JDFSL

The Journal of Digital Forensics, Security and Law

Volume 5, Number 2
2010

JDFSL

The Journal of Digital Forensics, Security and Law

Volume 5, Number 2

2010

Editors

ISSN 1558-7215

Call for Papers

The Journal of Digital Forensics, Security and Law is now calling for papers in, or related to, the following areas:

1) Digital Forensics Curriculum
2) Cyber Law Curriculum
3) Information Assurance Curriculum
4) Digital Forensics Teaching Methods
5) Cyber Law Teaching Methods
6) Information Assurance Teaching Methods
7) Digital Forensics Case Studies
8) Cyber Law Case Studies
9) Information Assurance Case Studies
10) Digital Forensics and Information Technology
11) Law and Information Technology
12) Information Assurance and Information Technology

To be considered for inclusion in the 4th issue of the 2010 volume of the Journal of Digital Forensics, Security and Law, manuscripts should be submitted prior to midnight October 31, 2010.

Guide for Submission of Manuscripts

All manuscripts should be word-processed (letter or correspondence-quality font). If the paper has been presented previously at a conference or other professional meeting, this fact, the date, and the sponsoring organization should be given in a footnote on the first page. Funding sources should be acknowledged in the "Acknowledgements" section. Articles published in or under consideration for other journals should not be submitted. Enhanced versions of book chapters can be considered. Authors need to seek permission from the book publishers for such publications. Papers awaiting presentation or already presented at conferences must be significantly revised (ideally, taking advantage of feedback received at the conference) in order to receive any consideration.

Manuscripts should be submitted through the JDFSL online system in Word format using the following link: http://www.jdfsl.org/submission.asp.

Manuscripts may also be submitted to the editor in Word format as well. The editor of the JDFSL, Dr. Glenn S. Dardick, may be reached via email at editor@jdfsl.org.

The copyright of all material published in JDFSL is held by the Association of Digital Forensics, Security and Law (ADFSL). The author must complete and return the copyright agreement before publication. The copyright agreement may be found at http://www.jdfsl.org/copyrighttransfer.pdf.

Additional information regarding the format of submissions may be found on the JDFSL website at http://www.jdfsl.org/authorinstructions.htm.

Contents

Digital Records Forensics: A New Science and Academic Program for Forensic Readiness

Luciana Duranti
School of Library, Archival and Information Studies
The University of British Columbia
IKBL 470, 1961 East Mall
Vancouver, British Columbia V6T 1Z1 CANADA
e-mail: luciana.duranti@ubc.ca

Barbara Endicott-Popovsky
Center for Information Assurance and Cybersecurity
University of Washington
4311 11th Ave NE Suite 400 Box 354985
Seattle, Washington 98105
e-mail: endicott@u.washington.edu

ABSTRACT

This paper introduces the Digital Records Forensics project, a research endeavour located at the University of British Columbia in Canada and aimed at the development of a new science resulting from the integration of digital forensics with diplomatics, archival science, information science and the law of evidence, and of an interdisciplinary graduate degree program, called Digital Records Forensics Studies, directed to professionals working for law enforcement agencies, legal firms, courts, and all kind of institutions and business that require their services. The program anticipates the need for organizations to become "forensically ready," defined by John Tan as "maximizing the ability of an environment to collect credible digital evidence while minimizing the cost of an incident response (Tan, 2001)." The paper argues the need for such a program, describes its nature and content, and proposes ways of delivering it.

Keywords: digital records, records authenticity, graduate education, record theory, records forensics science, records forensic discipline, forensic readiness, Digital Records Forensics, digital preservation

1. INTRODUCTION

Two of the most challenging issues presented by digital technology to the law enforcement, records management, archival and legal professions, researchers, business, government and the public are the identification of "records" among all the digital objects produced by complex dynamic and interactive systems, and the determination of their "authenticity." The first issue—the identification of digital records—is addressed by Digital Diplomatics, a contemporary development of a

centuries-old discipline that studies the nature, genesis, formal characteristics, structure, transmission and legal consequences of records (Duranti, 1996, 1998). The second issue—the assessment of the authenticity of digital records—is only indirectly addressed by Digital Forensics, 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).

The determination of the authenticity of individual medieval records of questionable provenance was the original reason for the development, in the 17th century, of the science of Diplomatics, and, in the context of the development of a Digital Diplomatics, its theory and methods have been successfully applied to contemporary digital records (Duranti, 2009a, Duranti, 2005; Duranti and MacNeil, 1997; Duranti, Eastwood and MacNeil, 2002; Duranti and Thibodeau, 2006). 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 of Evidence 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.

2. THE DIGITAL RECORDS FORENSICS PROJECT

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 and the hearsay rules. 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. 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).

At common law, to be admissible, records must constitute the "best evidence." The best evidence rule requires that the original of any document, regardless of medium or form (e.g., a letter, a recording), be used as evidence at trial. A copy will be allowed into evidence only if the original is unavailable for a legitimate reason. However, in the digital environment, we no longer have originals. In fact, we cannot keep digital records. We can only maintain our ability to reproduce or even to re-create them as needed. As a consequence, the authenticity of digital records is difficult to establish on the records themselves and becomes an inference that one draws regarding the integrity of the system (*Electronic Transactions Act (B.C.),* s. 8, 2001; *Canada Evidence Act*, s. 31.2(1), 1985).

Nevertheless, the law requires that an authentication of the record submitted as evidence is made by a competent third party who either recognizes the record, if it is an original, having seen it before, or provides an expert opinion on its

authenticity. Traditionally, archivists have been able to provide the needed expertise, but their body of knowledge is inadequate to assess the authenticity of digital records and would profit from an understanding of the methods Digital Forensics uses to analyze and evaluate the environment in which the records existed. In turn, Digital Forensics methods will not only benefit from, but be extraordinarily enriched by Digital Diplomatics, which has established very sophisticated methods for assessing record trustworthiness and developed a strong conceptual model of an authentic record rooted in jurisprudence, administrative history and theory, and on recordkeeping practices in bureaucratic organizations (MacNeil, 2004). This model is especially important for answering questions about the authenticity of digital records extracted from their original environment and about procedures for extracting records so that their identity and integrity can be maintained intact, thus allowing them to be later authenticated.

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; 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 digital records they produce will be relied upon as evidence in civil and criminal trials, thus necessitating advanced preparation to ensure admissibility (Nevins, et.al., 2008; Endicott-Popovsky, et.al. 2007, 2005, Endicott-Popovsky and Frincke 2007a, 2006, Taylor, et.al., 2007). InterPARES recommendations and guidelines ensure that it will be possible to preserve authentic copies of these records permanently.

The additional problem that needs to be addressed, using the knowledge of digital records trustworthiness developed by the InterPARES project and the new concepts and methods of Digital Diplomatics derived from it, is that presented by records that have been extracted from the system in which they were generated and/or maintained either by the creating body itself or by third parties, such as police departments or archival organizations or units. These records may have been removed from the original system and placed on portable media by the creator for storage elsewhere, 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).

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.

2.1 Relevant Scholarly Literature

The legal profession has been fully aware of the problems presented by documentary evidence in digital form for a long time, to the point that a dedicated group of legal experts, the Sedona Conference, has already issued two editions of principles to be followed in the production of digital records, realizing, along with the InterPARES project and the archival profession at large (International Council on Archives, 2008; European Commission, 2008), that the key to having trustworthy record sources is to generate them according to specific authenticity requirements and maintain them in the correct way throughout their existence (Sedona Conference Working Group Series, 2007). However, this does not solve the problem of documentary evidence that has already been created in systems that do not satisfy authenticity requirements, especially if it no longer resides in the original system or in any system at all, having been stored in external media. This is a major issue for the law enforcement and legal professions, and the judiciary, as demonstrated by the large number of scholarly writings on the subject (Gahtan, 1999; Arkfeld, 2002-2006; Rice, 2005). The judiciary has tried to address the problem by specifying minimum requirements for admissible digital evidence and by providing guidelines for meeting these requirements, but has not provided guidelines for assessing material that does not obviously correspond to the requirements (British Columbia Electronic Evidence Project, 2006; Guidelines for the Discovery of Electronic Documents, 2005, Supreme Court of B.C., 2006). Digital Forensics does not focus on the documentary evidence per se, but on the environment of its creation and maintenance, regardless of the efforts made by scholars in the field to find appropriate methods

to assess the digital entities themselves (Casey, 2004; Carrier, 2005; Pollit and Shenoi, 2005).

The importance of using Diplomatics to acquire an understanding of digital entities as records and assess their authenticity on the basis of their characteristics is widely recognized by archival and diplomatic scholars (Bearman, 1992 and 2006; Barbiche, Blouin, Delmas, Delmas and Blouin, Guyotjeannin, 1996; Ansani 1999; Guyotjeannin, 2002, 2003). Standards developing bodies, like the Canadian General Standards Board, have attempted to address these needs by issuing requirements based on archival concepts (CAN/CGSB-72.34—2005), and scholarly archival literature on the subject has pointed out the pitfalls of leaving such responsibility to legislators rather than to researchers (Iacovino, 2005; Cox, 2006). Very recently, archival educators have recognized that education on digital records requires the contribution of a variety of disciplines and professional fields (Duff, Marshall, Limkilde and van Ballegooie, 2006). As well, writers on digital forensics have identified the need for interdisciplinarity in the formal programs aiming to educate professionals in their field (Irons, 2006; Boucher and Endicott-Popovsky, 2008; Irons, Stephens and Ferguson, 2009; Casey 2007; Nance, Armstrong and Armstrong, 2010). This requirement has also been amply demonstrated by a plethora of research projects on digital preservation, all of them inter- or multi-disciplinary (e.g. ERPANET, www.erpanet.org; Digital Curation Centre (DCC), www.jisc.ac.uk; Digital Preservation Europe, www.digitalpreservationeurope.eu; CASPAR, www.casparpreserves.eu; and, mostly, InterPARES, www.interpares.org, which is the only digital preservation project entirely focused on records).

All these digital preservation projects have identified the evidentiary issues discussed earlier, but have not dealt with them—their priority being long-term preservation of aggregations of materials—and have not included digital forensics knowledge in their research. However, some of the concepts developed by the InterPARES project constitute the necessary foundation for understanding digital documentary evidence, assessing its record nature and determining its authenticity, including the concepts of 'formal record elements' versus 'attributes' and 'digital components,' 'accuracy' versus 'authenticity,' 'digital authentic copy,' 'fixed form' versus 'bounded variability,' 'manifested record' versus 'stored record,' and 'instructive record' versus 'enabling record;' all of which will support the determination of what constitutes a record among the various digital entities extracted from computer systems, and of which instance or manifestation of those entities has the force of an original and can be assessed as authentic. Traditionally, police evidence rooms and public archives have implicitly guaranteed that the records kept by them are as authentic as they were when first acquired, but this presumption is no longer tenable for digital documentary evidence; thus, it is essential to develop procedures that can reassure the public and the court system that no undetectable manipulation of such evidence can occur throughout the time of its maintenance, especially when the keeping of the

evidence is entrusted to one of the parties having a stake in it (i.e. the police).

2.2 Methodology

To develop a Digital Records Forensics science, the research team has conducted an in depth literature review and developed a data base of annotated writings from all the areas of knowledge covered by the research (see http://www.digitalrecordsforensics.org/drf_biblio_db.cfm). This database serves as a fundamental resource for the research program, and will be continuously enriched and maintained as a resource for the education program under development. At the same time, the team has built a data base of case law related to the issues identified above, such as authenticity, integrity, recordness, etc. (not yet accessible to non team members); and a terminology database which aims at defining the key terms for the project in each of the disciplines involved, and indicating the preferred definition in the context of the Digital Records Forensics area of knowledge (in progress, but available at http://www.digitalrecordsforensics.org/drf_term_db.cfm). From this accumulated knowledge, the team has developed an activity model of the digital records forensics processes, and prepared separate questionnaires for semi-structured interviews of digital forensics experts, law enforcement officers, records managers for law enforcement departments, court clerks, lawyers and judges (see http://www.digitalrecordsforensics.org/drf_questionnaires.cfm). The purpose of the interviews is to discover what are the criteria that these professions consider to be the basis for determining the trustworthiness of digital evidence, what methods they believe must be used to maintain digital evidence trustworthy from the moment they start interfering with its original digital environment, and what kind of education program would best serve the needs of Digital Records Forensics experts. To date we have conducted more than fifty interviews. A web administered questionnaire aimed at establishing shared beliefs about the fundamental means of establishing and maintaining digital record trustworthiness and discovering the gaps and the problematic areas in existing digital forensics knowledge will target members of the digital forensics, law and records professions, and selected members of the public (e.g., journalists and scholars).

The research team is also conducting ethnographic investigations involving the examination of the forensic and recordkeeping procedures of the Vancouver Police Department (VPD), which is our test bed partner. In addition, graduate students under the direction of the team's experts in the Law of Evidence and in Digital Forensics are examining and describing the hierarchy for policy changes and decision-making, the current court procedures governing the admission of digital evidence, and the problems noted by the personnel responsible for digital evidence. The team is using the preliminary findings from the interviews as points of reference for studying the environment and as the basis for their discussions with the professionals working at the VPD. The graduate students, under the supervision of the researchers from the VPD, are also examining the digital

evidence identified as records preserved by the VPD, which, in the view of the Department itself, is problematic for various reasons (e.g., unreadable because of obsolescence; produced in a legacy system no longer available; of unknown lineage). Inspection of the material is conducted using the analytical methods of all disciplines involved in this research program. Solutions to the identified problems will be implemented on copies of the material and tested in light of the Law of Evidence. As needed, the team will elaborate on existing concepts and procedures or develop new ones. As both the ethnographic approach and the case studies constitute action research, the team collaborates with the subjects of the investigation, who are co-participants and stakeholders, to develop together practical methods and new knowledge. The team will synthesize its findings into structured content for a Digital Records Forensics science as part of a proposal for a new interdisciplinary program of graduate education in Digital Records Forensics Studies.

3. THE DIGITAL RECORDS FORENSICS BODY OF KNOWLEDGE

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.

An example of the process described above can bee seen in an article aiming at comparing the concepts of Digital Diplomatics with those of Digital Forensics (Duranti, 2009b). As mentioned earlier, Digital Diplomatics is really a branch of Diplomatics, rather than a separate discipline, developed as a result of the application of the knowledge of the latter to the analysis of digital records (Duranti, 2009a). The article discusses the concepts of trusted custodian, digital record, reliability, authenticity, accuracy, integrity, etc. from the perspective of both fields, and the methods of identification and analysis used by each, showing

the similarities and the divergences and identifying the areas in which each can benefit from the other. In the course of this comparison, also the perspective of the law of evidence in North America is kept into account. It is very important to continue this type of investigation to develop a Digital Records Forensics science that can form the core of an academic program for digital records forensics professionals.

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.

4. A DIGITAL RECORDS FORENSICS GRADUATE PROGRAM

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).

How can this body of knowledge be delivered in the context of a graduate program without having to establish at the outset a full fledged degree in Digital Records Forensics? In one example that the Master of Archival Studies at the University of British Columbia and the School of Information at the University of Washington are pursuing at this time, the two schools would make an agreement according to which the students enrolled in the Master of Archival Studies take a semester in the School of Information receiving credit for their courses in their home program, and vice versa. The combination of courses would encompass the entire body of knowledge outlined above and the University of British Columbia students would receive a Master of Archival Studies degree with specialization in Digital Records Forensics, while the students of the University of Washington would have the same specialization attached to a Master of Information.

It will be necessary to develop one new course in one of the two programs to provide the intellectual framework for the specialization, and to adjust some of the course content in both, but this collaboration offers an opportunity for testing the viability of a graduate program in Digital Records Forensics, proving to universities that there is a demand for such a program, and developing an integrated body of knowledge on which to build innovative, original knowledge. This can happen because such a program would be based on the three educational principles already shared by the two programs contributing to it: 1) professionals must be educated in the core theoretical and methodological knowledge that identifies their profession; 2) they must be educated in international standards as well as in the specific, local and unique aspects of the juridical-administrative environment in which they will work; and 3) they must be educated in the scholarly as well as the practical nature of their work.

The third of these principles is the most important for university programs. Research is a critical component of a graduate level program, because it is an expression of the intellectual nature of the study, the scholarly substance of the work that professionals do, and the status of the program with respect to other graduate programs. Several course offerings can enable students to engage in scholarly enquiry of various kinds, from the thesis to directed research projects involving in-depth investigation of a specific issue or problem. Moreover, it is a requirement for every faculty member to conduct scholarly research and granting agencies are more than willing to provide funds for the participation of graduate students in research, thus, they may work as paid research assistants on faculty members' research projects. It will be this engagement in research that will produce new knowledge and support the creation of dedicated full-fledged programs in Digital Records Forensics.

However, in a Master's level program, the cultivation of research skills must be balanced with the development of professional knowledge. Accordingly, it is important to inculcate in students engaged in research a sense of the relevance of their investigations to their professional lives. This is why the study of research

methods should be a required component of any program of education, as it will equip students with the knowledge necessary not only to produce new knowledge, but also to understand and interpret research conducted by others.

Graduate programs are judged to a significant degree by the quality and quantity of the research produced by faculty and students, thus, expanding the opportunities for research is vital to their success and growth. Students benefit enormously from the opportunities research projects provide for acquiring research skills and contributing to the advancement of disciplinary knowledge. Once the students graduate and begin their working lives, the knowledge and experience they have gained through their participation in research translates into a benefit to the institutions and organizations that employ them.

Talking of the practical component of such a graduate program, it is important to emphasize that experiential learning in the context of the education of professionals is not an exercise to discover theory and methods empirically. Its main purpose is to provide future professionals with a way of applying the theoretical and methodological knowledge learned in class and testing it in the professional arena. This is the best way of demonstrating to the students that theory and practice feed each other and neither could have value without the other. Recently, some programs have introduced co-operative work experience opportunities for their students. Co-operative education is a learning method that, through pre-employment workshops, coaching by career specialists, and workplace experiences, offers students the opportunity to combine real world experience with their classroom education and develop employment skills specific to the records professions. Simply stated, universities and employers co-operate to provide students with an opportunity to learn in a workplace setting by alternating practical, paid work experience in various fields of interest with their academic studies. Most importantly, at this stage of program development, the practical experience would allow digital records forensics students and their professors to assess the value of their education, to identify gaps, and to work towards a course and curriculum development that better serves the needs of professionals. At the same time, the students and their program of education would be visible to professionals, who will appreciate the value of both and generate the demand required by universities to support such programs.

5. CONCLUSION

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 the digital forensics profession 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.

Barbiche, B. (1996), "Diplomatics of Modern Official Documents (Sixteenth-Eighteenth Centuries): Evaluation and Perspectives." *American Archivist* (59): 422-436.

Bearman, D. (1992), "Diplomatics, Weberian Bureaucracy and the Management of Electronic Records in Europe and America." *American Archivist* (55): 168-81.

_____. (2006), "Moments of Risk: Identifying Threats to Electronic Records." *Archivaria* (62): 15-46.

Blouin, F. (1996), "A Framework for Consideration of Diplomatics in the Electronic Environment." *American Archivist* (59): 466-479.

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).

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

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

Casey, E. (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.

Delmas, B. (1996), "Manifesto for a Contemporary Diplomatics: From Institutional Documents to Organic Information." *American Archivist* (59): 438-452.

Delmas, B. and Blouin F. (1996), "De la diplomatique medievale a la diplomatique Contemporaine. Actes du colloque organise par l'Ecole nationale des chartes et la Bentley historical Library de l'universite de Ann-Arbor (Michigan, Etat-Unis). Paris, 6-10 Juillet 1992 et Ann-Arbor, 5-9 juillet 1993." *La gazette des archives* (172): 7-106. [Also in *American Archivist* 59]

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.

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., 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.

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

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

Guyotjeannin, O. (1996), "The Expansion of Diplomatics as a Discipline." *American Archivist* (59): 414-21.

Guyotjeannin, O. ed. (2002), "Exportations de la diplomatique, I, Mondes anciens." *Bibliothèque de l'École des chartes* (160): 475-564.

Guyotjeannin, O. ed. (2003), "Exportations de la diplomatique, II, Documents contemporains." *Bibliothèque de l'École des chartes* (161): 493-623.

Iacovino, L. (2005), *Recordkeeping, Ethics and Law*. *Regulatory Models, Participant Relationshipsand 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

International Council on Archives, ICA (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

International Council on Archives, ICA (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., P. Stephens, R.I. Ferguson. (2009), "Digital Investigation as a distinct discipline: A pedagogic perspective." *Digital Investigation* 6: 82-90.

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.

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

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

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

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

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.

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.

Taylor, C., Endicott-Popovsky, B., and Frincke, D. (2007), "Specifying Digital Forensics: A Forensics Policy Approach." I*n 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.

Subscription Information

The Journal of Digital Forensics, Security and Law (JDFSL) is a publication of the Association of Digital Forensics, Security and Law (ADFSL). The Journal is published on a non-profit basis. In the spirit of the JDFSL mission, individual subscriptions are discounted. However, we do encourage you to recommend the journal to your library for wider dissemination.

The journal is published in both print and electronic form under the following ISSN's:

ISSN: 1558-7215 (print)

ISSN: 1558-7223 (online)

Subscription rates for the journal are as follows:

Institutional - Print & Online: $395 (4 issues)

Institutional - Online only: $295 (4 issues)

Individual - Print & Online: $80 (4 issues)

Individual - Online only: $25 (4 issues)

Subscription requests may be made to the ADFSL.

The offices of the Association of Digital Forensics, Security and Law (ADFSL) are at the following address:

Association of Digital Forensics, Security and Law
1642 Horsepen Hills Road
Maidens, Virginia 23102
Tel: 804-402-9239
Fax: 804-680-3038
E-mail: office@adfsl.org
Website: http://www.adfsl.org