4-12-2006

Taxonomy of computer forensics methodologies and procedures for digital evidence seizure.

Krishnun Sansurooah
Edith Cowan University

DOI: 10.4225/75/57b13730c7056
4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 4th 2006.

Taxonomy of computer forensics methodologies and procedures for digital evidence seizure.

Krishnun Sansurooah
School of Computer and Information Science (SCIS)
Edith Cowan University Perth, Western Australia.
ksansuro@student.ecu.edu.au

Abstract

The increase risk and incidence of computer misuse has raised awareness in public and private sectors of the need to develop defensive and offensives responses. Such increase in incidence of criminal, illegal and inappropriate computer behavior has resulted in organizations forming specialist teams to investigate these behaviors. There is now widespread recognition of the importance of specialised forensic computing investigation teams that are able to operate. Forensics analysis is the process of accurately documenting and interpreting information more precisely digital evidence for the presentation to an authoritative group and in most cases that group would be a court of law. At the level of practice these investigative skills extend beyond a methodological approach. The scope of this paper will compare the different methodologies and procedures in place for the gathering and acquisition of digital evidence and thus defining which model will be the most appropriate taxonomy for the electronic evidence in the computer forensics analysis phase.

Keywords

Forensic Computing methodologies, digital evidence, evidence acquisition.

INTRODUCTION

The changing face of communication has made computer-based information a primary source of evidence in many legal matter and investigations. World cultures are forming ever-increasing dependencies on digital systems and networks. Nowadays due to the technological improvement 93 percent of all the organizations communication is created electronically, with the remaining being communication ever printed. Hence this dependency is therefore becoming commonplace and in some cases a necessity in many people's normal day-to-day tasks. However, nowadays society tends to be more digitized and the needs for skilled people in this field become more and more pressing. The scope of this paper is to come up with a comparison of the computer forensics methodologies and procedures for the seizure of electronic evidence.

COMPUTER FORENSICS

Computer forensics investigation is generally the term used to describe the process of investigating and analyzing evidence, data or information magnetically stored on the computer. There is a basic, inherent process to computer forensics. It is often more than an art than a science, but as in any discipline, computer forensics analysts or specialists will follow clear, well defined methodologies and procedures, and flexibility is expected and encouraged when encountering with the unusual.

The basic methodology consists of what you can think of as the three A's which are described as follows:

1. Acquire the evidence without altering or damaging the source
2. Authenticate that you recovered evidence in the same as in the seized source
3. Analyze the data without altering it.

However, with the technology advancing rapidly the basic methodology will need to be revised and improved else this basic methodology and procedure will be out-dated.

One recent attempt to addressing these issues has been the European Union (EU) funded project 'Cyber Tools On-Line Search for Evidence (CTOSE)'. CTOSE has developed a methodology that aims to provide a consistent approach for identifying, preserving, analysing and presenting digital evidence.

The CTOSE project began by developing a reference model process resembling organizational, technical, and legal guidelines to the organization in order to address these issues and improve the ability of companies. The purpose of that model is based on the acquisition of digital evidence and on how it is to be collected, conserved and analyzed in such a way that the source will not be subject to tampering and that will be legally admissible should court proceedings be instigated. Figure 1 below illustrates how this reference model link to a detailed examination of technical, legal and presentational requirements.

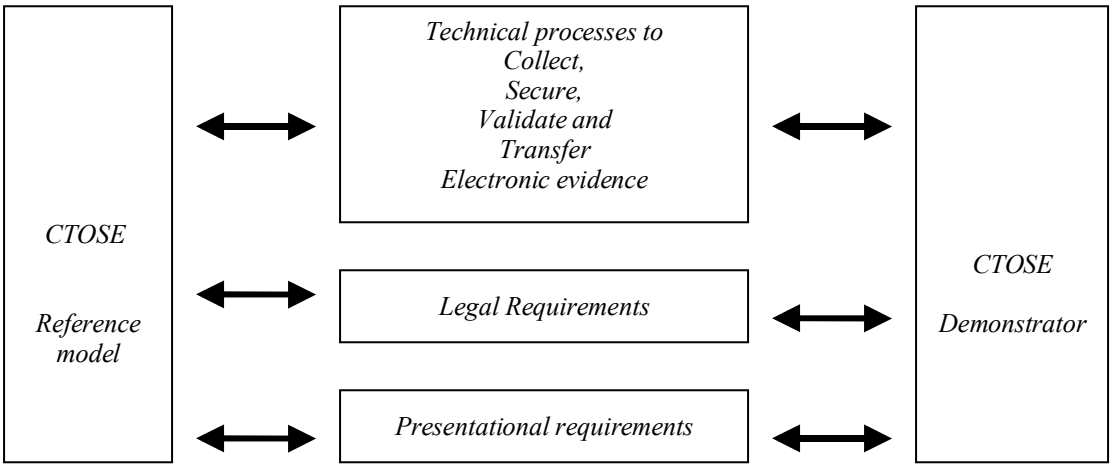

Figure 1: CTOSE Project reference model is composed of five phases: preparation, running, assessment, investigation and learning phases.

PROCESS

It does not matter whether we're approaching computer forensics for one or more data sources, it does not matter what those data sources are but there is a basic, inherent process to computer forensics which can be outlined as such:

- Identification Phase
- Acquisition of Evidence
- Authentication of Evidence
- Analysis Phase
- Presentation Phase

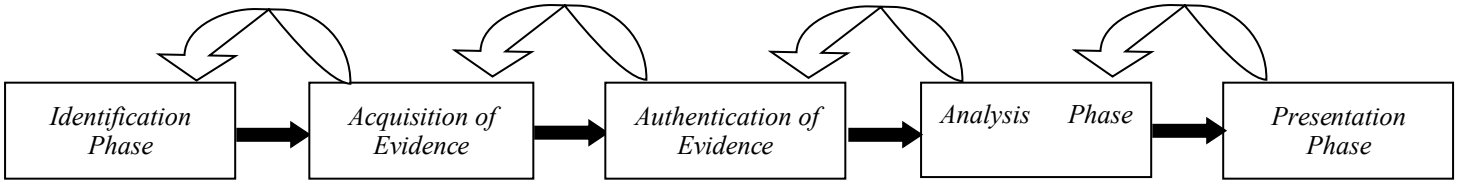

Figure 2: Process flowchart

The process flowchart is generally straight forward but occasionally we might have to back up certain steps. Such examples would be:

- During the analysis we could find out that references to data sources have not been acquired.
- During the acquisition phase we might need to reconsider the acquisition plan to include more data sources.
- During presentation we could be shot with questions that might require to do further analysis in order to provide satisfactory answers.

Identification Phase

Identification deals normally with intelligence gathering. Information about the information that we require. Information mapping to data sources. The question that we would be asking ourselves here would be what information is needed? Where can we obtain the information from – i.e. the source? How to gather it? Pre-seizure or acquisition actions that would be needed? In what order should the information be seized? So, the identification phase will foresee the challenges that will be encountered during the analysis and presentations phases and try to provide for them.

IDENTIFICATION PHASE	*Basic Forensics Methodology*	*European CTOSE Methodology*	*Data Recovery UK (DRUK)*	*The Recommended Methodology*
Objectives of forensics being approached				
• *Liturgical v/s non-liturgical forensics*	*No*	*Yes*	*Yes*	*Yes*
• *Past v/s ongoing crime*	*No*	*Yes*	*Yes*	*Yes*
Information harvesting				
• *How?*	*Yes*	*Yes*	*Yes*	*Yes*
• *When?*	*Yes*	*Yes*	*Yes*	*Yes*
• *What?*	*Yes*	*Yes*	*Yes*	*Yes*
• *Who?*	*Yes*	*Yes*	*Yes*	*Yes*
Intelligence gathering				
• *User Profiling*	*No*	*Yes*	*No*	*Yes*
• *Trend analysis on ongoing scenarios*	*No*	*Yes*	*No*	*Yes*
Information to data source mapping				
• *Logical v/s physical location of evidence*	*Yes*	*Yes*	-	*Yes*
Legal Framework				
• *General international issues*	*No*	*Yes*	*Yes*	*Yes*
Data source reconnaissance				
• *Is strong encryption being used?*	*Yes*	*Yes*	*Yes*	*Yes*
• *Is steganography being used?*	*Yes*	*Yes*	*Yes*	*Yes*
• *Is evidence local or remote*	*No*	*No*	*Yes*	*Yes*
Live data consideration				
• *How to seize live data*	*No*	*Yes*	*Yes*	*Yes*
• *Legal aspects of live data seizure*	*No*	*Yes*	*Yes*	*Yes*
Acquisition Plan Development				
• *Adjusting the level of detail to current needs*	*No*	*Yes*	*Yes*	*Yes*

• *Timing and geographical location considerations* • *Scheduling, sizing and coordinating the acquisition*	*Yes* *No*	*Yes* *Yes*	*Yes* *Yes*	*Yes* *Yes*

Table 1: Illustrates the different identification phases for the three methodologies

Acquisition of Evidence

Acquisition is to put to execution the acquisition plan designed in the earlier phase that is the ***identification***. The aim of the acquisition phase is to obtain forensics copies of all the digital evidence/data that will be required during the next stage which is the Analysis Phase.

Note that specialized software should be used, as the simple act of booting a computer system is almost certain to change the nature of data on disks drives connected to the computer.

This result in the contamination of digital evidence often causes vast amounts of data to be destroyed or altered before it can be imaged.

This acquisition of digital evidence would be snapshots and live datasets as needed. All snapshot data sources are to be seized or forensically imaged and live data is acquired in a notarized way to maintain the chain-of-custody.

In the actual evidence acquisition, procedures are focused primarily on maintaining proper forensics techniques to ensure that any evidence acquired will be acceptable to the legal proceeding and can be duplicated and if necessary should be done by an independent third party.

So, different factors need to be considered during that evidence acquisition and these are described below:

- Environmental Assessment and Documentation
- Drive Assessment and Documentation
- Evidence and Anti-Tampering Tagging and Documentation
- Drive Removal and Imaging Documentation
- Hardware and Software Tools Documentation
- Procedural Documentation.

ACQUISITION OF EVIDENCE	*Basic Forensics Methodology*	*European CTOSE Methodology*	*Data Recovery UK (DRUK)*	*The Recommended Methodology*
Pre-Acquisition considerations • *Legal implications of acquisition* • *Chain of custody*	*Yes* *No*	*Yes* *No*	*Yes* *Yes*	*Yes* *Yes*
Acquisition Plan • *Snapshots of data acquisition* • *Live data acquisition*	*Yes* *No*	*Yes* *No*	*Yes* *Yes*	*Yes* *Yes*
Post-acquisition considerations • *Handling of forensics images* • *Handling of seized evidence* • *Conservation* • *Transportation*	*Yes* *Yes* *No* *No*	*Yes* *Yes* *Yes* *Yes*	*Yes* *Yes* *Yes* *Yes*	*Yes* *Yes* *Yes* *Yes*

Table 2 considers the different acquisition plans for the three models.

Handling the Evidence

As mentioned previously the first actions of an investigator takes may blow out a case. This is very important as if you do not take care of your evidence the rest of the process will be compromised. All the hard work processing will be reduced to naught when the court throws it out because of inadequacies in your process of handling evidence. Also that the investigator or the forensics officer will need to maintain a chain-of-custody not only to protect the integrity of the evidence but also to make it difficult for the other side of the court to successfully argue that the evidence was tampered while it was in your custody. An effective process of documenting the complete journey of your evidence during the life of the case including the following questions:

- Who collected it?
- Who took possession of it?
- How and where?
- How was it stored and protected in storage?
- Who took it out of storage and for what reasons?

Anyone who has possession of the evidence should have correct entries in the evidence log book about the time that it was taken out, why it was taken out, by whom, where was it taken to, for what purposes. All this must be documented so that this can be produce as a legal piece of information in court. The table 3 below illustrates the advantages and disadvantages of the different methods used to protect the evidence and avoid altering the source information.

Table 3. Illustrates the level of effort to protect the evidence and avoid tampering the original source

Method	Advantages	Disadvantages
Use a dedicated forensic terminal to examine a write–protected hard drive or image	No concern about the validity of either the software or hardware on the suspect host. Produces evidence most easily defended in court.	Inconvenient, time consuming. May result in loss of volatile information or data
Boot the system using a verified, write protected disk with kernel and tools on it.	Convenient, fast. Evidence is defensible if suspect drives are mounted as read-only	Assumes that hardware has not been compromised which is *rare* this may result in the lost of volatile information.
Building a new system containing the image of the suspected system to examine it	Completely replicates operational environment as suspect computer, without running the risk of altering its information	Requires the availability of hardware that is identical to suspect computer. This may result in loss of information.
Examination of the system using external media with verified software	Convenient, quick, allows examination of volatile information	If a kernel is compromised, it will results in misleading information as the external media may not have the necessary utility on it.
Verify the software on the suspect computer and then use the verified local software to conduct examination	This requires minimal preparation. Allows examination of volatile information.	Lack of write-protection for the suspect drives makes evidence difficult to defend in a legal field. Finding source for hash values and verifying the local software requires several hours. Thus being time consuming

Authentication of Evidence

It is difficult to show that evidence (any kind of evidence) that we've gathered or collected is the same as was left behind by a criminal. In a digital environment, we even have an advantage in that we can show that the evidence did not change or been altered after we've collected it. While we cannot show exactly when the evidence was gathered, simple techniques enable us to timestamp it thus allowing us to demonstrate that the evidence was in existence at that specific moment. When we initially collect data, we should create a *hash* value (this is a cryptographic technique that calculate a value that functions as a sort of electronic fingerprint for an individual file or even for an entire floppy or hard disc) and record it as after having collecting the evidence, we can still prove that the acquisition of evidence is still identical to the original source by comparing the hash values (i.e. CRC32, MD5 or even SHA) of both the image and the original source.

Analysis Phase

The analysis refers to the interpretation of the recovered data and placement of it in a logical and useful format (e.g. how did it get there, what does it mean, where did it came from?). The analysis is the phase in which acquired data turn to evidence. When conducting the evidence examination, the followings steps should be taken into considerations:

- *Preparation:*

This would be to prepare the working directory or directories on separate media to which evidentiary files and data can be recovered or extracted.

- *Extraction:*

In this paper we will be looking at the two different types of extraction, Physical and logical. The physical extraction phase identifies and recovers the data across the entire physical drive without regard to the ***file system***. The logical extraction phase identifies and recovers files and data based on installed operating system(s), file system(s), and/or application(s).

1. Physical extraction

During this stage the extraction of the data from the drive occurs at the physical level regardless of file systems present on the drive. This may include the following methods: keyword searching, file carving, and extraction of the partition table and unused space on the physical drive.

i) Performing a keyword search across the physical drive may be useful as it allows the examiner to extract data that may not be accounted for by the operating system and file system.

ii) File carving utilities processed across the physical drive may assist in recovering and extracting useable files and data that may not be accounted for by the operating system and file system.

iii) Examining the partition structure may identify the file systems present and determine if the entire physical size of the hard drive is accounted for.

2. Logical extraction

During this stage the extraction of the data from the drive is based on the file system(s) present on the drive and may include data from such areas as active files, ***deleted files***, ***file slack***, and unallocated file space. The following steps may include:

i) Extraction of the file system information to reveal characteristics such as directory structure, file attributes, file names, date and time stamps, file size, and file location.

ii) Data reduction to identify and eliminate known files through the comparison of calculated hash values to authenticated hash values.

iii) Extraction of files pertinent to the examination. Methods to accomplish this may be based on file name and extension, file header, file content, and location on the drive.

iv) Recovery of deleted files.

v) Extraction of ***password-protected***, encrypted, and compressed data.

vi) Extraction of file slack.

vii) Extraction of the ***unallocated space***

3. Analysis of extracted data

Analysis is the process of interpreting the extracted data to determine their significance to the case. Some examples of analysis that may be performed include timeframe, data hiding, application and file, and ownership and possession. Analysis may require a review of the request for service, legal authority for the search of the digital evidence, investigative leads, and/or analytical leads.

a) Timeframe analysis

Timeframe analysis can be useful in determining when events occurred on a computer system, which can be used as a part of associating usage of the computer to an individual(s) at the time the events occurred.

i) Reviewing the time and date stamps contained in the file system metadata (e.g., last modified, last accessed, created, change of status) to link files of interest to the timeframes relevant to the investigation. An example of this analysis would be using the last modified date and time to establish when the contents of a file were last changed.

ii) Reviewing system and application logs that may be present. These may include error logs, installation logs, connection logs, security logs, etc. For example, examination of a security log may indicate when a user name/password combination was used to log into a system.

b) Data hiding analysis

Data can be concealed on a computer system. Data hiding analysis can be useful in detecting and recovering such data and may indicate knowledge, ownership, or intent. Methods that can be used include:

i) Correlating the file headers to the corresponding file extensions to identify any mismatches. Presence of mismatches may indicate that the user intentionally hid data.

ii) Gaining access to all password-protected, encrypted, and ***compressed files***, which may indicate an attempt to conceal the data from unauthorized users. A password itself may be as relevant as the contents of the file.

iii) Steganography.

iv) Gaining access to a ***host-protected area (HPA)***. The presence of user-created data in an HPA may indicate an attempt to conceal data.

c) Application and file analysis

Many programs and files identified may contain information relevant to the investigation and provide insight into the capability of the system and the knowledge of the user.

Results of this analysis may indicate additional steps that need to be taken in the extraction and analysis processes.

Some examples include:

i) Reviewing file names for relevance and patterns.

ii) Examining file content.

iii) Identifying the number and type of operating system(s).

iv) Correlating the files to the installed applications.

v) Considering relationships between files. For example, correlating Internet history to cache files and e-mail files to e-mail attachments.

vi) Identifying unknown file types to determine their value to the investigation.

vii) Examining the users' default storage location(s) for applications and the *file structure* of the drive to determine if files have been stored in their default or an alternate location(s).

viii) Examining user-configuration settings.

d) Conclusion

In and of themselves, results obtained from any one of these steps may not be sufficient to draw a conclusion. When viewed as a whole, however, associations between individual results may provide a more complete picture. As a final step in the examination process, be sure to consider the results of the extraction and analysis in their entirety.

While we must continue to treat our collected evidences with due respect and care during the analysis phase, it is interesting to be actively analyzing the evidence instead of doing paperwork.

Aggregation, correlation, filtering, transformation and meta-data generation are the key components through which data is analyzed.

But remember that a note should be included in your reports about every single step that is being carried out, the exact time of every operation carried out on the evidences and also maintain a chain-of-custody for not allowing the court legal adviser to successfully question the process of handling and analyzing the information.

General forensics principles apply when examining the digital evidence. Different types of cases and media may require different methods of examination.

Presentation Phase

The presentation phase will definitely involve in creating a final document or report to present the final digital evidence obtained. Therefore the examiner is responsible for completely and accurately reporting his or her findings and the results of the analysis of the digital evidence examination.

This report must be self contained, self explanatory written document in which all the relevant details and actions taken during every single process mentioned above – i.e. Identification, Acquisition, Authentication, Analysis phases be reflected into. Documentation is an ongoing process throughout the examination. It is important to accurately record the steps taken during the digital evidence examination along with all the needed details necessary for a third party examiner to reproduce and validate every piece of evidence. All documentation should be complete, accurate, and comprehensive.

The resulting report should be written for the intended audience.

Documentation should be contemporaneous with the examination, and retention of notes should be consistent with departmental policies.

The following is a list of general considerations that may assist the examiner throughout the documentation process.

i) Take notes when consulting with the case investigator and/or prosecutor.

ii) Maintain a copy of the search authority with the case notes.

iii) Maintain the initial request for assistance with the case file.

iv) Maintain a copy of chain of custody documentation.

v) Take notes detailed enough to allow complete duplication of actions.

vi) Include in the notes dates, times, and descriptions and results of actions taken.

vii) Document irregularities encountered and any actions taken regarding the irregularities during the examination.

viii) Include additional information, such as network topology, list of authorized users, user agreements, and/or passwords.

ix) Document changes made to the system or network by or at the direction of law enforcement or the examiner.

x) Document the operating system and relevant software version and current, installed patches.

xi) Document information obtained at the scene regarding remote storage, remote user access, and offsite backups. During the course of an examination, information of evidentiary value may be found that is beyond the scope of the current legal authority. Document this information and bring it to the attention of the case agent because the information may be needed to obtain additional search authorities.

Table 4. Shows the comparison of the different methodologies under the Analysis Phase.

ANALYSIS PHASE	*Basic Forensics Methodology*	*European CTOSE Methodology*	*Data Recovery UK (DRUK)*	*The Recommended Methodology*
Data Availability • *Forensics copies: analysis and backup*	*Yes*	*Yes*		*Yes*
Conceptualization: Aggregation, correlation, filtering, transformation and meta-data generation • *Primitives to digital processing* • *Ideally presented in a non-technology dependant approach though this could prove non-technology bound explanation followed by notes on key areas or e.g. which are technology related*	*Yes* *No*	*Yes* *No*	*No* *No*	*Yes* *Yes*
Pre-analysis • *Aggregation and the transformation: Data recovery and unification* • *Meta-data Generation: Categorization, indexing, hashing…*	*Yes* *No*	*Yes* *Yes*	*Yes* *Yes*	*Yes* *Yes*
Analysis: Process Flow & Data Flow • *Process and data flow during analysis phase* • *Milestones and key decisions areas*	*No* *No*	*No* *No*	*No* *No*	*Yes* *Yes*

Data to Evidence Mapping , isolation and Contextualization • *Difference from data and evidence – i.e. what's data and what's evidence?* • *How to create evidence out of data* • *Self sustained evidence*	- - -	*Yes* *Yes* *Yes*	*Yes* *No* *Yes*	*Yes* *Yes* *Yes*

- Examiner's report

This section provides guidance in preparing the report that will be submitted to the investigator, prosecutor, and others. These are general suggestions; departmental policy may dictate report writing specifics, such as its order and contents. The report may include:

i) Identity of the reporting agency.

ii) Case identifier or submission number.

iii) Case investigator.

iv) Identity of the submitter.

v) Date of receipt.

vi) Date of report. Descriptive list of items submitted for examination, including serial number, make, and model.

vii) Identity and signature of the examiner.

viii) Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files.

ix) Results/conclusions.

Table 5 showing a comparison of the presentation and reporting phase of the methodologies.

ANALYSIS PHASE	*Basic Forensics Methodology*	*European CTOSE Methodology*	*Data Recovery UK (DRUK)*	*The Recommended Methodology*
Birds eye view of the case, determining the role of digital evidence • *What's the real role of digital in the current case?*	*Yes*	*Yes*	*Yes*	*Yes*
Report Development • *Title* • *Table of content* • *What is required of the report?* • *Evidence identification and presentation* • *The equipment involved along with a description on how it is referred to throughout the paper,*	*Yes* *Yes* *No* *Yes* *No*	*Yes* *Yes* *No* *Yes* *Yes*	*Yes* *Yes* *Yes* *Yes* *Yes*	*Yes* *Yes* *Yes* *Yes* *Yes*

• *The art of 'vulgarizing' technical explanation, - i.e. do's and don'ts.* • *What if any conclusions were drawn* • *Executive summary consideration.* • *Appendices*	*No* *No* *No* *Yes*	*No* *No* *Yes* *Yes*	*Yes* *Yes* *Yes* *Yes*	*Yes* *Yes* *Yes* *Yes*
Legal Proofreading	*No*	*No*	*Yes*	*Yes*

CONCLUSION

At the level of theory, accurately defining forensics computing has proven to be a difficult task. Further, whilst different definitions have been presented by different organizations, we can still find some relationships in the different methodologies approached to achieve the end results. Yet, there is not much information that can be gathered from the different organizations as everyone has it's own system in place to handle evidence so that it can't be said to have been tampered during it's storage with the forensic officer.

However, there should be more research in this field so that an up-to-date or an appropriate methodology be implemented and put in place and which is recognize by the legal body which here would be the court of law and that every organization be bound to follow these methodologies and procedures.

REFERENCES

Anderson, M.R. (1998) "*Computer Evidence Processing: Good Documentation Is essential"* New Technologies, Inc, URL http://www.forensicsintl.com/art10.html Accessed on 21st October 2005.

Bates, J. (1997) "*Fundamentals of Computer Forensics.*" International journal of Forensics Computing.

Forensicon. *Best practices for using electronic evidence*, URL http://www.forensicon.com. Accessed on 14th October 2005

Hailey, S. (2003) *"What is Computer Forensics?"* URL http://www.cybersecurityinstitute.biz/forensics.htm Accessed on 13th October 2005

Hannan, M. & Turner, P. (2003a) "Beyond the Matrix: Research on Competence Among Australian Forensic Computing Investigation Teams" Proceedings of the 2nd European Conference Information Warfare and Security, University of London, June30-July 1 2003. Reading: UK.

Hannan, M. & Turner, P. (2003b) "Australian Forensic Computing Investigation Teams: Research on Competence" Proceedings of The Seventh Pacific-Asia Conference on Information Systems, July 10-13, 2003. Adelaide: Australia.

Hannan, M. & Turner, P. (2004) "The Last Mile: Applying traditional methods for perpetrator identification in forensic computing investigations" Presented at the 3rd European Conference Information Warfare and Security, University of London, UK 28-29 June 2004.

Hanson, D. (2005) *"Computer forensic analysis"* Law Enforcement Technology **32**(4) , URL www.officer.com Accessed on 13th October 2005

Kessler, G.C., & Schirling, M. (2002) Computer Forensics: *The Issues and Current Books in the Field.* , URL www.garykessler.net/library/computer_forensics_books.htm Accessed on 28th August 2005

Kruse II, W.G., & Heiser, J.G. (2002) Computer Forensics: *Incident Response Essentials.* Addison Wesley.

Loper, D.K. (2001) "*A case study in the forensics of computer crime: email address spoofing"* Journal of Security Administration **24**(2): 45-68.

Mercer, L.D. (2004) *"Computer Forensics: Characteristics and Preservation of Digital Evidence"* FBI Law Enforcement Bulletin **73**(3) ProQuest Law: 28.

Nimsger, K.M. & Lange, M.C.S (n.d.) Examining the Data: *A beginners to computer-based evidence.* , URL http://www.krollontrack.com/ Publications/securityproducts.pdf #search='a%20beginners%20 to%20computerbased %20evidence'. Accessed on 10th October 2005.

Pierce, M. (06/11/2003). "*Detailed Forensic Procedure for Laptop Computers"* , URL http://www.sans.org/rr/whitepapers /casestudies/1141.php Accessed on 1st October 2005.

Rude, T. (2000) "*Evidence Seizure Methodology For Computer Forensics*", URL. http://www.crazytrain.com/seizure.html Accessed 27th October 2005.

COPYRIGHT

MainHeading

Affiliation

Abstract

Abstract paragraph

Keywords

Keywords Paragraph

HEADINGMAJOR

HeadingMinor

Paragraph

Heading – very minor

Figure caption

CONCLUSION

REFERENCES

Reference list

COPYRIGHT