The Adaptability of Electronic Evidence Acquisition Guides for New Technologies

Benjamin Turnbull
Defence and Systems Institute, University of South Australia
F Building, Mawson Lakes Campus
University Blvd, Mawson Lakes, South Australia 5095
+61 8 8302 6509
Benjamin.Turnbull@unisa.edu.au

ABSTRACT
The use of evidence acquisition guides for the identification and collection of electronic evidence is supported internationally as a means of providing best practice methodologies, as a legal framework and to ensure that sources of evidence are not tainted before examination and analysis can occur. This work seeks to analyse and discuss several of the more publicly known and available evidence collection guides as a means of determining how adaptable they are to modern devices and technologies; in particular, wireless and VOIP-based technologies.

General Terms
Documentation, Performance, Design, Human Factors, Standardization, Legal Aspects.

Keywords
Digital evidence, Digital forensics, Standard Operating Procedures, Evidence Acquisition, Emerging Technologies

1. Introduction
Forensic Computing may be defined as the securing, analysis and presentation of electronic evidence [1], and each of these areas must be considered independently. Whilst the area of *analysis* represents most of the field, both practically and in research, the other two sections are of importance. Specifically, the *secure* phase is important in that it provides the sources for analysis, and the *presentation* phase is vital in that it represents the outcome of the work.

The *secure* phase of forensic computing involves the identification and collection of devices that may contain electronic evidence a manner that ensures that the information contained within is preserved. The main discussion surrounding this area is based upon several evidence collection guides, targeted at law enforcement, which describe the processes used to achieve these ends.

Without constantly improving identification and collection processes, potential sources of evidence may become contaminated or may remain uncollected and therefore unanalysed. A failure in the effective securing of physical devices containing potential electronic evidence is cascading, as breaking the chain of custody or inappropriately securing a device cannot be undone in later analysis. However, in many cases, this work is left with officers with little formal technical training rather than forensic experts, and there is therefore a high reliance on procedural evidence collection guides that are able to refresh officers of best practice. These guides are either developed in-house, or, more often, are based on one of several known guides and then adapted as required. This work seeks to identify and discuss the several known electronic evidence collection guides that are within the public domain, and compares the processes with new and emerging consumer technologies, to understand if these guides are still applicable for the range of devices that may be found during a search and seizure involving electronic evidence.

2. Current Procedural Guides
With international differences in legislation and policing factors, it is unsurprising that such a plethora of evidence identification and collection guides exist. These guides include:

- *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, [2]
- *Best Practice Guide for Seizing Computers and other Electronic Evidence*, produced by the Australasian Centre for Computing Research [3]
- *The Good Practice Guide for Computer Based Electronic Evidence*, [4]
- *Electronic Crime Scene Investigation – a guide for first responders*, produced by the United States Department of Justice, National Institute of Justice [5].
- *Best Practices for Seizing Electronic Evidence* [6],
- *Best Practices for Computer Forensics*, developed developed by the Scientific Working Group on Digital Evidence [7]
- *Information Technology Crime Investigation Manual*, developed by The European Working Party on Information Technology Crime of Interpol [8]. The *Information Technology Crime Investigation Manual* serves to replace the previous *Computer Crime Manual* from the same group. Both of these guides are considered restricted, and available only within the law enforcement community.

Beyond this, there are also a small number of specialised guides, designed exclusively for mobile phones and PDA-type devices, but these will not be discussed in any depth, as they are very specific in their scope and do not discuss methods of identifying general devices [9, 10].

It is possible that a substantial number of policing agencies, internationally, will have developed in-house guides that match particular circumstances and legal requirements for that area.

However, such guides cannot be discussed in detail, as they are not within the public domain, as the guides listed above are (with the exception of the Interpol guides, of which the existence is known publicly).

In addition, it is likely that evidence acquisition guides developed internally of an organization or law enforcement agency would not be developed entirely in isolation, but would use an existing guide as a template or for reference. Therefore, whilst this work only directly encompasses evidence acquisition guides that are within the public domain, the parallels and inferences drawn may have further applicability and may have relevance to other guides. The following section will introduce and discuss each of these guides in greater detail.

2.1 Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

The Computer Crime and Intellectual Property Section (CCIPS) of the United States Department of Justice have produced a document entitled *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, [2] . However, it is less a technical discussion on the identification and collection of electronic evidence but more a primer on United States legislation and electronic crime, and is therefore beyond the scope of this work.

2.2 Best Practice Guide for Seizing Computers and Other Electronic Evidence

The *Best Practice Guide for Seizing Computers and other Electronic Evidence*, produced by the Australasian Centre for Computing Research [3], is a guide for police officers without forensic computing experience on seizing electronic evidence. This document provides the basic rules for seizing computers and other electronic devices. However, this guide is designed as a double-sided sheet of A4 sheet of paper, and as such has little in-depth discussion on any specific topic. The *Best Practice Guide for Seizing Computers and other Electronic Evidence* is designed primarily as an aid to memory, and as such is less a complete process model than a series of dot-points.

2.3 The Good Practice Guide for Computer Based Electronic Evidence

In 2003, the then-named National Hi-Tech Crime Unit, a United Kingdom-based unit comprised of several UK law enforcement agencies, released *The Good Practice Guide for Computer Based Electronic Evidence*, [4]. This guide aims to provide acquisition procedures to maintain untainted digital evidence and outlines the stages of an investigation, and to allow non-technical officers to collect sources of electronic evidence without the need to consult experts. Whilst not a definitive manual for electronic evidence collection, *The Good Practice Guide* does provide an overview for the more common electronic scenarios. Beyond this, *The Good Practice Guide* also gives a brief overview to the process of analysis and presentation of digital evidence, but does not give much detail.

Within the acquisition of electronic evidence, *The Good Practice Guide* provides several flowcharts discussing the stages recommended by the guide for the identification, collection and preservation of digital evidence. The major flowchart that is provided describes the process of identifying and collecting digital evidence within a forensically sound manner. Much of the remainder of this guide discusses each of these stages, and provides a glossary and information about what devices may yield potential evidence. An adaptation, ensuring that all stages discussed are included, is provided in Figure 1.

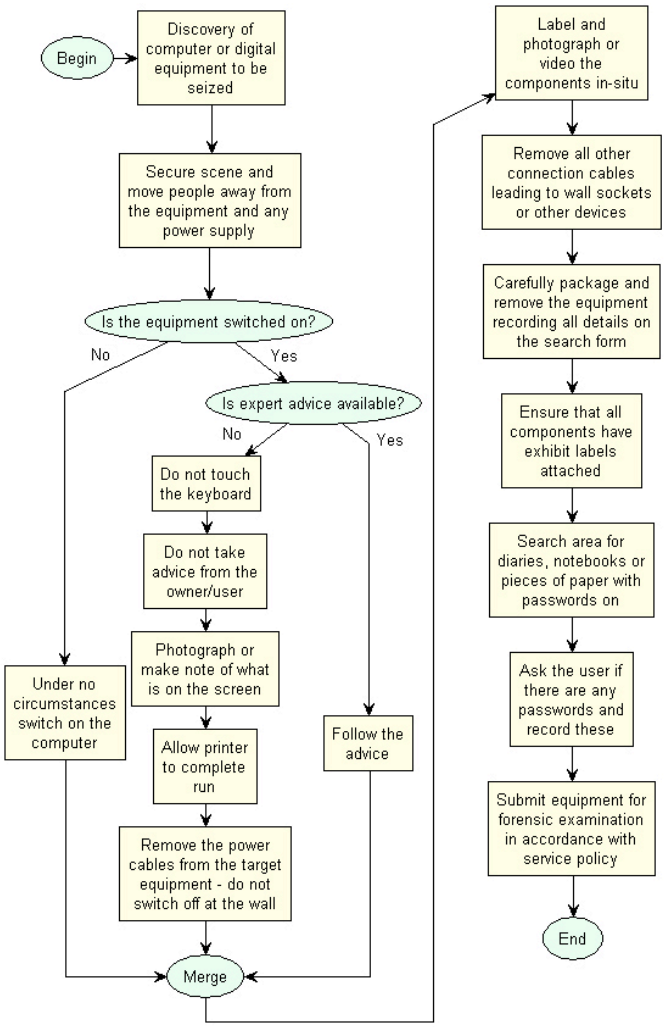

Figure 1 – A flowchart based on *The Good Practice Guide for Computer Based Electronic Evidence*, [4]

The flowchart given in Figure 1 is quite extensive, and is designed for first responders to a policing investigation. It is comprised of the stages required to secure a crime scene and how electronic devices are to be collected within this framework. *The Good Practice Guide* provides a comprehensive procedural process for all stages of the identification and collection of electronic goods in an area of interest or as part of a search and seizure. There is a difference in both the aims and volume of information found within *The Good Practice Guide* when compared with the *Best Practice Guide for Seizing Computers and other Electronic Evidence*, as *The Good Practice Guide* aims to be a formalised and repeatable process for each stage of the evidence collection process.

2.4 National Institute of Justice – Electronic Crime Scene Investigation – a guide for first responders

Similar in content to the *Good Practice Guide* and also of note is the *Electronic Crime Scene Investigation – a guide for first responders* written by the United States Department of Justice, National Institute of Justice [5]. Despite its age, this is one of the more comprehensive publicly-accessible documents detailing acquisition of digital evidence and is complemented by the more recent Forensic Examination of Digital Evidence: a guide for law enforcement, which discusses the analysis component of a computer forensic investigation [11].

The *Guide for first responders* has a more extensive scope than the similar *Good Practice Guide*, as it details not only the collection of electronic evidence, but also other, non-electronic evidence-based stages of an investigation. Whilst comparable with *The Good Practice Guide*, the *Guide for first responders* does not utilise flowcharts, and this makes interpreting the discussed sequences of events more difficult, as there is little context for each stage of the response. The following flowcharts are an interpretation of the sequence of events, based on discussion from the *Guide for first responders*. Whilst every effort has been made to ensure accuracy with the original material, some components of the original document are open to interpretation in regards to where they would occur within the sequences described in the document. These will be discussed where appropriate.

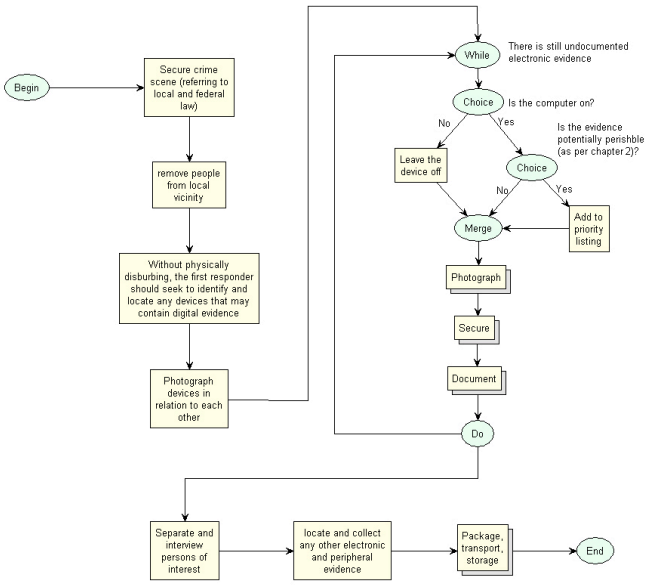

Figure 2 Flowchart detailing the process for collecting digital evidence, outlined in *Electronic Crime Scene Investigation – a guide for first responders*

The flowchart portrayed in Figure 2 gives an overview of the entire process described within the *Guide for first responders*. Whilst the sequence of events is mostly linear, a large proportion of the flowchart contains a loop, which needs to be executed for each piece of evidence. Each of the sub-processes within this section, 'Photograph', 'Secure', and 'Document' is described separately, and indicates a more complex sequence of events. Whilst these stages are discussed within the overview of the document, the boundaries between these, within the flowcharts, have been inferred, and may be open to interpretation. The last stage, 'Package, transport, storage' is also a sub-process, which will be discussed in more depth.

As can be seen from the diagram, the *Guide for first responders* is far more complex than other crime scene investigative guides, and covers several related stages of collecting electronic evidence, that whilst not directly related to the discipline of forensic computing, are nevertheless related investigative stages. For example, the task entitled 'separate and interview persons of interest' is expanded upon within the document, detailing what information would be of use regarding electronic evidence. Specifically, within these preliminary interviews, the document discusses the need to recover information, listed as follows:

- *"owners and/or users of electronic devices found at the scene, as well as passwords, user names, and Internet service provider".*
- *"Passwords. Any passwords required to access the system, software or data."*
- *"Purpose of the system"*
- *"Any unique security schemes or destructive devices"*
- *"Any offsite data storage"*
- *"Any documentation explaining the hardware or software installed on the system" [11].*

This is well beyond the scope given by other, similar guides.

An interesting point, though, is that although the correct securing of computers is the focus of the majority of the stages within this document, whereas the instruction on identification of computers and other electronic devices is comparatively short. Also, when identifying computers as potential evidence, there is a stage dedicated to learning how to infer whether the data contained within it is perishable, yet the same stage is not afforded to other devices [11]. Some modern electronic systems do contain volatile information and the disruption of these devices may have negative consequences in terms of data retention. The collection of all other, non-computer electronic devices is not afforded the same procedures as devices that are obviously computers. It may be appropriate to generalise these processes to allow for greater flexibility in processing all computing devices.

Also of interest is that the *Guide for first responders* does not discuss several devices specifically. Whilst mobile phones are discussed, procedures for their collection are not, even when it is possible, even likely, that each person being interviewed in the 4th-to-last stage may be carrying a mobile phone or PDA. Again, whilst some effort is made to discuss the volatility of data that is inherent in many PDA-type devices, the process for their identification and collection is not as substantial or complete as found in *The Good Practice Guide*. Following this guide, PDAs and devices with volatile memory will be given priority, but will still have their batteries removed before transportation, which has the potential to permanently remove evidence.

Overall, the G*uide for first responders* is a comprehensive guide to the acquisition of devices containing potential electronic evidence, but published in 2002, is becoming out-of-date in several areas.

2.5 International Association of Chiefs of Police Advisory Committee – Best Practices for Seizing Electronic Evidence

Similar to the *Guide for first responders* [5] is a smaller, compact version entitled *Best Practices for Seizing Electronic Evidence*

[6], which may be considered a companion guide. Whilst there is significant overlap between this guide and *Guide for first responders*, the *Best Practices for Seizing Electronic Evidence* focuses more on the identification of potential sources of digital evidence, and does not discuss details in the same way. Of note is that, whilst the companion guide does discuss several forms of devices that may contain electronic evidence, such as cordless telephones, mobile phones and Global Positioning Systems, computer-based wireless networks are not discussed at all, despite being mentioned in the more comprehensive guide. The guide itself contains far less detail than the *Guide for first responders*.

2.6 Scientific Working Group on Digital Evidence – Best Practices for Computer Forensics

The most recent publicly accessible guide on best electronic evidence collection practices has been developed by the Scientific Working Group on Digital Evidence, in 2005, and is entitled *Best Practices for Computer Forensics* [7]. The guide itself is brief, totalling only five pages, and discusses the collection of potential digital evidence, handling of evidence, forensic imaging, analysis and examination, documentation, reporting and reviewing of evidence. This is a broad gamut of skills, encompassing the majority of the forensic computing field. Rather than working sequentially, as the other discussed guides have, *Best Practices for Computer Forensics* gives general guidelines. It is therefore unable to be developed into workflows, or directly compared with the other discussed guides.

The *Best Practices for Computer Forensics* section entitled 'Seizing evidence' is accurate, and gives general principles, discussion on evidence handling and then discusses several specifics involving stand-alone computers, networked computers and servers [7]. Interestingly, whereas *The Good Practice Guide* and the *Guide for first responders* both clearly state that if a computer is networked, expert advice is necessary to ensure forensic integrity, *Best Practices for Computer Forensics* guide specifically states that this is unimportant and that the stages for securing evidence are the same. *Best Practices for Computer Forensics* also discusses the forensic acquisition of servers, stating that *"a determination should be made as to the extent of data that should be seized"* [7] and that based upon this, the shutdown of the server may or may not be necessary. The implications of this are that if there is potential evidence on a server, there are other options for copying this and a full shut down of the server may not be necessary. *Best Practices for Computer Forensics* also states that *"Pulling the plug [of a server] could severely damage the system; disrupt legitimate business; and/or create officer and department liability"* [7]. Therefore the need for forensically sound evidence collection must be balanced with practical needs, which in turn are determined by several factors. This dichotomy is not discussed in any detail beyond this. The remainder of *Best Practices for Computer Forensics* will be discussed within the next section which details guides that define procedure within the *analyse* and *present* stages of forensic computing.

2.7 Interpol – Computer Crime Manual

The European Working Party on Information Technology Crime of Interpol has developed the *Computer Crime Manual* (which outlines evidence acquisition processes for criminal investigators) and is only available within the law enforcement community [8]. Both this manual and its predecessor, the *Computer Crime Manual*, are widely referenced, and are widespread within the law enforcement community. The *Information Technology Crime Investigation Manual* aims to provide several key areas of information, and is an ongoing project [8]. However, these guides are released exclusively within the law enforcement domain, and are therefore not available for public scrutiny or discussion.

The next section of this work discusses the adaptability of each of the guides introduced in this section. From this, it is hoped to determine the continuing effectiveness of the current electronic evidence identification and acquisition guides.

3. Adaptability of Electronic Evidence Identification and Collection Guides

One of the interesting points to note about all of these evidence acquisition guides is their relative age. This ranges from 2001 – 2004 and whilst this is not old, the intervening time period has seen several technologies that were at the time emerging become ubiquitous, and has also seen the rise of several new ones. Computing technologies such as wireless networking were becoming increasingly common over this time period, but had not become the networking standard that it is today; MP3 music and video devices have also raised in both capacity and complexity, the technology found within game consoles has also appreciably changed, and such these devices may be forensically examined.

Also, since the development of these guides, technologies such as Voice Over Internet Protocol (VOIP) have expanded rapidly, and reached consumers in massive numbers [12]. VOIP represents an interesting trend in that it converges telephony with computer connectivity, and as such, VOIP devices may have electronic forensic value, but appear similar to standard telephony equipment.

This section discusses each of the technologies in turn, discussing how the evidence collection processes would assist in the identification and collection processes.

3.1 Wireless

There is a potentially fundamental issue when discussing wireless networking in context with these procedural guides; that all of the discussed procedural guides are designed to collect evidence from only the most common installations; single, isolated computers. Anything beyond this is either explicitly referred to experts, or it is implied, depending on the guide itself. However, wireless networking poses an issue on this, as, unlike wired networking, it is difficult to determine when a wireless network exists, let alone determining the number of and types of device that are connected to one.

Therefore, there is an issue in the collection of electronic devices that involves wireless networking, as there is no reliable means of determining if a computing device is networked or not. This in turn invalidates several aspects of all guides, specifically *The Good Practice Guide for Computer Based Electronic Evidence*, [4] and *Electronic Crime Scene Investigation – a guide for first responders* [5], as there is no means of a non-technical officer involved in the collection of evidence at a scene of interest knowing whether a device is networked or not. The presence of wireless networking at a crime scene may therefore severely compromise the limitations imposed by several of the known evidence collection guides. There is obviously a reason why these

limitations are given, and the use of wireless networking bypasses them.

Also of note in reviewing the evidence collection guides listed and their ability to handle the collection of new technologies is the lack of any meaningful discussion on wireless networking devices in any depth by any of them. Of all the discussed guides, only *The Good Practice Guide for Computer Based Electronic Evidence*, [4] specifically mentions any kind of wireless technology when it states that 802.11-based wireless cards should be collected if discovered in an area of interest. However, this guide fails again to take into account that wireless devices are more than physical devices, but are networking mechanisms capable of communication. This is the only guide to discuss 802.11-based or Bluetooth wireless networking devices at all. This lack of discussion can partially be attributed to the age of the guides, but the 802.11b standard was created in 1999 and these devices were becoming increasingly popular after this point.

3.2 MP3/Video Players

Whilst personal music and video players existed and were readily available in the time period when the discussed guides were developed, the numbers of units, breadth of competition, capacity and the features of these devices has massively expanded. This increase in the feature-set of such devices has expanded beyond the playback of music and allows video playback and the storage of contact lists – all of which may have evidentiary value within an investigation.

From a forensic analysis perspective, there have been several research projects that have forensically analysed the Apple iPod as a means of extracting information relating to contacts, connected machines and other personal information contained within the device, but the major evidentiary value in the device has been as a data storage medium [13].

Relating personal music and video players to the evidence collection guides discussed is not an easy task, as they are not specifically listed as a source of evidence in any of the guides listed. Their inclusion would be a simple process in either the *The Good Practice Guide for Computer Based Electronic Evidence*, [4] or the *Electronic Crime Scene Investigation – a guide for first responders* [5] guides, as items of interest to be searched for in an area of interest or on an individual's person. However, the decision of whether to seize a piece of evidence such as a personal music player must be made in the context of the investigation, given that for certain types of investigation it may not be required, but for others an individual's personal storage mechanism may be of evidentiary value.

3.3 Game Consoles

Game consoles have developed rapidly since the release of , with the seventh and current generation of gaming machines rivalling the power of high end workstations [14], containing wireless networking, photograph and video viewing capability, internet connectivity and messaging facilities. Such facilities were not available on the previous generation of game consoles, and it is therefore not surprising that they were not considered as worth collecting for evidentiary purposes when these guides were developed. Therefore, none of the guides listed mention game consoles as a potential evidentiary source in any way.

The specific lack of discussion regarding game consoles in the listed evidence collection guides is an issue, as they are extremely common in private residences, and therefore unless they are specifically given as a source of evidence, it is likely that they will not be identified as such.

3.4 VOIP Devices

Voice Over Internet Protocol (VOIP) represents one of the fastest growing telecommunication trends currently occurring [12] and further blurs the line between information technology and telecommunications. The result of this is that whilst VOIP devices are considered computing devices, there is also a communication aspect which needs to be considered.

Although VOIP devices are not referenced directly within any of the discussed evidence acquisition guides, there are several ways in which these devices may be collected. VOIP phones are, by their very nature, networked devices on an Internet connection, either as a stand-alone device or as a program within a computer. Therefore, if all computer workstations are seized as sources of electronic evidence, the use of VOIP may be examined as a component of a larger investigation. This may involve an examination of logs, or if this is not possible or inconclusive, further investigation with the provider.

If the VOIP installation merely uses a normal phone and an end-point, it would provide little information beyond that possible from a normal phone, except that it may lead to the existence of the VOIP provider. This may be required as a means of determining the carrier used as a means of gathering further documentation and call listings from this company.

However, VOIP does provide new evidential issues in that need to be addressed, as potentially there are many types of device that can act as a VOIP client; workstations, mobile phones and gaming consoles are all capable of sending and receiving voice calls, and, in some cases, videos. In addition, when combined with other discussed technologies such as wireless networking, there are several potential issues with current evidence acquisition guides, but these are covered in other areas of this work.

4. Conclusion and Discussion

It has become evident from the comparison of several new technologies to the information found in electronic evidence collection guides that consumer-based technology changes quickly, and that as potential sources of evidence, there is the potential for non-technical investigators to fail to identify information sources that are potentially of use. This is not through any fault in the original publication, but as the breadth of technology available has expanded, there are a greater variety of electronic devices that may contain evidence than when these guides were developed.

There is a fine balance to be achieved within guides for the identification and collection of electronic evidence in the approach taken between being too descriptive and too generic. Being overly descriptive increases the size and complexity of a guide and makes it more vulnerable to changes in technology, whereas a guide that is too generic leaves a user at risk of not identifying or collecting sources of evidence that should be referenced.

Many of the technologies discussed within this work do not significantly change the process, particularly the collection of portable music players and gaming consoles, and these could be added to existing procedural guides with relative ease. The mechanisms for isolating and seizing devices are, for the most part, still accurate and the processes discussed valid, although

some additions may be periodically considered that reflect changes in technology. However, the intricacies of some technologies, such as wirelessly networked devices, may need a more fundamental change to the procedures outlined within several of the guides. The changes required are beyond the scope of this work, but may require both changes in process as well as technology.

Overall, this work has identified that electronic evidence identification and collection guides, aimed at non-technical persons, cannot be both succinct and in-depth, and that without regular updates, they become outdated as new technology becomes commonplace.

5. References

1. G.M. Mohay, A. Anderson, B. Collie, R.D. McKemmish, and O. de Vel, *Computer and Intrusion Forensics*, Artech House, 2003.
2. United States Department of Justice - Computer Crime and Intellectual Property Section Criminal Division, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," 2001; www.usdoj.gov/.
3. Australasian Centre for Policing Research, "Seizing computers and other electronic evidence: best practice guide," 2003; www.acpr.gov.au/.
4. National Hi-Tech Crime Unit & Association of Chief Police Officers, "Good Practice guide for computer based electronic evidence," 2003; www.nhtcu.org/.
5. National Institute of Justice, " Electronic Crime Scene Investigation – a guide for first responders," 2001; www.usdoj.gov/.
6. International Association of Chiefs of Police, and United States Secret Service, "Best Practices for Seizing Electronic Evidence," 2002; http://www.secretservice.gov/electronic_evidence.shtml.
7. National Center for Forensic Science Scientific Working Group on Digital Evidence, "Best Practices for Computer Forensics " 2005; http://ncfs.org/swgde/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf.
8. Interpol European Working Party on Information Technology Crime, "Computer Crime Manual (restricted release)," *Book Computer Crime Manual (restricted release)*, Series Computer Crime Manual (restricted release) 2005, ed., Editor ed.^eds., Interpol Publishing, 2004, pp.
9. W. Jansen, and R. Ayers, "Guidelines on PDA Forensics; Recommendations of the National Institute of Standards and Technology," *Book Guidelines on PDA Forensics; Recommendations of the National Institute of Standards and Technology*, Series Guidelines on PDA Forensics; Recommendations of the National Institute of Standards and Technology, ed., Editor ed.^eds., National Institute of Standards and Technology, 2004, pp.
10. W. Jansen, and R. Ayers, "Guidelines on Cell Phone Forensics; Recommendations of the National Institute of Standards and Technology " *Book Guidelines on Cell Phone Forensics; Recommendations of the National Institute of Standards and Technology* Series Guidelines on Cell Phone Forensics; Recommendations of the National Institute of Standards and Technology ed., Editor ed.^eds., National Institute of Standards and Technology, 2006, pp.
11. National Institute of Justice, "Forensic Examination of Digital Evidence: a guide for Law Enforcement," 2004; www.usdoj.gov/.
12. M. Simon, "Voice over Internet Protocol: Evidence recovery using imaging techniques," Advanced Computer and Information Science (Honours), School of Computer and Information Science, University of South Australia, Adelaide, Australia, 2006.
13. C.V. Marsico, and M. Rogers, "iPod Forensics," *International Journal of Digital Evidence*, vol. Vol. 4, no. Issue 2, 2005.
14. VG Charts, "Hardware Comparison Charts," 2007; http://www.vgchartz.com/hwcomps.php.