Memory Forensics: Integrating Digital Forensics with Archival Science for Trusting Records and Data

Luciana Duranti
University of British Columbia

Corinne Rogers
University of British Columbia

Abstract. Both archival and digital forensics methods and principles evolved out of practice and grew into established professional disciplines by developing theoretical foundations, which then returned to inform and standardize that practice. Digital Records Forensics is a new discipline arising from the intersection of digital forensics and archival science to identify records in digital systems, assess their authenticity, and establish the requirements for their long-term preservation. This paper introduces areas of convergence between digital forensics and archival preservation activities in order to understand moments in which digital records as understood by archival science, and digital evidence as understood by digital forensics, may be identified, their authenticity assessed, their reliability and integrity managed and preserved. The paper shows how digital forensics can enhance archival science and practice, and how the integration of archival theory of records and archives can further develop digital forensics as a discipline and help it in accomplishing its purposes.

Keywords: Archival science, InterPARES, digital forensics, digital records forensics, digital forensics models, digital evidence

What you will learn: Readers will be introduced to the concepts of archival diplomatics made explicit in the Chain of Preservation model of record creation, maintenance and preservation, and links these concepts to concepts of digital forensic investigation.

What you should know: Basic familiarity with archival theory would be helpful, but is not essential. Readers should know the principles of digital forensics.

1 Introduction

Trusting the reliability and assessing the authenticity of digital files, records, documents and data is critical for law enforcement and security professionals, archivists and records managers, and all kinds of organizations and individuals. Digital forensics practitioners are tasked with finding, securing, and analyzing such material in an increasing variety of contexts. While digital forensics excels at collecting, preserving, transporting, and storing digital material, other functions of the

digital forensics process are not as highly developed, for example, the ability to attribute authorship and provenance, or to analyze trustworthiness (Carrier, 2003; Cohen, 2012). The "single largest gap" in digital forensics practice has been identified as the explicit identification of information flows in investigations, for example how identity is tracked, how evidence is authenticated, or how chain of custody is maintained (Ciardhuáin, 2004). The knowledge of the digital archivist can help. A significant challenge to both forensic and archival fields is the identification of records (archival focus) and evidence (digital forensics focus) in digital systems, and establishing their contexts, provenance, relationships, and meaning. The authors present areas of cross-fertilization and introduce a new research project that will take this work further.

While the tools and technological challenges of digital forensics are determined by the medium that is the subject of analysis (for example, forensic techniques specific to mobile devices, hard drives, or networks), and those of archival science are determined by the nature and characteristics of the information that it is meant to control, preserve and make accessible, there are common theoretical underpinnings. The digital forensics specialist is concerned with identifying digital objects and traces that may serve as evidence of criminal or other activity, and analyzing those objects for their evidentiary capacity, that is, for their attribution, integrity, and verifiability. Privileged or confidential information must also be identified and protected from unauthorized disclosure. The digital archivist is concerned with identifying digital objects that have been created as records of actions and transactions, facts and events, and assessing their reliability, authenticity, and accuracy in order to guarantee a trustworthy memory and historical accountability.[1] When an archivist acquires material from a digital storage device or network for appraisal and accessioning into a trusted repository, it is critical that s/he be able to uniquely identify the records, analyze them to ascertain their provenance, assess their authenticity and accuracy, establish existing issues regarding intellectual property, copyright, legal privilege, or track personal information that will be subject to redaction, data privacy protection, or access restrictions.

In assessing the identity and integrity of records stored in a variety of digital media, attesting to their accuracy, locating and protecting sensitive information, and acquiring them without alteration, archivists are required to act as forensic investigators. Digital forensics experts are similarly called to act as archivists when identifying, describing and preserving digital documentary evidence. Each domain possesses skills necessary and relevant to the other. Digital forensics has already claimed its place among the tools of archival processing of digital cultural heritage holdings (John, 2008; Rogers & John, 2013). Memory forensics tools are being used in digital archives and libraries for image capture, analysis, and reporting with increasing sophistication (c.f. The British Library, Stanford University Library, Emory University to name but a few sites employing these tools).

---

1 The archivist defines 'record' with distinct specificity: in archival science a record is a document (i.e. recorded information) made or received in the course of a practical activity, and saved for future action or reference. Records serve accountability—both legal-administrative and historical; are the basis of future decision-making, are evidence of past events, actions and transactions etc., and must satisfy admissibility requirements when submitted as evidence at trial.

The theoretical connections between archival science and digital forensics are still being explored. The principle of provenance is generally considered the foundational principle or theory of archival science. Through analysis and description of the provenance of records archivists can assess "the source, authority, accuracy, and value of the information which [the records] contained for administrative, legal (including access to information), research and cultural uses" (Abukhanfusa & Sydbeck, 1994). The application of the principle of provenance is widely discussed in the archival community, and the complexity of digital records and data, and of the digital information systems containing them has encouraged archivists to explore how definitions and uses of provenance are employed in related disciplines (Niu, 2013). In the digital environment, provenance information (also known as data lineage) has a wide range of critical application areas, and generally involves ownership information and process history documentation. However, the issue of "secure provenance," that is, providing assurances of integrity, confidentiality, and availability to the provenance records themselves is lacking. Furthermore, secure provenance "is the essential bread and butter of digital forensics and post-incident investigation of intrusions" (Hasan, Sion, & Winslett, 2007). Archival theory about records' provenance and provenance analysis can bolster digital forensics practice in this area--to give one example.

The following discussion presents one experiment of integration of knowledge between archival science and digital forensics. The Digital Records Forensics Project,[2] whose purpose was to adapt digital forensics methods for the archival purpose of assessing and maintaining the trustworthiness of digital records, developed a draft integrated model of an archival-forensic process (DRF model). In particular, the goal of the model was to identify points at which complementary knowledge might aid the investigative process, whether the investigation were archival in nature, aiming to preserve trustworthy sources of societal memory, or forensic, aiming to solve a crime or cybersecurity event. The DRF model, particularly well-suited to explain a workflow of "memory forensics," is descriptive and retrospective in nature, in that it seeks to abstract a workflow or process from observation of existing situations. It can then be used prospectively to identify points of weakness in the design of new processes, and to propose solutions to specific problems or issues.

Many models have been put forward to explain the digital forensic investigative response process (Beebe & Clark, 2005; Blackwell, 2011; Carrier & Spafford, 2003; Ciardhuáin, 2004; Ieong, 2006; Kahvedžić & Kechadi, 2009; Reith, Carr, & Gunsch, 2002; Selamat, Yusof, & Sahib, 2008). However, for the purposes of the Digital Records Forensics project, the researchers sought an abstracted model that included the basic elements of a digital investigation in a general framework. Carrier and Spafford have presented such a model, approaching the problem from a

2 The Digital Records Forensics (DRF) project was initiated in 2008 by Luciana Duranti, Principal Investigator, School of Library, Archival and Information Studies and Anthony Sheppard, Co-Investigator, Faculty of Law (see www.digitalrecordsforensics.ca). DRF was a three-year research collaboration between the School of Library, Archival and Information Studies and the Faculty of Law at the University of British Columbia, and the Computer Forensics Division of the Vancouver Police Department funded by the Social Sciences and Humanities Research Council (SSHRC) of Canada.

point of view of the computer as a crime scene, subject to crime scene investigative techniques (Carrier & Spafford, 2003). The investigation of this digital crime scene is broken down into six phases: preservation, survey for digital evidence, documentation of the evidence and the scene, search for digital evidence, reconstruction of events, and presentation of the reconstruction theory. Documentation that reports on provenance, that is, where the evidence originated and how it was handled, is key to a forensically sound case. “In addition to characteristics of the evidence source, such as a computer hardware clock or the number of sectors of a hard drive, an audit log and chain of custody enable an independent examiner to authenticate the evidence and assess its integrity and completeness” (Casey, 2007). Forensic soundness, expressed through reporting of secure provenance, provides accountability.

Digital forensics specialists are bound by the demands of the scientific method to justify their tools and techniques in identifying and authenticating digital evidence. Scientific testimony presented at trial may be tested for credibility against four criteria:

- Has the theory or technique been reliably tested?
- Has the theory or technique been subject to peer review?
- What are the theories’ or techniques’ known or potential error rates?
- Has the theory or technique been generally accepted as a standard in its scientific community? (Marsico, 2005)

Digital objects are therefore not examined as documentary residue of business activity—as is the case when archivists conduct such examination, but as latent trace evidence of digital processes. They are bound not by business rules and procedures, but by “the physics of digital information,” which governs “the artificial digital world of bits and machines that operate on them” (Cohen, 2011). It is the physics of digital information that is the scientific grounding of the digital forensic examiner and the source of expanded understanding of provenance and other information for the digital archivist.

The roots of authority conferred upon archival and digital forensics professionals derive from the particular ontological view each has of the evidence they seek to authenticate. Despite their different perspectives on analysis of digital material, however, their investigative goals are the same: to identify and authenticate digital evidence of actions and events. To that end, examiners from either profession must establish, document, and be prepared to justify, or account for, the identity, integrity, and context of the evidence, and their role in discovering and describing it.

The archival model of management of digital resources throughout their existence is termed the Chain of Preservation (CoP) [3], and was developed by the InterPARES (International Research on the Preservation of Authentic Records in Electronic Systems) Project (1998-2012) (Duranti & Preston, 2008). The purpose of the DRF model is to unify in one model the concepts of digital

3 The Chain of Preservation was developed by InterPARES to model all the functions and activities required from the moment of record creation throughout the record’s life cycle necessary to ensure that records are created reliable and maintained authentic over time and across technological change.

forensics practice that have been previously captured in several process models and incorporate in it the InterPARES Chain of Preservation (CoP) model for managing records throughout their life cycle. The Digital Records Forensics research team modeled the process of conducting a digital forensics investigation in order to assess the moments in which records, as understood by archival science and laws of evidence, could be identified, their authenticity assessed, and their reliability and integrity managed and preserved. The intention was to integrate the core requirements of digital forensics of establishing, documenting, and protecting the chain of custody, with the CoP model for preservation of digital records that can be presumed authentic and maintained reliable. The activities represented in the model are intended to ensure the creation and/or collection/acquisition of trustworthy digital records to be used as evidence, their maintenance throughout the judicial process, and their preservation over the long term for accountability, reference, further action, or societal memory.

The DRF model has within its scope all the phases or stages in the lifecycle of digital material that may be subject to forensic analysis in the process of investigation of a crime or security incident. It situates this material in the context of a juridical system and considers the whole process of investigation as a balance among available inputs, constraints or controls on the investigation, mechanisms used in the investigation, and desired outcomes or outputs from the investigation. As well, this model will seamlessly adapt to apply digital forensics knowledge to archival processing of digital material, thereby showing the integration of knowledge in both directions.

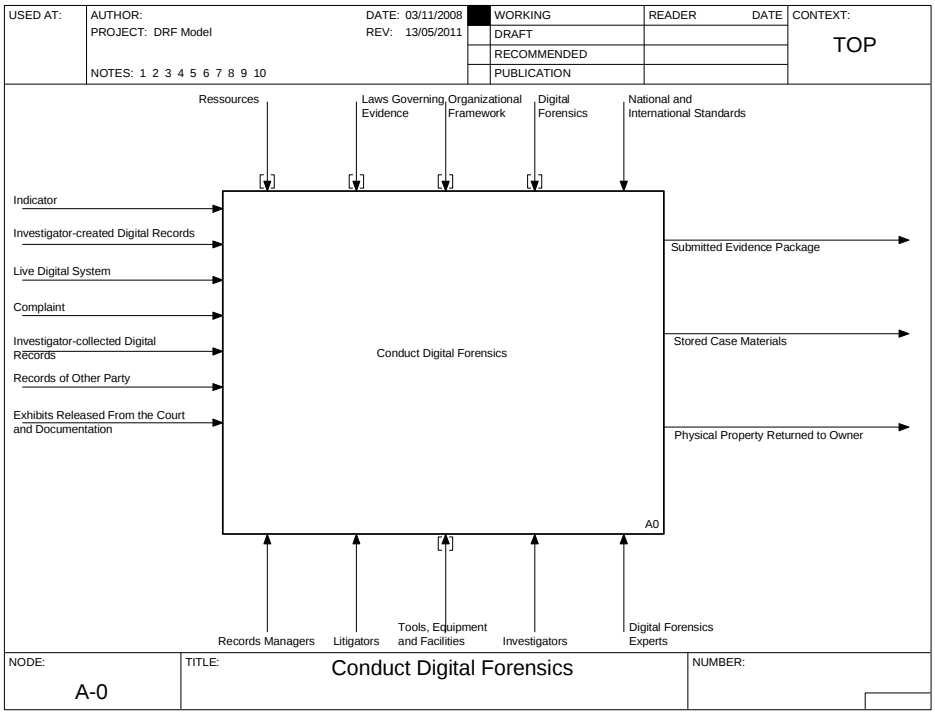
2 Overview of the Digital Records Forensics Process Model[4]

A-0: Conduct Digital Forensics. This top-level diagram delineates the subject of the model and its overall context. The bounding arrows represent the primary inputs, controls, mechanisms, and outputs. The activities represented in this diagram and all subsequent decompositions are intended

4 Both the DRF model and the CoP model use the IDEF∅ function modeling method, a graphical representation of the decisions, actions, and activities of an organization or system in order to analyze and communicate the functional perspective of that organization or system. Released by the National Institute of Standards and Technology (NIST) in 1993 as a standard for Function Modeling [34], it proceeds in a top-down, general-to-specific modeling approach which results in a hierarchical series of diagrams that gradually increase the level of detail in describing functions or activities and their interfaces within the context of a system. The most general features come first in the hierarchy, as the whole top-level activity is decomposed into sub-activities comprised in it. Those sub-activities may be further decomposed until all the relevant details of the system being modeled are adequately exposed and described.
Each box represents a single function or activity to be modeled. For each function or activity, the inputs, controls, outputs, and mechanisms are identified. Inputs are information, materials, objects, or data that are consumed, or transformed by the activity to produce outputs. Controls are conditions required to produce the correct output. Controls impose rules that regulate the performance of an activity. Mechanisms are the physical resources or means used to perform or facilitate the activity. They may be people, infrastructure, or equipment. Outputs are information, materials, objects, or data that are produced by the activity. If an activity does not produce any outputs, it should not be modeled.

to ensure the creation and/or collection of trustworthy digital records to be used as evidence, their maintenance throughout the judicial process, and their preservation over the long term for accountability, reference, or further action (see Fig. 1).

Fig. 1: Conduct Digital Forensics A-0



What are the constraints on the digital records forensics process? Digital forensics is always conducted within the context of constraints and controls imposed by the juridical system in which the investigation takes place, the resources available to undertake the investigation, and the principles of digital forensics that are recognized through methodological and theoretical development of the discipline.

Resources available to the investigator include personnel, financial support, tools and technology, and specialized, or domain knowledge.

Digital Forensics Principles have developed to support the purpose of digital forensics investigations. They have been summarized by a variety of domain experts, and include under the guiding principle: “Action taken to secure and collect electronic evidence should not change that evidence” (US Department of Justice, 2001) concepts of

- Integrity
- Authentication
- Reproducibility
- Non-interference
- Minimalization

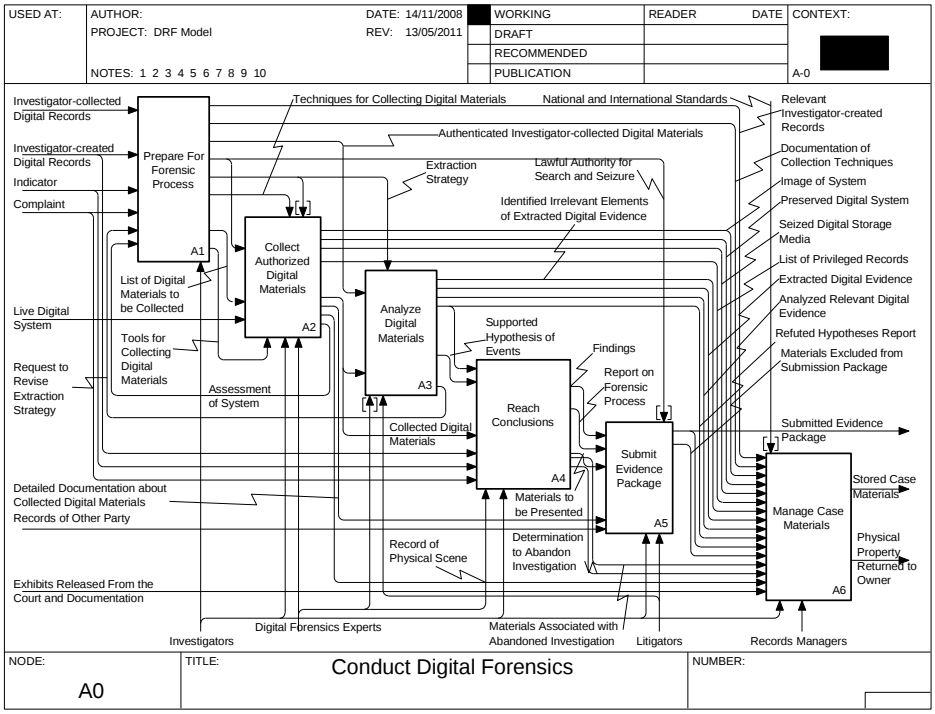
These principles are themselves governed by the laws of evidence, and relevant national and international standards. Finally, the investigation will also be constrained by the organizational framework within which it directly takes place.

What are the mechanisms instrumental to the digital records forensics process? Many resources are required to conduct a successful digital forensic investigation. Most commonly, these will include litigators, investigators, digital forensics experts, and the tools, equipment and facilities they use. The model recognizes that, in a digital records forensic process, records managers also play an important role in identifying records in context and offering domain expertise in records related issues such as privacy, assessment of authenticity, reliability, and accuracy, and requirements for preservation and access.

What are the important inputs to the digital records forensics process? By definition, the inputs at the top level of the model represent information or objects that originate outside of the activity being modeled. In a digital records forensics investigation of a crime or system breach, an indicator is required – some information about unusual, suspicious, or criminal activity. The indicator may result in a complaint – a written or oral request to investigate. The activity may be conducted on a live digital system, on digital materials collected by an investigator, or materials produced by the other party. The activity may also be supported by records authored by the investigator, or by exhibits released from the court with their accompanying documentation.

What are the key outputs of the digital records forensics process? Many different outputs may proceed from the top level activity, but all can be categorized as evidence submitted to counsel or to court, materials stored or preserved from the case and its investigation, and physical property that may be returned to its rightful owner at the completion of the investigation or trial.

Fig. 2: Conduct Digital Forensics A0



The model distinguishes six main activities (Fig. 2): 1) Prepare for forensic analysis; 2) Collect authorized digital materials; 3) Analyze digital materials; 4) Reach Conclusions; 5) Submit evidence package; and 6) Manage case materials.

3 Integrating digital forensic and archival practice models

The traditional archival practice of ensuring the authenticity of records over time through evidence of an unbroken chain of custody alone is inadequate for digital records. The creation, maintenance, and preservation of digital records that can be proven reliable and presumed authentic over time and across technological change rely on processes and controls that protect them from corruption and maintain their identity and integrity (Duranti & Preston, 2008). Mapping activities in the DRF

model to the CoP model allows for greater cross-disciplinary understanding of common terminology, and identifies moments at which domain knowledge may be shared to enhance the process of analysis of digital material.

The following example illustrates this process, and the possibilities for further research. The CoP model distinguishes four main record activities: (1) managing the framework for the chain of preservation, (2) managing the process of records creation, (3) managing records in a recordkeeping system, and (4) preserving selected records (Duranti & Preston, 2008). This example compares activity decomposition from the fourth activity of the CoP model (A4 Manage Records in a Permanent Preservation System) with the activity decomposition from the third activity area of the DRF model (A3 Analyze Digital Materials).

Fig. 3: Manage Records in a Permanent Preservation System (CoP)

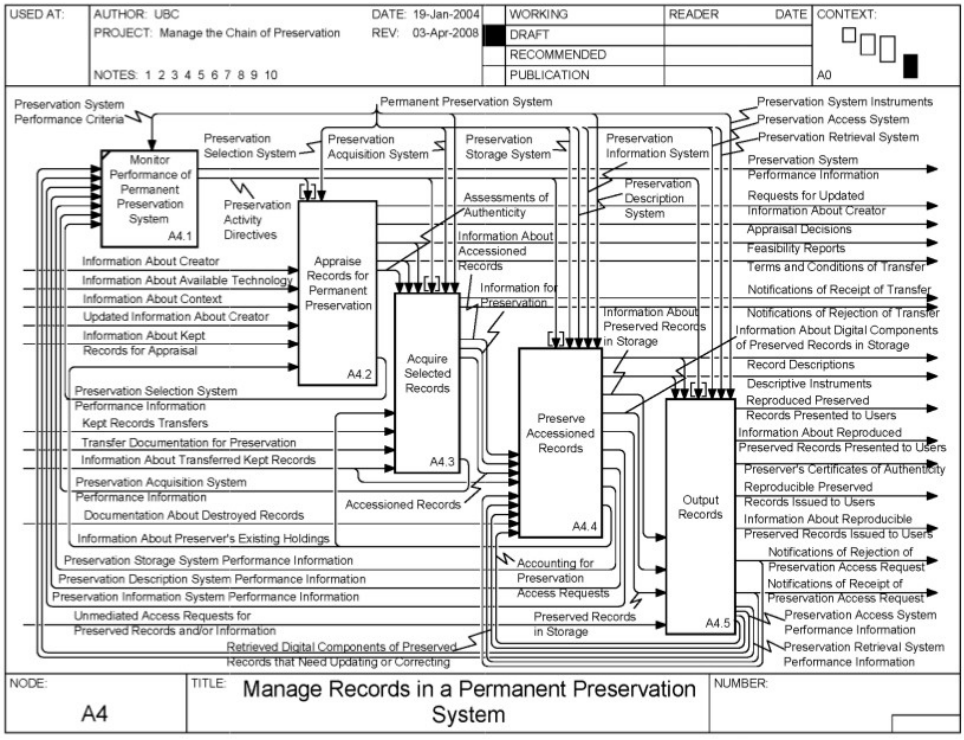
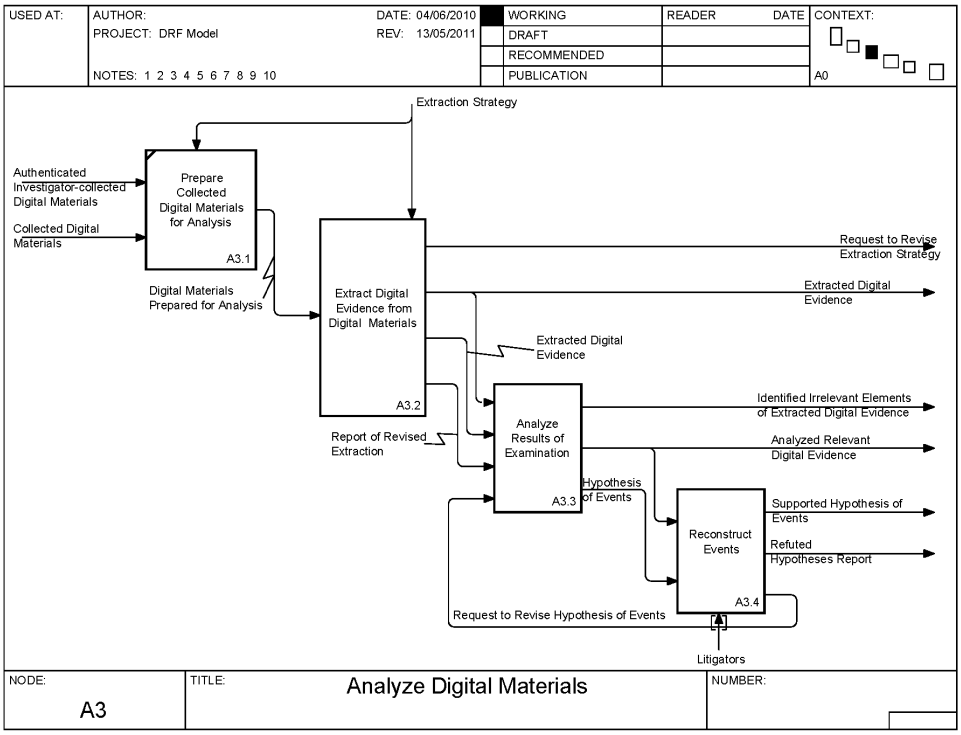


Figure 3 shows the overview of the activity, *Manage Records in a Permanent Preservation System*, from the CoP model. This activity involves actions associated with preserving records to ensure their continuing authenticity while in the custody of the designated preserver. Key activities

include appraisal and selection of records of permanent value, capture, preservation, description, and output of selected records. These activities may be mapped to the activities involved in analyzing digital materials – A3 of the DRF model. For example, the process of record appraisal and acquisition (CoP A4.2-4.3) shares features and purposes of preparation and extraction of digital material (DRF A3.1-3.2) (see Fig. 4). By integrating the archival principles embedded in the CoP model that ensure records' authenticity and reliability into the principles of digital forensics that guarantee integrity, authentication, and verifiability of digital material, patterns may be developed that solve issues challenging both domains.

Fig. 4: Analyze Digital Materials (DRF)



4 Next steps – InterPARES Trust

The CoP model used to map to the general model of the digital records forensics process is undergoing review and revision as a result of the rapid adoption of cloud services in the creation, management, storage and preservation of digital records. Modeling the Chain of Preservation specifically for records in the cloud is necessary to address concerns over issues related to jurisdiction, privacy, security, authenticity, validity, integrity, and completeness. Thus, in April

2013, a new international multidisciplinary project involving universities, governments, businesses, and cultural heritage institutions in six continents and thirty countries began its research activities aimed to address such issues. This project, which is funded until 2019 by the Social Sciences and Humanities Research Council of Canada and by all participating partners, is the fourth phase of InterPARES research, and addresses the issue of trust in records and archives created, used, maintained and/or permanently preserved online, thereby taking the name of InterPARES Trust (ITrust).

The goal of ITrust is to generate the theoretical and methodological frameworks that will support the development of integrated and consistent local, national and international networks of policies, procedures, regulations, standards and legislation concerning digital records entrusted to the Internet, to ensure public trust grounded on evidence of good governance, a strong digital economy, and a persistent digital memory.

Reviewing the Chain of Preservation model and revising it for records and data hosted by third party service providers addresses the following questions:

- Are requirements for the preservation of digital records identified in InterPARES 1 and 2 applicable to records in the cloud?
- What additional requirements does forensic readiness impose on preservation of records in the cloud?
- How can these requirements be satisfied when records are stored by third party service providers?
- Are there special requirements for records that are discovered and delivered via the internet?
- How can such requirements be implemented?

Because records and archives entrusted to third party providers must satisfy the requirements of reliability, authenticity (i.e. identity and integrity), accuracy, usability, accessibility, and preservability, so that transparency and accountability (legal, administrative, and historical) are ensured, and documentary evidence is protected together with the documentary sources for history, the collaboration of all disciplines concerned with these qualities of records and archives is necessary to the success of InterPARES Trust, and digital forensics has a special role in determining the outcome of this research project.

The theory and methods identified to reach the objectives of InterPARES Trust are those of archival science, resource management, policy design, textual analysis, visual analytics, risk management, and modeling. Although digital forensics is not expressly indicated in the research proposal, it is not an absentee; rather, digital forensics is a stone guest. The ancient expression “stone guest” refers to a looming but invisible presence, silent and therefore disturbing and unpredictable, of which everyone is aware but which no one mentions. While it is clear that digital forensics practices and procedures would be useful, if not outright necessary, in carrying out this research project, it is difficult when outlining a theoretical and methodological approach to

research to refer to specific activities or processes rather than to the body of knowledge of a recognized discipline. And digital forensics is hardly perceived as an autonomous discipline.

There is a vast literature on the concept of discipline that proposes very different definitions and interpretations. Liles et al. (1995) build upon the analysis of the existing definitions and suggest that a discipline must have "six basic characteristics: *(1) a focus of study, (2) a world view or paradigm, (3) a set of reference disciplines used to establish the discipline, (4) principles and practices associated with the discipline, (5) an active research or theory development agenda, and (6) the deployment of education and promotion of professionalism*" [italics in the original text]. Digital forensics has some of these characteristics but what separate it from a full-fledged discipline are its reactive approach, and its retrospective outlook, which confines it to the examination of what exists.

Several decades after its recognition as an established practice, digital forensics has accumulated a large body of knowledge that can allow it to identify recurring concepts, ideas, and principles capable of guiding the design of systems for data, records and archives created and/or kept by third party service providers, systems that do not have to trade transparency for safety, or control for economy. Much has still to be done to ensure that digital forensics knowledge can be used to prevent rather than to detect cybercrime, but the key is active collaboration with allied disciplines in the context of multidisciplinary projects like InterPARES Trust. Just as archival science is expanding its body of theory to incorporate knowledge from digital forensics, digital forensics experts can benefit from the study of concepts, laws and models from the other fields involved with the InterPARES research project to foster useful transfers to their own field, to encourage the development of a digital forensic theory in emerging areas of endeavor and investigation, to eliminate the duplication of theoretical efforts in different fields, and to promote consistency of scientific knowledge.

However, in order to develop the knowledge of digital forensics, when experts bring those extraneous concepts, laws and models into their body of knowledge, they have to make them consistent with all of its parts (i.e., confront them with forensics concepts, principles, practice and scholarship), subject them to a feedback process, and insert them into the fundamental structure of their knowledge system. Only in this way will they be able to build up digital forensics as a discipline, maintaining its integrity and continuity while at the same time fostering its enrichment and growth. This paper is an invitation to start this process of growth and change and to do it by helping records professionals to ensure that records and archives in the cloud can be protected without renouncing transparency, accountability, and accessibility…in a word, democracy.

References

Abukhanfusa, K., & Sydbeck, J. (Eds.). (1994). The Principle of Provenance: Report from the First Stockholm Conference on Archival Theory and the Principle of Provenance, 2-3 September 1993. Stockholm.

Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2(2), 147–167.

Blackwell, C. (2011). A Framework for Investigating Questioning in Incident Analysis and Response. Oxford, UK.

Carrier, B. (2003). Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. International Journal of Digital Evidence, 1(4), 1–12.

Carrier, B., & Spafford, E. (2003). Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, 2(2), 1–20.

Casey, E. (2007). What does “forensically sound” really mean? Digital Investigation, 4(2), 49–50.

Ciardhuáin, S. Ó. (2004). An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3(1), 1–22.

Cohen, F. (2011). The State of the Science of Digital Evidence Examination. Presented at the IFIP 11.9, Orlando, FL: unpublished.

Cohen, F. (2012, September 24). The Future of Digital Forensics. Presented at the Trust and Conflicting Rights in the Digital Environment, Vancouver, BC.

Duranti, L., & Preston, R. (2008). Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential. Interactive and Dynamic Records. Padova: Associazione Nazionale Archivistica Italiana.

Hasan, R., Sion, R., & Winslett, M. (2007). Introducing secure provenance (p. 13). ACM Press. doi:10.1145/1314313.1314318

Ieong, R. S. C. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. Digital Investigation, 3(Supplement 1), 29–36.

John, J. (2008). Adapting Existing Technologies for Digitally Archiving Personal Lives: Digital Forensics, Ancestral Computing, and Evolutionary Perspectives and Tools. In Proceedings of The Fifth International Conference on Preservation of Digital Objects (pp. 46–55). Presented at the Joined Up and Working: Tools and Methods for Digital Preservation, London, England: The British Library. Retrieved from http://www.bl.uk/ipres2008/ipres2008-proceedings.pdf

Kahvedžić, D., & Kechadi, T. (2009). DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge. Digital Investigation, 6(Supplement 1), S23–S33.

Liles, D.H., Johnson, M. E., Meade, L. M., and Ryan, D.: Underdown. Enterprise Engineering: A Discipline? (1995), http://webs.twsu.edu/enteng/ENTENG1.html

Marsico, C. V. (2005). Computer Evidence v. Daubert: The Coming Conflict. Purdue University. Retrieved from https://www.cerias.purdue.edu/apps/reports_and_papers/view/2819/

Niu, J. (2013). Provenance: crossing boundaries. Archives and Manuscripts, 41(2), 105–115. doi:10.1080/01576895.2013.811426

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence, 1(3). Retrieved from

http://www.worldcat.org/wcpa/oclc/223384589?page=frame&url=http%3A%2F%2Fwww.ijde.org%2F%26checksum%3D85756f448e9f3f33b58f16d99aa26bcf&title=&linktype=digitalObject&detail=

Rogers, C., & John, J. (2013). Shared Perspectives, Common Challenges: A History of Digital Forensics & Ancestral Computing for Digital Heritage. In The Memory of the World in the Digital Age: Digitization and Preservation (pp. 314–336). Presented at the The Memory of the World in the Digital Age: Digitization and Preservation, Vancouver, BC: UNESCO. Retrieved from http://www.unesco.org/webworld/download/mow/mow_vancouver_proceedings_en.pdf

Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping Process of Digital Forensic Investigation Framework. IJCSNS Internation Journal of Computer Science and network Security, 8(10), 163–169.

US Department of Justice. (2001). Electronic Crime Scene Investigation: A Guide for First Responders. Washington, DC. Retrieved from www.ojp.usdoj.gov/nij