PhD Gordana Buzarovska Lazetik
PhD Olga Koshevaliska

Digital evidence in Criminal procedures

- A comparative approach -

ABSTRACT

Digital evidence can be a litigant's best friend or worst nightmare, depending on the type of evidence, how it is used, and in what court it is presented. Therefore this article aims to provide an overview of computer forensics from general definitions on digital evidence, their potential sources and basic principles regarding the evaluation of phases of "crime scene investigation" and seizure of data in order to determinate the "fingerprints" of the crime. We illustrated the procedure regarding digital evidence in the USA because of its contemporariness. At last the purpose of this paper is to illustrate the “handling” of digital evidence in Macedonia and to give recommendations for a better compliance with the international instruments regarding this issue.

Key words: digital evidence, digital forensics, digital investigation, criminal procedure.

Electronic evidence - General definitions and principles

The Internet has removed the geographical dimension in terms of the borders of sovereign nations, and correspondingly, criminals have become much more difficult to identify and apprehend. With the rapid advancements in computer technology over the past few years, there has been increasing concern of the need to develop laws in order to take full advantage of technological improvements, and also to ensure that states can respond to computer crime and related criminal law issues.

This article aims to provide an overview of computer forensics from general definitions on digital evidence, their potential sources and basic principles regarding the evaluation of phases of "crime scene investigation" and seizure of data in order to determinate the "fingerprints" of the crime. Finally, the purpose of this paper is to illustrate the "handling" of digital evidence in Macedonia and to give recommendations for a better compliance with the international instruments regarding this issue.

Using personal computers as their weapons, hackers have attacked the Internet, government agencies, financial companies, small businesses, credit card accounts of individuals and etc.[1] With the rapid advancements in computer technology over the past few years, there has been increasing concern for the need to develop the law in order to take full advantage of technological improvements, and also to ensure that states can respond to computer crime and related criminal law issues.[2] Unlike other forms of real evidence, digital evidence can be created almost instantaneously with a few rapid keystrokes or with no immediate human input.

Digital evidence provides unique information that may not otherwise be available in concrete form or from other sources. If we compare a print-out of an electronic version of a document with a hand-developed hard copy of the same record we can see that the hard copy will provide information not only about the content but other visible information, such as handwritten notations. The electronic version, on the other hand, will provide the same content information generated by a computer as well as more information, including metadata (but not the handwriting). The electronic version captures many details that may otherwise be unavailable. Illustratively, the metadata may indicate the title and the name of the author, the date it was created and last saved, the date of the last printed version, changes that were made, and more. Other electronic evidence may reveal activity on the computer before and

[1] John R. Vacca (2005): Computer Forensics: Computer Crime Scene Investigation, Volume 1, Cengage Learning, p.7;
[2] Commonwealth Secretariat (2001): Law in Cyber Space, Commonwealth Secretariat, p.1;

after the key electronic document was drafted or sent. In many regards, the metadata provide insight and detail not only about the contents but also about what was transpiring at and around the time that the document was created.[3]

General Definitions relating to digital evidence

Defining digital evidence is not easy or simple. At first, there was no consensus of either these evidence being "digital" or "electronic" or even "computer" evidence. The last term is used in restrictive manner when one refers only to evidence involving a computer. The terms "digital" and "electronic" are more extensive and refer to all of the digital or electronic devices that are used to commit a crime. In times past, computer evidence meant a regular print out from a computer. Computer evidence today means data from storage media such as hard drives and floppy disks, captures of data transmitted over communications links, emails and log files generated by operating systems. What was formerly called computer evidence is now called digital evidence, including new classes of evidence drawn from a plethora of digital devices which do not fit the conventional concept of a computer (PDAs, mobile phones, engine management systems in cars etc.).[4] Consequently we can conclude that the term digital evidence is a moving target due to the continual emergence of new digital technologies.

One of the definitions of digital evidence is an interpretation of data, either inert (when found on a hard drive) or in motion (network communications) or a combination of the two. But there are also other generally accepted definitions that have been given by leading organizations and authors and serve to outline the theory. These are presented below:[5]

SWGDE[6] defines **digital evidence** as information of probative value that is stored or transmitted in binary form;

IOCE defines **digital evidence** as information stored or transmitted in binary form that may be relied upon in court**. Original Digital Evidence** are physical items and those data

---

[3] Mark L. Krotoski (2011): Effectively Using Electronic Evidence Before and at Trial, Obtaining and Admitting Electronic Evidence, United States Department of Justice Executive Office for United States Attorneys Washington, DC 20530, Volume 59, Number 6, p.52;

[4] Olga Koshevaliska, Lazar Nanev: Digital forensics and digital evidence in Macedonian criminal procedure, First scientific conference: the Influence of the technological development on law, economy, culture, education and security in Republic of Macedonia, EuroBalkan University, Skopje, 2013,

[5] Bradley Schatz (2007): Digital Evidence: Representation & assurance, Information Security Institute, faculty of Information Technologies, Queensland University of Technologies, Austria, p.13;

[6] The Scientific Working Group on Digital Evidence (SWGDE) forms the U.S. based component of the IOCE. It is a USA organization composed of law enforcement agency members created in February 1998 as a collaborative effort of the Federal Crime Laboratory Directors and is a joint effort of the U.S. Secret Service (USSS) and the Federal Bureau of Investigation (FBI). Its committees include: an Audio Committee, a By-Laws Committee, a Forensics Committee, a Membership Committee, an Outreach Committee, a Research Committee, a Standards and Accreditation Committee, and a Training Committee.

objects, which are associated with those items at the time of seizure. **Duplicate Digital Evidence** is an accurate digital reproduction of all data objects contained on the original physical item. **A copy** is an accurate reproduction of information contained in the data objects independent of the original physical item.

The UK Association of Police Chief Officers of England, Wales and North Ireland defines Computer Based Electronic Evidence as: *information and data of an investigative value that is stored on or transmitted by a computer (ACPO).*[7]

A *digital Crime Scene* is the data contained in the digital device, such as a hard drive or an mp3 player, found at a physical crime scene. The use of the term "digital crime evidence" acknowledges that the mere presence of data at the physical crime scene (by way of being stored in a digital device) does not make it evidence.[8]

Finally, according to the international definition in the field of forensic science, digital evidence is any information in digital form, which has probative value and can be adapted as reliable evidence in court. Hence, digital evidence is any information generated, processed, stored or transmitted in digital form that can be accepted by the court as authoritative evidence as well as other possible copies of the original digital information that have a probative value that the court can rely.[9]

In the Macedonian Criminal Procedure Code (the old one and the new one) there are no definitions for digital evidence. In the Macedonian Criminal Code there is only a definition on computer data.[10] The old CCP[11] has no provisions for the use of digital evidence in the criminal procedure,[12] and the new CCP[13] has only one provision that establishes the use of digital evidence in criminal procedures, but has no other provisions that refer to this matter. This issue will be discussed below.

Potential sources of evidence

It is beyond the scope of this paper to provide an extensive list of all the potential sources of evidence and their importance in criminal procedure. But aiming to illustrate

[7] The usage of the terms "digital evidence" and "computer based electronic evidence" under this law are sinonymous.
[8] Bradley Schatz (2007): Digital Evidence: Representation & assurance, Information Security Institute, faculty of Information Technologies, Queensland University of Technologies, Austria, p.17;
[9] Николоска, С.: Методика на истражување на компјутерскиот криминал, http://www.fb.uklo.edu.mk/aktivnosti.Nikoloska.aspx последен пристап 0.03.2013 година;
[10] In Art. 122 ph.27 from the Criminal Code of Macedonia computer data are defined as follows: computer data means presenting fact, informations or concepts in a form suitable for processing by a computer system, including a program suitable for making the computer system operational.
[11] Criminal Procedure Code, Official Gazette no. 15/1997; 44/2002; 74/2004; 83/2008; 67/2009 и 51/2011, hereinafter former and current LPC;
[12] Even though they are often used by applying the provisions of general evidence;
[13] Criminal Procedure Code, Official Gazette no. 150 from 18.11.2010;

potential sources of digital evidence we will give an elaborated preview of the potential evidence in the USA legislation. A part of the sources listed below are typical existing records and logs, which can become evidence if the competent authority knows how to turn them into admissible evidence in the USA.[14]

Main transaction records. *These include all purchases, sales and other contractual arrangements.*

Main business records. *These include all of the above, but also all documents and data that are likely to be necessary to comply with legal and regulatory requirements.*

Email traffic*. Emails potentially provide important evidence of formal and informal contacts.*

Records held by third parties. *For example a cloud computing provider where records may not be under its immediate direct control. On what basis can those records be seized? Cloud computing*[15] *is a very problematic because of the providing data from third party.*

Selected individual personal computers (PCs). *If individuals are under any form of suspicion, the authorities will need to be able to seize their PCs and make a proper forensic "image", which produces a precise snapshot of everything on the hard disks (this includes deleted material which technicians may be able to recover).*

Selected mobile phones / smart phones tablets/PDAs etc. *These devices can hold substantial amounts of data. Technical methods for preserving and investigating them are more complex than those for PCs;*

Selected data media. *Most computer users archive all or part of their activities on external storage media. These include CDRoms, Digital Versatile Discs (DVDs), floppy disks, tape, external hard disks, memory cards and Universal Serial Bus (USB) thumbdrives. There needs to be a routine for identifying all of these and securing them, pending examination.*

Access control logs. *All but the simplest of computer systems require a password or authenticating device before allowing admission. Usually, these access control systems can be configured to maintain records of when usernames and passwords were issued, when*

---

[14] *Peter Sommer* , (2012): Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers, The Information Assurance Advisory Council (IAAC), Third Edition, p. 25-27;

[15] For more on cloud computing see: Josiah Dykstra, Damien Riehl (2013): Forensic collection of electronic evidence from infrastructure-as-a-service cloud computing, Richmond Journal of Law & Technology, Volume XIX, Issue 1 p.6. Also It is important to distinguish between cloud services and cloud computing. For instance Facebook and Gmail are remote cloud services, but they are not cloud computing;

passwords were changed, when access rights were changed and/or terminated. In addition, many systems also maintain logs of accesses or, at the least, of failed accesses. These logs, properly managed and preserved, are powerful evidence of tracking activity on a computer system.

Configuration, event, error and other internal files and logs. *All computers contain files which help to define how the operating system and various individual programs are supposed to work. In the current generation of Windows systems, the most important set of configuration information is the registry. From this, forensic technicians can discover a great deal about recent and past activity, including recently accessed files and passwords. Often, there are important configuration files associated with individual programs. Many operating systems also generate error and other internal logs.*

Internet activity logs*. Individual PCs maintain records of recent web access in the form of the history file and the cache held in the temporary internet files folder. But many corporate networks also maintain centralised logs, if only to test the quality of service and check against abuse. When properly managed and preserved, these logs are powerful evidence of activity on a computer system.*

Anti-virus logs. *Related to the above mentioned logs are logs created by corporate installations of anti-virus software. These record the detecting and destruction of viruses and "trojans". A common defence tactic is to suggest that suspicious behaviour has been caused by a rogue program; anti-virus logs often contribute to resolving such claims.*

Intrusion detection logs*. Larger computer systems often use intrusion detection systems as part of their security measures. They are intended to detect and prevent several forms of hacking. Producing such logs may help to identify perpetrators, or demonstrate that reasonable precautions have been taken to secure the system.*

Back-up media. *All computer systems need to have back-up procedures, if only to enable rapid recovery after a disaster. Some organisations back up their entire systems every 24 hours; others have in place a partial, incremental policy. Back-up archives are extremely important sources of evidence, as they can show if "live" files have been tampered with. They can also provide data which has been deleted from the "live" system.*

Telephone logs. *Private Branch Exchanges (PABXs) usually have extensive features for recording usage activity. There may be difficulty in using these in evidence; there are also significant problems associated with intercepting the content of conversations. However, these are potentially very important sources of intelligence and evidence.*

Telephone Recordings*. Data provided from interception of telecommunications. .*

***Physical security access control logs**. Many buildings control physical access by the use of swipe cards or other tokens. There may be additional facilities to deal with parking or to give access to particularly sensitive areas. There is usually a central control system which generates logs. This can be extremely useful in pinpointing individuals' movements.*

***CCTV recordings.** Until recently cctv material was stored on tapes in analogue format. But the cost of digital storage – to fast hard-disk – has plummeted. Digital storage means that cctv images can be rapidly identified by date and time of incident. In addition motion detection and other analytic software can be deployed. At the same time the cost of cameras has collapsed as well, so that many more locations can be made the subject of surveillance.*[16]

Digital evidence and IOCE standards

As we previously stated, the Internet has removed the national borders of a crime scene. As a result of this, in the 1990s a global collaboration was created. This collaboration includes the International Organization on Computer Evidence and the Scientific Working Group on Digital Evidence.[17] The International Organization on Computer Evidence (IOCE)[18] is an international organization created in 1992, which by 2006 evolved into an "organization of organizations" that works with regional law enforcement organizations and government agencies already in existence.[19] In addition, it promotes the proliferation of regional IOCE components in areas that are lacking such an organization. Its mission is to provide an international forum for the exchange of both computer and digital forensic investigation information.

Its main goal is to provide a framework of standards, quality principles and approaches for the detection, preservation, recovery, examination and use of digital evidence for forensic purposes in compliance with the requirements of an accrediting body and or an organization widely recognized in the digital forensic community.[20]

---

[16] Peter Sommer , (2012): Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers, The Information Assurance Advisory Council (IAAC), Third Edition, p.40;

[17] ForensicScience.org,, official expert Anthony Falsetti, http://www.forensicscience.org/resources/digital-evidence/ last access 18.09.2013

[18] Official web site: http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html last acces 17.10.2013;

[19] In March 1998, IOCE was appointed to develop international principles for the procedures relating to digital evidence, to ensure the harmonization of methods and practices among nations and guarantee the ability to use digital evidence collected by one state in the courts of another state. In March 2000, the first report of IOCE was presented to the subgroup, proposing a series of definitions and principles, following the International high-tech crimes and forensics conference in London in October 1999;

[20] Guidelines for Best Practice in the Forensic Examination of Digital Technology;

International Standard ISO/IEC 27037 - Information technology, Security techniques, Guidelines for identification, collection, acquisition, and preservation of digital evidence

The IEC (International Electro-technical Commission), the world's leading standards body in electro technology, and ISO (International Organization for Standardization), through the Joint Technical Committee JTC 1 Information Technology, have released an International Standard - *ISO/IEC 27037* - Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence. The main purpose of this ISO standard is to ensure the reliability and credibility of digital evidence when they are used in court cases and legal disputes.[21]

Digital evidence is inherently fragile, as it may be easily altered, tampered with or destroyed through improper handling or examination. Decision-makers can rely on the standard to determine the credibility of digital evidence. It can also be used by organizations involved in protecting, analyzing and presenting digital evidence, as well as policy-making bodies creating and evaluating related procedures. The standard does not replace specific legal requirements of any jurisdiction.

ISO/IEC 27037 provides a harmonized and globally accepted methodology to safeguard its integrity and authenticity. Also it aims to facilitate the exchange of digital evidence between jurisdictions by making sure that requirements and procedures are consistent. This recognizes that crime, and in particular cybercrime, increasingly takes place across borders.

This International Standard intends to provide guidance to those individuals responsible for the identification, collection, acquisition and preservation of potential digital evidence. These individuals include Digital Evidence First Responders (DEFRs), Digital Evidence Specialists (DESs), incident response specialists and forensic laboratory managers. This International Standard ensures that responsible individuals manage potential digital evidence in applied ways that are acceptable worldwide, with the objective to facilitate investigation involving digital devices and digital evidence in a systematic and impartial manner while preserving its integrity and authenticity.

This ISO Standard gives guidance for the following devices and/or functions that are used in various circumstances:

[21] All ISO standards that in any part refer to digital evidence are elaborated in David Watson, Andrew Jones (2013): Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements, Newnes;

- 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.[22]

The application of this International Standard requires compliance with national laws, rules and regulations. Also this standard may assist in the facilitation of potential digital evidence exchange between jurisdictions. In order to maintain the integrity of the digital evidence, users of this International Standard are required to adapt and amend the procedures described in this International Standard in accordance with the specific jurisdiction's legal requirements for evidence.

There are also other ISO standards that need to be taken in consideration during the process of "digital investigation". Hence, before the incident takes place, the following standards should be applied: ISO/IEC 27035 Part I – Incident management, operation and response; ISO/IEC 27043 Investigation principles and process and ISO/IEC 30121 Governance of Digital Forensics. During the incident, the following standards should be applied: ISO/IEC 27035 Information security incident management (existing versions as well as all parts of the proposed multi part version), ISO/IEC 27041 Guidance on assuring suitability and adequacy of the investigation methods; ISO/IEC 27043 Investigation principles and processes. And finally, Post Incident: ISO/IEC General criteria for the operation of the various types of bodies performing the inspection; ISO/IEC 17025 General requirements for the competence of testing and collaboration laboratories; ISO/IEC 27035 Information security incident management (existing versions as well as all parts of the proposed multi part version); ISO/IEC 27037 Guidelines for the identification, collection, acquisition and preservation of digital evidence; ISO/IEC 27042 Guidelines for the analysis

[22] ISO/IEC 27037 prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques, Reference number ISO/IEC 27037:2012(E);

and interpretation of digital evidence; ISO?IEC 27043 Investigation principles and processes.[23]

Principles concerning evaluation of digital evidence

The principles by which digital evidence is *evaluated*, accepted into legal proceedings, and ascribed weight vary widely from jurisdiction to jurisdiction. Countries with a common law background, which includes the UK, Australia and USA, share a number of common principles. In 1998, Sommer described the following basic principles for evaluating the acceptability of the new types of evidence not previously considered by courts:[24]

- **Authentic** – the evidence should be: "specifically linked to the circumstances and persons alleged, and produced by someone who can answer questions about them.[25] Unless a party shows that the evidence is what that party claims it to be, the court will view the evidence as irrelevant.[26]
- **Accurate** – the evidence should be "free from any reasonable doubt about the quality of procedures used to collect the material, analyze the material if that is appropriate and necessary and finally to introduce it into court – and produced by someone who can explain what has been done.
- **Complete** – the evidence should be able to tell, within its terms, a complete story of (a) particular set of circumstances or events".

Principles for the procedures relating to digital evidence

To help create cooperation between the USA and other nations, the G8 Group[27]of major industrialized nations has proposed six principles for procedures relating to digital evidence:[28]

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.

---

[23] Chang-Tsun Li (ed.) (2013): Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security, Idea Group Inc (IGI), p.240;
[24] Bradley Schatz (2007): Digital Evidence: Representation & assurance, Information Security Institute, faculty of Information Technologies, Queensland University of Technologies, Austria, p.3;
[25] For this see: Leah Voigt Romano (2005): VI. Electronic Evidence and the Federal Rules, 38 Loy. L.A. L. Rev. 1745, Loyola Marymount University and Loyola Law School Digital Commons at Loyola Marymount University and Loyola Law School
[26] See Genci Fejzula and Jonuz Mazreku vs. Macedonia, Appeal No.23065/07 Council of Europa, Court of Human Rights:
[27] Official web site: www.g8online.org , last access 05.10.2013;
[28] John R. Vacca (2005): Computer Forensics: Computer Crime Scene Investigation, Volume 1, Cengage Learning, p.673;

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 whilst the digital evidence is in their possession.

6) Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.[29]

This set of principles can act as a solid foundation. However, as one principle states if someone must touch the evidence they should be properly trained. Training helps reduce the likelihood of unintended alternation of evidence. It also increases one's credibility in a court of law if called to testify about actions taken before the arrival and/or involvement of the police.[30]

Many of these principles are similar to the *Good Practice Guide* of the UK's Association of Chief Police Officers (ACPO).

Principle 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.

Principle 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.

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

Principle 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.

Computer-based electronic evidence is no different from text contained within a document. For this reason, the evidence is subject to the same rules and laws that apply to documentary evidence. The doctrine of documentary evidence may be explained thus: the onus is on the prosecution to show to the court that the evidence produced is no more and no

[29] G8 Proposed Principles For The Procedures Relating To Digital Evidence

[30] Xuejia Lai, Dawu Gu, Bo Jin, Yongquan Wang, Hui Li (2010): Forensics in Telecommunications, Information and Multimedia: Third International ICST Conference, E-Forensics 2010, Shanghai, China, Revised Selected Papers, Springer, p.227;

less now than when it was first taken into the possession of the police. Operating systems and other programs frequently alter and add to the contents of electronic storage. This may happen automatically without the user necessarily being aware that the data has been changed. In order to comply with the principles of computer-based electronic evidence, wherever practicable, an image should be made of the entire target device. Partial or selective file copying may be considered as an alternative in certain circumstances e.g. when the amount of data to be imaged makes this impracticable.[31]

Phases of the Digital Forensic Investigation

One of the main issues relating digital evidence refers to the procedure for its collection, assessment and presentation before the court.

An opposed to the ambiguous or indefinite legislation of Macedonia, the comparative legal systems have very precise procedure concerning digital evidence. For instance the US National Institute of Justice (NIJ), in their "Electronic Crime Scene Investigation: A Guide for first Responders"[32] describe a four phase process, consisting of the following four phases:

1. Collection: "search for, recognition of, collection of and documentation of electronic evidence".
2. Examination: "make evidence visible and explain its origin and significance … search for information … data reduction"
3. Analysis: "looks at the product of the examination for its significance and probative value to the case. Examination is a technical review that is the province of the forensic practitioner, while analysis is performed by the investigative team."
4. Reporting: "outlines the examination process and the pertinent data recovered".

The first phase was modified in 2004 and today is a phase with two sub phases – assessment and acquisition.

Digital evidence – case of Macedonia

Given the fact that in many cases the courts decisions are based, partly or entirely, on digital evidence, the procedure for the handling digital evidence should be regulated so as to make the procedure flawless. The transformation of digital data (which consists of a sequence of coded bytes) into a judicial evidence is an abstract process. Because of this we

[31] Peter Sommer, p.42

[32] U.S. Department of Justice Office of Justice Programs: (2001) Electronic Crime Scene Investigation: A Guide for First Responders, written and Approved by the Technical Working Group for Electronic Crime Scene Investigation, Washington, USA,

think that there must be a strong legal framework (which is absent in Macedonia) that will define the procedure for collection and storage of digital evidence and the procedure of forensic acquisition[33] and analysis of digital evidence.[34]

We are of the opinion that the CPC must be amendment in the part regarding the use of electronical evidence in Macedonian criminal procedure by implementing a definition. The definition that we recommend is the international accepted definition from IOCE:

''Electronical evidence is information stored or transmitted in binary form that may be relied upon in court ''.

Our criminal law gives no rules for the right and just way of preserving this evidence. In our new CPC there are general provisions that in cases of digital evidence, the general rules for preserving evidence will be applied?[35] These evidences will be presented by their reproduction.

The competent authority for the identification, presentation, collection, examination, analysis and presentation of evidence of digital nature is the Department for Criminalistics Techniques under the Ministry for Internal Affairs. But neither the Criminal Procedure Code, the Code for Internal Affairs nor the Code for police, nor any other legal source gives any provisions for the processing of digital evidence by this body. We only know for certain that the processing of these data is within the special unit of the Department for Criminalistics Techniques liable for the technical investigation of photo, video, audio and digital data. Also there is no available Rulebook or any other legal act for the procedure of processing the digital evidence, the security of the same or any other issues regarding these kind of evidence (for example the educational background of the persons that deal with these most sensitive evidences).[36]

In the absence of the competent legislation, we can only wonder what happens with the seized digital evidence after its collection. Can it be changed and modified in a manner to be compatible with the allegations of the prosecution. Can it be guaranteed that nothing will be changed and, in case of changes, will the defense have the opportunity to challenge this evidence? Who will guarantee that the digital evidence will not be compromised?

Also of great importance is the validation of the evidence. Therefore only properly evaluated tools, techniques and procedures should be used for the forensic examination of

[33] The term acquisition means detection, extraction and proving of digital evidence in proceedings;
[34] Risto Hristov, Atanas Kozarev (2011): Digital evidence - Annual Review, Year II, No. 3, European University, Republic of Macedonia, Skopje, p.873 – 891;
[35] Article 251 from Criminal Procedure Code, Official Gazette no.150 from 18.11.2010;
[36] If there are such rules and provisions, then they should be available to the wider public, according with the Code of Free Access to Public Information;

digital technology and the interpretation of their evidential significance in the context of the case. In this manner, the validation process in the USA requires as a minimum the following: that there is a minimum acceptable criteria for the technique or procedure; that the critical aspects of the examination procedure and tools have been identified and the limitations defined wherever possible; that the methods, materials and equipment used have been demonstrated to be fit for its purpose; that there are appropriate quality control and quality assurance procedures in place for monitoring performance; that the technique or procedure is documented; and that the results obtained are reliable and reproducible. Our opinion is that these requirements regarding the validation should be implemented into the Macedonian law as well.

The old and current CPC in article 142 b ph.2 provides a special investigative measure for insight and search in the computer system, removal of the computer system or a part of the computer system or the base for storage of computer data. In the new CPC this measure becomes **secret** insight and search in a computer system.[37] The provisions for these old / new measures are illicitly to general so authorities can abuse its broadnes and use them in a maner that is corensponding to their needs. What authority, precisely, has guided and will guide this process and who will guarantee that the evidence will not be changed, destroyed or hidden? The Law provides that the police will be liable for the conduct of these measures but what about the real educational background on the "expert" that is liable for the acquisition. For instance, appropriate experts reduce the liklihood of unintended alternation of evidence. It also increases one's credibility in a court of law, if called to testify about actions taken before the arrival and/or involvement of the police.[38]

We think that there have to be special provisions for this matter. Another issue is the term **secret insight.** What does *secret* really means. That the authorities will complete the insight from a distance, or when the owner of the computer is not at the desk? Where is the justice in this special investigative measure? If the authorities can control the computer system from a distance and without the knowledge of the owner / suspect then it will be very easy for the authorities to plant whatever they want to prove. Evidence, provided with these special investigative measures, will be challenged before the court and they will have to be rated as inadmissible.

[37] Article 252 ph.4 new CCP;
[38] Xuejia Lai, Dawu Gu, Bo Jin, Yongquan Wang, Hui Li (2010): Forensics in Telecommunications, Information and Multimedia: Third International ICST Conference, E-Forensics 2010, Shanghai, China, Revised Selected Papers, Springer, p.227;

The terms of the new CPC regarding the preservation of persons and evidences, contain special provisions referring to the search in computer systems and computer data (art.184) and temporary seizure of computer data (art.198). Hence, article 184 p. 1 provides that the person that is using or has access to a computer or another device or data carrier, is obliged to provide access to these devices at the request of the executor of the order. We again ask: who is this executor?[39] Also the person that is using the computer is obliged to take measures to prevent the destruction or alternation of data. If this person is in any way involved in the computer crime, how can be the police make sure that the person will not take measures to change the computer data while he is taking measures in accordance with art.184 ph.2? We think that in these cases the authorities should seek a solution by quarantine of the evidence.[40] The first responder has to establish a quarantine around the suspect equipment, moving everyone away from it to ensure that no one has the opportunity to tamper with it. This removes the potential for any accusations of evidence being "planted" or for the user/owner to attempt to damage any evidence of which they are aware.

Therefore the CPC has to have answers to the following questions: How will the evidence be acquired, physically and practically? How will the evidence be preserved, and how will continuity be demonstrated? Are there any legal obstacles, such as data protection, human rights legislation or compliance with the Law for interception etc.? Will the material be admissible? Our opinion is for such delicate matters there must be strict provisions. This is because digital evidence can be easy to manipulate. Also there have to be special provisions that will guarantee the access to digital evidence to the defense for adequate preparation of the defense.

But the lack of provisions does not apply in cases of financial crime. When the Financial Police are in charge the Financial Police of the crime, then, according to the Code for Financial Police,[41] there is a special procedure for the identification, presentation, collection, examination, analysis and presentation of evidence in digital form. Hence, according to article 7 p.9 of the Law for Financial Police, the Financial Police have the authority to perform expert computer analysis of seized items, computer information or data of any other electronical and mechanical devices that contain information that can be used as

[39] In article 181 ph.2 it is provided only that for the search on a computer device there must be a written and reasoned order at the request of the public prosecutor or in cases of emergency at the request of the Judicial Police.

[40] For more on quarantine see in: Angus M. Marshall, (2008): Digital Forensics, Digital Evidence in Criminal Investigation, University of Teesside, UK, JohnWiley & Sons, Ltd, London, p.22 - 25;

[41] Article 7 from the Code for Financial Police, Official Gazette No.55/2007;

evidence in the conduct of the preliminary investigation or misdemeanor proceedings that are under its jurisdiction.

Conclusion

The purpose of this paper was to give a brief overview of the general definitions on digital evidence in the comparative jurisdictions, in order to identify the possible sources of digital evidence and to elaborate the basic principles relating the acquisition and evaluation of these evidence in order to show their treatment in the Macedonian criminal legislation. Because of all the flaws in our code of criminal procedure when it comes to digital evidence, we are of the opinion that our Code for Criminal procedure must be amendment with definition on what is digital evidence and to give a precise procedure for the collection, handling, storage and presenting these evidences on the evidentiary hearing before court. The definition that we recommend is the international accepted definition from IOCE:

‘’Electronical evidence is information stored or transmitted in binary form that may be relied upon in court ‘’.

We also believe that it is necessary to implement the specific principles that address the evaluation of digital evidence in judicial proceedings. Finally, we emphasize the need, once more, of a clear procedure for collection, handling and storage of these evidences. Also we emphasize the urgent need of the implementation of the IOCE and ISO standards regarding the digital evidence in order to be able for successful international mutual legal assistance in criminal matters.

Bibliography

A Road Map for Digital Forensic Research, Report from the First Digital Forensic Research Workshop (DFRWS), August 7-8, 2001, Utica, New York;

Ali Obaid Sultan Alkaabi (2010): Combating Computer Crime: an international prespective, Doctoral Thesis on Information Security Institute, Faculty of Science and Technology, Queensland University of Technology;

Angus M. Marshall, (2008): Digital Forensics, Digital Evidence in Criminal Investigation, University of Teesside, UK, JohnWiley & Sons, Ltd, London, p.22 - 25;

Bradley Schatz (2007): Digital Evidence: Representation & assurance, Information Security Institute, faculty of Information Technologies, Queensland University of Technologies, Austria, p.13;

Chang-Tsun Li (ed.) (2013): Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security, Idea Group Inc (IGI), p.240;

Colin Evans, Criminal justice: Evidence, 2010 by Infobase Publishing, New York, p. 17 -28

Commonwealth Secretariat (2001): Law in Cyber Space, Commonwealth Secretariat, p.1;

David Watson, Andrew Jones (2013): Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements, Newnes;

ForensicScience.org,, official expert Anthony Falsetti, http://www.forensicscience.org/resources/digital-evidence/ last access 18.09.2013

Genci Fejzula and Jonuz Mazreku vs. Macedonia, Appeal No.23065/07 Council of Europa, Court of Human Rights:

IOCE Princips & Definitions, IOCE 2. Conference, Marriott Hotel, London;

ISO/IEC 27037 prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques, Reference number ISO/IEC 27037:2012(E);

John Jackson, Máximo Langer, Peter Tillers (ed.) (2008): Crime, Procedure and Evidence in a Comparative and International Context - Essays in Honour of Professor Mirjan Damaška, Hart Publishing, Oxford and Portland Oregon;

John R. Vacca (2005): Computer Forensics: Computer Crime Scene Investigation, Volume 1, Cengage Learning, p.7 and 673;

Josiah Dykstra, Damien Riehl (2013): Forensic collection of electronic evidence from infrastructure-as-a-service cloud computing, Richmond Journal of Law & Technology, Volume XIX, Issue 1;

Code for Financial Police, Official Gazette No.55/2007; United States v. Bennett, 363 F.3d 947 (9th Cir. 2004) (reviewing the admissibility of a customs officer's testimony about global positioning satellite data);

Criminal Procedure Code, Official Gazette no. 15/1997; 44/2002; 74/2004; 83/2008; 67/2009 и 51/2011, hereinafter former and current LPC;

Criminal Procedure Code, Official Gazette no. 150 from 18.11.2010;

Leah Voigt Romano (2005): VI. Electronic Evidence and the Federal Rules, 38 Loy. L.A. L. Rev. 1745, Loyola Marymount University and Loyola Law School Digital Commons at Loyola Marymount University and Loyola Law School;

Mark L. Krotoski (2011): Effectively Using Electronic Evidence Before and at Trial, Obtaining and Admitting Electronic Evidence, United States Department of Justice Executive Office for United States Attorneys Washington, DC 20530, Volume 59, Number 6, p.52;

Nikola Matovski, Gordana Buzarovska Lazetik, Gordan Kalajdziev: Criminal Procedure Law, second and amendment issue, Academik Skopje, p.438;

Official web site: http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html last acces 17.10.2013;

Peter Mell & Tim Grance, The NIST Definition of Cloud Computing, NAT'L INST. OF STANDARDS & TECH., 2 (Sept. 2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf last access 18.10.2013;

Peter Sommer , (2012): Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers, The Information Assurance Advisory Council (IAAC), Third Edition;

Računalna forenzika NCERT-PUBDOC-2010-05-301, Nacionalno središte za sigurnost računalnih mreža i sustava, Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Risto Hristov, Atanas Kozarev (2011): Digital evidence - Annual Review, Year II, No. 3, European University, Republic of Macedonia, Skopje, p.873 – 891;

Terrence F. Kiely (2001): Forensic evidence: science and the criminal law, CRC Press LLC, New York, p.140;

U.S. Department of Justice Office of Justice Programs: (2001) Electronic Crime Scene Investigation: A Guide for First Responders, written and Approved by the Technical Working Group for Electronic Crime Scene Investigation, Washington, USA;

Xuejia Lai, Dawu Gu, Bo Jin, Yongquan Wang, Hui Li (2010): Forensics in Telecommunications, Information and Multimedia: Third International ICST Conference, E-Forensics 2010, Shanghai, China, Revised Selected Papers, Springer, p.227;

Zakona o kaznenom postupku Hrvatska, »Narodne novine« br. 121/11, precisteni tekst;

Николоска, С.: Методика на истражување на компјутерскиот криминал, http://www.fb.uklo.edu.mk/aktivnosti.Nikoloska.aspx последен пристап 0.03.2013 година;