Merging Concepts of Forensic Disciplines for the Control of Digital Records

Luciana Duranti

When thinking about forensic disciplines one tends to consider those that are taught to legal students in law faculties. Few realize that there are forensic disciplines that are not a required component of legal education, yet are strictly linked to the law, and in large measure partake of fundamental legal concepts, gave origin or contributed to develop them, or support their application to specific realities. Among these disciplines are archival science and diplomatics.

In the Western world, archival science originated from the writings of the Roman jurists of the 11th century AD, although its fundamental concepts were already embedded in the Justinian Code, the *Corpus Iuris Civilis*, which in the 6th century collected the Roman law known to date and the new laws issued by Justinian. By the time the first course in law was delivered at the University of Bologna in 1158, these concepts and the principles descending from them were already entrenched in the legal and social understanding of archives. An archives was defined as *locus publicus in quo instrumenta deponuntur* (i.e., the public place where deeds are deposited), *quatenus incorrupta maneant* (i.e., so that they remain uncorrupted), *fidem faciant* (i.e., provide trustworthy evidence), and *perpetua rei memoria sit* (i.e., and be continuing memory of that to which they attest).

Thus, the archives was regarded as a place of preservation under the jurisdiction of a public authority. The place, by providing the documents with trustworthiness, gave them the capacity of serving as evidence and continuing memory of action. A German jurist, Ahasver Fritsch, in 1664, commented that archival documents did not acquire authenticity by the simple fact of entering the designated place, but by the fact that 1) the place to which they were destined belonged to a public sovereign authority, as opposed to its agents or delegates, that 2) the officer forwarding them to such a place was a public officer, that 3) the documents were placed both physically (i.e., by location) and intellectually (i.e., by description) among authentic documents, and that 4) this association was not meant to be broken.

These legal concepts were never superseded or lost. The "archival right," that is, the right to keep a place capable of conferring authority to the documentary by-products of action by endowing them with authenticity, was in time acquired by all those bodies to which sovereignty was delegated by the supreme secular and religious powers--among these, city states and churches. In Medieval times, corporations of every kind, including universities, deposited the documents of their activities in the *camera actorum* (i.e., chamber of the acts) of the municipality having jurisdiction over them or in the archives chests of ecclesiastical institutions, chests anchored by at least three chains to the floor. The public officer would read aloud to the interested assemblies the inventories of the documents that had crossed the threshold of the archives and become depositories of truth (Lodolini, 1991, p. 43).

The basic difference between the Tabularium and the Medieval places of preservation is that the former belonged to the same authority of which those producing the documents were agents or delegates--just like today the central archives of a state is part of the central government of that state, while the latter belonged to bodies having some form of sovereignty over those creating the documents, but quite distinct from them. In the 16th century, the "inviolability" of the archives was emphasized to the point that the jurists recognized the capacity of the place to endow documents of private origin deposited there with trustworthiness. The fact that the documents were preserved to guarantee the rights of the monarchs to their jurisdictions and to protect the boundaries of their lands when challenged by other territorial sovereigns, rather than to allow the citizens to scrutinize the actions of the government or to look after their own interests, does not diminish the authenticating power of the archives. When the question

became whether the documents deposited in an archives should be considered evidence only under the jurisdiction in which the building belongs or anywhere, there was no doubt among international legal scholars that the character of evidence given by an archives to the documents it contains is universal (Carolus Molineus, 1552).

From antiquity to the eighteenth century, the creation of documents in the course of business has been highly controlled. The degree of reliability of the documents was based on three factors: 1) the degree of control exercised on the procedure of creation, 2) the degree of control exercised on the authors, and 3) the degree of completeness of the documents themselves. However, to create reliable documents was not sufficient if one wished to use them later on as evidence. It was necessary that an authority different from the creating one recognized them as being what they purported to be, and accepted them into custody. These actions of recognition and acceptance into custody represent a declaration of authenticity. In fact, while reliability is linked to creation, authenticity is linked to transmission and preservation. To declare a document authentic means to say that it is precisely as it was when first transmitted or set aside for preservation, and that its reliability, or the trustworthiness it had at that moment, has been maintained intact. But, acceptance into custody is more than a declaration of authenticity. It is taking responsibility for preserving that authenticity, and it requires taking the appropriate measures for guaranteeing that authenticity will never be questioned, measures that go much beyond physical security. The identification of the documents, the assignment to them of an intellectual and physical place in the whole of the authentic documents, that is, their location and description in context, by freezing and perpetuating their interrelationships, ensure that possible tampering will be easy to identify. Because of all this, any document that has passed the archival threshold, for as long as it exists, is truly a permanent monument to its creator's actions.

On October 5, 1789, the populace of Paris put fire to the royal archives building, seen as the ultimate bastion of privilege. In the mind of the people, the archives was more than a symbol: it was what gave authority and power to the feudal titles deposited in it. No-one thought of attacking the chancery offices, where all the information was kept for reference and administrative action, because nothing was enforceable which was not in the inner sanctum of the archives. The destruction of the French monarchy's archives marked also the end of a view of archives as an integral component of people's life. July 25, 1994 is not an entirely happy date for archives. The documents of defunct bodies, concentrated in the National Archives of France, were declared the patrimony of the nation and made accessible to the public. By virtue of this declaration, the State recognized its duty to preserve such patrimony for the next generations. However, the documents created by living bodies were for the first time subtracted to a controlled procedure aimed to ensure the reliability of their creation and the authenticity of their transmission and preservation, and were kept by the creators or their successors until old age transformed them into sources for history. The dichotomy between administrative and historical archives was born.

However, to believe that this development would have determined an eradication of the archival discipline from its legal roots making of it more of an historical discipline is wrong. Not many years passed since the first concentration of the records of defunct agencies or organizations in one general archives before the law of several European countries began to determine the method of arrangement and description of the records to ensure that their nature, characteristics and, mostly, trustworthiness would be forever protected: legislation in Naples (1812), the Grand Duchy of Tuscany (1822), the Papal State (1829), the French State (1840), Holland (1857) and the Prussian State (1882) prescribed the principle of provenance or *respect des fonds* and *respect pour l'ordre original* (Lodolini, 1987). Law and jurisprudence continued to provide the logical thread along which archival science evolved in the second half of the century. Everywhere in Europe the conception of the State and the laws of the State constituted the catalyst that allowed for the evolution of archival science into an organic and unitary system (Duranti, 1996).

However, archival science was not the only records related forensic discipline developing as a complex organic system in Europe in the 17th and 18th centuries. In fact the use of archival material by various authorities as proof of their rights and privileges led to the development of methodologies for testing the authenticity of the records in question and gave rise to a new science called diplomatics, which studied the nature, genesis, formal characteristics, structure, transmission and legal consequences of records (Duranti, 1996, 1998). The history of diplomatics is directly linked to the so-called "diplomatic wars" (bella diplomatica), judicial controversies over political or religious claims based on records of disputed origin, which, in the 17th century, especially in Germany and France, assumed a doctrinal character and prepared the ground for scientific debates that, from the courts, moved into academia, where diplomatic knowledge became the core theoretical knowledge taught to law students in the most important European universities (Duranti, 1998). Since then, it has been used by scholars of the records to identify records of unknown origin and to attest the authenticity of records of disputed origin.

It is not surprising that archivists' core knowledge consists of two forensic disciplines, because, as Hilary Jenkinson put it, records are material evidence of the activities producing them (Jenkinson, 1980). These disciplines have served archivists well in the analogue environment, but digital records present new complexities with which also the legal system starts having serious issues. The legal systems, both common and civil law, consider records to be a very special kind of documentary evidence. Records are defined in archival science as any document made or received in the course of a practical activity by a natural or an artificial person (or, physical or corporate, moral, or juridical person, depending on the country) and kept for action or reference. In civil law environments, a record is admissible as evidence in court simply on the basis of the recognition of its record nature. In common law environments, in addition to relevance, disputed records may require further steps to gain admissibility, such as proof of authenticity, and compliance with the best evidence rule, which prefers an original to drafts or copies, and the exception to the hearsay rules, which considers records a special kind of evidence, imbued with inherent trustworthiness by the circumstances of its creation.

Thus, it is vital to establish clear and stable parameters for the identification of records among all the digital entities that may exist in a digital system, be it a document management system, a geographic information system, an assembly of separate applications, like e-mail, or any other form of information technology. This issue keeps coming up at trials and in political discussions and remains unresolved. In an example, the British Columbia Rail case, where the judge pointed out that legislation speaks of preserving "records," the Liberal MLA Ralph Sultan asked "What is the definition of a record?" referring "to the controversy over to what extent e-mails qualify" (Palmer, 2010). In another example, the Supreme Court of Canada is deciding whether hyperlinks in a text are akin to footnotes or make of the material to which they connect the reader a component of the document being read (Tibbetts, 2010).

The identification of records among all kinds of digital entities is addressed by Digital Diplomatics, a contemporary development of diplomatics which has successfully applied its theory and methods to contemporary digital records (Duranti, 2009a, Duranti, 2005; Duranti and MacNeil, 1997; Duranti, Eastwood and MacNeil, 2002; Duranti and Thibodeau, 2006). The related and equally complex issue of the authenticity of digital records, is addressed by both Digital Diplomatics and Digital Forensics, a new discipline which is defined by Ken Zatyko as "the application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation" (Zatyko, 2007). More specifically, the Digital Forensics Research Workshop, in 2001, defined "digital forensics" as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering

the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (*Digital Forensics Research Workshop*, 2001). Thus, in several ways, the objects of study of Digital Forensics and Digital Diplomatics overlap and their methods of inquiry complement each other (Duranti, 2009b). At the same time, their perspectives are very different and the sum of their bodies of knowledge is not at this time able to address all the issues of 'recordness' and authenticity with which our legal system is constantly confronted, due to the extremely rapid obsolescence of information technologies and to the manipulability, mutability and fragility of the digital entities that these technologies produce and store, especially after those entities have been removed from the original system.

Thus, a team composed of diplomatics, archival science, information science, evidence law and digital forensics specialists has undertaken a research program, the purpose of which is to develop a new science called "Digital Records Forensics" (*Digital Records Forensics Project*, 2008-2011) by integrating the concepts and methods of all these bodies of knowledge. This integration will 1) enable those who need to assess the trustworthiness of digital records that no longer reside in the original system in which they were made or received and maintained to ascertain whether they are accurate and authentic, having preserved their original identity and integrity; 2) foster development of methods for maintaining the authenticity of these records over the long term, regardless of their format; 3) ensure that the Law maintains an awareness of the changing nature of documentary evidence determined by digital technologies and adjusts its requirements and procedures to the changing characteristics of such evidence; 4) contribute to organizational forensic readiness as firms and agencies anticipate the need to support legal action with admissible digital evidence (Nevins, et.al., 2008; Endicott-Popovsky, et.al. 2007, 2005; Endicott-Popovsky and Frincke 2007a, 2006; Taylor, et.al., 2007); and 5) allow for the development of education programs forming professionals capable of acquiring, as well as creating, assessing, controlling and maintaining reliable, accurate and authentic records for as long as they are needed.

This integration will need to start with an examination of the concepts on which digital diplomatics and archival science on the one hand, and digital forensics on the other hand, are based, compare them, and assess their compatibility with one another. Among these concepts, as already alluded to, the most important ones are the concepts of records and authenticity. The identification of "records" among all the digital objects produced by complex dynamic and interactive systems, and the determination of their authenticity, are issues that have been and continue to be directly dealt with by a research project called InterPARES (*InterPARES Project*, 1999-2012), the goal of which is to develop the knowledge necessary to support the reliable and accurate creation and the long-term preservation of authentic digital records (MacNeil, 2000, 2001, 2002, 2004; Duranti, 2005; Duranti and Thibodeau, 2006). The objects of InterPARES research are digital records that exist as large aggregations in live systems and are still in the hands of the creating organizations. These organizations must anticipate the possibility that the digital records they produce will be relied upon as evidence in civil and criminal trials, thus necessitating advanced preparation (Nevins, et.al., 2008; Endicott-Popovsky, et.al. 2007, 2005, Endicott-Popovsky and Frincke 2007a, 2006, Taylor, et.al., 2007).

What are the characteristics of digital records according to our disciplines? Starting with the traditional definition of records as "a document made or received in the course of a practical activity as an instrument or a by-product of such activity, and set aside for action or reference" (InterPARES 2, Terminology Database), InterPARES established that digital record must have 1) an identifiable context; 2) an originator,[1] an author,[2] a writer,[3] an addressee,[4] and a creator;[5] 3) an action, in which the record

[1] The physical or juridical person assigned the electronic address in which the record has been generated and/or sent.

participates or which the record supports either procedurally or as part of the decision-making process; 4) explicit linkages to other records within or outside the digital system, through a classification code or other unique identifier; 5) a fixed form; and 6) a stable content (MacNeil, 2000). Most of these requirements are self explanatory, but the concepts of fixed form and stable content require elaboration, as these two characteristics of a digital record are the most problematic not only for the purposes of trusted record keepers, but also for those of digital forensics experts.

A digital record has a fixed form if its binary content is stored so that the message it conveys can be rendered with the same documentary presentation it had on the screen when first saved, even if its digital presentation has been changed, for example, from Word to .pdf. A digital record has a fixed form as well if the same content can be presented on the screen in several different ways but in a limited series of pre-determined possibilities; in such a case we would have different documentary presentations of the same record (e.g., statistical data viewed as a pie chart, a bar chart, or a table). This situation raises the issue of the difference between a stored record and a manifested record.

A "stored record" is constituted of the linked digital component(s)[6] that are used in re-producing the record, which comprise the data to be processed in order to manifest the record (i.e., content data and form data) and the rules for processing the data, including those enabling variations (i.e., composition data). A "manifested record" is the visualization of the record in a form suitable for presentation to a person or system. Sometimes, a manifested record does not have a corresponding stored record, but is re-created from fixed content data when a user's action associates these data with specific form and composition data (e.g., a record produced from a relational database). If the same user's action always results in the same documentary presentation with the same content, the manifested entity is considered to have fixed form and stable content, even when it does not have a corresponding stored record, and, if all other requirements for the existence of a record are present, it is a record. In contrast, when one stored record may be manifested in several documentary presentations, the creator has to determine whether the official record is the stored one or one or more of the manifested ones by assigning to the chosen entity a classification code and/or a retention period. There might be situations in which a stored record is never manifested, as is the case with interacting business applications, workflow generated and used to carry out experiments, analyses of observational data carried out by interpreting software, etc. Also in this case, the creator determines which entities should be retained with other records of the same activity, manifested or not. Clearly, these decisions are based on the functions and activities in which the records participate, both as aggregates and as individual entities.

Stable content has a more intuitive explanation. A digital entity has stable content and can be considered a record, if all other conditions are satisfied, if the data and the message in it are unchanged and unchangeable, meaning that data cannot be overwritten, altered, deleted or added to. However, there are cases in which entities that demonstrate "bounded variability" can be said to have stable content. A digital entity has bounded variability when changes to its form are limited and controlled by fixed rules, so that

---

[2] The physical or juridical person(s) having the authority and capacity to issue the record or in whose name or by whose command the record has been issued.

[3] The physical or juridical person(s) having the authority and capacity to articulate the content of the record. It may be the same name as the author and/or originator of the record.

[4] The physical or juridical person(s) to whom the record is directed or for whom the record is intended.

[5] The physical or juridical person in whose *fonds* the record exists

[6] "Digital components" are digital entities that either contain one or more records or are contained in the record and require a specific preservation measure.

the same query or interaction always generates the same result, and when the user can have different views of different subsets of content, due to the intention of the author or to the character of the operating systems or applications. While the first definition of stable content applies to static digital entities, the second is significant when the entities we are looking at are interactive.

A "static digital entity" is one that does not provide possibilities for changing its manifest content or form beyond opening, closing and navigating; for example, emails, reports, sound recordings, motion videos, and snapshots of web pages. These entities, if all other requirements are satisfied, are records, because they have fixed form and stable content. By contrast, an "interactive digital entity" presents variable content, form, or both, and the rules governing the content and form of presentation may be either fixed or variable. Interactive entities may or may not be records, depending on whether they are non-dynamic or dynamic. "Non-dynamic entities" are those for which the rules governing the presentation of content and form do not vary, and the content presented each time is selected from a fixed store of data. Examples are interactive web pages, online catalogs, and entities enabling performances: if the other conditions exist, they are records. "Dynamic entities" are those for which the rules governing the presentation of content and form may vary: these entities may be components of information systems or "potential records," in that they can become records if the digital system in which they exist, given the purpose that it fulfills, is supposed to contain records and is therefore redesigned in such a way that it will produce and manage records, or if the entities that should exist as records are moved to another system that only maintains digital records (i.e., static or non-dynamic entities) (Duranti and Thibodeau, 2006).

Digital forensics has a similar understanding of static and dynamic entities. Mocas writes: "For example, imaging a single hard drive and then performing a search on that image provides a static technical environment. In contrast, a dynamic technical environment is one in which one or more of the components from which data are retrieved have a potential for modification, independent of any system changes that might be introduced during the investigative process. In other words, live systems and systems connected to the Internet qualify as dynamic" (Mocas, 2004). Digital diplomatics is, however, more specific about dynamic entities and allows for an easier identification by describing their behaviour. Examples of dynamic entities are: entities whose variation is due to data that change frequently (e.g., the design permits updating, replacement or alterations; it allows data collection from users or about user interactions or actions; or it uses these data to determine subsequent presentations); entities whose variation is due to data continually received from external sources and not stored within the system; entities produced in dynamic computing applications that select different sets of rules to produce documents, depending on user input, sources of content data, and characteristics of content (e.g., weather sites); entities produced by evolutionary computing where the software generating them can change autonomously (e.g., scheduling and modeling of financial markets; edutainment sites), etc. (Duranti and Thibodeau, 2006).

In order to establish whether entities of the kind described above are records, it is essential to establish in which way they participate in activities, if at all, in the context of the functions of their creator. There are different ways in which a record may participate in an action, and, depending on its function with respect to the action in which it takes part, a record may acquire a specific qualifier. Thus, if a record is meant to provide evidence of an act that came into existence and was complete before being manifested in writing, it is qualified as a *probative* record, while if it is meant to put the act into being and constitutes therefore the essence and substance of the act, it is qualified as a *dispositive* record. Examples of probative records are certificates, registrations, transcripts, and receipts. Examples of dispositive records are contracts, grants, applications, and money orders. These types of records all have in common the fact that their existence and written form are required by the legal system within which they are created, and therefore they are all legal records. Traditionally, these records have a very formal documentary presentation, but in the digital

environment they are increasingly becoming informal, to the point that a simple email can have the effects of a contract.

Records whose existence is not required by the legal system for carrying out actions and the written form of which is discretionary are considered non-legal records. They have been distinguished in two categories: *supporting* records, whose function is to inform the activity in which they take part; and *narrative* records, whose function is one of free-form communication of information. While both categories of records participate in some kind of act, neither is able either to provide evidence of such act by itself or to carry it out. Examples of supporting records are teaching notes and maps, and examples of narrative records are notes, unsolicited reports, and informal accounts of events. In the digital environment, we find two additional categories of records, *instructive* records and *enabling* records. The former indicate the way in which data, documents or records are to be presented (e.g., forms with embedded instructions for filling them out and formatting), and the latter enable a presentation, such as the performance of artworks (e.g., software patches), execution of business transactions (e.g., interacting business applications), conduct of experiments (e.g., a workflow generated and used to carry out the experiment of which it is instrument, byproduct and residue), or analysis of observational data (e.g., interpreting software). The salient characteristic of instructive records is that the record as it is stored differs from the record as it is manifested on the computer screen, while the salient characteristic of enabling records is that they usually do not have a corresponding manifested record (Duranti and Thibodeau, 2006).

Digital forensic experts have been concerned with the different types of records that can be found in digital systems, although only in relation to their ability to be admissible evidence. In fact, the courts of common law countries (like the United States, Canada, The United Kingdom, and Australia) have generally admitted digital records under the business records exception to the hearsay rule mentioned earlier.[7] The identification of what constitutes a business record has never been problematic with traditional records, but, with computer records, forensic experts are beginning to make distinctions. They distinguish "computer-stored" records from "computer generated" records. The former category, *computer-stored* records, includes the writings of physical persons that happen to be in electronic form. Examples are email messages, word processing documents, and Internet chat room messages. Like any traditional document containing human statements, computer-stored records are admissible in court. The latter category, *computer-generated* records, contains the output of computer programs, produced without direct human interference. These records can be computer-recorded events, like transactions recorded by ATM machines; data sets produced by a system that performs analysis or calculations of input provided by humans; simulations modelling behaviours or predicting outcomes of events; or decision trees, which lead a user to a destination through a path that depends on questions provided along the way; and of course records that digital diplomatics includes in the "stored only" and "enabling" records category (Paul, 2008). Unlike computer-stored records, computer-generated records are regarded as containing no human statements, as they are produced by a computer program designed to process input following a defined algorithm. The idea that computer-generated records do not contain human statements is very significant because the fact that a computer rather than a human being has generated the record means that they are not business records. As a consequence, the evidentiary issue is no longer whether the statement in the record is truthful and accurate—a question of reliability—but whether the computer program that generated the record was functioning properly—a question of authenticity.

[7] This rule considers all written evidence hearsay because it contains statements made by humans who cannot be cross-examined on the stated matter. However, written documents which 1) are produced in the usual and ordinary course of business, 2) at or near the time of the facts or acts of which they are offered as evidence, 3) by someone who is under a duty to create them for the purposes of the business and is familiar with the procedure for doing so, are considered "business records" and admissible under an exception to the hearsay rule.

The characteristics of computer-generated records make them similar to scientific evidence, which is usually assessed on the basis of four criteria: 1) whether the theory, procedure or process generating it has been tested or can be tampered with; 2) whether it has been subjected to peer review or publication; 3) what is the known or potential error rate; and 4) whether it is generally accepted within the relevant scientific community (Carrier, 2002). This author does not believe the equation of technological evidence with scientific evidence to be defensible or reasonable, because software programs are designed and selected by humans and their output therefore results from human intervention. Furthermore, by considering computer-generated records equivalent to scientific evidence—and therefore by focusing on their source in terms of capability rather than intentions—a legal system would degrade them from substantive evidence, that is, evidence offered to prove a factual issue, to demonstrative evidence, that is, evidence that has in itself no probative value but is used to illustrate and clarify the factual matter at issue. Digital forensics experts identify a third category of computer records, those which are both *computer-generated and computer-stored*. An example is a spreadsheet that has received human input followed by computer processing (the mathematical operations of the spreadsheet program). This very common category (e.g., most student records in a student registration system) can be considered both substantive and demonstrative evidence.

The categorization of digital records made by forensics experts is clearly based exclusively on evidentiary purposes, but it is useful to all professionals who fulfill the function of trusted record keeper or records custodian in that it supports their responsibility of guaranteeing and perpetuating the authenticity of the records placed in their trust. Equally important are the ideas that digital forensics experts hold about the larger concept of trustworthiness.

Diplomatically, a digital record is trustworthy if it is accurate, reliable and authentic. Record *accuracy* is the trustworthiness of the data (i.e., the smallest meaningful indivisible pieces of information) within a record, and is defined as their truthfulness, exactness, precision or completeness. In the digital environment, it is necessary to consider and assess accuracy as a separate quality of a record because of the ease with which data can be corrupted during transmission across space (between persons and/or systems) and time (when digital systems are upgraded or records are migrated to a new system). Consequently, accuracy is a shifting responsibility that moves over time from the creator's trusted record keeper to the trusted custodian.

Reliability is the trustworthiness of a record as a statement of fact, as to content. It is assessed on the basis of 1) the completeness of the record, that is, the presence of all the formal elements required by the administrative-legal system for that specific record to be capable of achieving the purposes for which it was generated; and 2) the controls exercised on the process of creation of the record, among which are included those exercised on the author of the record, who must be the person competent, that is, having the authority and the capacity, to issue it. The reliability of a record is the exclusive responsibility of its creator and the trusted record keeper, that is, of the person or organization that made or received it and maintained it with its other records.

Authenticity is the trustworthiness of a record as a record and is defined as the fact that a record has not been tampered with or corrupted, either accidentally or maliciously. An authentic record is one that preserves the same identity it had when first generated and can be presumed or proven to have maintained its integrity over time. The identity of a record is constituted of those characteristics that distinguish it from any other record, and is assessed on the basis of the formal elements on the face of the record, and/or its attributes, as expressed for example in a register entry or as metadata. The metadata that attest to the identity of a record are the names of the five persons concurring in its creation; the date(s) and time(s) of its issuing, creation and transmission; the matter or action in which it participates; the expression of its archival bond (e.g., its classification code); its documentary form; its digital format; the indication of any attachment(s); the

indication of the presence of a digital signature, if applicable; and the name of the person/office handling the business matter in which the record participates. The integrity of a record is linked to its ability to convey the message it was intended to communicate when generated. Thus, it does not matter if the ink is fading, the medium (i.e., the material support) is falling apart, or the bit-stream is not the same as in the first manifestation of the record, as long as the content is readable and is the same as it was originally intended, the medium does not have missing parts, or the manifestation we see on the computer screen is the same as it was the first time the record was saved. The integrity of a record is inferred not only from its appearance, which might be deceiving in the case of good forgeries, but also from the circumstances of its maintenance and preservation: an unbroken chain of responsible and legitimate custody is considered an insurance of integrity until proof to the contrary, and integrity metadata are required to attest to that. They are: the name(s) of the persons/offices handling the record over time; the name of the person/office responsible for keeping the record; the indication of annotations, if applicable; the indication of technical changes, if applicable; the indication of presence or removal of digital signature; the time of planned removal of the record from the digital system; the time of transfer to a trusted custodian; the time of planned deletion; and the existence and location of duplicates outside the system. In the absence of sufficient evidence linked to the record, authenticity can be inferred on the basis of the trustworthiness of the record system in which the record exists. The authenticity of a record is a movable responsibility, as it shifts from the creator's trusted record keeper, who needs to guarantee it for as long as the record is in its custody, to the trusted custodian, who guarantees it for as long as the record exists.

The trustworthiness of a record, consisting of its accuracy, reliability and authenticity, should not be confused with one of the means of protecting and/or establishing it, authentication. *Authentication* is defined as a declaration of authenticity made by a competent officer, and consists of a statement or an element, such as a seal, a stamp or a symbol, added to the record after its completion. While authenticity is a quality of the record that accompanies it for as long as it exists as is, authentication only guarantees that a record is authentic at one specific moment in time, when the declaration is made or the authenticating element or entity is affixed. In the digital environment extreme authentication is usually provided by a digital signature. The authentication provided by a digital signature is considered "extreme" because the test fails if even one bit changes. Digital forensics experts are beginning to see that biometric identification systems and cryptography, not being in common use, cannot be considered the prevalent means of authentication. Mocas writes that, although "[w]ithout such mechanisms, authentication (computer security) can be difficult to positively establish based simply on digital evidence," "there is interesting research on ways that digital information can be used to indicate a possible author. For example, there is work on establishing personal characteristics based on document features" (Mocas, 2004). Clearly, this is a reference to the method of diplomatic analysis.

Another form of authentication is a declaration made by an expert who bases it on the trustworthiness of the system containing the record and of the procedures controlling it. This raises the issue of when a record system can be trusted. Digital diplomatics assesses the trustworthiness of a record system according to the same criteria used by general diplomatics to assess the trustworthiness of chancery procedures and processes: the level of standardization of and control on record systems, that is, on the set of rules governing the making and keeping of records, and the set of tools and mechanisms used to implement these rules. In order to generate reliable and accurate records, every record-making system should include in its design integrated business and documentary procedures, record metadata schemes, records forms, and record-making access privileges, and should fulfill technological requirements that ensure the integrity of the system. In order to maintain accurate and authentic records, a trusted recordkeeping system should include in its design a recordkeeping metadata scheme, a classification scheme, a retention schedule, a registration system, a recordkeeping retrieval system and access privileges, and procedures for maintaining authentic records (Duranti and Preston, 2008).

Digital forensics does not use the term trustworthiness in relation to records or records systems other than in a general way. The terms most commonly found in digital forensics literature are authenticity, accuracy, reliability, and integrity. Although these qualities are all required to support "circumstantial guarantees of trustworthiness" of digital materials presented as evidence of facts at issue, the first two are primarily used in relation to records, while the other two are applied to systems or media and only indirectly to records. The term *authenticity* refers to the fact that "the data or content of the record" are what they purport to be and were produced by or came from the "source"[8] they are claimed to have been produced by or come from. In digital forensics, like in diplomatics, while authenticity implies integrity, the opposite is not true, that is, integrity does not imply authenticity. Proof of authenticity is provided by a witness who can testify about the existence and/or substance of the record on the basis of his/her familiarity with it, or, in the absence of such person, by a computer programmer showing that the computer process or system produces accurate results when used and operated properly and that it was so employed when the evidence was generated. Galves and Galves write that, to enhance the strength of circumstantial digital evidence one could examine metadata "which records (1) the exact dates and times of any messages sent or received, (2) which computer(s) actually created them, and (3) which computer(s) received them." Although in a different context, these authors also argue the importance of a chain of legitimate custody for inferring authenticity (Galves and Galves, 2000). A presumption of authenticity is afforded to evidence such as x-rays, photographs, tape recordings, computer-generated records or scientific surveys produced by an automated process that is shown to render accurate results, and is commonly extended to records managed by software performing data storage, collection or retrieval functions, if the operation of the software can be proven to have been reliable.

Regardless of the fact that, in digital forensics, references to authenticity appear to focus on the data or content in the record rather than on its formal aspects, like diplomatics, the importance of protecting both documentary and digital presentation of a record for purposes of authentication is implicit in the discussion of digital forensics practices. For example, Ghirardini and Faggioli state that, although conversion of digital evidence to forms and formats different from the original is a process useful to its accessibility and analysis, it "modifies its nature." This implies that converted records cannot be used as evidence and must always be accompanied by the records in the original presentation (Ghirardini and Faggioli, 2007). Original presentation does not mean original record though. In the digital environment, there are no originals in the diplomatics sense, that is, there are no records which, in addition to being complete and capable of reaching the purposes for which they were generated (i.e., effective) are also the first instance of each item under consideration, because when we close a digital record for the first time we destroy the original and every time we open it we create a copy. However, we can state that each digital record, in the last version used by the creator in the usual and ordinary course of business, is a copy in the form of original and, in any version kept by the preserver, is an authentic copy of the record of the creator. They are both authoritative and authentic if their identity is intact and their integrity can be either presumed or proven.

The concept of *accuracy* is not clearly defined in digital forensics, primarily because the law does not include it in its procedures or rules concerning the presentation or evaluation of evidence. However, accuracy is used by both legal and digital forensics writers as a component of authenticity and, specifically, integrity, in a meaning very similar to that given to the term by digital diplomatics, and it is one of the qualities of the evidence to which digital forensics practitioners pay more attention. In fact, their processes for extracting digital evidence must, first of all, avoid altering the data, and are guaranteed reliable in such sense by ensuring that they are repeatable. "Repeatability," which is one of the fundamental precepts of digital forensics practice, is supported by the accurate documentation of each and every action carried out on the evidence. This is certainly an area in which archivists would have much to learn from digital forensics,

[8] In digital forensics, the term "source" is used in a general way to refer to either a person (physical or juridical), a system, software, or a piece of hardware.

especially when this knowledge is used in a prospective way to support the selection of the best software for a record-making or a recordkeeping system and the definition of transfer procedures from the creator to the preserver, as will be seen later.

There is a general agreement among legal and digital forensics experts that open source software is the best choice from an evidentiary point of view both as a records source and as a tool for extraction of records from their digital environment and their preservation. Their arguments are based on the fact that the judiciary, in assessing accuracy, integrity, and reliability, uses measurements such as objectivity, transparency, verifiability, and repeatability (Carrier, 2002; Kennelly, 2001). In addition, digital forensics experts value the availability of open source, which, at the same time, allows modification and encourages dissemination, thereby making it possible to submit the software together with the records presented as evidence, so that their accuracy can be tested promptly by anyone at any time. This is especially true when conversion or migration occurs, because it would allow a practical demonstration that the software could not simultaneously manipulate the files' content while copying them and that nothing could be altered, lost, planted, or destroyed. Finally, open source is preferred because of the possibility of exchange of evidentiary material between the parties in the course of e-discovery (Crowley, 2007).[9]

The concept of *reliability*, used in reference to the source of the records, is defined in digital forensics in a way that points to a reliable software, measured by principles similar to those the courts use to determine evidentiary reliability, that is, empirical testing, subjection to peer review and publication, determination of error rate, and general acceptance within the relevant community (Paul, 2010). Also these principles point to open source software, because the processes of records creation and maintenance can be authenticated with evidence either by describing a process or system used to produce a result or by showing that the process or system produces an accurate result.

The concept of *integrity* is more nuanced. Digital forensics distinguishes *data integrity* from *duplication integrity* and clearly this distinction is very important for digital diplomatics, which concerns itself with the authenticity of the copies made in the course of digital records maintenance and preservation. Indeed, considering that it is not possible to preserve digital records, but only the ability to reproduce them, the concept of duplication integrity is key to digital preservation and the functions of the designated trusted custodian. Landwehr defines data integrity as the fact that data are not modified either intentionally or accidentally "without proper authorization." (Landwehr, 2001) Duplication integrity is ensured when "given a data set, the process of creating a duplicate of the data does not modify the data (either intentionally or accidentally) and the duplicate is an exact bit copy of the original data set." (Mocas, 2004) Mocas believes that separating these two notions of integrity is important because the concept is too broad to be able to address the aspects of each given situation, and because most of digital forensics work, just like records maintenance and preservation work, is carried out over duplicates. One could enrich further the concept of integrity by adopting also the link between integrity and time proposed by digital forensics experts and define record integrity differently in each phase of the record life cycle and/or custodial history (Duren and Hosmer, 2002).

Clearly, digital forensics has a very high stake in the trustworthiness of the evidence gathered, maintained and submitted to court. Two principles that are at the foundation of forensic practice and could be very useful to a trusted preserver are those of *non-interference* and *identifiable interference*. The former means that the method used to gather and analyse digital data or records does not change the original digital

[9] The Sedona Conference defines "discovery" as "the process of identifying, locating, securing, and processing information and materials for the purpose of obtaining evidence for utilization in the legal process." Similarly, it defines electronic discovery as the process of "collecting, preparing, reviewing, and producing electronically stored information (ESI) in the context of the legal process."

entities. The latter means that, if the method used does alter the original entities, the changes are identifiable (Casey, 2002). These principles, which embody the ethical and professional stance of digital forensics experts, are consistent with the traditional impartial stance of the archivist, as well as with his/her new responsibility of neutral third party, of trusted custodian. They are at the core of digital forensics procedures, the knowledge of which could provide great support to the archivist working with digital records, especially with regard to the activity that represents the weakest link in the chain of records preservation, the transfer of the records from the creator to the preserver. In this regard, a specific problem that needs to be addressed is that presented by records that have been extracted from the system in which they were generated and/or maintained and placed on portable media by the creator for storage elsewhere, or by its legitimate successor, or by other parties, such as law enforcement officers, for use as evidence in criminal investigations. Thus, they may end up on CDs or DVDs accumulated in an office drawer, or on backup tapes in an off-site warehouse. They may also end up being acquired at auctions, either inadvertently, for example by individuals who, after buying what they assumed were blank, used tapes, later discover that they actually contain records, or intentionally, for example by collectors of digital art, unaware of the difficulty of assessing the authenticity of such art when separated from its original technological context. These records are often of uncertain origin and/or exist in proprietary formats that are hard to maintain over time, yet often must be maintained intact with their identity and integrity for long periods of time (e.g., while waiting to serve as documentary evidence in a trial, or for their ongoing research value). To deal with these issues digital forensics knowledge is necessary to archivists. As well, digital forensics experts could derive useful input from the theory of archival science and diplomatics and their methods of identification of records among other types of materials and of assessment of their trustworthiness. Thus, the following section briefly outlines the research project that intends to bring all the forensic disciplines together and develop from their integration new original knowledge.

The objectives of the Digital Records Forensics research program are:

1. to develop concepts and methods that will allow the records management, archival, legal, judicial, law enforcement and digital forensics professions to recognize records among all digital data objects produced by complex digital technologies once they have been removed from the original system;
2. to develop concepts and methods to determine the reliability, accuracy and authenticity of records no longer in the original digital environment;
3. to identify, develop and organize the content of a new science and discipline called “Digital Records Forensics;” and
4. to develop the intellectual components of a new program of education for Digital Records Forensics experts.

In order to determine the content of the body of knowledge that would identify Digital Records Forensics as a science and a discipline, it is appropriate to reflect on the characteristics of both. A science comprises the ideas about the nature of the object of its study (i.e., theory) and about the principles and procedures for handling, controlling, examining, and maintaining such an object (i.e., methodology). The analysis of these ideas, principles and methods; the history of the way they have been applied over time in different contexts (i.e., of practice); and the literary criticism of both analysis and history (i.e., scholarship) are also an integral part of a science. Thus, a science can be defined as a system inclusive of theory, methodology, practice, and scholarship, which owes its integrity to its logical cohesion and to the existence of a clear *purpose* that rules it from the outside, determining the boundaries in which the system is designed to operate.

If we regard a science of Digital Records Forensics as an organic and unitary system, we have to accept that we would be dealing with a special type of discipline. A discipline encompasses the rules of

procedure that *discipline* the search of the scholar, and the knowledge so acquired. In the case of a digital records forensics system, however, the rules that will guide the investigation of scholars into issues, problems or concepts would have to be determined by its theory and methods. This is especially noticeable when research aiming to develop methods, strategies and/or standards for the treatment of new types of material looks for a starting point, or fundamental terms of reference.

To explain, it is useful to identify the components of the system in the case of a Digital Records Forensics science. The object of its study would be digital records. Consequently, its theory would be constituted of ideas about the nature of records in the digital environment, their characteristics, components, relationships and behaviour. Its methodology would encompass ideas about location and acquisition of digital records, identification and analysis, evaluation and interpretation, maintenance, transmission and preservation. Its practices would comprise accepted standards and the specific processes followed in various cases in different contexts, as well as the tools and instruments selected to carry out those processes and their performance. The purpose ruling this system from outside and determining its boundaries would be the acquisition/production of digital records capable of serving as reliable, authentic and accurate evidence, and their preservation for as long as required by the relevant juridical system. Scholarship would therefore aim at gaining an understanding of types of records and systems, of methods and practices, of legal, administrative and technological issues, and, on the basis of such understanding, developing more effective methods and practices, solutions, proposals for changes to the law, for design of new tools, etc. However, it is clear that, in order to be useful, such scholarship would have to be guided by the theoretical and methodological ideas that constitute the foundation of the system, such as the concepts of record, authenticity, evidence, forensic process or digital record systems.

Digital Records Forensics as a field of study is highly interdisciplinary. Some of the disciplines/sciences/ practices whose knowledge is to be brought to bear on Digital Records Forensics are centuries old, while others may be very recent but are entrenched in their very established views of things. To make a new science out of a field of study cross-fertilized by several bodies of knowledge requires a very detailed work of comparison and reconciliation of concepts, carefully aimed at maintaining consistency with the ultimate purpose of the new field. Thus, the selection of terms, definitions, principles, etc. should not occur on the basis of what is best in absolute terms, but of what best serves the purposes of Digital Records Forensics and is consistent with the other accepted ideas within it. Again, it is necessary to regard this new science as a system made up of parts, structure and processes. The parts are theory, methodology, practice and scholarship, each of which is, in turn, composed of parts. The structure is a hierarchical one, where each level descends from and depends on the previous one, with theory being the determinant and cohesive element. The process most relevant to us, at this stage of scientific system development, is that of feedback, a process by which our hypotheses, ideas, findings or realities are brought into the system, confronted with the ideas ruling the system from the inside and with the purpose guiding it from the outside, and either absorbed by and integrated within the system, renewing and enriching it, or rejected.

But it is not necessary to wait for a full-fledged science to be developed before delivering the knowledge that already exists in the form of a graduate university program. While it is true that a graduate program is given legitimacy in the eyes of a university by the existence of a substantial body of knowledge in a well defined area, it is equally true that the development of such a body of knowledge is the consequence of the existence of a graduate program that educates both professionals and scholars in conducting ongoing theoretical and applied research. Thus, it is possible to start now in a small way, but "thinking big" and maintaining our focus on the ultimate goal.

At this stage of development of the body of knowledge of a Digital Records Forensics Science, we have established that its theory, methodology and practice would mostly derive from:

- The Law of Evidence, which rules the whole system from outside and provides its purpose;
- Diplomatics (and specifically Digital Diplomatics), which embodies the theory of the record;
- Digital Forensics, which comprises the core methodology related to the acquisition, analysis and evaluation of digital evidence and the related practices;
- Archival Science, which provides the theoretical and methodological knowledge related to recordkeeping and long term preservation;
- Information Technology, which offers the necessary understanding of systems concepts, computer architecture, computer network communication, discrete mathematics, database design, algorithms and data structures, imperative programming, mark-up languages, and end-user programming tools; and
- Organizational Information Assurance, a relatively new field that examines concepts, elements, strategies, skills related to the life cycle of information assurance -- involving policies, practices, mechanisms, dissemination and validation -- that ensure the confidentiality, integrity, availability, authentication and non-repudiation of information and information systems (Endicott-Popovsky and Frincke, 2005a, 2004).

It will be necessary to develop one new course to provide the intellectual framework, but existing courses in each of these disciplines can be used to build up an interdisciplinary program across faculties.

The Digital Records Forensics Project began two years ago with the objectives of producing much needed new knowledge and creating dedicated graduate programs of education delivering it. The research conducted to date has demonstrated the need for Digital Records Forensics specialised knowledge among several different professions: digital forensics experts, lawyers, law enforcement officers, judges, court clerks, records managers, archivists, systems designers, etc. In addition, the research has shown that, in light of recent court decisions that have increased the length of retention of digital evidence used in trials, in some cases requiring permanent retention, long term digital preservation has become a major issue, to the point that recordkeeping and archival knowledge must become part of the intellectual armour of every professional responsible for digital evidence. That the type of educational program we envision would produce a professional in high demand in a variety of environments has been abundantly demonstrated to our research team by the responses given in the course of our interviews by judges, lawyers, court services administrators, and last, but definitely not least, digital forensics specialists and members of forensics units within police departments. As Mark Johnstone, Sergeant, Forensics Services Division, Financial Crime Unit, Vancouver Police Department, put it, “people need to understand what exactly a record is. And then understand the manner in which it’s maintained. So you’d have to have the knowledge of what it is you’re trying to maintain and then the knowledge of the systems that are maintained. So, yes, there’s some very specific knowledge needed” (transcript of interview, part 2 of 2, 12-09-2009). It is our hope that, in the next year, we will have moved quite far in reaching our goals and will have earned the support of all forensics professions for establishing a Digital Records Forensic science in academia, in whatever form will be most appropriate and useful.

6. REFERENCES

Ansani, M. (1999), “Diplomatica (e diplomatisti) nell’arena digitale.” *Scrineum* (1): 1-11.

Arkfeld, M. R. (2002-2006), *Electronic Discovery and Evidence*. Law Partner Publishing, LLC. Phoenix, Arizona.

Boucher, K., and Endicott-Popovsky, B. (2008), "Digital Forensics and Records Management: What We can Learn from the Discipline of Archiving." In *Proceedings of Information Systems Compliance and Risk Management Institute.* Seattle, WA: University of Washington.

British Columbia Electronic Evidence Project. (2006). Available at http://www.courtsgov.bc.ca/sc/ElectronicEvidenceProject/ElectronicEvidenceProject.asp.

Canada Evidence Act, R.S.C. 1985, c. C-5 as am.

Canadian General Standards Board, (2005). *Electronic Records as Documentary Evidence* (CAN/CGSB-72.34).

Carolus Molineus (Charles Du Moulin), *In regulas Cancellariae Romanae Hactenus in Regno Franciae receptas commentarius analyticus*, Lugduni, 1552. After many editions and additions, the work was published again in Paris with the title *Caroli Molinaei Opera quae extant omnia*, Lutetiae Parisiorum sumptibus N. Buon, 1612.

Carrier, B. (2005), *File System Forensic Analysis*. New York: Addison-Wesley.

_____. (2002), "Open Source Digital Forensics Tool. The Legal Argument," available at http://www.digital-evidence.org/papers/opensrc_legal.pdf.

Casey, E. (2002), "Error, uncertainty and loss in digital evidence," *International Journal of Digital Evidence* 1. 2.

_____. (2004), *Digital Evidence and Computer Crime*. Maryland Heights, MO: Academic Press.

_____. (2007), "Digital evidence maps-a sign of the times." *Digital Investigations* 4 (1-2): 1-2.

Consultative Committee for Space Data Systems (2002), *Reference Model for an Open Archival Information System (OAIS)*. Blue Book, Issue 1 (Washington, D.C.: CCSDS Secretariat). Available at http://public.ccsds.org/publications/archive/650x0b1.pdf.

Cox, R. (2006), *Ethics, Accountability, and Recordkeeping in a Dangerous World*. London, UK: Facet Publishing.

Crowley, C. Esq., (2007), Labaton Sucharow & Rudoff LLP and Sherry B. Harris, Hunton & Williams LLP eds., *The Sedona Conference Glossary: E-Discovery and Digital Information Management,* second edition. Available on line at http://www.thesedonaconference.org/dltForm?did=TSCGlossary_12_07.pdf.

Department of Defense (2002), *DoD 5015.2 STD, Design Criteria Standard for Electronic Records Management Software Applications*. Available at http://jitc.fhu.disa.mil/recmgt/standards.html (DoD 5015.2-STD, dated April 2007).

Digital Forensics Research Workshop (2001). Available at http://www.dfrws.org/2001/dfrws-rm-inal.pdf, p. 16.

Digital Records Forensics Project (2008-2011). Available at http://www.digitalrecordsforensics.org/index.cfm.

Duff, W. M., Marshall, A., Limkilde, C. and van Ballegooie, M. (2006), "Digital Preservation Education: Educating or Networking?" *The American Archivist* (69): 188-212.

Duranti, L. (1996), "Archival Science," in *Encyclopedia of Library and Information Science*. Allen Kent ed., vol. 59. New York, Basel, Hong Kong: Marcel Dekker, INC., 1-19.

_____. (1998), *Diplomatics: New Uses for an Old Science*. Lanham, Maryland, and London: Scarecrow Press, with Society of American Archivists and Association of Canadian Archivists.

_____. ed. (2005), *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*. San Miniato, IT: Archilab.

_____. (2009a), "Diplomatics," in *Encyclopedia of Library and Information Science*. Marcia Bates, Mary Niles Maack, Miriam Drake eds. New York, Basel, Hong Kong: Marcel Dekker, INC.

_____. (2009b), "From Digital Diplomatics to Digital Records Forensics," *Archivaria* (68): 39-66.

Duranti, L. and MacNeil, H. (1997), "The Preservation of the Integrity of Electronic Records: an Overview of the UBC-MAS Research Project." *Archivaria* (42): 46-67.

Duranti, L., Eastwood, T. and MacNeil, H. (2002), *The Preservation of the Integrity of Electronic Records*. Dordrecht: Kluwer Academic Publishing-.

Duranti, L. and Thibodeau, K. (2006), "The Concept of Record in Interactive, Experiential and Dynamic Environments: the View of InterPARES." *Archival Science* (6): 13-68.

Duranti, L. and Preston, R. eds. (2008), "A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-Term Preservation of Digital Records," in *InterPARES 2: Interactive, Dynamic and Experiential Records*. Padova, ANAI. http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_appendix_19.pdf.

Duren and Hosmer, C. (2002), "Can digital evidence endure the test of time?" *Proceedings of the Second Digital Forensic Research Workshop 2002*.

Electronic Transactions Act, S.B.C. 2001, c. 10.

Endicott-Popovsky, B., Frincke, D. and Taylor, C. (2007), "A Theoretical Framework for Organizational Network Forensic Readiness." *The Journal of Computers*, 2 (3), 1-11.

Endicott-Popovsky, B. and Frincke, D. (2007a), "Embedding Hercule Poirot in Networks: Addressing Inefficiencies in Digital Forensic Investigations." In *Proceedings of the Human Computer Interface (HCI) Conference.* Beijing, China, pp. 364-372.

_____. (2006), "Embedding Forensic Capabilities into Networks: Addressing Inefficiencies in Digital Forensics Investigations." In *Proceedings from the 7th IEEE Systems, Man and Cybernetics Information Assurance Workshop.* West Point, NY: United States Military Academy, pp.133-139.

Endicott-Popovsky, B, Ryan, D. and Frincke, D. (2005), "The New Zealand Hacker Case: A Post Mortem." In *Proceedings of the Safety and Security in a Networked World: Balancing Cyber-Rights & Responsibilities Conference*. Oxford, England: Oxford Internet Institute. Available at http://www.oii.ox.ac.uk/research/cybersafety/?view=papers.

Endicott-Popovsky, B.E. and Frincke, D. (2005a), "Redefining Computer Security to Include Forensics." Presented at 8th *Annual Recent Advances in Intrusion Detection (RAID) Conference*, Seattle, WA.

_____. (2004), "Adding the Fourth "R."" In *Proceedings of the 5th IEEE Systems, Man and Cybernetics Information Assurance Workshop*. West Point, NY: United States Military Academy, pp.442-443.

European Commission (2008), *Model Requirements for the Management of Electronic Records (MoReq2)*. Available at http://www.project-consult.net/Files/MoReq2_body_v1_0.pdf.

Farmer, D. and Venema, W. (2004), *Forensic Discovery*. New York: Addison-Wesley.

Fritsch, A. (1664), *De iure archivi et cancellariae*, Jenae.

Gahtan, A. M. (1999), *Electronic Evidence.* Ontario, CA: Carswell Thomson Professional Publishing.

Galves, F. and Galves, C. (2004), "Ensuring the Admissibility of Electronic Forensic Evidence and Enhancing Its Probative Value at Trial," *Criminal Justice Magazine*, 19:1.

Ghirardini, A. and Faggioli, G. (2007), *Computer Forensics.* Apogeo: Milano.

Guidelines for the Discovery of Electronic Documents (Ontario) (2005), Available at http://www.commonwealthlegal.com/pdf/E-DiscoveryGuidelinesOct2005.pdf.

Iacovino, L. (2005), *Recordkeeping, Ethics and Law. Regulatory Models, Participant Relationships and Rights and Responsibilities in the Online World.* Dordrecht: Springer.

International Council on Archives, ICA (2008), *Principles and Functional Requirements for Records in Electronic Office Environments. Module 1. Overview and Statement of Principles.* Paris: ICA, Module 1. Available at http://www.ica.org/en/node/38972.

_____. (2008), *Principles and Functional Requirements for Records in Electronic Office Environments. Module 2. Guidelines and Functional Requirements for Electronic Records Management Systems.* Paris: ICA, Module 2. Available at http://www.ica.org/en/node/38970.

_____. (2008), *Principles and Functional Requirements for Records in Electronic Office Environments. Module 3. Guidelines and Functional Requirements for in Business Systems.* Paris: ICA, Module 3. Available at http://www.ica.org/en/node/38968.

InterPARES Project (1999-2012). Available at www.interpares.org.

Irons, A. (2006), "Computer Forensics and Records Management-compatible disciplines." *Records Management Journal* vol. 16, no. 2: 102-112.

Irons, A.D., Stephens, P. and Ferguson, R.I. (2009), "Digital Investigation as a distinct discipline: A pedagogic perspective." *Digital Investigation* 6: 82-90.

Jenkinson, H. (1980), "The English Archivist: A New Profession," in *The Selected Writings of Sir Hilary Jenkinson.* Gloucester.

Justinian (1529-1565), *Corpus Juris Civilis, Novella 15* "De Defensoribus civitatum," "Et a defensoribus," *Digestum 48, no. 19* "De Poenis," *Codex I, no. 4* "De episcopali audientia."

Kenneally, E. (2001), "Gatekeeping Out Of The Box: Open Source Software as a Mechanism to Assess Reliability for Digital Evidence," *Virginia Journal of Law and Technology*, vol. 6, no. 3 , http://www.vjolt.net/vol6/issue3/v6i3-a13-Kenneally.html (accessed on 10 October 2010).

Kent, K., Chevalier, S., Grance, T. and Dang, H., National Institute of Standards and Technology Special Publication 800-86, Technology Administration, U.S. Department of Commerce. (2006), *Guide to Integrating Forensic Techniques into Incident Response: Recommendations of the National Institute of Standards and Technology.* Available at http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

Landwehr, C.E. (2001), "Computer security," *International Journal of Information Security,* 1: 3-13.

Lodolini, E. (1991), *Lineamenti di storia dell'archivistica italiana. Dalle origini alla metà del secolo XX*, La Nuova Italia Scientifica, Roma.

_____. (1987), *Archivistica, Principi e Problemi.* Franco Angeli, Milano.

MacNeil, H. (2000), "Providing Grounds for Trust: Developing Conceptual Requirements for the Long-Term Preservation of Authentic Electronic Records." *Archivaria* (50): 52-78.

_____. (2001), "Trusting Records in a Postmodern World." *Archivaria* (51): 36-47.

_____. (2002), "Providing Grounds for Trust II: The Findings of the Authenticity Task Force of InterPARES." *Archivaria* (54): 24-58.

_____. (2004), "Contemporary Archival Diplomatics as a Method of Inquiry: Lessons Learned from Two Research Projects." *Archival Science* 4: 199-232.

Mocas, S. (2004), "Building theoretical underpinnings for digital forensics research," *Digital Investigation*, 1:1: 62. Available at www.elsevier.com/locate/diin.

Nance, K., Armstrong, H. and Armstrong, C. (2010), "Digital Forensics: Defining an Education Agenda." In *Proceedings of the 43rd Hawaii International Conference on System Sciences.* Hawaii.

Nevins, T., Narvaez, J., Marriott, W. and Endicott-Popovsky, B. (2008), "Data Classification and Binding: Models for Compliance." In *Proceedings of Information Systems Compliance and Risk Management Institute*. Seattle, WA: University of Washington.

Palmer, V. (2010), "BC Rail controversy turns record keeping into a hot topic." *The Vancouver Sun* January 29: A3.

Paul, G. (2008), *Foundations of Digital Evidence*. Chicago: American Bar Association, 2008.

Pollitt, M. and Shenoi, S. eds. (2005), *Advances in Digital Forensics: IFIP International Conference on Digital Forensics WG 11.9, National Center for Forensic Science, Orlando, Florida*. New York: Springer.

Rice, P. R. (2005). *Electronic Law of Evidence and Practice.* Chicago: American Bar Association Publishing.

Supreme Court of British Columbia. (2006), *Practice Direction Re: Electronic Evidence*. Available at http://www.courts.gov.bc.ca/sc/ElectronicEvidenceProject/ElectronicEvidenceProject.asp.

Tan, J. (2001), *Forensic Readiness*, Cambridge, MA: @Stake. Available at http://stake.com/research/reports/acrobat/atstake_forensic_readiness.pdf.

Taylor, C., Endicott-Popovsky, B. and Frincke, D. (2007), "Specifying Digital Forensics: A Forensics Policy Approach." In *Proceedings of the 7th Digital Forensic Research Workshop*, Pittsburgh, PA, pp. 101-104.

The Sedona Conference Working Group Series. (2007), *The Sedona Principles: Second Edition. Best Practices Recommendations & Principles for Addressing Electronic Document Production, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)*. Jonathan M. Redgrave, ed. Available at http://www.thesedonaconference.org/content/miscFiles/TSC_PRINCP_2nd_ed_607.pdf.

Tibbetts, J. (2010), "Internet Case may have 'chilling' effect: expert," *The Vancouver Sun*, April 2: B2.

UKOLN (2003), "Open Source Software for Digital Repositories: DSpace and Fedora." Available at http://www.ukoln.ac.uk/metadata/resources/digital-repositories/.

Zatyko, K. (2007), "Commentary: Defining Digital Forensics." *Forensic Magazine* (Feb/March): 1-5.