced sign-out/in procedures, it will serve to maintain the chain of evidence. Therefore, access to the vault and its contents should be logged and monitored at all times.

There also needs to be adequate lockable storage space for various specialized equipment that will, over the course of investigations, be acquired and used for other investigations. This space must also accommodate consumables like CDs, DVDs, removable hard drives of various capacities, paper, toner cartridges, etc.

Hardware requirements

A number of computers is required, including a network server with large storage capacity (preferably configured for the standard removable hard drives). This server will be used to manage, document and administer cases, store various software tools, and manage one-off specialist hardware. The hardware that must be managed will include, for example, devices like Rimage CD production units, CopyPro floppy disk readers, printers, etc. The evidentiary copy of seized data is usually written to CD or DVD and, because of the large capacity of current hard drives, this can be a time-consuming process. The Rimage, and other units like it, make it possible to create, number and label the media unattended, producing as many as 50 CD/DVDs without intervention. Capturing the contents of floppy disks is even more time consuming, and devices like the CopyPro can acquire as many as 50 floppy disks without intervention. The capabilities of these types of devices may vary from model to model; the two mentioned above are merely examples with specific capacities.

There should also be separate Internet connection(s). (NEVER connected to the forensics server). The Internet will be useful for finding and sharing forensics information and techniques and for communicating with other forensics professionals. Staying abreast of developments in this field is a vital part of staying viable in the forensics arena. The Internet provides one source to help accomplish this need.

There should be a number of workstations that connect to the internal network. This number will depend on how many forensics people are employed. The workstations will enable them to work on individual cases simultaneously and have access to the shared devices and resources.

Portable acquisition computers (the kit) will be required. Ideally, each should be configured identically with the standard forensics suite of tools and removable hard drives (the same standard hard drives as above) of various capacities. Each kit should have a robust carrying case that can accommodate extra hard drives, an array of associated connection plugs and converters, and a hard drive write blocker such as FastBlock. The forensic kits will be used for on-site acquisition and/or seizure. It is usually preferable for acquisition to be undertaken in the controlled conditions of the laboratory, however there are circumstances where that is not practical and an evidentiary acquisition must be undertaken on site (for example, when dealing with an Internet service provider). These kits must also have an assortment of forms, labels, tags, pens, tape, evidence bags, an electronic camera, a GPSS, etc, all of which are vital to the process of seizure and acquisition.

There will be an ongoing need to obtain devices, media, cables, converters, and specialized media readers of various types, both for experimental purposes and for the acquisition of evidence from media other than hard drives or floppies (for example, SIMs, flash memory of various description, iButtons, etc).

The hardware and physical premises constitute the largest outlay of funds. This, however, is an ongoing process and funds must be allocated

Henry B. Wolfe

Henry B. Wolfe has a long computing career spanning more than 43 years. He currently specializes in cryptographic problems where related to forensic investigation, general computer security, surveillance, and electronic forensics teaching these topics to law enforcement (both in New Zealand and internationally) as well as at the graduate level in the University of Otago located in Dunedin, New Zealand, where he is an associate professor.

regularly for the purchase of new hardware as it finds its way into the public arena.

Software requirements

The standard forensics software packages, such as EnCase, Forensics Tool Kit, Password Recovery Tool Kit, etc, are expensive products. It is worth noting that some require dongles to work and that these must be managed. In most cases the capabilities of the software tool outweigh the nuisance and inconvenience of the required dongle. These products tend to be upgraded annually and, in each case, funds must be allocated for the upgrades. However, the software tools that are used comprise a far wider range that just those cited above. Many are freeware and many are not. No single tool performs the entire job of forensics acquisition, analysis and reporting, so we tend to use the right tool for the right task. Therefore, the forensics software tool library will be extensive and will probably continue to grow. Having the right tool may make the difference between capturing relevant evidence and not being able to do so — a case may be won or lost as a result.

In addition, of course, the standard operational software will be required. This includes LAN software, operating systems, administrative software, graphics software, etc. These too will need to be upgraded occasionally, so funds must be allocated for this ongoing process too.

While the continued cost of software acquisition and upgrades is smaller than that of hardware, it still constitutes a significant portion of any forensic laboratory budget and must not be overlooked. The physical price of operating a forensics laboratory is not insignificant.

Procedural requirements

Methods and procedures are an important part of operating a successful forensics laboratory. The main issues that can and usually are attacked when evidence is presented in a court of law are credentials and methodology. Therefore, close attention must be paid to strictly following and documenting the methodology formally adopted by the lab in the acquisition, analysis and reporting processes. Moreover, it is equally important to have a formal procedure that documents the handling and control of evidence in order to be able to document the 'chain of evidence'. These are the two main issues that are unique to a forensics laboratory. There are other procedures and policies that should be in place and enforced, but they are the standards like Internet usage, email rules, back-up regimes, etc.

Summary

All of these parts, facility, hardware, software and procedures still rely on the skills, dedication and professionalism of the people involved. The commitment and dedication required of these people mean that esprit de corps and morale is vital to any such operation. This comes from leadership by example and good management — a topic for another forum.

This column concludes this series of articles about electronic forensics. We hope that you have found the series to be useful and illuminating. It has deliberately been broad in its scope and content and intended as an introductory briefing on electronic forensics. You may find a more detailed discussion in our soon-to-be published book (*Practitioner's Guide to Electronic Forensic Evidence Gathering*). Remember, if you have questions or comments (critical, complimentary or helpful), please contact us.

Management strategies for implementing forensic security measures

Jeni Wolfe-Wilson
Technology Shared Services Group, Ministry of Health, PO Box 5013, Wellington, New Zealand

Henry B. Wolfe
Information Science Department, Otago School of Business, University of Otago, PO Box 56, Dunedin, New Zealand

Abstract

We live in the age of electronic information and rapidly evolving technology. Almost every aspect of our lives is touched or somehow controlled by technology-driven processes, procedures and devices. It is therefore important to understand that because of the pervasive electronic influence, the opportunist or criminal element has turned its attention to exploiting weaknesses inherent in many traditional and electronic information systems. With that undisputable fact in mind, we must face the inevitable: a successful criminal or unacceptable incident occurring within the organization's perimeter of the information and/or computer and network infrastructure.

It has been said that 'opportunity makes a thief'[1]. Criminals, however, are not the only threat that we must face. When an opportunity presents itself to a willing protagonist, there is a high probability that the opportunity will be acted upon. Their actions may not be classed as 'criminal' if no prosecution has occurred. Actions may be defined as inappropriate or unacceptable as per the organization's code of conduct or security policy, and hence any breach or violation of the code of conduct or security policy may result in disciplinary action.

A large measure of inappropriate activity or computer crime takes place from within an organization [2]. Therefore, security measures must be put in place that will reduce unacceptable, undesirable or inappropriate behaviour by internal users, as well as protect from potential external threats.

This paper is directed at senior level management offering a non-technical basis upon which to make rational decisions to allocate resources necessary to protect the vital interests and resources of an organization. Resources include information, budget, staff, information technology (IT) infrastructure, processes, procedures and management directives. In our judgement, this resource allocation is not optional. Future legislation, statutory requirements and fiduciary obligations, with support of best-practice standards [3], will act as an incentive to encourage executive level management to be directly responsible for failure adequately to protect the vital functions of the organization that they direct [4]. This is in line with their normal fiduciary obligations to act with due care and diligence to protect the organization's assets and continued operation, in line with the organization's corporate governance practices.

1 Some Unpleasant Truths

Security will fail if top management does not take an active role in initiating, developing and supporting it. Security will fail if top management, because of their lofty importance, choose to exempt themselves from applying the secure policies and procedures implemented. This is not a new revelation. It has been stated repeatedly and management has continued to ignore it repeatedly. Because it is often ignored, to the detriment of those who do so, we feel compelled to restate it once again for this forum.

A real life example is as follows: a government department has at its head an individual who does not like the idea of being forced to change their password regularly and therefore, has exempted themselves from doing so. This, in turn, has allowed the number two also to be exempt from changing their password regularly. New policies that incorporate this as a required security measure have routinely not been signed off by these executives because they will have to abide by the policy. Of course those who are aware of this approach by top management can plainly see that security is not an important issue to these top executives. This filters downwards

and, as a result of the irresponsible attitude and incompetence, will continue to affect the quality of security measures and their effectiveness in this organization.

It is strongly recommended that the senior management team send a communication to all staff, for example: an image of the first page of the security policy showing all their signatures, directing that staff support the security policy as mandatory. Otherwise, as seen time and time again, unless top management focus on risk and actively support security, effective security management is almost impossible.

The example discussed is not unusual or unique. Individuals like those described above are far more common than we would like to think and can be found in every country and across both private and public sectors. Everyone believes that they are special and that they alone should be exempt from specific rules, and can make convincing arguments supporting their contention. However, in order to protect the continuity, integrity and confidentiality of any IT system, it is necessary to instil an ethos of security amongst the entire staff of the organization. This especially includes top management, since subordinates will follow top management's example. Leadership is born out of example, not from command. There should be no exceptions and all should be required to abide by the agreed policy. These policies should each be justified by a risk assessment, policed and have consequences for those who choose not to adhere to them. They should be communicated to all staff regularly so that there is no misunderstanding of what is appropriate behaviour and what is not.

Unfortunately, for many organizations or industries, this is not always reality! Government or large organizations may have identified the need for codes of conduct and security policies, due to fiduciary, statutory or government regulations, or possibly due to the impact of previous security events. Medium or small organizations may not have the resources, budget, inclination or regulatory requirements to identify or manage a risk management and business continuity plan.

It may take a business-disruption, politically sensitive or public-embarrassment type incident to gain the attention of senior management or the board of directors. Addressing the incident may still not be enough to prevent the organization from folding and going out of business. By then it may already be too late to recover if adequate measures have not previously been put in place.

2 What, in layman's terms, is electronic forensics

Forensic computing refers to the methodologies used to capture and authenticate data at its source, analyse that captured data for evidence relevant to the case at hand, produce an understandable report that can be introduced into evidence in a court of law, and testify as to the authenticity of evidence presented. The sequence of this methodology is specific and must be followed. Failure to do so can result in the entire investigation's failure.

Your organization and staff may be the subject of a denial of service (DOS) attack, an attempt to undermine customer confidence, an attempt to extract personal or business-related information to sell or to obtain a bribe, or the redirection of organization funds, or any other activity you deem to be unacceptable to the ongoing success of your organization. Typical sources are the opportunist, convicted

criminal, competitor or disgruntled employee, to name a few. Their motives and purposes may never be known.

We are not attempting to profile attackers or define all the types of intended agendas in this paper. Many security references have extensively profiled the would-be intruder from among the internal and external users, as well as defined unacceptable behaviours.

The operating system in any computing environment stores information in various storage devices using methods not normally known in detail to the average user. In addition, content that average users may not be aware of is also stored. With various tools and techniques, evidence can extracted that might address a specific timeline or relevant information thought to be deleted by the suspect or information about sites visited on the Internet by the suspect, or improper or illegal images held on the suspect machine and much more.

Throughout the process care must be taken to protect the original source data and the normal investigative chain of evidence must be kept. There are a number of guidelines for the collection of evidence published by various groups. The Internet Society has RFC3228 – Guidelines for evidence collection and archiving. It provides guidance for front line staff who are likely to be the first responder to an incident. The US Department of Justice has a number of publications that provide very thorough advice in this area as well [5]. An example is *Electronic Crime Scene Investigation: A Guide for First Responders*.

The chain of evidence is often referred to in criminal matters and document possession, and access to and control of evidence from the instant it is captured until well into the judicial process (to allow for one or more appeals). If the evidence is out of the control of the investigative authority, and can be shown to be so by opposition council, the court is likely to declare it inadmissible. This is done because while it is out of the control of the authority, the evidence may have been altered or tampered with and therefore, its integrity can no longer be guaranteed. All of the investigative and analytical work invested will be lost and the case may also be adversely affected as a result. Therefore, it becomes an important issue – especially at the very beginning of an investigation to ensure that first responders understand the necessity for protecting potential evidence.

Once an evidentiary copy of the original data source is made it must be authenticated. That process is designed to give credibility to the proposition that the evidentiary copy is identical in every way to the original. This is accomplished by using a mathematically proven hashing algorithm designed to create a fingerprint of any given file or group of files. This fingerprinting process is performed on both the original and evidentiary copy. The fingerprints for both must be identical for the relevant evidence found on the evidentiary copy to be accepted in court as evidence.

After the evidentiary copy is authenticated, analysis can begin. In some cases, data encryption may be encountered. This is not the forum to address issues surrounding how to deal with encryption; however, suffice it to say that there are several successful methods that can be used overcome blockages to analysis presented by encrypted data.

There are many tools that facilitate the analysis process. This process searches the entire evidentiary data set for information relevant to the case (the original is never used for anything other than capturing the evidentiary copy). Evidence that is found

must also be recorded and portrayed in a form that can be easily understood by those considering the case. In a court of law, if these findings are presented, the forensic investigator must be in a position to present and defend the processes and tools used to acquire the evidence.

The whole process is time consuming and labour intensive since typical hard drive storage capacities have increased to as much as 100 gigabytes or more. The profile of an electronic forensics investigator is part detective, part technician, and part performer. These qualities each, on their own, will constitute a person's entire profession. Finding them all together in one package is difficult. Universities are only now just beginning to provide tuition in this profession. Some product vendors are providing specialist training, but to put together all of the necessary foundation and specialist knowledge and experience will take a combination of sources. This is expensive. Be prepared to pay a premium to professionals in this discipline.

3 What happens when you have a security breach

For the purposes of this discussion, a breach may be defined as a potentially criminal action. A violation can be defined as an infraction of security policy.

First, the breach or violation must be detected. Much crime and inappropriate behaviour is not detected. Measures need to be put in place that will detect patterns of potentially unacceptable action. For example, intruder detection systems (IDS) or intruder prevention systems (IPS), attempt to identify events that occur when someone tries to hack into your system, or a staff member attempts to gain access to part of the network they are not permitted to access. IDS produce logs containing information about network traffic activities. These logs can be used for traffic analysis and enable the network administrator to identify network bottlenecks as well as network performance and capacity indicators to determine whether additional resources (server, memory, storage, network bandwidth) may be required in order to maintain acceptable performance levels.

Information captured and stored in these logs can also be used for forensic purposes to track individual activities depending on log file configuration parameters to capture everything or selectively capture only data that is desired. There is a trade off. When capturing everything, significant overhead in processing power, network performance and disk storage space may be required. Therefore, a balance is usually struck by network administrators to capture a subset of log data required for general analysis or potential investigative purposes. This subset is usually intended to provide enough data to be able to identify what has happened and how (if an intruder has been successful). This information assists the administrator to reconfigure the device and introduce measures to protect against a similar event or attack from occurring at a future date.

This is acceptable for hacking attacks; however, other potentially criminal or inappropriate activities may not be so easy to detect. It is possible and practical to use various audit devices to detect fraud, embezzlement, theft and the like. There are filtering tools that prevent access to forbidden Internet sites (porn and other questionable sites). These are important tools to reduce the 'opportunity' by making this behaviour difficult or easily detected.

Internal authorised users performing authorised activities often act upon opportunity. If taking advantage of the

opportunity is considered unacceptable behaviour, security controls may not pick up the immediate actions if the user is authorised to perform like-activities as part of their job description and function. For example, an unauthorised modification to a customer's bank account to redirect funds may only be picked up after the customer queries a missing payment.

It is important to understand that while an organization may identify actions by internal staff or external users as inappropriate or unacceptable, the actions themselves may not be deemed illegal or criminal, or at a level worth investigating by the law-enforcement community. This may be due to the low value of monetary loss, physical disruption or goodwill damage to the organization. Legal advice is recommended in such cases.

An organization can choose a civil remedy action against a staff member, such as dismissal or a formal warning. Management must ensure their evidential facts are clearly defined to counteract any potential employee legal action against their employer for wrongful dismissal. Civil remedy is not necessarily an option where an external person or another organization is responsible for damage. Legal advice may recommend monetary damages be sought in court from the responsible parties. However, when all of the best security practices have been observed, suitable security controls are in place, and a breach or violation is detected, certain procedures should be followed so that any useful and relevant evidence that may still be in place will not be corrupted or destroyed – either by purpose or by accident.

As with traditional forensics, the timing of the incident response, along with defining and securing the potential crime scene is critical. In the electronic world, this involves more intangible evidence and is not necessarily easily put into an evidence bag. Evidence may include PC and system logs, local and removable backups, removable media such as diskette and CDs, printouts, memory, as well as any other local, removable or remote storage devices or processing systems.

For example, the suspect equipment and all associated devices should be immediately isolated. If the PC is turned on, it should not be turned off. If it is turned off, it should not be turned on.

Third parties, ISPs, systems administrators and users may also be critical in the data and information discovery process. In the case where information or data may need to be obtained from outside your organization, court orders and warrants may need to be prepared and subpoenas sought. In these cases, the involvement of law enforcement and legal council is critical. It is recommended that the organization does not attempt to obtain evidential information from external parties without legal or law-enforcement advice. This may make the evidence inadmissible in a court of law and seriously jeopardize the likelihood of a successful investigation and prosecution.

It is critical that if a breach or violation is detected, the organization's IT support team does not compromise or contaminate the evidence. Only suitably trained security staff should attempt to take evasive action if the perpetrator is identified to still be online and in the process of the potential crime or unacceptable behaviour. Evasive action may include closing off the network around the perpetrator, following at a distance to collect additional information to assist in the subsequent investigation and hopefully identify the culprit.

Whether there are in-house forensic staff or not, these and other procedures should be followed until the forensics professional takes control and begins the investigation and data capture process if required.

4 What can be done about it

Incidents may vary in structure and substance. Where an activity is deemed criminal, local law enforcement should be contacted and the case investigated by them.

If management decides that the incident will be handled internally, as a civil remedy matter without law-enforcement assistance, there are several recommended approaches.

One approach is to contact a private forensics professional to handle the investigation. This is a fairly new profession with varying levels of skill available in the marketplace, so shopping around is definitely an important task. It makes sense to do this before there is an incident so that on the day you can call in an appropriate expert without delay. These cases are most often time critical. In various jurisdictions, there are professional groups, like Vogon [6] for example, that have excellent reputations, thus providing confidence that the best job that can be done will be done.

A second approach requires that the organization can set up an in-house forensics group trained to perform such activities. This would require highly technical professionals, a laboratory and a good deal of specialized hardware and software – probably warranted in very large organizations for a potentially large investigation only.

Another approach, as mentioned under section 6 'Here's a Plan', is to contact a local Computer Emergency Response Team (CERT [7]). These professional organizations are located in many countries and specialise in investigating security-related incidents and provide an important warning or alert service for similar events. Moreover, those who belong to FIRST [8] share information about new attack scenarios and potential patches or fixes that can be applied.

No matter which path is chosen by your organization, someone needs to be trained and responsible for this kind of activity. They need to know what measures to take to ensure that potential evidence is not destroyed or corrupted either deliberately or inadvertently before the forensics investigator arrives to begin the investigation. They need to know who to call to perform the investigation and who to report the incident to.

5 Why are forensic measures strategically important?

When a breach or violation is suspected, the organization's most likely intent is first to recover, then to seek a prosecution or discipline internal staff and, if losses have been sustained as a result of the breach, recover those losses. Even after a successful prosecution, there is no guarantee that the organization will remain operational. The impact and subsequent damage from the security incident may in fact put the organization out of business, or affect its position in the marketplace, such that it no longer has a viable business model or its reputation intact.

The organization's Business Continuity Plan is critical at this point. Recovery is vital from the immediate incident, whether this is installing a replacement server from backups or finding new premises during the incident's period of investigation. Resumption of normal business activities is also important after the recovery period

back to the same business operations level with hopefully enhanced security controls, as before the incident.

After the event, it is recommended that a full investigation around the handling of the incident is included to identify potential risks and mitigation plans to minimize the impact of a similar event in the future.

6 Here's a plan

It is recommended that senior and technical management should define the way in which an overall incident response plan will be managed, including forensics investigation, prior to the actual need arising. At the time an incident arises, as with traditional forensics, timing and evidence handling are critical and, in this case, electronic evidence may be deliberately or accidentally contaminated or corrupted. External partners may need to be contacted and court orders prepared in order to gather evidence from their systems or staff.

The approach to managing the incident internally has several critical foci. The gathering and analysis of evidence requires specialist expertise for identifying and extracting the electronic information, and to ensure that due process is followed for the purposes of protecting the chain of evidence.

The non-technical aspect of managing internal communications and external public relations information is one consideration that may not be immediately apparent. This includes an authorised forum for staff, management, customers or external parties or media to be advised of the situation. Early release, or incorrect, or unauthorised disclosure of information may not only affect the chances of a successful investigation and possibly of identifying the culprit, but equally critical is the financial and continued stability and viability of the organization, including political, statutory, board, management, staff, customer, partner and public confidence.

7 What happens when it all goes wrong

If management has taken their responsibilities seriously and have underwritten and actively and visibly supported a security ethos within the organization, then the continuity plan will be executed and recovery will proceed. During this process, the reason for the event will be identified, new measures will be put in place to prevent a similar occurrence in the future, and a decision as to whether to proceed with an investigation will be made. If an investigation is conducted, the relevant data will be protected by responsible staff until the investigator(s) can take over responsibility. If the investigation produces evidence that is conclusive and analysis suggests that a prosecution or civil remedy be pursued, then executive management must take the decision whether to proceed with that action or not.

Throughout all of this, someone must be assigned the authority to take control and be responsible for the release of information, for protecting potential evidential data and storage devices where it may reside, for informing the appropriate executive and technical staff of the incident, for documenting the incident in detail (which will be useful during the investigation), and for disseminating regular progress reports throughout the recovery and investigative process.

Without this authority and singular figure to monitor and manage progress, the likelihood of successful recovery is reduced, and the success of any potential investigation is also reduced. Management gets to choose whether to pay now or pay

later. Pay now by having planned ahead, hiring or training staff to an appropriate level of security understanding and granting them authority to manage security breaches. Or pay later by potentially unsuccessful recovery and/or potentially unsuccessful prosecution or punishment or civil remedy.

This is not a question of *if* a security breach will happen but rather of *when* it will happen. New attack strategies are evolving every day. Those who would execute these strategies share new techniques and system flaws that can and will be exploited. Determined and/or disgruntled individuals may pursue an agenda of disruption, fraud or destruction for any number of reasons. Therefore the probability of being the victim of a breach is very high.

8 In summary

Implementing forensics security measures is intended to be part of an organization's larger information security strategy. It may be integrated with the fiduciary, regulatory, legal, and policy compliance requirements, as well as in the approach to investigating security incidents. It is intended to incorporate ideas and practices already accepted as part of business and security best-practice processes.

Many of the ideas in this paper are not intended to be new. The 'new' aspect, although it has been around for the last decade in specialist areas, is in the management of electronic information and potential evidence, which is being incorporated more and more in legislation.

Electronic evidence gathering or computing forensics should follow the same procedures of traditional evidence gathering. It is critical that they comply with the same stringent requirements in order for the evidence and its analysis to stand a up in a court of law, and be proven not to have been tampered with or compromised during any stage of the process. One critical element in the electronic world is that the evidence is not necessarily of a tangible and static form and may exist on local, national or international systems. The event may be detected in real time or after the fact. Determining the perpetrator can be difficult if insufficient data is logged.

An emerging trend in some jurisdictions is with government and regulatory bodies attempting to force or strongly encourage private and public organization to be held accountable and liable for protecting their information, staff and technical infrastructure from internal and external threats, as well as proving that this is the case before or after an incident has occurred.

The aim of this paper has been to define the law enforcement and legal aspects of traditional and computing forensics for senior management in an organization, where the assets including staff, customers, processes, data, information and technical infrastructure, are part of a critical value proposition for the organization to remain in business.

Consideration of the impact and likelihood of potential risks and threats to the organization's assets should include the process for management and staff on how to respond to a security incident, whether criminal or civil, and the investigative requirements. If assets are not considered important then, in the event of a breach or violation, there would be no need to determine the cause or impact to the overall organization and whether the business would remain operational.

9 The bottom line

It all comes back to the organization having a risk focus with senior management providing a governance and strategic plan and security policies, supported by operational procedures, to manage and minimise the known and potential risks.

Security audits, reviews and investigations are part of the continued assurance that the risk-management plan is effective. An audit and review confirms that good practices are being followed and tests the controls in place. An investigation may be used to determine the impact, accurately gather evidence to prove the cause, and hopefully achieve a successful prosecution or disciplinary action. All of the best security products, policies, audits, reviews or controls in place will not stop a would-be attacker. There is no 100% solution 100% of the time.

Defining a risk model, following best practice security standards, implementing good security products, defining security policies and procedures, training IT staff and educating users, continually reviewing the security threats, knowing and monitoring the organization's IT infrastructure, are a few highly recommended security practices.

Even if the incident is not deemed criminal or for other reasons is not worthwhile pursuing in a court of law, evidence is still a critical factor for ensuring a successful civil remedy outcome and minimising the dispute from an employee for wrongful dismissal or for being dealt with unfairly.

Defining and implementing 'best practice' security policies and practices may assist the organization to protect itself in the event of an investigation, limit the impact or risk; minimise the organization's legal liability, lower the actual cost to the organization to recover, minimise the loss of customer, stakeholder and shareholder confidence; and maybe minimise the statutory impact to the organization.

The organization is required by the stakeholders and, in some jurisdictions, statute to protect its information, resources, staff and assets, of which a forensics investigation is only part of the bigger risk-management picture.

10 Conclusions

This paper has addressed in broad non-technical terms the role of electronic forensics within an overall security policy and strategy. It is but one part of an all-encompassing holistic view of protecting the assets, integrity, reputation, continuity and operation of any given organization.

Security measures must be implemented in concert with an overall plan to minimize risk. Having the world's best firewall, for example, and failing physically to protect servers from someone destroying them with an axe is false security.

Security begins with policy and ends with a continuity plan that will facilitate recovery when all else fails. It also entails everything in between such as physical security, internal audit measures, anti-virus protection, firewalls to thwart intruders into your network, encryption to protect the privacy or confidentiality of organizational information and many more issues. It is not one-dimensional but holistic in its nature.

References

[1] Francis Bacon (1561-1626) in a letter to the Earl of Essex 1598

[2] CSI/FBI Annual Security Survey 2003 – (Computer Security Institute/Federal Bureau of Investigation) the number of internal and external incidents over the past five years is approximately equal, see page 7 of the

Survey. The 2003 Survey can be obtained from: www.gocsi.com/press/20020407.jhtml;jsessionid=LY1UTACFKM3BCQSNDBCSKHSCJUMEIJVN?_requestid=87673

[3] Sources of standards – ISO/IEC 17799:2001 Information Technology – Code of Practice for Information Security Management (http://csrc.nist.gov/publications). Other risk management standards may be found at: SANS (SysAdmin, Audit, Network, Security Institute, www.sans.org) and NIST (National Institute of Science and Technology, www.nist.gov).

[4] FTC settles with Guess on Web vulnerabilities, Computerworld 19 June 2003, www.computerworld.com.

[5] US Department of Justice, Electronic Crime Scene Investigation: A Guide for First Responders, Washington DC, July 2001, NCJ-187736, www.ojp.gov:80/nij/pubs-sum/187736.htm

[6] Vogon International Limited – this UK organization provides forensics as well as data recovery services, www.vogon-computer-evidence.com

[7] CERT – Computer Emergency Response Team located at Carnegie-Mellon University, Pittsburgh, Pennsylvania, www.cert.org. There are several such organizations around the world – for example: Janet-CERT, DoD-CERT, AusCERT, DFN-CERT.A definitive list may be found at www.first.org/team-info

[8] FIRST – Forum of Incident Response and Security Teams. This can be found on the Internet at www.first.org