Abstract
The paper investigates what computer forensic is at the most basic level. The concept of Computer Forensic is thought to be widely known, but in essence is it? At the most fundamental level can computer forensics be defined. This paper will focus on a variety of approaches to actually defining computer forensics.

Keywords
Computer Forensic, data and security.

INTRODUCTION
Due to the application of computer technology used to investigate computer-based crimes, a new specialised field called forensic computing has been developed, becoming famous worldwide amongst the digital crime scene. Computer related incidents can range from external intrusions into someone’s system, internal fraud or staff breaching a security policy. A constant development in information technology has posed challenges for those policing cyber crime. For many organisations, identifying, tracking and prosecuting these threats has become a full-time job (Borck 2001).

The aim of the paper is to look at what computer forensic is from the most basic level and discuss the implications.

COMPUTER FORENSICS DEFINED
Forensics is defined in the Merriam Webster’s dictionary as belonging to, used in, or suitable to courts of judicature or to public discussion and debate and relating to or dealing with the application of scientific knowledge to legal problems. It comes from the Latin “of the forum”. Computer forensics can be defined as the collection, preservation, analysis and court presentation of computer-related evidence (Patzakis, 2002). The forensics process can often involve the creation of bit stream copies of digital storage to both ensure the integrity of the data and to capture data which would otherwise be lost in a logical copy. This is often a resource and time consuming activity and its appropriateness and necessity is one of the most debated areas of incident response and computer forensics.

A number of models and methodologies have been developed in the computer forensic field.

Lucent Model
Warren Kruse is currently the Investigations Manager, Cyber Investigations and Forensics, for Lucent Technologies where he has worked since 1998. Jay Heiser, CISSP, is an Information Security Officer in the Group Risk office of UBS AG, the global Swiss financial services firm.

Kruse and Heiser have developed a methodology for computer forensics referred to as the three “As” that is acquire, authenticate and analyse (Kruse and Heiser, 2002). In detail the steps are:

1. Acquire the evidence without altering or damaging the original. Consisting of the following steps:
   - Handling the evidence
   - Chain of custody
   - Collection
   - Identification
Storage
Documenting the investigation

2. Authenticate that your recovered evidence is the same as the originally seized data;
3. Analyse the data without modifying it.

Kruse and Heiser suggest that perhaps the most essential element in computer forensics is to fully document your investigation including all your steps taken. This is particularly important if due to the circumstances you did not maintain absolute forensic integrity then you can at least show the steps you did take. It is true that proper documentation of a computer forensic investigation is the most essential element and is commonly inadequately executed.

KPMG Model - Australia

Rodney McKemmish is a Senior Manager with KPMG Brisbane Practice and is the National Leader of KPMG’s Computer Forensic Group. McKemmish had served in the Victoria Police with the Computer Crime Unit as a forensic examiner and later as the head of the Queensland Police Computer Forensic Unit. McKemmish undertook research in the area of Computer Forensics in 1999 under a Churchill Fellowship. In the paper he produced he identifies the four key elements in forensic computing (McKemmish, 1999). They were:

1. The identification of the digital evidence;
2. The preservation of digital evidence;
3. The analysis of digital evidence;
4. The presentation of digital evidence;

In addition he introduces four rules to allow for the presentation of digital evidence in a judicial environment.

Rule 1 Minimal handling of the original;
Rule 2 Account for any change;
Rule 3 Comply with the rules of evidence;
Rule 4 Do not exceed your knowledge.

His fourth rule states that an examiner should not go beyond his area of knowledge saying “It is essential that the forensic computer examiner is aware of the limit of their knowledge and skill.”(McKemmish, 1999) He suggests the examiner cease his examination and seek assistance from a more experienced examiner. While this sounds like excellent advice it does lend itself to an interpretation that only the most experienced computer forensic examiner should attempt an examination if of a complex or unknown nature. If the proper safeguards are in place and the examiner is not working on the only copy of the evidence going beyond one’s knowledge would not only be low risk but also in many cases necessary.

Dittrich and Brezinski Model

Dominique Brezinski is a Senior Technical Advisor at In-Q-Tel, a non-profit technology incubator formed by the United States Central Intelligence Agency (CIA). David Dittrich is a Senior Security Engineer and for the University of Washington's Computing & Communications University Computing Services Security Operations group. Dominique Brezinski and David Dittrich presented a technical training session on Intruder Discovery / Tracking and Compromise Analysis at Black Hat 2000 (Dittrich and Brezinski, 2000). In that session they also described their methodology for forensic examination. It had the following steps:

(A) Formulate plan;
(B) Approach and Secure Crime Scene;
(C) Document Crime Scene Layout;
(D) Search for Evidence;
(E) Retrieve Evidence;
(F) Process Evidence.
As you can see in this methodology they do not provide any pre-determined approach as to how to conduct the forensic examination they simply describe the steps. This black box approach is more practical as the demands of each situation are variable thus the method of forensic examination will need to vary.

**Yale University Model**

Eoghan Casey is a System Security Administrator at Yale University where he investigates computer intrusions, cyber stalking reports, and other computer-related crimes, and assists in the research and implementation of university wide security solutions. He is the also the author of Digital Evidence and Computer Crime (Casey, 2000) and the editor of the Handbook of Computer Crime Investigation (Casey, 2002). Casey has conducted numerous training and education sessions in investigating computer crime. Casey has developed the following digital evidence guidelines (Casey, 2000).

Casey: Digital Evidence Guidelines

1. Preliminary Considerations
2. Planning
3. Recognition
4. Preservation, collection and documentation
   a) If you need to collect the entire computer (image)
   b) If you need all the digital evidence on a computer but not the hardware (image)
   c) If you only need a portion of the evidence on a computer (logical copy)
5. Classification, Comparison and Individualization
6. Reconstruction

Casey identifies that there is a decision point whether you need all the evidence on a computer and to consider imaging or whether you just need a portion then a logical copy can be considered.

**Mitre Model**

Gary L. Palmer is an Information Security Scientist with The Mitre Corporation. He maintains that in general, the digital forensic information must possess the following characteristics (Palmer 2002):

- Relevant and/or Material: Will this information assist decision-makers in their tasks?
- Credible and/or Competent: Is the information believable, trustworthy, and true and, if so, by what measure?

This more legalistic approach is of interest as it addresses important investigatory issues of relevance, which are often ignored in other methodologies over issues of completeness and credibility (Palmer 2002).

**US Department of Justice**

The US Department of Justice (DOJ) in their guide to “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations” list the following four basic Strategies for Executing Computer Searches (DOJ 2002):

- Search the computer and print out a hard copy of particular files at that time;
- Search the computer and make an electronic copy of particular files at that time;
- Create a duplicate electronic copy of the entire storage device on-site, and then later recreate a working copy of the storage device off-site for review (Bit stream Copy);
- Seize the equipment, remove it from the premises, and review its contents off-site.

DOJ comment that which option is best for any particular search depends on many factors. They say the single most important consideration is the role of the computer hardware in the offence (DOJ 2002).

**CONCLUSION**

One of the authors was previously in Police Service and recalls a Police computer forensic examiner explaining to an investigator that as the computer he had seized had been tampered with there was no point in examining it any further. He found this surprising given that he knew while the courts were particular about the admissibility of evidence they were also very particular about exploring any possible avenue for evidence. The possibility of
exculpatory evidence, which may have been overlooked because of such high standards, may impact an otherwise strong case. Courts expect that every effort will be made to bring relevant evidence before them. Also one must remember that crime scenes in the physical world are rarely pristine environments. In many crime scenes the primary focus initially is to save life. That is not to say that those crime scenes do not later produce evidence of a significant nature. The issue is more about accounting for that disruption rather than just writing any evidence off.

One contrary argument to support the purest approach could be because of this high standard the examiners are not usually challenged in later judicial proceedings, which is certainly generally the case. However one only has to look at other expert evidence such as that provided by medical practitioners in assault cases to see that often this type of evidence is usually admitted without any cross examination of the witness.

As Kruse puts it “computer forensics is often misunderstood as being somehow different from other types of investigations...if you were investigating a murder in Times Square...nobody expects you to rebuild Times Square in the courtroom, but that is often the expectation (of some practitioners) in a computer crime case (Kruze 2002).”

Computer Forensics is not fundamentally different from other types of investigations and this needs to be understood. But major differences exist in the basic definition of what computer forensics actually is. The reasons for this are hard to define and will be the focus of future research.

REFERENCES


COPYRIGHT

[S McCombie & M Warren] © 2003. The authors assign to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to ACIS to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.