# Contents

Introduction ................................................................................................................ 2  
Computer Forensics and System Administration ....................................................... 3  
“It won’t happen to me!” .............................................................................................. 4  
Identifying an incident ................................................................................................. 5  
  What to do .............................................................................................................. 6  
Collecting evidence .................................................................................................... 8  
  Applying the Rules ................................................................................................ 10  
  Chain of Custody .................................................................................................. 13  
How to collect the evidence ...................................................................................... 15  
  The Ideal Situation ............................................................................................... 15  
  The less-than-ideal situation ................................................................................ 17  
  Offline Copy of Tools ............................................................................................ 20  
  Testing the tools ................................................................................................... 20  
The System Administrators Forensic Toolkit ............................................................. 21  
Presenting the Evidence .......................................................................................... 23  
Conclusion ............................................................................................................... 24  
Annex A Sample Chain of Custody form .................................................................. 25  
References ............................................................................................................... 26  

Title page image taken from: http://electronicevidenceretrieval.com/eer_computer_forensics_defined.htm
**Introduction**

In many cases that involve the use of forensic investigation after an incident has occurred, whether by law enforcement or internal organisation security, vital evidence has been destroyed or made unusable by the system administrators responsible for operating the system. This isn’t to say that they have been negligent in their responsibilities; it is quite the opposite. The destruction of forensic data has occurred due to the fact the system administrator has been undertaking their primary function; running their systems and ensuring that they keep running.

What this demonstrates is that the goals of these two fields, computer forensics and system administration, are at times mutually exclusive. The computer forensic specialist needs to keep the “scene of the crime” just as it was when the intruder left it. The system administrator needs to get things back to business as usual as quickly as possible.

The intent of this paper is to develop a common ground between the two fields where the primary objectives of each can be reached as closely as possible.

The areas that this paper will cover are:

- Educating system administrators in what to do after an incident has occurred to ensure that forensic evidence is not lost
- Cover the basic rules and regulations surrounding proper evidence handling
- Developing a system administrators forensic tool kit

The areas that this paper will *not* cover are:

- An in-depth knowledge of computer forensics. This paper is intended only to provide system administrators with front-line first response knowledge. Its intention isn't to make you a forensic expert, but just to provide enough knowledge to secure data for further analysis by computer forensic specialists. A real world analogy is that this will teach you how to put the police tape around the scene of the crime, collect basic information and hand it over to the detectives when they arrive
Computer Forensics and System Administration

So far we have talked about concepts of System Administration and Computer Forensics. Before we continue too far into this paper, let’s define these terms a little more accurately.

Computer forensics “is the use of specialized techniques for recovery, authentication, and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer forensics generally requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel1”.

Put simply, computer forensics involves looking at the normally unseen events happening “under the hood” of the computer system. Examples can include:

- Installing an application on a Microsoft Windows system.
  This action will generally not only place files on the hard drive in one or more directories, but will also write entries to a number of locations in the system registry.

- Creating and editing a Microsoft Word document.
  This action will leave traces linking it to the computer it was created on.

- Deleting files from any contemporary operating system.
  The method in which most operating systems handle this action will allow deleted files to be retrieved with minor and trivial effort.

1 http://en.wikipedia.org/wiki/Computer_forensics
A definition of System Administration is a little harder to determine. The tasks given to a generic position of System Administrator are many and varied. A reasonable definition for the purposes of this paper is “a person employed to maintain, and operate a computer system or network for a company or other organisation”. The main duties of a System Administrator will generally include installing, supporting and maintaining servers or other network devices, and planning for and responding to outages, problems or incidents (as described in the next section) that occur with those devices.

Based upon these definitions it is clear that they are very distinct fields within the Information Technology industry. However, the one main area where these fields crossover is in the “planning for and responding to outages or problems that occur with those devices”.

It is an unfortunate fact of modern computing that there are people who “don’t play nice with others” in the digital world. System Administrators need to respond to these efforts by ensuring the systems are available for their organisation. Forensic personnel need to respond to these efforts by ensuring those responsible are identified and dealt with appropriately.

“*It won’t happen to me!*”

The first thought you may have is that this won’t happen to me so why should I bother? I have my virus patterns up-to-date, a great firewall and IDS protecting my system, so spending time and effort on this stuff is really a waste.

Granted, statistics are proving that electronic attacks are generally on the decrease over the last few years (only a slight increase was measured from last year). This is relatively good news and possibly an indication that security systems are getting to a sufficient level to protect from most attacks. However, some disturbing figures are still true:

---

2 http://en.wikipedia.org/wiki/System_administrator
• The total average annual loss for electronic attack or computer crime has increased by 63% from the previous years figures. This represents an average loss of $241,150 per organisation.

• The great sources of financial losses in 2006 were due to theft or breach of proprietary or confidential information.\(^3\)

While we may be winning on one front in regards to electronic attacks, the attacks that are still successful are more devastating than ever.

This means that more than ever, a proactive approach to protecting your systems in any way you can is essential.

**Identifying an incident**

A general definition of an incident is any adverse event in an information system or network or the threat of the occurrence of such an event. Depending upon the nature of the organisation, types of incidents may vary. Some examples may include:

• Hackers
• Employee error
• Malicious employee activity
• Natural disasters
• Bomb scare (either at your facility or in the surrounding area)
• Power outage
• Storm
• Industrial action
• Hazardous material spill
• Software failure
• The list goes on and on!

Although the list is large, for the purposes of what we are discussing with this paper, it is a little narrower. In terms of incidents that may require protection or examination

\(^3\) 2006 Australian Computer Crime and Security Survey
of data in a forensic manner, the list is reduced to incidents that directly relate to the system or network. This then becomes something like:

- Hackers
- Malicious employee activity
- Industrial action (or in this case, more industrial sabotage)

The main point to remember about incidents is that the system or network administrator will generally be the first to discover it. If the firewall or IDS administrator detects it, generally we are looking at an attempt, not a successful incident. When the system or network administrator discovers the incident, then it should be considered serious because it has already bypassed the perimeter security and made it safely into the internal confines of the network.

**What to do**

Remember we aren’t discussing what to do in terms of how to bring your systems back online, we are talking about what to do in terms of maintaining forensic data after an incident similar to that describe above has occurred. From here you have a number of choices:

**Option #1 Ignore it**

When your systems are up and running the crisis is over. Why not continue on with business as usual? Depending upon the incident this may be a consideration. If no data was lost or compromised, money wasn’t lost to the business what harm can it do?

Consider these points:

- *Is the incident over?*
  Are we sure that there is no remnant of the incident left? Has the intruder left a backdoor program or virus in the system? What may seem like a harmless insignificant incident today could turn out to be a major one tomorrow. Due to the volatile nature of forensic data, unless the work is done to collect it at the time it happens; it may be too late to collect it at all.
• *What happens next time?*
  This incident may well have been minor and insignificant and no harm was done to the organisation, but what about next time? Next time the intruder may do more damage, particularly if there was no consequence from the first intrusion.

• *What is the organisation’s liability?*
  No harm may have come to your organisation, but what about others? Has the intruder launched an attack on another organisation from your infrastructure? If this is the case, then the liability for this attack may rest with your organisation. One of the key factors in determining liability in this case is if the organisation involved took reasonable steps to ensure the security of their systems. Ignoring an incident doesn’t fall under “reasonable steps”.

**Option #2 Rebuild the systems**

All things being equal, you could simply take the systems offline and rebuild from image disk and/or backup tape. While this may bring the system into a working state again, it does really address the problem that caused the situation in the first place; the vulnerability that let the attacker into your system. This means that it is likely only a matter of time before the same thing happens again.

As you can quickly determine from the options presented above, there really is only one legitimate course of action to take in response to an incident such as an intrusion:

1. Bring your system back online as quickly as possible
2. Find who/what is responsible and ensure that it doesn’t happen again

Any action other than this puts the organisation involved in the incident, and potentially other organisations as well, at risk from repeat attacks.
Collecting evidence

To paraphrase the Heisenberg Uncertainty Principle in physics which states that “if you observe it, it will change”, the same can be said of evidence collection; “it you collect it, it will change”.

This means that the evidence left behind from an intrusion is incredibly volatile and great care needs to be taken when collecting it to ensure that it doesn’t become invalidated.

A definition of what constitutes digital evidence is:
“…any information, whether subject to human intervention or otherwise, that has been extracted from a computer. IT evidence must be in human readable form or able to be interpreted by persons who are skilled in the representation of such information with the assistance of a computer program.”

In the corporate environment, examples of evidence could include:
- Any data file of any kind, either present or recently deleted
- Audit log entries
- Registry settings
- User account information
- Network traffic
- And the list continues!

An examination of how to collect evidence will be covered later in this paper. Firstly, let’s examine a number of general principles that need to be followed when collecting evidence.

1. The evidence must be admissible

Fairly simple one would imagine, but certainly something that can easily be forgotten in the middle of the collection process. A few factors come into play with this rule:
- The evidence must be collected in a manner that is forensically sound. It needs to be collected using proper procedures and correct tools.

---

4 HB 171-2003 Guidelines for the management of IT evidence
• The evidence must follow the relevant legislation regarding evidence. Australia is currently working towards a form of standardisation in terms of evidence legislation and some states are currently compliant. However, differences between State and Commonwealth need to be understood and followed.

2. Authentic
You need to conclusively tie the evidence to the incident in question and demonstrate how it is relevant.

3. Complete
Evidence must be collected from all perspectives. Simply collecting evidence of what the attacker did isn’t enough from an evidentiary perspective. A broader look at the entire environment needs to be included. For example, in the event of an incident relating to internal employee misuse, a possible piece of evidence would be log entries indicating that the user in question was logged in at the time the incident took place. This piece of evidence alone can show that the user in question could have done it, but what about other users logged in at the same time? What evidence is there to show that the other users didn’t cause the incident?

4. Reliable
This is where procedures for collecting evidence become vital. They need to be tested and sound and most importantly, proven.

5. Understandable
The evidence needs to be clear and easily understood by non-technical people such as a jury. There is no point in presenting a binary dump of process memory if the jury has no idea what to make of it. That said if you produce a version of evidence that is simplified to allow non-technical people to understand it; a clear link to the original evidence will also need to be demonstrated as well.
Applying the Rules

The above rules provide some general high level guidance on what to do in terms of collecting evidence. Once again, the purpose of this paper isn’t to make you forensic experts, but just to give you a background to allow you to prepare the way for their work to be completed. Applying these rules will help you to do this.

Using these rules, further practical guidelines can be developed. The following is a list of practical points which should be followed.

1. Comply with the five rules of evidence
   This should be simple enough. The rules are there for a reason and provide good guidance on what to do when a situation arises.

2. Minimise handling/corruption of original data
   Every time you touch or handle the evidence you either change an attribute or run the risk of corrupting or overwriting required data. When undertaking work on evidence always ensure:
   - it is on a copy and not the original (more on this later)
   - you have a clear plan on what you want to do with the evidence
   - you know exactly the steps you need to take.

3. Account for any changes and keep detailed logs of your actions
   There is one overarching rule to follow when working on evidence; write everything down! You can’t take too many notes. Another point to remember is that the notes need to be contemporaneous and handwritten. Keeping an electronic text file won’t be admissible as evidence and is therefore useless.

4. Do not exceed your knowledge
   If you don’t know or aren’t comfortable with a particular action, don’t do it. Leave it to the experts or ask for help. There is no second chance when collecting evidence. Once it is gone, it is gone.
5. **Follow your local security policy and obtain written permission**

This point is vital. In the course of collecting evidence, you may be called upon to access other user’s files and resources. Before you do this make sure that you have permission from management and that you are fully compliant with any and all regulations such as organisational security policy and/or privacy legislation. Failure to ensure this could result in either the evidence being invalidated or the evidence collector facing organisational disciplinary action and/or legal charges.

6. **Capture as accurate an image of the system as possible**

In the ideal situation, the capture will be done by forensic experts with specialized tools. But often an immediate capture may be called for. In this situation, a slightly imperfect capture is better than no capture at all. Details on how to go about capturing data will be covered later. The main point you need to remember about this activity is to detail, in writing, exactly how you took the capture. This may be called upon as part of the evidence package at a later stage.

7. **Prepare to testify**

This may or may not be a requirement. But you should really prepare for the possibility, especially if the incident has done significant damage to your organisation. In most cases this type of activity would be done by someone within the IT security section of your organisation who has experience with legal proceedings; but if you are undertaking evidence collection, it is a possibility that you may be called.

8. **Ensure your actions are repeatable**

This is where taking comprehensive notes becomes valuable. You need to ensure that the evidence you collected was done in a systematic and robust manner; not just luck! You also need to ensure some one else can follow the steps outlined and generate the same results.

9. **Work fast**

Time really is of the essence. As stated previously, you are dealing with volatile evidence, so the quicker you can collect it and secure it the better.
10. Proceed from volatile to persistent evidence

A lot of the evidence that falls into the volatile category is data that can really only be collected by using dedicated forensic analysis tools. The main thing to remember from this point is to ensure you understand what evidence is volatile and what is not and also work to protect the most volatile evidence as much as possible.

Some examples of evidence that may be collected during an incident in order of most volatile to least volatile are as follows:

- Registers and Cache
- Routing tables
- Arp cache
- Process table
- Kernel statistics and modules
- Main memory
- Temporary file systems
- Secondary memory
- Router configuration
- Network topology

11. Don’t shutdown before collecting evidence

The act of shutting down a system will potentially overwrite valuable data. A number of the items on the above list of potential evidence that are the most volatile will be destroyed as part of the operating system shutdown procedure.

Any affected system needs to be maintained in an operational state until evidence is collected. If there is potential that the system may cause harm if left on (such as in a DDOS attack), then it should be disconnected from the network only. However, this action should be weighed against the potential loss of evidence as well. Computer forensic data in an incident may well include traffic flow. Where ever possible the decision to remove any device off the network should be made by computer forensic personnel.
12. Don’t run any programs on the affected system
Every program you run on an affected system may destroy valuable evidence.

Chain of Custody
This is not an issue that is unique to digital evidence. All evidence for use with legal proceedings needs to follow chain of custody guidelines.

Chain of Custody is a concept in jurisprudence which refers to the handling and integrity of data. The intent here is to answer the following questions:

- What is the evidence?
- How did you get it?
- When was it collected?
- Who has handled it?
- Why did that person handle it?
- Where has it travelled, and where was it ultimately stored?

What this aims to ensure is that the exact evidence collected is the exact evidence eventually presented in court.

As with evidence collection, there are a number of rules that need to be applied with chain of custody:

1. Set your evidence storage and handling policy now, not when you actually have evidence.
There are no second chances with any evidence, particularly not digital evidence. If an incident involves legal proceedings, any break in the chain of custody could invalidate the evidence you have collected. What you need to address here is the following:

- A secure place to store the evidence. Something such as a safe or secure room. Any location where access is limited to essential personnel only
- Documentation supporting the chain of custody procedures. This needs to be a document that is attached to the evidence itself that sets out what the
evidence is, when it was collected and who has handled it. A simple form is included in Annex A as an example.

2. Guard the “best evidence” closely
The term “best evidence” refers to the evidence collected as soon after the original incident as possible. The longer the delay in collecting the evidence, the more it will change and become less useful as evidence. You may want to consider categorizing the best evidence separately from anything else collected and potentially storing it separately as well.

3. Do your work on copies only
Although covered earlier, it is important to stress this in terms of chain of custody. Don’t work with your original or best evidence, always make a copy. Conducting examinations or analysis using originals will invalidate the chain of custody.

4. Keep the chain of custody forms up-to-date
No one likes paper work, but in this case it is more than essential. A failure to record a link in the chain of custody will result in the evidence being invalidated.

5. When not in use, keep your evidence in tamper proof containers
It is no good recording a chain of custody if your evidence is left in the open for anyone to handle. Although you will likely lock the evidence away in a secure room or safe, an additional layer of protection that is advisable is a tamper proof container. This doesn’t need to be an unbreakable container, just a container that will show signs of any tampering. The Australian Government Security Equipment Catalogue has a number of endorsed products (designed for both government and private industry) that can fulfil this requirement.\(^5\)

How to collect the evidence

Any examination of digital evidence needs to be done using legally robust and sound techniques and tools. Usually the purpose of examining this data is to build evidence for use in legal or internal organisational disciplinary proceedings. The nature of the adversarial legal system used within Australia and most Western countries will result in this evidence being called into question in terms of validity. If the techniques used to collect the evidence are flawed, this can invalidate the results proven by the evidence.

For the most part, the main evidence collected in any major incident will likely be undertaken by trained forensic experts using specialized tools. This is the preferred method. However, the system administrator will be the person first on the scene and in a unique position to potentially collect information that may no longer be available by the time a full forensic analysis is undertaken.

For any data that will be used as evidence, particular care needs to be taken when either producing a copy of the original for examination or taking a copy from the system in question. Regular copying programs will usually alter some or most of the attributes that each file contains. These can include date and time last modified, ACLs, ownership information etc. In a lot of cases, these are vital elements required from the evidence.

The Ideal Situation

The precise method of evidence collection will greatly depend upon the circumstance. In all cases, the ideal situation is having properly trained computer forensic personnel undertake the evidence collection. The following is a list of different options (in order of preference) that can be used in a range of situations.

1. Take the computer offline

If this is at all possible, this is the preferred option. Note that it is take the computer offline, not turn the computer off. Turning the computer off will destroy volatile
evidence that may be needed for the investigation. Simply isolate the computers involved in the incident from the rest of the network.

As discussed previously, you need to be aware of the potential that a traffic flow may be an evidence requirement. The specific situation will need to be examined and a judgment made.

2. Remove and replace the hard drive
Given that most systems can’t be simply taken offline and left offline without significant detriment to the business, replacing the hard drive is another option. Remove the hard drive and replace it with new drives and restore the system from backup. This will result in some downtime, but the system will fairly quickly be brought back up. If this option is undertaken a few factors need to be taken into account:

- The system will still not be able to be powered down. The architecture of the computer will need to support removal of the hard drives while still powered. This also includes supporting the removal safely and taking into account all occupational health and safety requirements.
- When the hard drives are removed, full details of the computer it was taken from will need to be recorded. These details should include:
  - Time/date settings
  - Full hardware specifications
  - Computer role
  - IP address
  - Technician who undertook the task

3. Copy the hard drive
If the drives can’t be replaced a forensically sound copy will need to be made. Ideally this should be done by trained forensic personnel; however in the event this isn’t possible the following section will outline some methods and tools available to system administrators that will produce as close to a forensically sound copy as possible.
4. **Live bit-stream copy**

If it is impossible to take the system offline at all, a live bit-stream copy can be made of the drives. The tool netcat (see next section) is capable of undertaking this function; however this is not a simple process and should only be undertaken by the system administrator if no other option is available.

5. **CD/DVD Copy**

This is an option to consider if all else is unavailable. Care should be taken to ensure that as much of the meta-data as possible is copied from the original source.

6. **Live analysis**

This should only be undertaken if suitably qualified personnel are available. This option presents the greatest risk to the evidence.

**The less-than-ideal situation**

As identified above, this activity should be undertaken by properly trained computer forensic personnel using specialist tools. However, the ideal situation is not always possible and sometimes a choice between getting the data in a potentially flawed manner and not getting the data at all needs to be made. In this circumstance, the following system administration tools should be considered for use.

**Netcat**


This tool, originally Linux with a port to Windows, is capable of taking an exact snapshot of a hard drive including swap space partitions and non-overwritten clusters. These attributes make this an ideal tool for collecting evidence for forensic analysis.
**MD5 Utility**

*All platforms* - [http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html](http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html)

An MD5 utility is an implementation of the MD5 message-digest algorithm described in RFC1321. This algorithm takes as input a message and produces a 128-bit “fingerprint” or a “digital signature” of the input\(^6\).

In terms of digital evidence collection, this means that assurance can be demonstrated that a copy made of digital evidence is a precise and accurate copy. For any system administrator making copies of data collected, an MD5 has value should be calculated to ensure the integrity of the copies can be proven.

It should be noted that while RFC1321 (1992) states it is conjectured that “it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest”, recent research has shown that a collision attack\(^7\) can be conducted against the MD5 algorithm using a standard home PC in a reasonably short amount of time.

This, combined with other similar research, has resulted in the use of MD5 digests being brought into question from an evidentiary viewpoint. Prior to any use of this utility for legal evidence, advice from legal personnel or proper authorities should be sought.

**TCPFlow**

*Unix/Linux* - [http://www.circlemud.org/~jelson/software/tcpflow/](http://www.circlemud.org/~jelson/software/tcpflow/)

*Windows – unknown*

Tcpflow is an open source tool used to break network traffic into individual flows. Each flow is then recorded in a separate text file for later analysis.

---

\(^6\) RFC1321 1992

\(^7\) A collision attack is the process of finding two arbitrary values whose hashes are identical (referred to as collide). In terms of the use of MD5 for ensuring the integrity of forensic evidence, this vulnerability would potentially allow a change in the evidence to be made with no change to the MD5 hash value.
**TCPDump**


Tcpdump is a basic network traffic monitoring utility that is included with most Unix and Linux distributions and has also been ported to Windows (see above link). It can monitor traffic and display header information directly to screen or to text file for later analysis.

As with tcpflow, it monitors data of a temporal nature and can be deployed quickly where and when required.

**XCOPY**

*Unix/Linux – Windows only

*Windows – included with operating system*

This is possibly the least suitable tool to use for forensic copying, but it is a tool that is available in all Windows environments and if nothing else exists to do the job, there are switches that can be used with the command to take as much of the data as possible.

When running xcopy for the purposes of a forensic copy (or as close to as the tool will allow), use the following switches:

/O – copies file ownership and ACL information

/H – copies hidden and system files also

/Z – copies networked files in restartable mode

/C – continues copying even if errors occur

/E – copies directories and subdirectories, including empty ones.

/V – verifies each new file

**Robocopy**

*Unix/Linux – Windows only


Robocopy is a free utility from Microsoft which allows copying of files over a network connection. It also has the capability of restarting the copy process should problems occur with the network connection.
By itself, I would not recommend this tool for use at all. However, add-on utilities are available that use Robocopy and are designed specifically for forensic investigation. One such tool is FriendlyRoboCopy. This tool provides a GUI interface which is designed to assist the forensic investigative process.

*Friendly RoboCopy - http://www.cleardigitalevidence.com/

**Offline Copy of Tools**

This can’t really be stressed enough. If you are going to use tools to examine your systems after or during an incident, can you be certain that these tools haven’t been tampered with or replaced?

If an attacker discovers a copy of Netcat, TCPFlow or any of the tools mentioned in this section on the system they are attacking, they may well delete or tamper with those tools to derail or slowdown any investigation that may take place.

The only safe alternative is to create a known good CD ROM copy of any tools you will be using.

**Testing the tools**

Another important thing to remember is that the output of the tools may need to be called into evidence in some type of formal proceeding. If any of the above mentioned tools are going to become part of your forensic toolkit, undertaking testing with the tools where the results are known is recommended. Depending upon the tool, this test could vary but an example would be undertaking a netcat transfer of selected files where the properties (date stamp, permissions etc) are known in advance and then comparing the results on the copy. Basically you are just validating that the tool functions correctly.
The System Administrators Forensic Toolkit

Preparation prior to the incident will prevent poor performance during the incident. Just like as you would prepare a toolkit for any desktop field work undertaken, the same should be done for forensic investigation or response. The following is a list of items which should be kept within the toolkit.

Notebook
As discussed previously, written notes are essential and are often required to be submitted as evidence. For that reason, the notebook used should have the following attributes;

- Numbered pages
  This will ensure that there can be no question of any pages missing from the notebook and that all observations or actions are written and recorded
- Bound pages
  For the same reason the pages are numbered, a bound notebook will ensure that no pages can be removed without showing a noticeable trace

A few general guidelines also need to be observed when taking notes:

- Notes should be taken as soon as practicable after the event has occurred
- Notes should include date, time, day and location of the event as well as a signature
- Notes that involve conversations should be as accurate as possible. If precise wording of any conversation can’t be specifically recalled it should be noted as such.

CD copy of all relevant tools
As discussed in the previous section, an offline copy of tools you will use should be kept

A clean laptop
During the early stages of an incident, you may not know what has or has not been compromised. A clean laptop will ensure that you have some computing power that
is known to be secure. You should also include the image disks for the laptop as well in the event it becomes compromised during the incident.

*Blank CD/DVDs*
A good supply of media ready for copying collected evidence.

*Label maker*
One thing that will also invalidate evidence is if you can’t be sure exactly what it is. As soon as any CD/DVD is made is should be labelled with details such as:

- Date
- Time
- Server/workstation data was taken from
- Who copied the data

The label maker should be able to print labels that can be securely fixed to the media or object being labelled.
Presenting the Evidence

Evidence collected after an incident will often be used in either legal action or internal disciplinary action. Whichever direction the circumstance takes, action undertaken during the course of the collection of evidence will be brought into question either formally in a court room or in proceedings conducted by the organisation.

The main factor that you need to remember is that you will need to explain and defend the procedures, actions and outcomes you have been involved in.

An example can be seen in the case of T Lewis and Toyota Motor Corporation\(^8\). In this case evidence obtained from the employee’s computer system was collected to support the dismissal of the employee. During the cross examination, a number of challenges was put to the computer forensic expert:

- Although the computer was principally used by the employee, the evidence could have been derived from the actions of other employees who also used the computer occasionally
- The evidence collected belonged to the previous owner of the computer
- How is the copy of the computer system a true and correct copy of the original data and can it be relied upon
- The technology and procedure used in the analysis is questionable and cannot be relied upon

Although as System Administrators, it is more than likely you won’t be in a position to need to testify in any formal or legal proceedings and this type of activity will be left solely to the computer forensic experts, it is still a possibility and one that should at least be prepared for.

\(^8\) 2006 Australian Computer Crime and Security Survey
Conclusion

This paper has attempted to bring together two disparate areas of Information Technology. Each area has its own priorities and requirements, but they also can’t complete their roles effectively without some understanding of the other and cooperation.

From the information presented here, a few overarching guidelines should be remembered:

1. If in doubt, don’t do it
2. If you have access to specialized forensic expertise, let them do it
3. If you have to do it, write down what you do
## Annex A Sample Chain of Custody form

<table>
<thead>
<tr>
<th>Description of item(s) obtained:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Obtained from: (Title, name, location, phone number, date)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Temporary disposition of item(s): (where stored; show releases below)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(Included printed name and signature for all releases)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Released by:</td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Final disposition of item(s):</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
References


How to Keep A Digital Chain of Custody. CSOonline.com. Sarah D Scalet.
http://www.csoonline.com/read/120105/ht_custody.html

MD5 Homepage (unofficial). Mordechai T Abzug.
http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html