Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic

Conference Paper · July 2015

CITATIONS
4

READS
7,390

2 authors, including:

Zdenek Smutny
University of Economics Prague
40 PUBLICATIONS **57** CITATIONS

SEE PROFILE

In: 14th European Conference on Cyber Warfare & Security,
Hatfield, UK, 2-3 July 2015. Reading: ACPI

Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic

Jaromir Veber and Zdenek Smutny
Faculty of Informatics and Statistics, University of Economics, Prague, Czech Republic
jaromir.veber2@vse.cz
zdenek.smutny@vse.cz

Abstract: Collection of digital evidence in criminal investigation is gaining in importance. It is an outgrowth of the development and penetration of ICT into society (informatization). After a brief introduction of ISO/IEC 27037:2012, this paper compares the suggested practices with those that are currently used by investigators (criminal police) and analysts (forensic laboratory). This is followed by a discussion of general experience in collecting and analysing digital evidence in the Czech Republic. The contribution allows experts from other countries to compare their practices with the standard, and also with practical approaches that are applied by Czech departments.

Keywords: digital evidence, ISO 27037, expert opinion, acquisition, collection, Czech Republic

1. Introduction

Technological development – especially informatics – is still moving forward. Information technology is increasingly penetrating not only into the lives of professionals but also into the lives of ordinary people. People spend a significant amount of time of both their working and leisure time in cyberspace. Because people move between the real physical world and cyberspace (immersion environment), there is a blending of these two quite different environments.

Unfortunately, negative aspects of real life also penetrate into cyberspace, and this includes cybercrime. Further, the fact that people spend a lot of time in cyberspace means that they leave there a significant amount of data. Crime investigation was originally based in the real world, but evidence/data can now be also obtained from cyberspace (in digital form). Forensic methods for obtaining digital evidence are still evolving, as the volume of digital data grows. The number of people who deal with digital evidence is also growing. (Hegarty, Lamb, Attwood, 2014)

International Organization for Standardization (ISO) is engaged in the development and publication of standards for almost all areas of human activity. This concerns standards for products, services and best practices. The family of standards ISO 27000 focuses on information security including digital forensic investigation (Veber, Klíma, 2014), which also includes standard ISO/IEC 27037: 2012 (ISO, 2012) - hereafter referred to simply as ISO 27037 or the standard. ISO 27037 describes procedures for the handling of potential digital evidence. This standard belongs to the group of standards for best practices and summarizes the procedures that should be followed during the identification, collection, acquisition and preservation of potential digital evidence.

It has been three years since the standard was released, so now seem to be a good time to evaluate the (contents of the) standard. This article briefly introduces the standard, but at its core are the opinions of digital evidence analysts (judicial experts and criminologists) on the procedures specified in the standard, as well as on the current state of digital evidence collection.

The benefit of this paper lies in its observations about what should be considered when deploying ISO 27037 (for example, what to do differently or what to look for in addition to what the standard mentions). Moreover, it could provide guidelines for future standard updates.

2. Standard ISO/IEC 27037:2012 for identification, collection, acquisition and preservation of digital evidence

The international standard (ISO, 2012) mainly deals with the initial process of collecting and storing potential digital evidence and disregards subsequent work with the evidence, such as its analysis, presentation and disposal. The persons who handle digital evidence should be able to identify and manage risks that can arise when working with this kind of evidence, in order to prevent its debasement and rendering it useless. DEFR

(Digital Evidence First Responder) should follow certain general principles to maintain the integrity and reliability of digital evidence. The objectives of these specific procedures must include the following:

- Minimizing manipulation with digital devices or digital data.
- Documenting all actions and changes made to the digital evidence, so that an independent expert is able to form their own opinion regarding the reliability of submitted evidence.
- Proceeding in accordance with the laws of the country.
- DEFR should not act beyond his or her competence.

Observation of these fundamental principles should lead to the preservation of evidence for investigation purposes. In case a change to the evidence cannot be avoided, all actions that were carried out and the reasons for them are properly documented. Below follows a brief description of the sub-processes involved in handling digital evidence.

A) Identification

The identification process includes searching, detecting and documenting digital evidence (digital evidence is represented in both the physical and the logical form). All devices which could contain digital evidence should be identified in the course of this process. DEFR should carry out a systematic search of the crime scene to prevent overlooking small, camouflaged devices or material which seems irrelevant at first sight. In addition, DEFR should consider the possibility of existence of hidden evidence in the form of virtual components – e.g. Cloud Computing (Chung et al., 2012; Federici, 2014). In case of instability of certain devices (their state may be subject to change over time), it is necessary to prioritize these devices when obtaining evidence. The appropriate order of collection and subsequent processing should minimize possible damage to digital evidence.

B) Collection

After the identification of devices that may contain digital evidence, these devices are removed from their original location and transferred to the laboratory where they are analysed and processed as the next step. The collection process is at all times documented, including packaging and transport to the laboratory. It is important that DEFR also secures any other physical material which may be related to the digital data that has been collected (e.g. notes on paper which may contain passwords, cradles and power connectors for the devices and other hardware necessary for obtaining digital information from the identified devices).

C) Acquisition

The initial processing of digital evidence consists mainly in producing a copy of the evidence (e.g. the content of an entire hard drive) and documenting the methods used. If necessary, allocated and as well as unallocated space (including deleted files) should be obtained. Generally, the original and any copies thereof should generate the same output (hash) of the same verification function (proven accurate at that point).

Depending on the circumstances (situation, time, price), DEFR should select the most appropriate procedure and method for acquiring data. If this process results in inevitable changes in the created copy, as compared to original, it is necessary to document what data was changed. In those cases in which verification process cannot be carried out (e.g. while acquiring data from a running system, when the original contains bad sectors, or when the time for acquiring data is limited), DEFR should use the best possible way and then be able to justify and vindicate his or her choice of methods. If the created digital copy cannot be verified, then this must be documented and justified. In the case that the source of digital evidence (data) is too big to handle, DEFR can acquire only the relevant part (selected files, folders or paths). All other steps of forensic analysis are performed on copies of digital evidence – see (Sindhu, Meshram, 2012).

D) Preservation

In terms of preserving digital evidence, it is necessary to protect its integrity to make it usable for the purposes of investigation. DEFR should be able to demonstrate that the evidence has not been changed since its collection and to provide documentation and justification of all actions that led to its changes.

Professionals conducting such activities are usually police or forensic experts. Standard was released in 2012 and we do not know about any ongoing document rework or innovation. ISO 27037 gives guidance for the following devices and circumstances (Buzarovska, Lazetik, Koshevaliska, 2013; ISO, 2012):

- Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto optical disks, data devices with similar functions,
- Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards,
- Mobile navigation systems,
- Digital still and video cameras (including CCTV),
- Standard computer with network connections,
- Networks based on TCP/IP and other digital protocols, and
- Devices with similar functions as above.

Standard is purposed for:

- Forensic laboratory managers
- DEFR (Digital Evidence First Responders)
- DES (Digital Evidence Specialists)
- Incident response specialists

3. Expert opinions

In this section we bring core of the article - a discussion of field experts to the standard, including deviations, which may be typical for the Czech Republic. The debate is not limited to the issue of collecting digital evidence, but also takes into account the opinion of experts, who does the analysis of collected digital evidence.

The first expert (Section 3.1), is focused on digital evidence gathering process (Ladislav Vyskocil) is a representative of the Department of Information Crime – Section of analytics and cyber-crime, Criminal Police and Investigation, Police of the Czech Republic. Currently, it is the most advanced department in Czech Republic for digital evidence gathering. The second expert (Section 3.2), is focused on digital evidence analysis process (Marian Svetlik), who heads the Expert institute of company Risk Analysis Consultants (RAC). He's also forensic expert in the field of criminology and forensic computer expertise.

3.1 Collection of potential digital evidence

The area of informatics is constantly evolving and therefore it is difficult to introduce long-term stable and applicable standards to this area. Procedures and recommendations for collecting digital traces are evolving not only along the increasing number of investigations, but also along with the development of digital devices. Procedures of a similar nature should ideally be frequently updated, in order to allow to factor any new circumstances that may occur during the investigation.

At the beginning of the standard (Chapter 5 and 6) there are introduced a common and in the field well known general recommendations, which are generally held by investigators in the Czech Republic (and probably anywhere else in the world), however some of the following (Chapter 7) practical recommendations are already obsolete given the current date.

The first slight discrepancies (Chapter 6.8) are related to the fact that the expert on digital footprints (DEFR or DES) should decide what equipment will be collected/acquired on scene and he also determine the order of device collection. In practice, in the Czech Republic DEFR is not a person to carry out investigations and, therefore, he can only deliver recommendations to investigating officer on how to proceed with an investigation, however, decision-making competencies are held by investigating officer.

Another relatively significant aspect concerns that the standard does not mention the involvement independent person (that may be a device owner or for example maid in the room where the digital evidence gathering took place). Such a person is required in order to sign a protocol of potential digital evidence gathering and thus confirms that the collection of potential digital evidence was independent of those who are investigating.

Collected devices are completely packed (and sealed), preferably in an opaque container (often plastic) so that nobody may manipulate with them. However, the standard also recommends (Section 6.9.3.2, 7.1.2.1.2, 7.1.2.1 .3, 7.1.2.2.2, 7.1.2.2.3) placing tape over the power switch and placing tape over the floppy (CD/DVD) disk slot, if present.

Standard divides investigation on procedures for devices that are not connected to the network, and procedures for devices that are connected to the network. This division is no longer necessary, because nowadays almost all the devices are connected to network thus it is required to use only procedures for devices that are connected to the network.

Securing traces at camera systems is in the Czech Republic work for experts on audiovisual equipment, and not specialists on gathering digital evidence. That's because there are certain specifics of audiovisual equipment especially their stores and especially the fact that most of them provide audiovisual records.

Securing digital footprints on mobile devices (especially phones) is a matter experts (DES) on such devices and the common practice of DEFR in this case is to switch the device to airplane mode and seal it in an opaque shielded container attach the charging adapter send it to a specialist (DES) on mobile devices.

It is hardly surprising that the standard does not even mention the existence of a third party (non-participating) that often appears in investigations (third party often owns hardware or the building in which the hardware is stored). In Czech Republic such party mustn't be damaged during investigations.

The standard in several places mentions the need to create a checksum to verify data, but there is not much stressed that the creation of hash should be recorded in the protocol of digital evidence collection. Such procedure ensures verification that the collected evidence was not tampered.

3.2 Analysis of potential digital evidence

It is not easy to briefly comment on the standard which was issued by ISO, because the experts from RAC Company were directly involved in commenting it. It should also be noted that our suggestions, which were more or less in line with the previously given opinion of police practitioners (and also consistent with the view of colleagues from the UK, the Netherlands and other countries), were not adopted by ISO. This fact will not be further discussed here.

It is not our intention to criticize certain technical obsolescence or inconsistency, particularly of the final part of the standard. It is vital to realize that it is practically the first list of recommendations which is officially recognized at international level. Like any standard of "best practices", also ISO 27037 is a living standard and its practical application is always an adaptation of recommendations to specific conditions, so that conflicts between the demands of standard and practice is avoided. It is also clear that the dynamics of the development of information technology is greater than the ability to update a particular ISO standard. It is therefore not surprising that requirements which are objectively identified as obsolete or not applicable in the given conditions are not implemented in practice.

Regrettably, it must also be observed that conditions (in terms of organization and competence) in the Czech Republic are not favourable for consistent interpretation and subsequent implementation of the standard. This regards not only implementation into police practice, but also into the practice of experts in the field, as well as into the operation of Computer Emergency Response Team (CERT) and other organizations dealing with security incidents. All of those institutions can participate in collecting digital data that can then be used as evidence.

The standard should also serve as a basis for assessing qualifications needed for expert practice. This is because actual practice shows that many judicial experts are not acquainted even with the basic requirements for collection and acquisition of digital evidence, which are listed at the beginning of the standards. Judicial experts can find themselves in different positions – for example as consultants in police work, as independent experts, or they can work as experts in their (own) laboratories. The standard should therefore be one of the most important documents when considering qualification requirements of ICT security specialists.

Since its creation, the standard ISO 27037 has had some – perhaps cardinal – shortcomings. One can wonder why it has not also been based on other documents and recommendations that had long been accepted by the international community of digital forensics experts (e.g. recommendations of Association of Chief Police Officer, Digital Forensic Research Workshop, and International Organization for Cooperation in Evaluation, European Network of Forensic Science Institutes). Nevertheless, the standard unified at least the rudimentary principles and rules of providing digital evidence. Many of those procedures (in the Czech Republic, probably mainly in police practice) seem obvious and such that would already be used in practice. However, our experience shows that even police practice is not perfect in terms of its ability to establish general procedures.

This standard could also give rise to regulatory measures, because providing digital evidence is a process from which ensues obtaining of evidence. This fact is so significant that some elementary rules should never be violated. Unfortunately, violation of the most basic rules is a reality in the Czech Republic. If a biological sample is proved to be contaminated, it cannot be used as evidence. Paradoxically, the violation of fundamental procedures in working with digital evidence does not exclude the contaminated data from evidentiary proceedings.

In conclusion, it can be stated that the standard is understood as a convenient first step towards a process that will lead to increased awareness of the specifics of working with digital evidence – despite some of its obvious shortcomings. This standard also contributes to a gradual improvement in the work of all people who come into contact with digital evidence, whether they be police technicians, legal experts, investigators, lawyers, judges, as well as security specialists and ICT administrators or members of CERT.

4. Conclusion

This article briefly discussed the content of the standard ISO 27037. It was then subjected to analysis by experts on gathering digital evidence. The result is an interesting confrontation of procedures deployed in practice with procedures suggested by the standard.

The opinions of experts clearly indicate that the standard in its current version is not entirely suitable for practical use, especially because of the section which concerns practical procedures (Section 3).

The first expert (from the Police of Czech Republic) discusses the main differences in the collection of potential digital evidence. He identifies the shortcomings, such as omissions of third parties, differences in the approach to evidence packaging or the specifics of distributing work among multiple experts. The second expert discusses the standard generally, from the perspective of experts who carry out evidence analysis. This reveals two related issues:

- Poor knowledge of basic principles of collecting potential digital evidence displayed by all persons that are involved at various levels in a case under investigation (e.g. police officers intervening at a crime scene or court experts). It is no exception that potential digital evidence is collected by someone who specializes in gathering physical evidence, rather than by an expert on cyber-crime and collecting digital data.
- Related with it is the problem of using procedures which violate those included in the standard and those which are otherwise generally accepted, but which in the Czech environment may not affect the value of evidence in court proceedings. This is rather irregular and it is necessary to address this issue in the Czech context.

General recommendations mentioned in the introduction of standard, however, are well formulated. In practice, the used procedures are based on requirements that standard refers. So generally the first part of the standard can be regarded as binding in the case of formation of procedures for collecting digital evidence. However, the second part of the standard already provides specific procedures and in this case we have willy-nilly these procedures take only as a concrete deployment example (not as best practice). The reason is definitely a rapid development of ICT and for this reason it is necessary to make also rapid adaptation of digital evidence collection procedures.

However, the standard very well presents a general framework for collecting digital evidence, which becomes internationally presented and accessible also for wider use (not only for police and experts in the field). Standard, however, allows a better international cooperation and transfer of digital evidence between jurisdictions of different countries (well if those jurisdictions would use introduced framework for digital evidence gathering).

Acknowledgements

This paper was prepared thanks to the IGA grant VSE IGS F4/74/2014.

References

Buzarovska Lazetik, G., Koshevaliska, O. (2013) "Digital Evidence in Criminal Procedures", *Balkan Social Science Review*, Vol. 2, pp 63-83.

Chung, H., Park, J., Lee, S., Kang, C. (2012) "Digital forensic investigation of cloud storage services", *Digital Investigation*, Vol. 9, no. 2, pp 81-95. DOI: 10.1016/j.diin.2012.05.015

Federici, C. (2014) "Cloud Data Imager: A unified answer to remote acquisition of cloud storage areas", *Digital Investigation*, Vol. 11, no. 1, pp 30-42. DOI: 10.1016/j.diin.2014.02.002

Hegarty, R., Lamb, D., Attwood, A. (2014) "Digital Evidence Challenges in the Internet of Things", *9th International Workshop on Digital Forensics and Incident Analysis*, Plymouth, pp 163–172.

ISO. (2012) *ISO/IEC 27037:2012 Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*, International Organization for Standardization, Geneva.

Sindhu, K.K., Meshram, B.B. (2012) "Digital Forensic Investigation Tools and Procedures", *International Journal of Computer Network & Information Security*, Vol. 4, no. 2, pp 39-48. DOI: 10.5815/ijcnis.2012.04.05

Veber, J., Klíma, T. (2014) "Influence of Standards ISO 27000 Family on Digital Evidence Analysis", *22st Interdisciplinary Information Management Talks (IDIMT)*, Poděbrady, pp 103-114.