Digital Forensic Standards: International Progress

M. Grobler

Council for Scientific and Industrial Research, Pretoria, South Africa
e-mail: mgrobler1@csir.co.za

Abstract

With the explosion of digital crime, digital forensics is more often applied. The digital forensic discipline developed rather rapidly, but up to date very little international standardisation with regard to processes, procedures or management has been developed. This article provides a brief overview of the current international standards in the digital forensics domain. It describes the necessity of international standards and briefly explains the international standard structure. This article also explains the practical problems that editors of international standards face, especially with regard to digital forensic standards. Lastly, this article looks at future standardisation work in the digital forensics field.

Keywords

Digital forensics, International standards, SABS, ISO/IEC, evidence management, digital forensic governance, forensic readiness

1. Introduction

Moore's law predicts that computing power doubles every 18 months (French 2008). This ever increasing power enables humans to undertake tasks that are more complex and resource intensive. With the boom of Information Technology (IT) and enhanced technological developments, the IT environment evolved to the specialised Information Security (IS) discipline. This, in turn, acted as catalyst for the development of the digital forensics discipline.

The intention of these technology advances is to make human lives easier and more fulfilling: hand biometric applications can ensure that only authorised people can operate guns; online social communities such as Facebook and MXit can globally connect people; and iris recognition can lead to a keyless environment. Computers enable humans to an inconceivable amount of power. However, not all humans can suitably handle power. Accordingly, it is necessary to incorporate digital forensics in the everyday business environment to address the collection and acquisition of digital evidence dispersed through digital systems. The eventual purpose of this evidence collection might be either internal organisational investigations, or prosecution in a court of law.

Since internal investigations and prosecutions in a court of law may span more than one organisation (in the case of multiple branches) or more than one continent, the need for international agreement on a number of digital forensic aspects are paramount. Thus, the worldwide interoperability of information systems and the cross-border nature of digital crime necessitate the drive to formulate substantial and

procedural rules against digital crime with regard to digital evidence, both on a local and international level (Završnik 2008). The digital forensic discipline developed rather rapidly, but up to date has very little international standardisation with regard to processes, procedures or management (Grobler & Dlamini 2010). Digital forensics, as a developing discipline, presents a number of opportunities for international standardisation.

This article provides a brief overview of the current international standards in the digital forensics domain. It describes the necessity of international standards and briefly explains the international standard structure. This article also explains the practical problems that editors of international standards face. Lastly, this article looks at future standardisation work in the digital forensics field. This article is based on the author's own perceptions and does not necessarily reflect the opinions of ISO (International Organization for Standardization), the IEC (International Electrotechnical Commission), ISO/IEC JTC (Joint Technical Committee) 1/SC (Sub Committee) 27 or the South African national body.

2. The necessity of international standards

"The larger and more indiscriminate the audience, the greater the need to safeguard and purify standards..." - Moses Hadas

According to the South African Bureau of Standards (SABS), a standard is a published document that lists established specifications and procedures to ensure that a material, product, method or service is fit for its purpose and perform in the manner it was intended for (Amsenga 2008). It is an agreement that can have a profound influence on matters such as safety, reliability and efficiency (ISO 2009a). International standards are a vital necessity to ensure conformance and mutual compliance across geographical and jurisdictional borders. It provides an essential framework for both industry and government to maintain national and international confidence in a country's goods and services (SABS 2008).

Generally when procedures are standardised, the associated costs are lower, training is simplified and consumers accept products and services more readily. *"Standards are also the key to enhancing our global competitiveness, attracting investment and encouraging and supporting innovation"* (SABS 2008). Some standardisation benefits include:

- improving the suitability of products, processes and services for their intended purposes;
- preventing barriers to international trade; and
- preventing unsafe products and procedures from reaching consumers through the regulatory use of safety standards (SABS 2008).

By adopting internationally recognised standards, member countries are assured of a high quality and trusted reference with input and insight from a number of international subject experts, as well as the widespread applicability of the standards. In general, standard adoption is voluntary and standards are developed in response to

market demand. The standards are developed through international participation and are based on consensus among interested parties (Amsenga 2008). A number of standardisation bodies exist, introduced next.

2.1. WSSN (World Standards Services Network)

WSSN is a publicly accessible network of standards organisations around the world. (WSSN 2006). The three main standards organisations listed on this site are the International Organization for Standardization (ISO), the International Electro-technical Commission (IEC) and the International Telecommunication Union (ITU). For the purpose of this article, IEC and ITU will not be discussed in detail. Where appropriate, ISO has liaison agreements with IEC to provide technical input on matters pertaining to specific IT-related international standards. The WSSN website www.wssn.net also links to a complete list of the international standardising bodies, regional standardising bodies, as well as national members of ISO and IEC.

2.2. ISO (International Organization for Standardization)

ISO is the world's largest developer and publisher of international standards. This organisation is a network of the national standards institutes of 162 countries, one member per country. South Africa is a member country with SABS as its ISO member and representative (ISO 2009b).

The ISO secretariat is situated in Switzerland and coordinates the interaction between member countries' mandates (some countries are mandated by government, whilst other are mandated by the private sector). As a result, ISO facilitates consensus between member bodies on solutions that meet both the requirements of business and the broader needs of society (ISO 2009b). ISO, in collaboration with IEC (through JTC 1), published a whole portfolio of standards related to generic methods, techniques and guidelines for information, IT and communication security. This includes the digital forensic domain and will accordingly be the main focus of the remainder of the article.

ISO and IEC standards are developed industry wide, with consensus of member countries that volunteer contributions. This ensures global solutions to satisfy industries and customers worldwide, the views of all interests are taken into account, and a market driven approach is adopted based on voluntary involvement of all interests in industry (ISO 2009b). ISO currently has more than 580 nominated organisations (such as the Forum for Incident Response and Security Teams) that participate in JTC 1 as liaison partners. These organisations are nominated based on their regional and international connections, and the opportunity to exchange documents, new work item proposals and working drafts. Liaison partnerships provide a way for international and broadly-based regional organisations to participate in (category A liaison) or be informed about (category B liaison) the development of standards. The motivation is that their involvement will ensure wider acceptance of the final result and ensure coordination of parallel standardisation activities in different bodies.

2.3. SABS (South African Bureau of Standards)

The SABS is the recognised national institution for the promotion and maintenance of standards in South Africa. It is an autonomous body established through legislation in 1969. The SABS prepares and publishes South African National Standards (identified by the letters SANS) that reflects national consensus on a wide range of subjects. It administers more than 450 technical committees and sub committees to produce standards (Amsenga 2008). The SABS is committed to providing standardisation services that improve the competitiveness of South Africa through the understanding and development of standardisation products and services within South Africa and internationally (SABS 2008).

3. Digital forensics and international standards

During a typical business day, employees email documentation and access information on an organisation's servers. As a result, it is inevitable that sensitive business information has become more exposed and vulnerable to misuse by technology-adept individuals, both on a local and international scale. This necessitates the formalisation and international agreement of digital forensics and evidence management (Grobler & Dlamini 2010). In brief, digital forensics involves the preservation, identification, extraction and documentation of digital evidence stored as data that is electronically or magnetically encoded information (Vacca 2002). This extends to include the recovery, analysis and presentation of digital evidence in a way that is admissible and appropriate in a court of law. This necessitates a crucial accuracy in following forensic procedures, the rules of evidence and the legal processes.

3.1. International standard development procedure

Figure shows the role players and their responsibilities during the international standard development procedure. If the need for standardisation on a specific topic is identified, industry or the relevant business sector communicates the need to its national ISO member. The ISO member then proposes a new work item to the larger ISO community. If the new work item is accepted and supported by an adequate number of other ISO members, the work item is assigned to an existing technical committee (ISO 2009a).

The national delegations of experts of a technical committee generally meet twice a year to discuss and comment on draft international standards. Depending on the economic viability, a member country aims to send one or more delegates per working group to these international meetings. These delegates represent their member country by participating in various project meetings, and by providing and defending comments made by experts in the national mirror committee on the subject from the respective member country.

During the project meetings, the various delegations need to reach consensus on a draft agreement and negotiate the detailed specifications within the standard. After these meetings, the standard editors need to provide updated text and a disposition of

comments, stating which comments were accepted and rejected, with an explanation on the reasoning behind the decisions. The draft text and disposition of comments are then circulated to ISO member countries for comment and balloting. Once the voting on the text of the draft standard is favourable (75% acceptance of all voting members), the document is published as an International Standard (ISO 2009a).

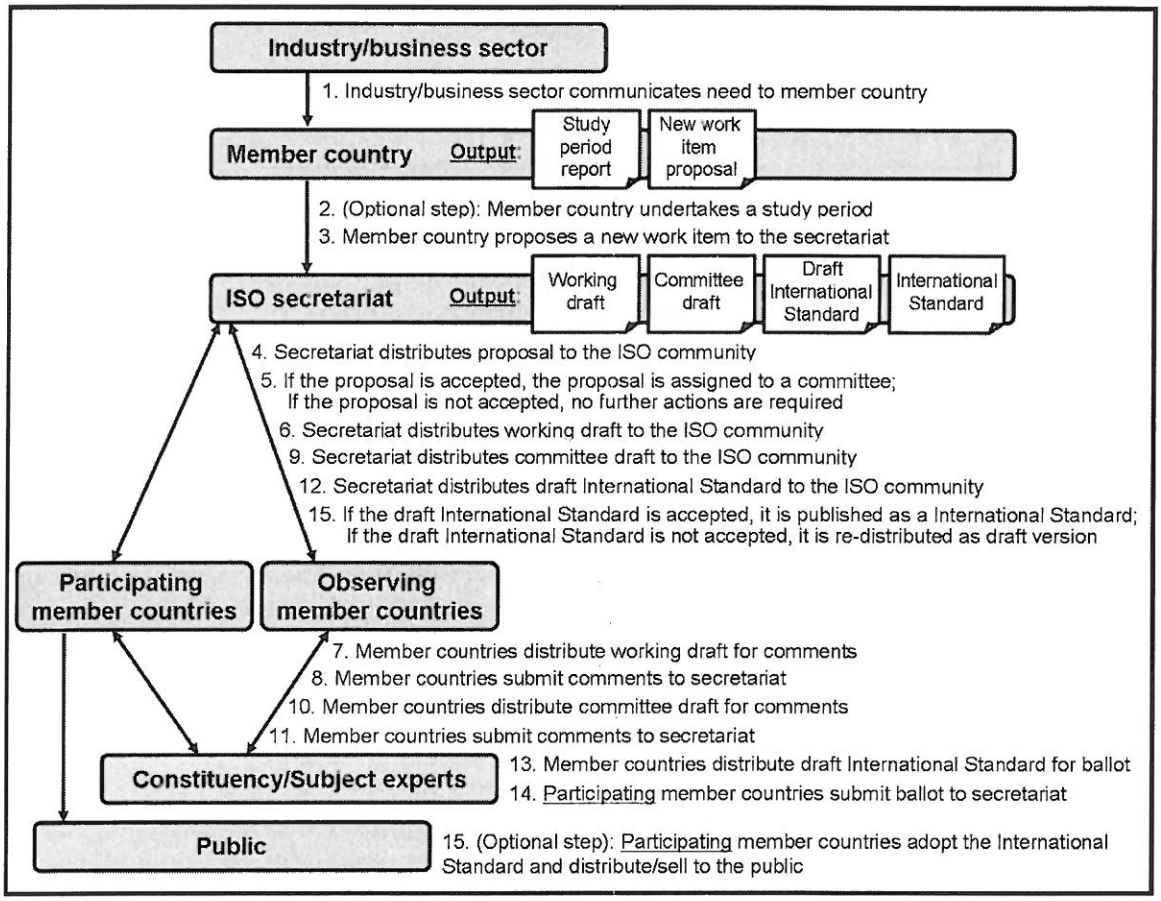

Figure 1: International standard development procedure (Own compilation)

3.2. International digital forensic standards

Searches on the BSI (British Standards Institution), ANSI (American National Standards Institute) and NIST (National Institute of Standards and Technology) websites indicate no standard directly related to digital forensics. The only current work related to digital forensics (at the time of writing) is done by ISO.

- ISO/IEC JTC 1 SC 27 (IT security techniques) is working on an international standard focusing on the identification, collection and/or acquisition and preservation of digital evidence. The finalised standard will ensure that responsible individuals manage digital evidence in accordance with worldwide accepted practices, with the objective to preserve its integrity and authenticity. The standard will not replace specific legal requirements of any jurisdiction, but may assist in the facilitation of potential digital evidence exchange between jurisdictions (ISO/IEC 27037 2010). The document will complement ISO/IEC 27001 and ISO/IEC

27002, and in particular the control requirements concerning potential digital evidence acquisition by providing additional implementation guidance (ISO/IEC 27037 2010).

- ISO/IEC JTC 1 SC 7 (Software and systems engineering) is working on an international standard focusing on the digital forensic governance. The new work item proposal has recently been circulated for ballot.

4. Problems regarding digital forensics standards

Computers and other digital devices have been used for a number of decades. Its relation with crime has proliferated enormously since the early 1990s, and is still growing at a rapid pace. Accordingly, digital evidence is more readily accepted within the legal boundaries. It can be problematic, however, when different disciplines need to come together to solve a crime (Grobler & Von Solms 2009). As a result, there are a number of problems related to the development of international standards pertaining to digital evidence and digital forensics.

4.1. Jurisdictional differences

Jurisdiction refers to the right of the court to make decisions regarding a specific person or a certain matter (Casey 2000). Currently, there is an international awareness of problems associated with discrepancies in the inter-jurisdictional transfer of information relating to legal proceedings. Different legislations apply in different jurisdictions, and these are not always compatible. In an inter-jurisdictional crime, an increasingly common occurrence in the digital era is that a specific act may be considered a crime in one country and not in another.

New digital crimes often do not have a distinct boundary. For example, consider the example of phishing, an attempt by a third party to solicit confidential information from an individual, group or organisation. Phishing may be classified as deception (of the victim computer user), identity theft (of the victim computer user), unauthorised use of domain specific information, logos and public image and web presence (of the victim organisation or online entity) or denial of service (of the legitimate owner of the online website). This inconsistent interpretation and accordingly, inconsistent application of laws is a major obstacle for smooth digital evidence processing.

Another example is when the perpetrator is situated in one country and the victim in another, and inter-jurisdictional transfer of information is necessary. This can cause conflict since the evidence is transitory in nature and saving or transmitting it could alter the character of the data. At present, there is no internationally accepted data exchange methodology that applies to all jurisdictions, to protect data whilst in transit. Further input from ISO member countries is required regarding specific requirements that will enable digital evidence transfer between jurisdictions.

4.2. Training, certification and competence discrepancies

Forensic investigators must be trained and qualified to handle digital evidence in a skilful manner and must have a sound technical knowledge to choose the best methods. Adequate and continuous training, as well as periodic assessment of knowledge and skills will ensure the competency of the investigator and enable them to handle digital devices that may contain potential digital evidence (ISO/IEC 27037 2010).

Required competence levels and competency demonstration of forensic investigators may vary from one jurisdiction to another. At the moment, there is no internationally agreed upon minimum level of training and certification. In parallel with the problems discussed regarding jurisdictional differences and inter-jurisdictional information transfer, discrepancies regarding investigator competency may facilitate problems in international investigations. ISO member countries are required to comment on initial competence tests and competence maintenance tests for digital investigators.

4.3. Availability of experts

ISO standards are developed by technical committees comprising of experts from the industrial, technical and business sectors which have interest in the specific standards. Especially with technology related subjects, such as digital forensics, it is difficult to get a sufficiently representative group of experts together that have satisfactory knowledge of the technical domain itself, the standardisation process, legal aspects, as well as different operational and legal aspects of various jurisdictions.

Not only is it difficult to get subject experts, but these experts should be available for the average standard development time of three years to be able to contribute to the standard. Most standards also require periodic revision, whether it is due to technological evolution, new methods and materials, or new quality and safety requirements (ISO 2009b). Again, the availability of experts may complicate the standardisation process.

It is estimated that 30 000 experts annually participate in the development of ISO standards. The experts participate as national delegations, chosen by the ISO member country (SABS is South Africa's ISO member) to represent the views of the organisations in which the experts work, as well as a full national consensus on the issues involved (ISO 2009a). The current distribution list of actively participating South African experts on digital forensics consists of six individuals.

5. Future work on digital forensic standards

The digital forensic discipline allows for at least two additional international standards. "... The rapid, widespread adoption of new technology often outpaces society's development of a shared ethic governing its use and the ability of legal systems to deal with it. The handling of digital evidence is a perfect example" (NCJ

211314 2007). The modern world evolves around digital information, whether it is word processing documents, electronic document repositories, email or commercial web presence. Electronic data is routine in the daily operation of many individuals.

5.1. Digital forensic governance

Governance in general is becoming increasingly important in contemporary management, but specifically the governance of digital forensics. In order to manage governance disciplines effectively, closer attention needs to be paid to the technical aspects of specialised fields covered within an organisation (Grobler & Dlamini 2010).

Similar to other existing organisational governance disciplines, digital forensic governance aims to assist organisations in guiding the management team and stakeholders in setting up mandates and expected actions from the organisation's incident response team. This process still needs to be formalised to ensure global conformity.

At present there are no ISO/IEC JTC 1 standards that focus specifically on the governance of digital forensics risk and services. The study group on Corporate Governance of digital forensics reviewed 18 ISO/IEC JTC 1 standards to locate elements that have a direct relationship to digital forensic practice. Although several considerations of risk, scientific processes, service level management, document management, certification of experts and incident management were found in many of the standards, in total too little information is currently available to adequately address the requirement of digital evidence matter (ISO 2009c).

At the time of writing, this project was still a new work item proposal and formal development work has not commenced. The study group recommended a single principle based Corporate Governance of Digital Forensics umbrella standard that addresses the concerns of the Corporate Board, and an implementation guide for the corporate governance of digital forensics that specifies harmonisation strategy for integrating all the disparate parts of ISO/IEC JTC1 standards that relate to best practice in the functional domains of digital forensics (ISO 2009c).

The study group also recommended that a digital forensic practitioner certification, professional practice audit, and review is required. Such a standard would provide a comprehensive single point of reference for Corporate Boards wishing to set corporate direction, mitigate legal risk, and to audit executive performance. The Corporate Governance of Digital Forensics is currently addressed by the ISO/IEC JTC 1 SC 7/WG 1A but is still in its early development stages (ISO 2009c).

5.2. Digital forensic readiness

Forensic readiness can be defined as the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation (Rowlingson 2004). It extends beyond the borders of the digital crime. It prepares

the environment for a potential digital crime and in many cases ensures the legal acquisition of evidence necessary to prosecute.

Although in many instances it is possible to successfully acquire digital evidence in a digital forensically sound manner, forensic readiness often makes the process much easier. Organisations can be proactive and install the legitimate software agents on machines (that is, prior to any digital incident). In a large organisation, these agents can be distributed to all machines by using network management software or USB scripts, or by issuing standard organisational clones (with the agent already installed) to all employees (Grobler 2010). After an incident has taken place, the forensic acquisition can be performed covertly, remotely and with minimum effort.

By ensuring that the system administrator or forensic investigator monitors the system continually, an organisation can ensure forensic readiness in the event of a digital crime. "Although digital forensic investigations are commonly employed as a post-event response to a serious Information Security or criminal incident, when forensics is used to its potential, it can provide both pre- and post event benefits" (Laubscher, Olivier, Venter, Rabe & Eloff 2005).

To a large extent forensic readiness raises issues regarding access and privacy, and questions regarding the benefits of forensic readiness as compared to the costs that need to be incurred in preparing for incidents that will hopefully never take place (Grobler 2010). International standardisation is required to address these matters to ensure international buy-in from all parties handling digital evidence. At the time of writing, no formal proposal for a standard on forensic readiness has been proposed, but a number of ISO member bodies have had meetings regarding a probable new project.

6. Conclusion

The draft report of the study group on Corporate Governance of Digital Forensics released in May 2009, states "The public appeal in many jurisdictions is for the standardisation of data management procedures to assure consistency in the acquisition, extraction (and preservation), analysis, and presentation of data that has potential to be evidential" (ISO 2009c). In many regards, the domain of digital forensics and digital evidence is crucial, and relates largely to both IT and IS on a local and international level. The development of international standards can accordingly only benefit the further development of the domain, and to some extent address the rising occurrence of digital crime and digital incidents worldwide.

However, it is necessary to address the problems that may hamper the development process (see Section 4). The development of an International Standard is an extended process that requires many resources. In many instances, the need for specific topic standardisation is only identified long after a specific technology has been introduced to industry. In addition to this late start of the standardisation process, the average timeline for developing an international standard is about three years. It is therefore recommended that members of specific industries proactively identify areas of concern and channel this information at an early stage to the

respective member bodies. This can speed up the process and potentially have the International Standard in place when the technology is as its peak and in need of international standardisation.

Linked to the proactive identification of possible standardisation areas, members of the public and especially industry members that are knowledgeable on a specific topic, should become involved in the standardisation process. Especially with technology related subjects, it is difficult to get a sufficiently representative group of experts together that have satisfactory knowledge of the technical domain. If more members of the public become involved, the entire standardisation process may proceed a lot smoother.

7. References

Amsenga, J. 2008. An introduction to standards related to information security. ISSA 2008 (Information Security South Africa). 7 – 9 July 2008. School of Tourism & Hospitality, University of Johannesburg, South Africa.

Casey, E. 2000. Digital evidence and computer crime: Forensic science, computers and the internet. Academic Press: Boston.

French, E. 2008. Will technology take over the world? URL: http://www.helium.com/items/609726-will-technology-take-over-the-world (Accessed 28 November 2008.

Grobler, MM. & Dlamini, IZ. 2010. Managing digital evidence – The governance of digital forensics. Journal of Contemporary Management, 7:1-21.

Grobler, MM. & Von Solms, SH. 2009. Fusing business, science and law: Presenting digital evidence in court. Journal of Contemporary Management. 2009(6):375-389.

Grobler, MM. 2009. Liforac – A model for live forensic acquisition. PhD thesis, University of Johannesburg. To be published in 2010.

ISO (International Organization for Standardization). 2009a. Standards FAQs [online]. URL: http://www.iso.org/iso/iso_ catalogue/faq_standards_2.htm (Accessed 5 January 2010).

ISO (International Organization for Standardization). 2009b. International Standards for Business, Government and Society [online]. URL: http://www.iso.org/ (Accessed 5 January 2010).

ISO (International Organization for Standardization). 2009c. Report of the study group on "The Corporate Governance of Digital Forensics" [draft]. ISO/IEC JTC1/SC7 N40XX.

ISO/IEC 27037. 2010. Guidelines for identification, collection and/or acquisition and preservation of digital evidence. Working draft text.

Laubscher, R., Olivier, MS., Venter, HS., Rabe, DJ. & Eloff, JHP. 2005. Computer forensics for computer-based assessment: the preparation phase. Pretoria: University of Pretoria. URL: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/100_ Article.pdf (Accessed 16 January 2008).

NCJ 211314. 2007. Digital evidence in the courtroom: a guide for law enforcement and prosecutors [online]. US Department of Justice. URL: www.ojp.usdoj.gov/nij/pubs-sum/211314.htm (Accessed 21 August 2009).

Rowlingson, R. 2004. A ten step process for forensic readiness. International Journal of Digital Evidence. 2004(2), Issue 2:1-28.

SABS (South African Bureau of Standards). 2008. The importance of standards [online]. URL: https://www.sabs.co.za/Business_Units/Standards_SA/ImportanceOfStandards.aspx (Accessed 6 January 2010).

Vacca, R. 2002. Computer forensics – computer crime scene investigation, Hingham: Charles River Media, Inc.

WSSN (World Standards Services Network). 2006. World standards services network [online]. URL: http://www.wssn.net/WSSN/ (Accessed 6 January 2010).

Završnik, A. 2008. Cybercrime definitional challenges and criminological particularities. URL: http://mujlt.law.muni.cz/storage/1236041878_sb_01-zavrsnik.pdf (Accessed 7 January 2010).