STANDARDIZATION OF COMPUTER FORENSIC PROTOCOLS AND PROCEDURES

Marcelo Abdalla dos Reis* and Paulo Lício de Geus
Computing Institute
State University of Campinas
Campinas, SP Brazil
{*marcelo.reis,paulo*}*@ic.unicamp.br*

November 14, 2001

ABSTRACT

In the last few decades, the use of computers has become part of everyday's life. Unfortunately, those who commit crimes are not apart from this computer revolution. As a consequence, procedures which allow investigators to recover data from computers involved in illegal acts and use them as evidence in criminal investigations are becoming fundamental to law enforcement agencies. This work discusses the need to adopt procedures and standards, scientifically evaluated, to conduct forensic examinations in computer systems. To this effect, a standardization model is proposed to develop and to evaluate procedures for the computer forensic science. Some standards are proposed to populate the model and issues surrounding the standardization of forensic procedures are discussed.

1 Introduction

In the last few decades, the use of computers has become part of everyday's life. Financial transactions and commerce can be made through the Internet, all sorts of information (from simple personal mail to confidential data) are stored and transmited electronically, digital devices are present in almost every kind of electronic equipment (from a simple cd player to the most advanced passanger aircraft), in fact, a true revolution has taken place.

Unfortunately, those who commit crimes are not apart from this computer revolution. The use of computers in criminal activities is a fact and is increasing everyday. In some cases, computers provide the means to consummate the crime. For example, the Internet can be used to spread computer viruses and images of child pornography, or to launch attacks against a computer network. In other cases, computers become storage devices for evidence of crime. For instance, a drug dealer might keep a list of drug suppliers in his/her personal computer, or a money laundering operation might retain false financial records on a network server.

The dramatic increase in computer-related crimes requires law enforcement agencies to work on new techniques for addressing and fighting crime, through training courses and partnerships with scientific research institutions, in order to understand how to obtain and use electronic evidence stored in computers [15]. As a consequence, procedures which allow investigators to recover data from computers involved in illegal acts and use them as evidence in criminal investigations are becoming fundamental to law enforcement agencies. Such procedures must be technologically robust to ensure that all probative information is recovered. Moreover, they must be legally defensible to ensure that nothing in the original evidence was altered [3].

*Sponsored by FAPESP

The importance of robust and defensible procedures to conduct a forensic examination can be illustrated by the trial of the american football player O. J. Simpson [20]. Simpson was charged of murdering his ex-wife and a friend of hers. Several blood samples where collected from the crime scene and a DNA analysis showed that they belonged to Simpson. The prosecutors had enough identification evidence to condemn him, however, the defense was able to nullify all DNA evidences and Simpson was declared innocent. The defense strategy was not to contest the probative value of DNA, but to raise suspicions against the procedures used to conclude that Simpson's DNA was in the blood samples from the crime scene, proving that such samples could be contaminated with Simpson's blood during their manipulation.

Simpson's trial motivated american forensic laboratories to revise their procedures in order to correct flaws that could lead to similar situations. The lack of good policies and reliable procedures is a serious problem when the scope comes to computer forensics, since it is a relatively recent forensic discipline and it deals with volatile and latent evidence that exists only in a metaphysical electronic form [3]. A survey conducted by the U.S. Secret Service, in 1995, reported that 70% of the law enforcement agencies that had computer forensic laboratories were doing the work without a written procedures manual [3].

The concern with computer-related crimes is not restricted to the most developed nations. It is a global sense once the use of computers in criminal activities increased worldwide. The connectivity resulting from the advance of the Internet enables criminals to act transjurisdictionally with ease [4]. Consequently, a criminal may be brought to justice in one country while the digital evidence required to prosecute him may reside in others.

This situation requires that all nations have the ability to collect and preserve digital evidence, not only for their own needs, but also for the potential needs of other countries [4]. Each jurisdiction has its own system of government and administration of justice and once it is not reasonable to expect all nations to know about the laws and rules of other countries, there must be a commom sense that allows the exchange of digital evidence [4]. In this case, procedures used to collect, preserve and analyze digital evidence must be coherent with legal and technical standards of the nations, in order to guarantee that evidence is lawful, defensible and so acceptable.

There are ongoing international efforts to develop examination standards and to provide structure to computer forensics. The formation of the International Organization on Computer Evidence (IOCE) [6] was the first step in order to provide international law enforcement agencies a forum for the exchange of information concerning computer crime. The Scientific Working Group on Digital Evidence (SWGDE) [7] was established as the U.S.-based component of IOCE and was charged with the development of guidelines and standards for digital evidence examination. The work towards standardization has originated a list of principles, discussed in [4], that were approved by IOCE delegates and has been adopted as the draft standard for U.S. law enforcement agencies.

Although research on computer forensic standards and procedures is starting to gain significance there is a lot to work out. Questions regarding, for example, privacy, authorship of digital information and computer forensic tools must be addressed.

This paper proposes an extension to the model for developing guidelines for computer forensic evidence presented in [3]. The new standardization model is detailed in all its aspects and standards are proposed to populate the model. This work is an evolution of the authors' research effort presented in [1, 2].

This paper is organized as follows. Section 2 contains a brief explanation of the computer forensic science. Section 3 describes, justifies and populates the proposed standardization model. Some issues

surrounding the standardization of forensic procedures are discussed in Section 4. And finally, Section 5 composes some conclusions about the work presented in this paper.

2 Computer Forensic Science

Computer forensic science is the science of acquiring, preserving, retrieving, examining and presenting computer evidence, might it be physical components or data that has been processed electronically and stored in computer media, in a suitable way for the courts of law [3].

The purpose of the computer examination is to find information related to the case, might it be data stored in files or memory, deleted or not, encrypted or possibly damaged. The search for evidence can be viewed as a detailed scanning within the sources of information of the computer system. Among these sources of information are the file system, log and audit records, free space on the storage device (file slacks and unallocated space, for example), temporary files, swap area, boot sector, memory, registers, peripherals and executing processes (a more detailed analysis of these sources of information can be found in [2]).

Forensic science has produced, all over the years, results that have been judged to be valid and reliable, affecting criminal investigations dramatically and providing compelling testimony in trials [3]. Forensic science relies on the ability of the scientists to produce a report based on the objective results of a scientific examination. As a consequence, forensic results are supported by scientific foundation, what increases their importance as probative information. A mistaken result can condemn an innocent or release a criminal.

In this sense, to support the results of a forensic examination, procedures and protocols are needed to ensure that the resulting information exists on the evidence analyzed and is unaltered by the examination process [3]. Such procedures and protocols must be detailed, documented and peer-reviewed, and acceptable to the relevant scientific community [3].

Computer forensic science is a research area relatively recent, but it is increasing the needs of development in this field, once the use of computers in criminal activities is becoming a common practise. Computers have reached tradicional crimes, such as extortion, robbery and drug dealing, and also have originated a new sort of crime, sometimes called "Internet crimes", such as denial of service attacks, network intrusions and dissemination of computer worms and viruses.

3 Standardization Model

The challenge to computer forensic science is to develop and evaluate protocols and procedures that provide valid and defensible results, while protecting the evidence from change. To attain this goal it is important to consider some features that differentiate computer forensic science from most traditional forensic disciplines, such as [3]:

- Computer forensic analysis attempts to recover only probative information from a large volume of data, while some traditional forensic analyses try to gather as much information as possible from an evidence sample;
- Computer forensic science is used most effectively when only the most probative information and details of the investigation are provided to the forensic examiner, in order to reduce the huge search scope. On the other hand, for example, a DNA examination can be conducted without knowledge of specific circumstances of the related crime;
- There commonly is a requirement to perform computer examinations at virtually any physical location, not only in a controlled laboratory setting;
- In the general case, computer forensic science does not need to make interpretive statements as to the accuracy or

reliability of the information obtained and normally renders only the information recovered;

- Computer evidence is primarily market-driven and almost never exists in isolation. It is a product of the data stored, the application used to create and store it, and the computer system that directed these activities. As a result, computer forensic science cannot rely on receiving similar evidence in every submission;

- Computer forensic science issues must be adressed in the context of an emerging and rapidly changing environment. In this sense, the science must adapt quickly to new products and inovations with valid and reliable examination techniques;

As a consequence of these features, computer forensic protocols should be written in a hierarchical manner so that common and essential principles remain constant, while examination techniques can adapt quickly to the computer system analyzed [3]. Moreover, computer forensic protocols and procedures should be coherent with legal and technical standards. This is in order to allow the exchange of digital evidence among different jurisdictions in a way that evidence is guaranteed to be reliable and defensible. A forensic examination is a multidisciplinary activity that attempts to produce suitable results for courts or public forum, and so it must be concerned not only with technical aspects but also with legal issues.

Technical standards refer to the practical issues of the computer forensic examination and must guarantee minimum requirements for the evidence, such as reliability, integrity, accuracy and durability. On the other hand, legal standards are related to the laws and rules of evidence that are essential to the acceptance of results and conclusions by courts and other agencies. As part of legal standards are the legal constraints applied to the seizure of evidence, to the examination process and to the forensic examiner.

To this effect, the authors propose a standardization model, illustrated on Figure 1, based on the model presented in [3]. The proposed model is an extension of the latter, distinguishing itself by concerns with the legal aspects of forensic science (represented by the inclusion of the legal standards class). This extension better represents the concerns of the forensic science and allows modelling the legal acceptance of examination results and procedures.

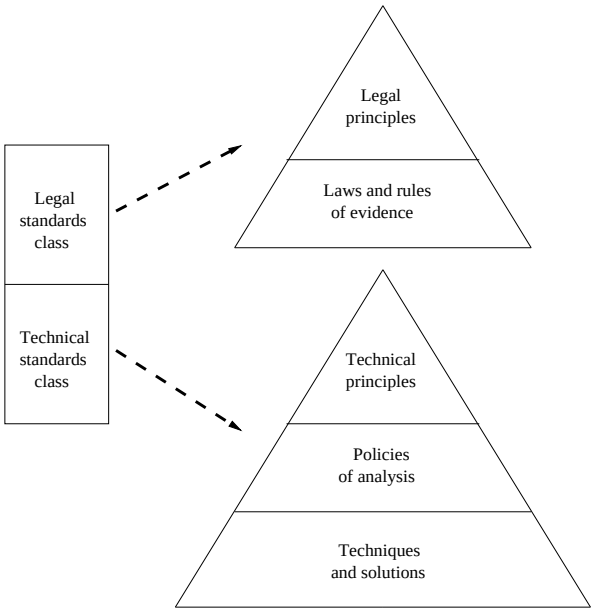

Figure 1: Standardization model.

The proposed model is a two-class hierarchical structure detailed as follows.

Legal Standards Class

Forensic is defined by [21] as meaning "appropriate for courts of law or for public discussion or argumentation". Forensic analysis is a scientific specialty whose purpose is to provide information suitable for presentation in the courts considering laws and rules of evidence for federal and state jurisdictions [5].

In this sense, legal standards are the laws and rules that dictate the admissibility of digital evidence in the courts of law. They consist of the formalities and judicial constraints that are applied to the experts, the

forensic science and the examination.

Since digital crimes can transcend country boundaries, it is not reasonable to expect all nations to have the same laws and rules of evidence. In order to allow the exchange of digital evidence, such legal constraints should be coherent with principles consistent with all legal systems. Based on Brazilian legislation and references [15, 17, 16], the authors propose some general features that might represent such principles:

- forensic analysis, as well as the development and evaluation of examination procedures and protocols, should be conducted by a graduate person, that is forensically competent and has technical and scientific skills related to the nature of the analysis. Besides that, this person should not have records that could raise suspicions against his/her moral strength and ethics;
- whenever a new forensic examination procedure is conceived, it should be evaluated and testified before use;
- minimum requirements for the evidence (such as reliability, integrity, accuracy and durability) should be predisposed and accurately defined;
- technical standards should guarantee the minimum requirements for the evidence;
- forensic procedures should be coherent with established standards;
- forensic procedures and standards should be generally accepted by the relevant scientific community and should be reviewed on a regular basis;
- forensic tools should be licensed or authorized for use in the examination. Such tools should be generally accepted in the field or supported by tests conducted in a scientific manner;
- the access rights over private information should be established (for instance, the expert could be granted the right to access all kinds of private information during forensic examination). Examination procedures should respect the established rights;
- forensic examination should produce a report according to some standardized model;
- the expert should be legally responsible for the examination results and evidence while it is in his/her possession;
- the situations in which one expert is legally prohibited to conduct a particular examination should be predisposed (for instance, when the perpetrator has some level of kinship with the examiner);
- forensic examination should be conducted by at least two experts, in order to reduce personal influence on the results;
- good working conditions should be guaranteed to the examiner, especially regarding the availability of equipament and material needed for the examination, resulting in an accurate and efficient work;
- the expert should weight his/her assertions and conclusions with scientific foundations, in a way that there is, from the scientific point of view, only one possibility to get to such assertions;
- forensic examination should be an indispensable part of investigation whenever there are evidence to be analyzed;
- forensic examination should preserve evidence in order to allow a second analysis;
- the original state of evidence should be protected until the arrival of the experts. Any alteration should be reported;
- the examination results should be as much elucidating as possible; to this effect, the use of photographs, drawings and diagrams should be allowed;

- warrant requirements for searching and seizing computers should be predisposed;

- situations in which searching and seizing computers without a warrant is allowed should be established.

Technical Standards Class

Technical standards are related to the practical requirements and conducts needed to carry out the examination. They are hierarchically arranged as follows.

_ Technical Principles

Technical principles are basic concepts that always apply to all sorts of examination. They are consensus directives that should guarantee minimum requirements to the evidence, such as reliability, integrity, accuracy and durability. Among the following principles, some are quoted [9, 4] and some are proposed by the authors:

- actions taken along the examination should not change the evidence;

- a chain of custody documentation should be maintained for all digital evidence. It should report the name of the examiner that is handling the evidence, date, time and activities performed;

- copies of the original digital evidence should be made and whenever possible the examination should be applied over the copies;

- the copies of the original digital evidence should be authenticated by means of cryptographic signatures [19];

- the examiner should not trust the analyzed system, because it might be corrupted;

- all assumptions that come up during examination should be reported for later scientific foundation;

- all media utilized during the examination process should be freshly prepared, completely wiped of non-essential data, scanned for viruses and forensically verified before use;

- all information (activities relating to the seizure, storage, examination or transfer of digital evidence, case notes and examiner's observations, and data extracted and analyzed) should be recorded in a permanent manner and should be available for review and testimony;

- precautions should be taken to prevent the transfer of viruses, destructive programs, or other inadvertent writes to/from the examined media and other media used for the examination;

- analysis techniques and tools should be known in each detail, in order to avoid unexpected implications and side effects over the analyzed system;

- care and attention should be taken in regard to metric units and mathematical approximations, in order to avoid missing any information in the storage devices;

- all resources that forensic science has available should be attempted to access information that is deleted, locked, hidden, password protected or encrypted. Resources used should be reported;

- evidence should be searched in every possible and relevant source of information, according to their volatility order;

- a complete examination may not be authorized, possible or necessary. In such instances, the examiner should report the reason for not conducting a complete examination.

_ Policies of Analysis

A Policy of analysis is a practical guidance that applies to forensic examinations, defining how they are planned, performed,

monitored, recorded and reported to ensure that technical principles are observed. There is, in the policy, the specification of everything that is necessary for the accomplishment of the analysis and step-by-step guidelines applied to most examinations (guidelines represent only the framework of the examination process). A sketch of a guideline is proposed as follows, based on [9, 10, 11, 12, 13].

- *Step 0*: Define the best approach for the examination, identifing all activities that will be required;
- *Step 1*: Prepare the examination system, providing the most suitable, properly tested and forensically sterilized hardware and software setup for the examination (in some cases it may be necessary to reproduce a specific setup, such as a network arrangement);
- *Step 2*: Stabilize the initial condition of the computer system subject of the examination, in order to preserve as much evidence as possible and protect systems and data out of the examination scope. The computer system should be described in its initial condition (hardware and software setups, executing processes, network connections, date and time accuracy, for example). Some issues should be evaluated at this point, such as the system shutting off (when and how it should be done), the maintenance of the system online or offline, the need to capture network traffic and detailed information of executing processes. Issues like these should be adressed in the policy of analysis;
- *Step 3*: Copy the information stored in the computer system. The copy should contain all the information in its original state and should be authenticated;
- *Step 4*: Extract as much relevant information as possible, regarding their order of volatility;
- *Step 5*: Examine each information separately, then in a correlative manner;
- *Step 6*: Correlate each evidence found (computer evidence or not). The examiner should establish a timeline, order of events, related activities and contradictory evidence;
- *Step 7*: Elaborate the final report based on the objective results of the examination.

– Techniques and Solutions

Techniques and solutions are hardware and software solutions to specific activities performed during examination. They are detailed instructions that describe the use of techniques and tools necessary for the examination process. An example of solution is presented as follows.

Solution for imaging a hard disk with IDE interface, using an *Intel Pentium III* hardware running *Red Hat Linux 7.1* operating system:

- *Step 1*: Describe the hard disk, reporting all relevant information that may be printed on its external surface, as well as the jumpers original setup;
- *Step 2*: Install the disk on the analysis system on an open second IDE port and boot the system. To avoid damaging the disk by possible master/slave conflicts on the IDE controller, install it as the only drive connected to the IDE cable on the second IDE interface. Consider in the next steps that the disk to be imaged is accessible by the block device */dev/hdc*;
- *Step 3*: Have the BIOS detect the disk on the analysis system. Verify and make notes of the disk geometry detected;
- *Step 4*: Identify the partitions on the drive using the command *fdisk -l /dev/hdc*. Make notes;
- *Step 5*: Generate the MD5 checksum of the information stored

on the disk using the command *dd if=/dev/hdc | md5sum -b*;

- *Step 6*: Copy each and every bit from the disk to the analysis sytem using the command *dd if=/dev/hdc of=filename*, where *filename* is the name of the file that will hold the disk image;

- *Step 7*: Generate the MD5 checksum of the file holding the disk image using the command *dd if=filename | md5sum -b*;

- *Step 8*: Compare the MD5 checksums generated on *Steps 5* and *7*. They should be exactly the same.

The previous example is meant to be an illustrative explanation and so does not take into account a series of adverse situations, such as the size of the file generated, the presence of bad sectors on the disk and the unmatching of the MD5 checksums.

4 Further Debate

Computer forensic science is an evolving forensic discipline that claims for standards and discussion. To this effect, some issues surrounding the standardization of computer forensic procedures are recommended for further debate.

Scientific Community Acceptance

The development and discussion of computer forensic science foundations should be carried in compliance with the relevant scientific community. It should not be carried in a commercial manner, in other words, all information (such as events, tools and techniques) should be shared and tested in a scientific manner.

General Purpose Discipline

The goal of the forensic analysis of computer systems is basically *persuasion based on factual evidence* [5]. As a consequence, forensic techniques might have a wider use than law enforcement purposes. The benefit would be a much higher confidence level in the information presented to decision makers in the business, industrial, government or military domains [5].

Proven Correct Tools

In the courts, admission and presentation of scientific evidence is guided by the established judicial rule and legal precedence. So, even though computer forensic scientists can do, for instance, a bit image of digital evidence and authenticate it with hashing algorithms, it will be the accuracy and reliability of the copy tool and hash employed that may be called into question [5]. It is importante to use *proven correct* tools to conduct a computer forensic examination. However, this assertion relies on a lacking definition of *proven correct*.

Proving that a tool is correct is definitely not an easy task that can fall into several levels of recursion. Consider the following:

One could use software engineering to build the algorithm and data flow of the tool. Then the correctness of the algorithm should be proved, as well as the accuracy of the implementation. The next step would be proving that the implementation compiles to the right machine instructions, and so one should prove that the compiler is *proven correct*. Besides that, one should prove that the operating system is *proven correct* and so the hardware, because the execution of the tool depends directly on them.

This approach would be impracticable (what to say, then, if only the binary code is available). The most practical and wise approach would be to test and evaluate the tools [8], in a way that if the scientific community agreed that the tools are accurate and reliable, they could be used as forensic tools.

Legal and Technical Standards Relationship

The relationship between legal aspects and technical practices can be better understood through the following example. Consider that the legal access right over private

information granted to the examiner does not allow him/her to examine some documents, such as communications between the suspect and their spouse, attorney or priest. Now consider an examination procedure that is strictly compliant with all technical principles and policies, but whose actions are based on the inspection of all kinds of documents stored in the computer system. This examination procedure would not be considered legally defensible.

Standardization Level

The standardization of computer forensic procedures and protocols may not be applicable to all levels of the model proposed in Section 3. This is as a consequence of the great variety of exams that may be requested and diversity of emerging and rapidly changing technologies. In this sense, standardization might be restricted to the levels of principles (legal and technical) and policies of analysis, allowing the use of non-standardized techniques and solutions, still coherent with the standardized levels. Another approach is the standardization only on the level of principles.

The hierarchical feature of the proposed model allows addressing the problem of diversity of examinations and evolving technologies. In the top of the hierarchy there are general and constant aspects. As the hierarchy is traversed, aspects become more specific and less constant, working as a set of primitive techniques. A new procedure might be developed by derivation of these primitive techniques. In this way, this new procedure, after being evaluated and testified according to the general and constant aspects, might then be included in the set of primitive techniques.

5 Conclusions

Criminal activity has also converted from a physical dimension, in which evidence and investigations are described in tangible terms, to a cyber dimension, in which evidence exists only electronically and investigations are conducted online [3]. Forensic science, as a discipline integrated by the different fields of the scientific knowledge, needs to remain up-to-date with regard to the scientific progress.

The role played by forensic science in a criminal investigation is the extraction and presentation of evidence in a suitable way for the courts of law. To this effect, procedures and protocols are needed to support the results of a forensic examination. As an evolving forensic discipline, computer forensic science claims for standards and scientific research.

In comparison with traditional forensic disciplines, computer forensic science is almost entirely technology and market-driven and generally located outside the laboratory setting. Also, the examinations present unique variations in almost every situation [3]. As a consequence, computer forensic procedures and protocols should be written in a hierarchical manner so that good principles remain constant. However, examination techniques must be allowed to quickly adapt to the computer system to be examined and to recognize the fast-changing and diverse world of computer science [3].

Moreover, computer forensic protocols and procedures should be coherent with legal and technical standards, in order to allow the exchange of digital evidence among different jurisdictions in a way that evidence is guaranteed to be reliable and defensible. To this effect, a standardization model (see Section 3) is proposed by the authors to evaluate and develop computer forensic procedures.

The work presented in this paper represents an effort to fulfill the lack of scientific research on computer forensic science. However, there is yet a lot of work to be done, with some issues still open for further research, such as:

- the difficulty in documenting every possible action in the form of operational procedures;
- the access rights over private information during the examination process.

Examiners have no ability to identify possible privileged information until after they read it. Also, probative information might be hidden inside privileged information;

- the lack of tools for analysis and correlation of evidence;
- the amount of information to be analyzed increases with the storage capacity of the devices. A complete and efficient examination becomes a challenge;
- the difficulty in accessing encrypted or password locked information;
- the development of security policies that maximize the usefulness of incident evidence data, and minimize the cost of forensic examination [14];

References

[1] M. A. Reis, F. Oliveira, P. L. Geus, and C. Guimarães. Forense Computacional: Aspectos Legais e Padronização. (Computer Forensics: Legal Aspects and Standardization). In *Proceedings of WSeg'2001: Workshop on Computer Security*, Florianópolis, SC, Brazil, March 2001. (in Portuguese).

[2] M. A. Reis, and P. L. Geus. Forense Computacional: Procedimentos e Padrões. (Computer Forensics: Procedures and Standards). In *Proceedings of SSI'2001: 3rd Symposium on Informatics Security*, São José dos Campos, SP, Brazil, October 2001. (in Portuguese, awarded with honorable mention).

[3] M. Noblett, M. Pollitt, and L. Presley. Recovering and Examining Computer Forensic Evidence. In *Forensic Science Communications*, Volume 2, Number 4, October 2000. U.S. Department of Justice, FBI.

[4] Scientific Working Group on Digital Evidence and International Organization on Digital Evidence. Digital Evidence: Standards and Principles. In *Forensic Science Communications*, Volume 2, Number 2, April 2000. U.S. Department of Justice, FBI.

[5] G. L. Palmer. CyberForensic Analysis.

[6] International Organization on Computer Evidence (IOCE) Web Site. In URL <http://www.ioce.org>. (last visited on November 2001).

[7] Scientific Working Group on Digital Evidence (SWGDE) Wb Site. In URL <http://www.forswg.org/swgdein.htm>. (last visited on November 2001).

[8] Computer Forensics Tool Testing (CFTT) Project Web Site. In URL <http://www.cftt.nist.gov>, September 2001. (last visited on November 2001).

[9] C. Hosmer, J. Feldman, and J. Giordano. Advancing Crime Scene Computer Forensic Techniques. In URL <http://wetstonetech.com/crime.htm>, 2000. WetStone Technologies Inc. (last visited on November 2001).

[10] D. Farmer, and W. Venema. Computer Forensics Analysis Class Handouts. In URL <http://www.fish.com/forensics/class.html>, 1999. (last visited on August 2001).

[11] R. Firth, G. Ford, B. Fraser, et al. Detecting Signs of Intrusion. In URL <http://www.cert.org/security-improvement/modules/m09.html>, 1997. Security Improvement Module, CERT Coordination Center. (last visited on August 2001).

[12] Evidence Examinations - Computer Examinations. In *Handbook of Forensic Services*, 1999. U.S. Department of Justice, FBI.

[13] D. Dittrich. Basic Steps in Forensic Analysis of Unix Systems. In URL <http://www.ic.unicamp.br/~ra000504/ftp/forensics/papers/dittrich/

basicsteps.html>. (last visited on November 2001).

[14] J. Tan. Forensic Readiness. In *The CanSecWest Computer Security Conference*, April 2001.

[15] O. S. Kerr. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. In URL <http://www.cybercrime.gov/searchmanual.htm>, 2001. Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U. S. Department of Justice. (last visited on August 2001).

[16] D. Tochetto, H. Galante, J. Zarzuela, et al. *Tratado de Perícias Criminalísticas*. (Treatise of Criminalistic Examinations). Sragra-DC Luzzatto, 1995. First edition. (in Portuguese).

[17] A. Espindula. A Função Pericial do Estado. (The Forensic Duty of the State). In URL <http://www.espindula.com.br/artigo1.htm>. (in Portuguese, last visited on August 2001).

[18] A. Espindula. Técnicas Criminalísticas para Conclusão de Laudo Pericial. (Criminalistic Techniques for the Examination Report Conclusion). In URL <http://www.ic.unicamp.br/~ra000504/ftp/forensics/papers/espindula/laudo.doc>. (in Portuguese, last visited on August 2001).

[19] S. Garfinkel, and G. Spafford. (1996). *Practical Unix and Internet Security*. O'Reilly and Associates, 1996. Second edition.

[20] CNN - O. J. Simpson Trial. In URL <http://www.cnn.com/US/OJ/index.html>, 1995. Cable News Network, Inc. (last visited on August 2001).

[21] The American Heritage Dictionary of the English Language. Houghton Mifflin Company. Fourth edition.