Chapter I

Introduction to digital forensics

SUMMARY: 1. Digital Evidence. – 2. Digital Forensics in the United States. – 3. Digital Forensics in Italy. – 4. The Amero case. – 5. The "Garlasco" case.

1. *Digital Evidence*

Amongst the myriad definitions proposed for digital evidence the world over, the most apt seem to have been forged by the International Organization on Computer Evidence (IOCE)[1] which views electronic evidence as "information generated, stored or transmitted using electronic devices that may be relied upon in court"[2] and the Scientific Working Group on Digital Evidence (SWGDE)[3] for which digital evidence is "information of probative value stored or transmitted in digital form"[4].

---

[1] The IOCE is an international organization set up in 1998 to serve as an international forum through which the law enforcement agencies of participating nations could exchange information and views on techniques for fighting cybercrime and digital forensics issues. The organization also draws up standardized guidelines on digital forensics with a view to harmonizing procedural rules amongst participant nations so that digital evidence acquired in one of them may be considered reliable and admissible at trial in another.

[2] Definition adopted by the IOCE in 2000.

[3] The SWGDE was established in 1998 as an international umbrella organization bringing together various bodies focusing on matters pertaining to digital evidence and the multimedia sector at national level in their respective countries, so as to promote cooperation and develop quality standards in respect of the acquisition, storage and analysis of electronic data to be proffered as evidence.

[4] As per the 1999 SWGDE document entitled *Digital Evidence: Standards and Principles*, available at: *http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/*.

According to Stephen Mason [5], even though it is commonplace for the terms "electronic evidence" and "digital evidence" to be used interchangeably, the latter is, in fact, merely a subset of the broader category of "electronic evidence" which, he posits, also includes evidence in the form of analog data, such as video and audio tape recordings, photographic film and tape-recorded intercepts of fixed-line phone conversations. Whilst all these types of data may well be "digitalized", they do not originate in digital form. Mason accordingly defines electronic evidence as "data (comprising the output of analogue evidence devices or data in digital format) that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the process of adjudication" [6].

Interestingly, a comparative study of the legal systems of 16 European countries [7], revealed that none of them were endowed with a settled definition of the electronic and/or digital evidence, although some were found to contain references to such a concept: under the Finnish code of civil procedure, hardcopies and data stored in digital format must be attributed equal evidentiary weight as "grounds in support of the action" [8].

The study also showed that under all the legal systems in question, digital documents, electronic signatures and e-mail were treated on the same footing at their more conventional counterparts.

The term "electronic document" is defined, for the intents and purposes of Italian law, in article 1(p) of Legislative Decree 82/05, also known as the "Digital Administration Code", as the "electronic representation of legally relevant deeds, events or data". Law 48/08 through which Italy ratified the Budapest Convention, did away with the regulatory dilemma arising from the fact that the definition just cited stood in

---

[5] A London-based barrister, Stephen Mason founded the Digital Evidence and Electronic Signature Law Review and sits on the IT Law committee of the Council of Bars and Law Societies of Europe.

[6] S. MASON, *Electronic Evidence. Discovery & Admissibility*, LexisNexis Butterworths, London, 2007, paragraph 2.03.

[7] The study covered the following countries: Austria, Belgium, Denmark, Finland, France, Germany, Greece, the Netherlands, Ireland, Italy, Luxembourg, Portugal, Romania, Spain, Sweden and the UK. See, further, F. INSA, *The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime-Results of a European Study*, in *Journal of Digital Forensic Practice*, 2006, at page 285.

[8] Legal Proceedings Code of Finland, Chapter 17, Section 11b.

competition with a different conception of "electronic document" entrenched in article 491-*bis* of the Italian Penal Code, under which the term denotes any electronic medium containing data or information of evidentiary value or otherwise, software specifically designed to process such data or information [9].

This latter notion placed particular emphasis on the material nature of the electronic medium containing the probative information or data. At present, therefore, an electronic document may be defined as any file featuring content expressed in binary code: text, images, sounds, through to e-mail and entire web pages.

Paolo Tonini has compellingly shown that a factual narrative remains substantially unchanged whether it is recorded in a written document or in form of digital data stored on electronic media. All that changes is the material means through which the facts are recorded. A hardcopy of an electronic text file is identical in all respects to a "conventional" written document setting forth the content of the digital file. The main difference between "conventional" and electronic documents accordingly lies only in the material means through which their respective content is recorded, and not in the way in which the said content is represented. Tonini argues that the means through which facts are recorded may be divided into two broad categories: analog and digital. An analog representation is "material" in nature inasmuch as it cannot exist without the physical medium on which it is recorded. A written document, for instance, is bound to leave a visible trace of any subsequent changes that may be brought to it. Digital documents, on the other hand, record factual representations on a "material medium in the form of variable physical values", i.e. a sequence of bits. As a result, digital representations are not material in nature since they exist regardless of the type of the physical support medium on which they are stored [10].

From a common-law standpoint, the American digital forensics inves-

---

[9] Article 491-*bis* of the Italian Penal Code, as amended by Law no. 48/08, currently provides: "If any of the falsities contemplated in this paragraph affect a public or private digital deed endowed with probative value, the provisions of this paragraph pertaining to public and private deeds respectively, shall apply".

[10] P. TONINI, *Nuovi profili processuali del documento informatico*, in *Scienza e processo penale: linee guida per l'acquisizione della prova scientifica*, compiled by L. De Cataldo Neuburger, 2010, Padua, Cedam, at page 427.

tigator Eoghan Casey[11], has defined digital evidence as 'any data stored or transmitted using a computer that support or refuse a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi'[12], whilst in the UK, Stephen Mason[13] has attempted to classify digital evidence into three distinct categories:

– User-generated digital evidence, and that is to say, any and all digital data that are the result of human action or intervention. This category of evidence may be further subdivided into two classes, in function of the type of action through which the resulting digital data were generated: *human-to-human*, as in the case of e-mail correspondence which implies interaction between at least two human beings, and *human-to-machine*, as in the case of document drawn up using a word processor. From an evidentiary standpoint, this category of evidence may be ruled admissible only subject to a showing that the digital data in question were not altered, and are reliable in all respects.

– Computer-generated digital evidence: any and all output of software programs, generated in accordance with specific algorithms and without human intervention (such as data recorded through electronic intercepts or by accessing server logs). For probative purposes, data of this sort may only be admitted subject to a showing that the software that generated the output functioned properly as well as, obviously, that the output data were not subsequently altered.

– Digital evidence generated by both computers and users: any and all data resulting from human input and electronic processing, subsequently stored in an electronic memory system (as in the case of a spreadsheet containing the results of electronic calculations carried out on figures manually input by the user). Digital evidence falling within this category is only admissible at trial, subject to a showing of not only the authenticity and genuineness of the data input by the human user but also the proper functioning of the electronic data processing system.

---

[11] Eoghan Casey holds a Bachelor's Degree in Mechanical Engineering from the University of California, Berkeley, and a Master's in "Educational Communication and Technology" through New York University, and currently serves as editor-in-chief of the journal "International Journal of Digital Forensics and Incident Response".

[12] E. CASEY, *Digital Evidence and Computer Crime*, 2004, Second edition, Elsevier, at page 12.

[13] S. MASON, *supra note 6 at* paragraph 2.03.

Given the rapid pace of development of digital forensics as a discipline in itself, since Collier and Spaul first raised the issue of the acquisition of digital evidence, almost 20 years ago in 1992[14], the need for a well-defined legal framework regulating the field, has become ever more pressing, and all the more so as technological advances whilst opening the door to increasingly sophisticated electronic interception capabilities, also generated highly innovative hardware and software for converting digital documents, and not just into bits.

2. *Digital Forensics in the United States*

Until recently, it was commonplace for authoritative commentators to refer to the field as "computer forensics", a term coined in 1984 when the FBI drew up the Magnetic Media Program, that subsequently led to the setting up of Computer Analysis and Response Teams (CART)[15].

Almost thirty years later, Ken Zatyko, adjunct professor with Johns Hopkins University, was amongst the first to prefer the term "digital forensics" over "computer forensics"[16].

Zatyko's terminology seems more appropriate since the main source of the electronic data subjected to forensic examination, is bound to shift from personal computers, per se, to other devices (smartphones, mp3 readers, playstations, sat-nav terminals), as well as remote forms of data storage (such as "cloud computing"). Since latest generation cell phones, with their advanced functions and storage capabilities, could well prove a wealthier treasure trove of probative material than certain models of personal computers, the term "computer forensics" seems a bit reductive and dated.

Eugene Spafford[17], a digital forensics pioneer, and one of the first to

---

[14] P.A. COLLIER, B.J. SPAUL, *A Forensic Methodology for Countering Computer Crime*, in 32 *J. For. Sc.*, 1992, at page 27.

[15] CARTs (Computer Analysis and Response Teams) comprise forensic experts specializing in the retrieval, processing, conservation and presentation of digital evidence. For further information on CART teams, see: *http://www.fbi.gov/about-us/otd/capabilities* as well as the Handbook of Forensic Services, 2007, available at: *http://www.fbi.gov/about-us/lab/handbook-of-forensic-services-pdf/at_download/file.*

[16] K. ZATYKO, *Commentary: Defining digital forensics*, in Forensic Magazine, 2007, available at: *http://www.forensicmag.com/node/128.*

[17] B.D. CARRIER-E.H. SPAFFORD, *Categories of digital investigation analysis techniques based on the computer history model*, in *Digital Investigation*, 3, 2006, p. 121.

address this specific issue, proposed three distinct categories of electronic data analysis:

– *computer forensics* in the narrow sense (i.e. analysis of data stored on a specific PC);
– *network forensics* (analysis of data derived from computer networking);
– *intrusion forensics* (analysis of data obtained through hacking computer systems).

This threefold distinction, albeit perfectly defensible, is at risk of obsolescence in light of technological progress, since, as noted above, unless they are connected via an online network, individual computers increasingly appear to be rather poor sources of probative material useful to criminal prosecutions, with the result that computer forensics in itself might well prove quite useless without the "networking" component.

However, given that the term "computer forensics" has gained currency in certain scholarly circles to apply to the field as a whole, in this paper the terms "computer forensics" and "digital forensics" will be used interchangeably [18].

Having disposed of potential terminological misunderstandings, it would perhaps be useful to provide an overview of the various definitions of digital and/or computer forensics that have developed in recent years, both in Italy and the U.S.

According to the National Institute for Standards and Technology (NIST) four computer forensics involves four phases, i.e. the collection, examination, analysis, and presentation of digital evidence [19].

Collection consists in identifying, labelling, registering and securing digital data, in accordance with procedures designed to ensure the utmost data integrity.

Examination involves the assessment of digital data using electronic and manual techniques aimed at protecting the data against alteration during and after the process.

Analysis entails verifying the results obtained through data examina-

[18] It is interesting to note that in the U.S., identical digital forensic techniques are referred to as "e-discovery" in civil cases, and as "computer forensics" within the framework of criminal investigations.

[19] K. KENT-S. CHEVALIER-T. GRANCE-H. DANG, *Guide to integrating Forensic Techniques into Indente Response*, NIST publication, 2006, *http://csrc.nist.gov/publications/nistpubs/800 86/SP800-86.pdf*.

tion, with a view to obtaining answers to the queries to be resolved through the evidence derived through data collection and examination.

Lastly, the presentation of the results of data analysis encompasses describing the forensic tools and techniques used, as well as listing any further procedures to be carried out to complete the forensic analysis.

According to the well-known "technology dictionary" (whatis.com) hosted on the Techtarget website, "computer forensics, also called cyberforensics, is the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law"[20].

Along similar lines, under the definition proposed during the Sedona Conference[21], computer forensics "consists in the use of specialist techniques to recover, authenticate and study electronic data, in cases where it is necessary to reconstruct computer usage, examine deleted data and certify that digital data have not been altered. Computer forensics requires specific skills that go beyond the mere collection and conservation of the data by the end-user, and generally requires the utmost respect for the chain of custody"[22].

On the basis of the definition of digital forensics as "the application of computer science and investigative procedures for a legal purpose", Ken Zatyko concluded that the scientific process involved in validating digital evidence, could be broken down into eight distinct steps:

1. Search authority
2. Chain of custody
3. Imaging/hashing function
4. Validated tools
5. Analysis
6. Repeatability (Quality Assurance)

---

[20] Search Security is one of the many websites that focus of data security, but unlike most others, includes a very helpful technology dictionary: *http://whatis.techtarget.com/*. The definition cited is to be found under the entry "Computer forensics" at *http://searchsecurity.techtarget.com/definition/computer-forensics*.

[21] The Sedona Conference Institute organizes seminars and training programs conducted by judges, legal experts and technical consultants, on a quarterly basis on a broad range of legal issues including questions of computer forensics, antitrust and intellectual property law, with a view to providing insight into emerging trends and forecasting future developments in the various fields of study. One of the most recent training programs, held in January 2010, focused specifically on e-discovery (*http://www.thesedonaconference.org/conferences/20100128*).

[22] The chain of custody is discussed in greater detail in subsequent chapters of this paper.

7. Reporting
8. Possible expert presentation

The above data validation process clearly requires the involvement of a technical consultant well-versed in the dynamics of digital forensics, and is best conducted in synergy between legal experts and computer science specialists.

This need for multidisciplinary synergy and coordination has led Ralph C. Losey[23] to observe that the relationship between legal advisors and computer forensic experts in the context of validating and presenting digital evidence, is very similar to the roles of Scotty, the engineer, and Capt. Kirk and the rest of the team of the spaceship Enterprise in the Star Trek series: when the going really got rough, the other members of Star Trek crew relied heavily on Scotty to get them out of trouble (leading to the pop culture catchphrase "Beam me up, Scotty!"). To highlight the damage that could result from a lack of coordination between the legal advisors and computer experts Losey cites the San Francisco patent infringement case of Kevin Keithley v. The Home Store.com[24], in which the defendants wrote code for and developed various popular websites promoting the sale of real estate, including homestore.com, with the unsurprising result that most of their key digital data custodians were software programmers and computer engineers. The technical team's disrespect of the law, lawyers, and the discovery process, as a whole, was so obvious that the senior Federal Magistrate Judge examining their conduct, Elizabeth D. Laporte, commented that it was "among the most egregious this Court has seen", and went on to impose a penalty of $320,000 in addition to issuing a particularly scathing adverse inference instruction. She reportedly even considered granting the plaintiff's motion for summary judgment against the defendants but refrained from going that far, recognizing that the case involved miscommunications, disrespect, and negligence, rather than outright fraud.

Care must be taken, however, to avoid excessive reliance on digital evidence: as John Patzakis[25], general counsel for Guidance Software,

---

[23] R.C. LOSEY, *Introduction to e-Discovery*, 2009, ABA Publishing, at page 113.

[24] *Kevin Keithley v. The Home Store.com*, August 12, 2008, U.S. Dist. LEXIS 61741 available at: *http://kevintren.posterous.com/?tag=homestore*

[25] John Patzakis served for many years as general counsel for Guidance Software which developed Encase, the most widely used digital forensics software package worldwide: 80% of all digital forensic investigations carried out in 2008 were undertaken using the package.

quite rightly points out, analysing a forensic copy of a hard disk containing very large volumes of data with a view to recovering and examining all the files deleted from the original, without precise guidelines allowing for most of the data to be disregarded, would result to little more than a exceedingly tiresome and probably fruitless fishing expedition.

In other words, according to Patzakis, digital forensic techniques must be precisely targeted and well-focused, since the broader the scope of investigative procedures, the more difficult it becomes to glean useful digital evidence from the mass of the electronic data seized.

Moreover, in the field of civil law, in the U.S., the Federal Rules of Civil Procedure[26] were revised in 2006 with, inter alia, the introduction of rule 26(b)(2)(B)[27] which significantly limits recourse to invasive techniques for the discovery of inaccessible data[28] and specifically provides that "a party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. […] ... the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). [...]"[29].

---

[26] Federal Rules of Civil Procedure, first adopted in 1938 and repeatedly amended and extended over the years, codify the procedural rules to be followed by Federal (District) Courts throughout the U.S. in civil cases. Individual states are free to enact their own civil procedural rules – to be followed by their state courts – although most states have adopted procedural rules along the lines established by the Federal Rules of Civil Procedure.

[27] See further on Rule 26(b)(2)(B), G.B. MURR, *Federal Rule of Civil Procedure 26(b)(2)(B) and "Reasonable Accessibility": The Federal Courts' Experience in the Rule's First Year*, in *Privacy & Data Security Law Journal*, available at: *http://www.bmpllp.com/files/1202334716.pdf*.

[28] "Specific Limitations on Electronically Stored Information. A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery".

[29] Rule 26(b)(2)(C): "When Required. On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues".

One of the first cases in which the revised rule was applied (Ameriwood v. Lieberman[30], involved an employer who was authorised by a Federal District Court in Missouri to appoint a digital forensic expert to create a mirror image of the computer equipment of the defendant employees, having satisfied the court that there was "good cause" for such imaging. "Good cause" is established especially in light of evidence suggestive of data tampering or destruction, such as when a party claims that an unidentified hacker deleted all its electronically stored information or otherwise, simply misplaced or lost a laptop just the day before a "subpoena duces tecum"[31] was issued.

In another 2007 case (Hedenberg v. Aramark American Food Services[32], the court construed Rule 26(b)(2)(B) very narrowly and denied an employer's motion seeking a mirror image of an employee's computer for subsequent subjection to forensic analysis. The court was unconvinced by arguments raised by counsel for the employer contending that analyzing such mirror images was "now rather widespread" and that "usually, something new does emerge", and dismissed the related motion for discovery as an attempted "fishing expedition". Rule 26(b)(2)(B) also aims at establish a degree of fairness in cases where the benefits a party stands to gain from the production of digital evidence could be dwarfed by the complexity and costs of the related digital forensic techniques.

The approach outlined above is, obviously, bound to be evolve in light of technological advances: the emergence of ever more effective and efficient hardware and software is set to change the courts' current tendency to narrowly construe the rule.

The fact remains that in civil trials, the U.S. courts will order the discovery of digital evidence that is particularly difficult to access, only subject to a showing of good cause, so as to prevent parties from using technical obstacles as a pretext to unduly delay the proceedings or defeat claims by attrition.

---

[30] *Ameriwood Industries, Inc. v. Lieberman et al*., 2007 U.S. Dist. LEXIS 93380, E.D. Mo. Dec. 27, 2006, available at: *http://www.jenner.com/files/tbl_s69NewsDocumentOrder/FileUpload500/1584/Ameriwood_v._Liberman.pdf.*

[31] In the U.S. a "*subpoena duces tecum*" is a summons requiring the person on whom it is served to personally appear in court together with specific material evidence or documents that may be useful at a particular hearing or trial.

[32] *Hedenberg v. Aramark American Food Services*, 2007 US Dist. LEXIS 3443, WD Wash. Jan. 17, 2007.

In an attempt to define "computer forensics" – and that is to say, the set of digital investigative methods and procedures applicable within the framework of the criminal law –.

Eoghan Casey, in 2004, distinguished, first and foremost, between computers used "as weapons" and those that serve as "containers of the data" pertaining to the electronic activities of their users [33].

Casey argues that computer forensics properly refers only to the analysis of electronic equipment used to engage in criminal behaviour, since, computers used simply to store user-related or user-generated data, merely bear witness to the impact of social dynamics on digital systems, and, in most cases, feature digital content that is readily accessible without recourse to forensic technology for data recovery and conservation.

A further crucial distinction that must be drawn between digital forensics, and computer security which is conventional field of information technology that focuses on data security. This field often intersects with digital forensics insofar as the latter is aimed at accessing and interpreting the data protected by computer security measures.

The basic difference between the two fields is that the purpose of digital forensics is not merely to protect data against alteration and unauthorised access, but also to interpret the data and present the results in court, with the result that computer forensic experts must not only be fully familiar with the complexities of information technology, but also well trained in law enforcement procedures and investigative techniques.

That said, it must be borne in mind that:

an in-depth knowledge of computer science and basic digital forensic techniques is required in both fields;

digital forensic technicians must, moreover, be trained to identify data storage locations and devices potentially rich in digital evidence;

digital forensic technicians must also be trained to conserve digital evidence, contextualize the same within the framework of the investigation and, above all, ensure the chain of custody and reliability of all electronically stored information to be used as evidence at trial.

---

[33] E. CASEY, *supra* note 12, at page 23.

3. *Digital Forensics in Italy*

Italian legal scholars have launched their own debate on the definition and subject-matter of digital forensics, focusing solely on the criminal law aspects of digital investigations. Whilst progress has been painfully slow, especially in light of inadequate guidance in the form of consolidated case law, the effort deserves the utmost support.

Cesare Maioli defines computer forensics [34] as "the study of all the activities involved in the analysis and solution of computer-related criminal cases, inclusive of offences committed using a computer, or against a computer or in which a computer could, in any event, constitute evidence", before pointing out that "the purpose of computer forensics is to conserve, identify, acquire, document or interpret the data stored on a computer.

In general terms, the goal is to identify the best techniques for:

– collecting the evidence without altering the computer system on which it is stored;
– ensuring that any and all digital evidence collected and stored on different storage media is identical to the original digital data;
– analyzing the data without altering the same".

The following conclusions may be drawn from Maioli's definition:

– the five main points of computer forensics are the identification, collection, conservation, documentation and interpretation of digital data;
– forensic experts are above all skilled computer technicians with a practical, rather than theoretical background.

For Marco Mattiucci and Giuseppe Delfinis, "forensic computing", another term of digital forensics, entails the processing of electronic data for investigative and/or judicial purposes [35]. The basic focus of the field is the "electronic document", and that is to say, the digital representation of judicially relevant facts or events.

This approach leads the authors to posit two definitions for forensic computing:

---

[34] C. MAIOLI, *introduzione all'informatica forenze*, in *La sicurezza preventiva della comunicazione*, compiled by P. POZZI, Turin, 2004, Franco Angeli, available at: *http://www.jus.unitn.it/-users/dinicola/criminologia-ca/topics/materiale/dispensa_4_1.PDF*

[35] M. MATTIUCCI,-G. DELFINIS, *Forensic Computing*, in *Rassegna dell'Arma dei Carabinieri*, 2, 2006, at page 52.

1) "The process of identifying, conserving, analyzing and presenting digital evidence (evidence admissible at trial, obtained using electronic tools);

2) The collection and analysis of data in accordance with a practice that ensures that the data are free from distortions and prejudices, with a view to reconstructing data and actions generated within the computer system in the past" [36].

The second definition seems preferable insofar as it emphasizes the need to protect digital data against alteration and manipulation during collection.

Lastly, a computer science expert, Andrea Ghilardini, and a legal scholar, Gabriele Faggioli, define computer forensics as "the field that focuses on the preservation and study of information stored on computers or in computer systems, with a view to deriving therefrom evidence useful to the conduct of the investigation".

Digital forensics is on the verge of opening a chapter in its history. The field will not longer be limited to technical aspects, but will also have to embrace all the interconnected legal issues involved, including:

– the problem of updating digital forensic techniques so as to avoid obsolescence and the risk of losing large volumes of data;

– the issue of "best practices" with regard to the collection and use of digital evidence;

– privacy issues and how they related to digital forensics (especially post-Sept. 11);

– the question of compliance with legal requirements, and above all, due process in criminal trials, the violation of which would reduce digital forensics to little more than purely technological interpretation.

The application of digital forensics in the field of criminal law, must necessarily take into account:

– the compatibility of the new evidence gathering techniques with respect for the fundamental values underlying the Italian legal system, on the one hand; and

– the effectiveness of individual digital forensic tools and techniques in ensuring respect for the due process rights of the accused, on the other.

---

[36] A. GHILARDINI, G. FAGGIOLI, *Computer Forensics*, Apogeo, Milan, 2008, at page 1.