Chapter 1

WHEN IS DIGITAL EVIDENCE FORENSICALLY SOUND?

Rodney McKemmish

Abstract "Forensically sound" is a term used extensively in the digital forensics community to qualify and, in some cases, to justify the use of a particular forensic technology or methodology. Indeed, many practitioners use the term when describing the capabilities of a particular piece of software or when describing a particular forensic analysis approach. Such a wide application of the term can only lead to confusion. This paper examines the various definitions of forensic computing (also called digital forensics) and identifies the common role that admissibility and evidentiary weight play. Using this common theme, the paper explores how the term "forensically sound" has been used and examines the drivers for using such a term. Finally, a definition of "forensically sound" is proposed and four criteria are provided for determining whether or not a digital forensic process may be considered to be "forensically sound."

Keywords: Digital evidence, forensically sound evidence

1. Introduction

Emerging from the needs of law enforcement in the 1980s, forensic computing (also referred to as digital forensics) has evolved to become an integral part of most criminal investigations. The digital forensic specialist plays a fundamental role in the investigative process – whether it is the forensic analysis of personal computers, cell phones and PDAs belonging to suspects and witnesses, or the acquisition and analysis of network traffic in response to computer security incidents. Forensic computing also plays an increasingly important role in civil litigation, especially in electronic discovery, intellectual property disputes, employment law disputes and IT security incidents.

Please use the following format when citing this chapter:

McKemmish, R., 2008, in IFIP International Federation for Information Processing, Volume 285; *Advances in Digital Forensics IV*; Indrajit Ray, Sujeet Shenoi; (Boston: Springer), pp. 3–15.

In the context of law enforcement, it has been argued that the emergence of forensic computing as a discipline was due to the need to provide technical solutions to legal problems [6]. The technical solution involves the extraction of electronic data by processes that ensure that the resulting product is legally acceptable as evidence. Some scholars argue that legal drivers are the principal force behind shaping the growth and evolution of forensic computing [19]. As in the case of criminal investigations, the need to meet evidentiary requirements also provides a strong stimulus for forensic computing in civil litigation. Not surprisingly, a common element that emerges from forensic computing in criminal and civil matters is the need to produce electronic evidence in a manner that does not detract from its admissibility.

The growing emphasis on admissibility in recent years has caused the focus of the forensic computing discipline to shift to the domain of forensic science. With this shift comes the need to formalize many of the forensic processes and procedures that have been developed in an unstructured or *ad hoc* manner. Evidence of the shift is apparent in NIST's Computer Forensic Tools Testing Program [15] as well as in the work of the Scientific Working Group on Digital Evidence (SWGDE) [20] and the Electronic Evidence Technical Advisory Group of the Australian National Institute of Forensic Science, which is helping integrate the forensic computing function into the forensic science domain [14].

The need to ensure that electronic evidence produced by a forensic process is admissible has given rise to the term "forensically sound" when seeking to describe the reliability of the forensic process. Before exploring what "forensically sound" means, we briefly examine current thinking about the discipline of forensic computing.

2. What is Forensic Computing?

Numerous digital forensics experts have attempted to define the term "forensic computing." As expected, their definitions are influenced by their perspectives and experience.

In 1999, based on an examination of digital forensic activities by law enforcement agencies from eight countries, McKemmish [12] defined forensic computing as a process encompassing the identification, preservation, analysis and presentation of digital evidence in a legally acceptable manner. Anderson, *et al.* [1] emphasize the scientific nature of forensic computing by defining it as the science of using and analyzing information in order to "reason *post hoc* about the validity of hypotheses which attempt to explain the circumstances or cause of an activity under investigation." On the other hand, Hannan, *et al.* [9] adopt an

investigative focus and define forensic computing as a set of processes or procedures focusing on the investigation of computer misuse.

Some definitions of forensic computing focus solely on the underlying legal scope. For example, Casey [5], a computer security and computer crime consultant, postulates a criminal basis for forensic computing by emphasizing that it focuses on establishing how an offense has occurred. On the other hand, Carrier [3], a research scientist and author of several forensic tools, provides a more detailed definition of forensic computing that encompasses the investigative and scientific elements:

> "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."

Despite the comprehensive nature of his definition of forensic computing, Carrier still restricts its scope to criminal-related activity.

Defining forensic computing is a difficult proposition. After examining various definitions of forensic computing, Hannan [8] concludes that "no single definition can adequately define the current meaning of forensic computing." McCombie and Warren [11] emphasize that digital forensics is fundamentally different from other types of investigations and that major differences exist in the basic definition of forensic computing.

Despite their differences, all the definitions share one common element – the need to maintain the evidentiary weight of the forensic computing product. McKemmish [12] uses the term "legally acceptable," Anderson, *et al.* [1] stipulate the need to meet "evidentiary requirements," and Casey [5] and Carrier [3] refer to digital evidence in the context of legal weight. All these authors highlight the need for a forensic process to maximize the evidentiary weight of the resulting electronic evidence. Indeed, when the evidentiary weight is maximized, the digital forensics community would generally concur that the evidence is forensically sound.

3. Forensically Sound Evidence

To better understand what the term "forensically sound" might actually mean, we first examine the usage of the term. An Internet search quickly shows that the term is used to characterize everything from disk imaging software to a particular approach for extracting computer data. In the context of disk imaging, digital forensics professionals qualify the term by stating that, to be forensically sound, the disk image must be a bit-for-bit copy of the original (i.e., an exact copy). Some go further by

adding that the disk imaging process must not only produce an exact copy, but must also include a means for verifying the authenticity of the copy and the reliability of the copying process. Authenticity is typically ensured by using some form of mathematical fingerprinting or hashing that provides a signature for a given block of data. To ensure reliability, it is often advocated that the disk imaging process include an audit trail that clearly records the success or failure of all or part of the copying process. Therefore, one might argue that, in order to be forensically sound, a disk imaging process must satisfy the following requirements:

- The disk imaging process must produce an exact representation (copy) of the original.
- The duplicated data must be independently authenticated as being a true copy.
- The disk imaging process must produce an audit trail.

A more authoritative overview of the disk imaging process is found in NIST's Disk Imaging Tool Specification (Version 3.1.6) [16]. The document specifies a number of mandatory and optional requirements for disk imaging tools. The principal requirements are:

- The tool shall make a bit-stream duplicate or an image of an original disk or partition.
- The tool shall not alter the original disk.
- The tool shall be able to verify the integrity of a disk image file.
- The tool shall log I/O errors.
- The documentation of the tool shall be correct.

When the term "forensically sound" is used to describe the forensic process as a whole, it is done so with two clear objectives:

1. The acquisition and subsequent analysis of electronic data has been undertaken with all due regard to preserving the data in the state in which it was first discovered.
2. The forensic process does not in any way diminish the evidentiary value of the electronic data through technical, procedural or interpretive errors.

It is often the case that to meet these objectives, the concept of "forensically sound" is expressed in terms of a series of steps or procedures to

be followed. While this approach is logical and is certainly the most measurable, in reality, it is the lack of uniformity that diminishes its value. Specifically, the steps or procedures often vary from one author to the next and may contain more or less detail. Additionally, the forensic perspective and experience of an author can have a significant bearing on the construction of the forensic process.

For example, consider the difference in the acquisition of data in computer forensics and intrusion forensics cases. In computer forensics, the focus is on obtaining a snapshot of the system at a given point in time (typically using a disk imaging process). In the case of intrusion forensics, the focus is more likely to be on monitoring and collecting data from a network over time. It is, therefore, difficult to advocate taking a disk image of a live system whose state changes over time and where the evidence (network traffic and log files) is in a dynamic state.

Compounding the uncertainty surrounding the meaning and use of the term "forensically sound" is the lack of a clear definition or concise discussion in the digital forensics literature. For example, "Guidelines for the Management of IT Evidence" [7] published by Standards Australia uses the term "forensically sound" in the context of evidence collection, but does not clarify its meaning.

An alternate approach used to qualify forensic processes centers on the adoption of several principles rather than the application of clearly defined steps or processes. The "Good Practice Guide for Computer Based Electronic Evidence" published by the Association of Chief Police Officers (United Kingdom) [13] lists four important principles related to the recovery of digital evidence:

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

2. In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

3. An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Similarly, the International Organization on Computer Evidence [10] has specified the following six principles:

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.

2. Upon seizing digital evidence, actions taken should not change that evidence.

3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.

4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.

5. An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in his/her possession.

6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence, is responsible for compliance with these principles.

The well-known U.S. Department of Justice publication, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" [22], does not list any principles *per se*. However, the publication does address many of the points discussed above and provides a comprehensive explanation of the forensic process and the related U.S. legal issues.

In a 1999 paper titled "What is Forensic Computing?" McKemmish [12] specified four rules aimed at maximizing the admissibility of digital forensic processes. These rules, which are similar to the principles described above, are:

1. Minimal handling of the original: The application of digital forensic processes during the examination of original data shall be kept to an absolute minimum.

2. Account for any change: Where changes occur during a forensic examination, the nature, extent and reason for such changes should be properly documented.

3. Comply with the rules of evidence: The application or development of forensic tools and techniques should be undertaken with regard to the relevant rules of evidence.

4. Do not exceed your knowledge: A digital forensics specialist should not undertake an examination that is beyond his/her current level of knowledge and skill.

4. Why Define "Forensically Sound?"

Despite the variations in the use of "forensically sound," there remains one universally consistent objective for a digital forensic process – the need to ensure that the end product does not lose its evidentiary weight and, therefore, its admissibility as evidence. Given this overriding consideration, it is not surprising to see an ever increasing number of digital forensics professionals referring to their work product as being derived from a "forensically sound" methodology and/or technology. Indeed, this term is commonly used in affidavits and expert reports, especially when justifying the use of a specific methodology or technology.

The greatest driver to defining the term "forensically sound" may, in fact, come from the legal community. In 2005, the Australian Law Reform Commission (ALRC) released a review of the various Australian uniform evidence acts [2]. The section titled "Reliability and Accuracy of Computer-Produced Evidence" examines the Australian legislative framework that facilitates the proof of electronic evidence. The ALRC analysis identifies several viewpoints. One viewpoint, which relies heavily on the work of Spenceley [21], emphasizes that "a higher threshold for the admission of computer-produced output into evidence [should be] established." Citing Spenceley's research, the ALRC review notes that a question could be raised about the reliability of computer-generated output because "it is impossible to test for either the inaccuracy or accuracy of computer operations, and impossible to give a statistical rate of failure, and that there is therefore no rational basis for assuming a high rate of reliability."

To negate the impact of questions about reliability, the ALRC review notes that "Spenceley builds a case for adopting an approach that relies on implementing a 'redundant mechanism' in the environment in which the computer is used to address the problem of reliability of computer output." The purpose of the redundant mechanism is to prevent or mitigate unreliability by helping "provide some level of verification that a failure in the computer has not occurred." To achieve this goal, the ALRC review cites Spenceley's test of admissibility:

> "It should be demonstrated that: (a) Some mechanism(s) of redundancy (however formulated and implemented) was or were utilized in connection with the production of particular material in the setting in which it was produced; and that (b) It is reasonably likely that any error(s) in the operation of that computer that affected the accuracy of infor-

> mation contained in that material would have been detected by such mechanism(s)."

Not surprisingly, when government entities such as ALRC begin to probe the evidentiary value of computer-generated output and, in particular, raise questions about the current reliance on computer-generated output, greater attention is automatically placed on the digital forensic process. Given the variation in the usage of the term "forensically sound" and the focus on the reliability of computer-generated output from an evidentiary perspective, two key questions arise:

- What does "forensically sound" mean?
- How does one know if something is "forensically sound?"

The answer to these questions is important when one considers that the term "forensically sound" is used to not only substantiate a particular forensic technology or methodology, but also to substantiate it in the context of proving the admissibility of the digital forensic output in legal proceedings. This last point makes it all the more critical that there be a clear understanding of what makes something forensically sound.

5. What Does "Forensically Sound" Mean?

The *Compact Oxford English Dictionary* [17] defines the word "forensic" as meaning:

> "(1) relating to or denoting the application of scientific methods to the investigation of crime. (2) of or relating to courts of law."

The same dictionary defines the word "sound" – in the context of "something is said to be sound" – as meaning:

> (1) in good condition. (2) based on reason or judgement. (3) financially secure. (4) competent or reliable. (5) (of sleep) deep and unbroken. (6) severe or thorough."

Utilizing these individual definitions it may be argued that the term "forensically sound" means "the production of reliable electronic evidence before a court of law." In the context of digital evidence, however, the question of reliability is perhaps the key element. Consequently (and given the variations in the use of the term as detailed above), a more concise definition of "forensically sound" is:

> "The application of a transparent digital forensic process that preserves the original meaning of the data for production in a court of law."

The word "transparent" in this definition implies that the reliability and accuracy of the forensic process is capable of being tested and/or verified. The phrase "preserves the original meaning" intimates that the

data derived from the forensic process must be capable of being correctly interpreted. In addition to these points, it is worth noting that the term "digital forensic process" covers not only the methodology employed, but also the underlying technology.

5.1 Evaluation Criteria

Reliability and completeness are the two most critical properties of evidence with respect to digital forensic processes. If the reliability and/or completeness of any potential evidence are questionable, its evidentiary value is greatly diminished. Obviously, the question of evidentiary weight and, in particular, admissibility is a legal question that is ultimately determined by the court. Therefore, it is imperative that a digital forensic process be undertaken in manner that does not diminish the authenticity and/or veracity of the evidence.

So what makes a process forensically sound? More specifically, how can a court or lawyer determine if a claim of forensic soundness is legitimate? Given that digital forensic processes comprise many variables, it is difficult to adopt a prescriptive approach that would apply in every circumstance. The solution is to subject the forensic process to several criteria that determine if forensic soundness is an inherent property or merely an unfounded claim. Once a claim of forensic soundness is shown to be appropriate, it becomes a matter of ascertaining the reliability of the electronic evidence.

We propose four criteria for ascertaining the forensic soundness of a digital forensic process. If all four criteria are satisfied, the forensic process possesses the key properties associated with the concept of being forensically sound.

Criterion 1: Meaning

> *Has the meaning and, therefore, the interpretation of the electronic evidence been unaffected by the digital forensic process?*

When potential electronic evidence is acquired and analyzed, it is important that it be preserved in the state in which it was found and that it not be changed by a digital forensic process unless absolutely unavoidable. While the preservation of the data and its associated properties are critical aspects of this concept, they tend to be used in the context of the acquisition of data as opposed to its analysis. Indeed, some digital forensic technologies may result in subtle changes in the way data is presented (e.g., dates and times may be shown in different formats). However, in this case, the raw binary data has not been directly altered; rather, it differs from the original only in the way it is presented. The

meaning of the data is unchanged, although its representation may be modified. Thus, the value of the data is not of itself diminished.

Criterion 2: Errors

Have all errors been reasonably identified and satisfactorily explained so as to remove any doubt over the reliability of the evidence?

It is imperative that all software and hardware errors encountered during a digital forensic process be identified and that their impact be clearly identified and explained. Merely saying that there was an error in copying a file is insufficient. The nature of the error, its impact on the accuracy and reliability of the evidence, and any potential interference on the forensic process are all issues that must be discussed. Therefore, a digital forensic process should be designed to avoid undetectable errors wherever possible. Undetectable errors usually arise when a new piece of software is being used during the evidence acquisition or analysis phases. In such circumstances, it is imperative that all the software tools used in the forensic process be properly tested and assessed prior to their use. When an error is identified, it is in the interest of the digital forensic process to ensure that the nature of the error and its impact if any are clearly identified. Failure to do so can affect the reliability of the evidence. Indeed, Casey [4] notes that "forensic examiners who do not account for error, uncertainty and loss during their analysis may reach incorrect conclusions in the investigative stage and may find it harder to justify their assertions when cross-examined."

Criterion 3: Transparency

Is the digital forensic process capable of being independently examined and verified in its entirety?

Given that the results of a digital forensic process are used to substantiate a particular event or activity, it is critical in the interests of natural justice that the entire forensic process be accurate and reliable. To enable such an assessment, it is of paramount importance that the forensic process be transparent and capable of being independently verified. A key element of verification is the ability to reproduce the forensic process under the same conditions with a consistent level of quality being observed each time the process is run [18].

Transparency can be achieved by documenting all the steps, identifying the forensic software and hardware used, detailing the analysis environment and noting any problems, errors and inconsistencies. A key exception occurs when a part of the forensic process is not disclosed for legitimate legal reasons (e.g., public interest immunity); obviously, determining the validity of any exception is at the discretion of the court.

The level of detail required to ensure transparency will, of course, reside in the overall scope and objectives of the forensic process.

Criterion 4: Experience

> *Has the digital forensic analysis been undertaken by an individual with sufficient and relevant experience?*

Fundamental differences exist between how a digital forensics professional undertakes the examination of computer data and how a person unfamiliar with the forensic process performs the same task. For a forensic process to possess the property of forensic soundness, it must have been designed and implemented with due regard to forensic issues. In digital forensics, such a quality is directly derived from the knowledge and skill of the individual performing the forensic analysis. Consequently, if the individual has inadequate experience, it is questionable how he/she could satisfy the court that the meaning of the resulting data has not been affected, or that any errors encountered do not impact the reliability of the resulting evidence.

6. Conclusions

Electronic data is very susceptible to alteration or deletion. Whether it is an intentional change resulting from the application of some computer process or an unintentional change arising from system failure or human error, the meaning of electronic data can be altered rapidly and easily. Indeed, just as electronic data is created, changed and/or deleted through the normal operations of a computer system, there is the possibility of change arising from the application of an incorrect or inappropriate digital forensic process. Given that the results of such a process may be tendered as evidence, it is critical that every measure be taken to ensure their reliability and accuracy. To this end, a digital forensic process must be designed and applied with due regard to evidentiary issues. Furthermore, it is important that the forensic process be capable of being examined to determine its reasonableness and reliability. It is only when the forensic process is judged to be reliable and appropriate, that a claim of forensic soundness can truly be made.

References

[1] A. Anderson, G. Mohay, L. Smith, A. Tickle and I. Wilson, Computer Forensics: Past, Present and Future, Technical Report, Information Security Research Centre, Queensland University of Technology, Brisbane, Australia, 1999.

[2] Australian Law Reform Commission, Review of the Uniform Evidence Acts, ALRC Discussion Paper 69, Sydney, Australia (www.austlii.edu.au/au/other/alrc/publications/dp/69/index.html), 2005.

[3] B. Carrier, Defining digital forensic examination and analysis tools using abstraction layers, *International Journal of Digital Evidence*, vol. 1(4), 2003.

[4] E. Casey, Error, uncertainty and loss in digital evidence, *International Journal of Digital Evidence*, vol. 1(2), 2002.

[5] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press, San Diego, California, 2004.

[6] P. Craiger, M. Pollitt and J. Swauger, Law enforcement and digital evidence, in *Handbook of Information Security, Volume 2*, H. Bidgoli (Ed.), John Wiley, New York, pp. 739–777, 2006.

[7] A. Ghosh, *Handbook 171-2003: Guidelines for the Management of IT Evidence*, Standards Australia, Sydney, Australia, 2003.

[8] M. Hannan, To revisit: What is forensic computing? *Proceedings of the Second Australian Computer, Network and Information Forensics Conference*, pp. 103–111, 2004.

[9] M. Hannan, S. Frings, V. Broucek and P. Turner, Forensic computing theory and practice: Towards developing a methodology for a standardized approach to computer misuse, *Proceedings of the First Australian Computer, Network and Information Forensics Conference*, 2003.

[10] International Organization on Computer Evidence, Guidelines for Best Practice in the Forensic Examination of Digital Technology, Digital Evidence Standards Working Group, 2002.

[11] S. McCombie and M. Warren, Computer forensic: An issue of definition, *Proceedings of the First Australian Computer, Network and Information Forensics Conference*, 2003.

[12] R. McKemmish, What is forensic computing? *Trends and Issues in Crime and Criminal Justice*, no. 118 (www.aic.gov.au/publications/tandi/ti118.pdf), 2002.

[13] National High Tech Crime Unit, Good Practice Guide for Computer Based Electronic Evidence, Association of Chief Police Officers, London, United Kingdom (www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf), 2003.

[14] National Institute of Forensic Science, Melbourne, Australia (www.nifs.com.au).

[15] National Institute of Standards and Technology, Gaithersburg, Maryland (www.nist.gov).

[16] National Institute of Standards and Technology, Disk Imaging Tool Specification (Version 3.1.6), Gaithersburg, Maryland (www.cftt .nist.gov/disk_imaging.htm), 2001.

[17] Oxford University Press, *Compact Oxford English Dictionary (Third Edition)*, Oxford, United Kingdom, 2005.

[18] L. Pan and L. Batten, Reproducibility of digital evidence in forensic investigations, *Proceedings of the 2005 Digital Forensic Research Workshop*, 2005.

[19] D. Ryan and G. Shpantzer, Legal aspects of digital forensics (www.danjryan.com/papers.htm), 2002.

[20] Scientific Working Group on Digital Evidence (www.swgde.org).

[21] C. Spenceley, Evidentiary Treatment of Computer-Produced Material: A Reliability Based Evaluation, Ph.D. Thesis, University of Sydney, Sydney, Australia, 2003.

[22] U.S. Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section, Washington, DC (www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm), 2002.