International Journal of Digital Humanities (2019) 1:13–28
https://doi.org/10.1007/s42803-019-00002-y

RESEARCH ARTICLE

From time theft to time stamps: mapping the development of digital forensics from law enforcement to archival authority

Corinne Rogers[1]

Published online: 4 March 2019

Abstract
The field of digital forensics seems at first glance quite separate from archival work and digital preservation. However, professionals in both fields are trusted to attest to the identity and integrity of digital documents and traces – they are regarded as experts in the acquisition, interpretation, description and presentation of that material. Archival science and digital forensics evolved out of practice and grew into established professional disciplines by developing theoretical foundations, which then returned to inform and standardize that practice. They have their roots in legal requirements and law enforcement. A significant challenge to both fields, therefore, is the identification of records (archival focus) and evidence (digital forensics focus) in digital systems, establishing their contexts, provenance, relationships, and meaning. This paper traces the development of digital forensics from practice to theory and presents the parallels with archival science.

Keywords Archival science · Digital forensics · Digital records forensics · Digital evidence

1 Introduction

The field of digital forensics seems at first glance quite separate from archival science and digital preservation, but these disciplines have overlapping histories and legacies deriving from similar goals, common challenges, and shared theoretical perspectives (Rogers and John 2013). In the 1980s forensic investigation of computer crime was largely unknown – indeed, some questioned whether computer crime existed. At the same time, archivists were beginning to discuss the characteristics and implications for practice of machine-readable records. Today, crime involving digital evidence is the norm and digital forensics is a growth industry in legal investigations. Archives and

✉ Corinne Rogers
cmrogers@mail.ubc.ca

[1] School of Library, Archival and Information Studies, University of British Columbia, Vancouver, Canada

records are increasingly born digital, and archivists need new tools to access digital sources, and assist in processing archival material. Elizabeth Diamond foreshadowed these developments when she wrote in 1994: “[i] f the historian is the lawyer in the court of history, then the archivist is the forensic scientist” (Diamond 1994: 140).

Both fields are concerned with discovering, understanding, describing, and presenting or making accessible digital material. Digital forensics was developed to assist law enforcement in investigations of crimes using computers in order to bring digital evidence to trial and is concerned with the authenticity, reliability, and accuracy of digital material. Archival science traces its roots to administration and law, and studies the relationships between records, the persons, procedures, actions, and means through which they are created. Archivists support accountability and trustworthiness of records by establishing their identity and assessing their integrity, reliability, and accuracy through analysis of records and record aggregations. But digital records require the mediation of technology to read and understand them, and so present the archivist with new layers of abstraction for analysis. In recent years, archivists have adopted and adapted digital forensics tools in service of accountability and preservation of societal memory (c.f. Kirschenbaum et al. 2010; Lee 2012), and digital forensics practitioners have noted similarities between their work and records’ management (c.f. Irons 2006).

Much of the published material about digital forensics focuses on the techniques and tools of practice, and is highly technical, falling within the realm of computer science and mathematics. The purpose of digital forensics is predominantly in service of legal evidence, admissible in court, incident response and security. But throughout the development of the discipline, there has been a small but steadily growing body of literature that calls for digital forensics research to be situated within a broader social and theoretical framework (Palmer 2001; Mocas 2004; Irons 2006; Duranti 2009; Duranti and Endicott-Popovsky 2010).

While the tools and techniques of digital forensics are necessarily technical, the conceptual underpinnings of the discipline can be examined through the lens of archival science, diplomatics, and law. The following review of predominantly non-technical literature endeavors to understand the genesis and evolution of digital forensics as law enforcement practice and academic discipline in order to explore parallels with archival science.

This paper traces the chronological development of digital forensics from its evolution in the 1980s to the present through the issues that have shaped it. These issues include the evolving challenges presented by society’s increasing reliance on computer technology, a collaborative approach by legal personnel, law enforcement, and IT specialists in identifying and solving these challenges, the spread of digital forensic practice from law enforcement to other domains, specifically archival practice.

A note about terminology: early practitioners referred to the practice of computer forensics. As digital devices became ubiquitous and were not necessarily traditional computers, the term “digital” began to replace “computer” (c.f. Whitcomb 2002). However, there is little consistency even today. While the tendency may be to preference “digital”, the term computer forensics is still in use.

2 The legal context

Digital forensics and archival science both have roots in law. The nature of archives and the responsibilities for their care and custody are discussed in the Justinian Code of ancient Rome, and in the literature of the jurists of the eleventh century (Duranti 1996). Archival research focuses on establishing the evidentiary capacity of records and documents. According to Menne-Haritz, '(e)vidence means patterns of processes, aims and mandates, procedures and results, as they can be examined. It consists of signs, of signals, not primarily of words. … All those are nonverbal signs that must be interpreted in context to disclose their meaning. To one who understands them, they will tell how processes worked and who was responsible for which decision' (1994, 537).

Digital forensics developed in response to the needs of law enforcement to investigate computer crime. It has been defined 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 (Palmer 2001).

While admissibility requirements for traditional documentary evidence have a long-established history and are well understood, digital evidence has raised a host of problems that the judicial system, regardless of jurisdiction, was (and in some cases may still be) ill equipped to handle. The inadequacies and inconsistencies of the law of evidence and rules of court to deal with digital media despite the passage of new laws to address it, the explosive increase in quantity of potential evidence to be examined, lack of understanding of the nature of digital media and its differences from traditional media all contributed to the need for a scientific and theoretical base for digital forensics.

The legal context has been approached in the digital forensics discourse in one of two ways. First, those concerned with the development of the discipline have sought, through standards, principles and guidelines, a scientific basis for practice. Second, several practitioners have advocated for the development of open source tools which, by nature of the availability of their source code, would support the forensic expert witness in asserting their reliability (Carrier 2003b; Kenneally 2001).

While it is not within the scope of this paper to address the legal context in full, it is worth citing a few milestones. In 1993 the ruling in *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 changed the law with respect to the admissibility of scientific evidence and expert testimony. *Daubert* required that scientific evidence be based on theory and technique that has been reliably tested, subject to peer review, with known or potential error rates, and generally accepted as a standard in its particular scientific community. These requirements were expanded in *Kumho Tire v. Carmichael* (1999) to include technology expertise. Because digital evidence is extracted from digital media, its reliability and integrity depends in part on the means of its extraction, which must be conducted and accounted for according to scientific principles. These two cases have, therefore, had a profound impact on the development of the digital forensics discipline (Marsico 2005).

3 A brief history of digital forensics: looking back to look forward

At the end of the 2010s, three short historical retrospectives captured past development and predicted future directions of digital forensics (Charters 2009; Pollitt 2010; Garfinkel 2010). These articles are important first-hand accounts of the evolution of the discipline and predictions for future growth reflecting the perspectives of the intelligence community, law enforcement and academic researchers. Each author has been and continues to be influential in shaping the field. Each has approached the task from his particular point of view, and yet there are similarities. All accounts track the changes in computer technology, which have driven the course of digital forensics, and arrive at complementary yet distinct conclusions about future directions.

Ian Charters' background is in IT security and information assurance spanning more than 20 years in the United States' Intelligence Community. He describes the development of computer forensics in terms of stages of evolution – the Ad Hoc Phase, the Structured Phase, and the Enterprise Phase. He suggests that these phases are cyclical, repeating as developments in technology offer new opportunities for criminality and introduce new challenges for investigators. Charters explains the development of digital forensics through the development of policy, procedure, and forensic tools. He characterizes the Ad Hoc Phase by shortcomings in investigative structure, goals, policies and procedures, and lack of accuracy of forensic tools. The resulting confusion of the Ad Hoc phase gives way to the imposition of structure expressed in policy-based programs, defined and coordinated procedures closely aligned with the policy, and a requirement for – and development of – more forensically sound tools – the Structured Phase. The Enterprise Phase is characterized by real-time collection, tailored field tools and forensics-as-a-service, built seamlessly into the technological infrastructure. The future, he predicts, will be aimed at greater automation and interoperability, proactive collection and analysis, and increased focus on standards in software architectures and reporting.

Mark Pollitt begins his paper *A History of Digital Forensics* with an apology. His is not, he claims, a fully-informed, objective and unbiased account of the rise of digital forensics, but his personal story – the journey of a digital forensic investigator (Pollitt 2010). One may argue, of course, that there is no such thing as an objective and unbiased account. No matter one's intention to present "the facts and nothing but the facts," every narrator chooses what to include and what to ignore in the telling of a story, and in so doing shapes that story through the material she choses. Pollitt's personal account is nevertheless a particularly clear summary of the development of the field, outlining the salient characteristics of the practice and the profession. He presents the history of computer forensics through the notion of epochs, beginning with pre-history, and then adopting a lifecycle model, moving from infancy through childhood and adolescence, with maturity still to come. Within that framework, he defines the discipline through the elements of people, targets, tools, organizations, and the community as a whole. Pollitt, a former military officer with over twenty years' service experience as a Special Agent of the Federal Bureau of Investigation, approaches the history from the perspective of law enforcement. His experience spans the epochs he describes, and his influence is evident in the development of standards, and the recognition of digital forensics as a forensic discipline by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board.

Simson Garfinkel is an academic practitioner who has developed computer forensics tools, conducted computer-related research and authored books and articles published in the academic and popular press. In *Digital forensics research: The next 10 years* (2010), he suggests a research agenda that will carry digital forensics into the next phase of development, and sets the stage by summarizing the characteristics of past phases. He argues that 2010 marks the approaching end of a “Golden Age” of computer forensics, characterized by relative stability of operating systems and file formats, examinations largely confined to a single computer system, removable storage devices, and reasonably good and easy-to-use tools coupled with rapid growth of research and increasing professionalism. An impending crisis looms, brought on by advances and fundamental changes in the computer industry – specifically increased storage capacity, proliferation and diversification of devices, operating systems and file formats, pervasive encryption, use of the cloud for remote processing and storage, and increasing legal challenges to search and seizure that limit the scope of investigations. Current forensics tools are challenged to meet these needs for law enforcement because they focus on finding specific pieces of evidence for presentation in court. However, this evidence-oriented model – what Garfinkel calls the ‘visibility, filter, and report model’, is well suited to archival processing needs, if not all law enforcement needs. Garfinkel has contributed to the development of forensics tools for archivists through his participation in the BitCurator project that supports digital forensics practices in libraries, archives, and museums (Lee 2012).

4 A view from the field – the 1980s and 1990s

Clifford Stoll’s book, *The Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage*, is an early account of finding a computer hacker and bringing him to court (Stoll 1989). An astronomer supporting the computer systems at a California research laboratory in the mid-1980s, Stoll stumbled upon a hacker when he investigated a 75-cent discrepancy in the accounting charges for computer use time in his lab. This led him on an intercontinental cyber chase that lasted over a year through the networks that linked research and military computers in Europe and the United States. Law enforcement and military personnel alike were slow to take interest; because there was no financial or other damage, they could not determine if a crime was being committed. Nor, until they could locate the hacker’s point of origin, could they agree on jurisdictional responsibility. This story highlights the characteristics of intentional computer misuse and response in the late 1980s: uncertainty about what constituted a crime using computers; the practice of a lone investigator working on his own, often with little support; and use of tools adapted or created by the investigator for a specific incident.

As early as 1984, some law enforcement agencies had begun to develop programs to examine computer evidence. The Computer Analysis and Response Team (CART), developed by the FBI, was duplicated in law enforcement agencies in North America and Europe (Noblett et al. 2000; Whitcomb 2002). However, while some progressive investigators delved into the new frontier of digital evidence, there was also reluctance, as Stoll’s experience illustrates. The Inspection Service Lab of the US Postal Service expressed dismay when first confronted in the late 1980s with a request for an examination of a computer – "What should we do with this?", they asked. They questioned how they could secure and preserve digital evidence, how they could collect it without changing it, what practices would withstand the scrutiny of the court, and what examination protocols they should follow. However within ten years the Postal Inspection Unit had not only established a Computer Forensic Unit, but considered changing the name to Digital Evidence Unit to reflect the growing variety of digital sources of evidence.

The first published use of the term "computer forensics" in the academic literature appeared in an article entitled *A forensic methodology for countering computer crime* (Collier and Spaul 1992). The authors proposed the term 'computer forensics' as a label for 'existing but very limited activities amongst the police and consultancy firms' (204) and advocated for its inclusion in the realm of traditional forensic sciences. They identified the skills required of a computer forensic expert to be multi-disciplinary, including investigative capacity, legal knowledge (including the law of evidence, rules of hearsay and admissibility), courtroom presentation skills as well as knowledge of computers.

The bulk of published material begins in the mid-1990s, originating from international gatherings of law enforcement. Some of these, like the FBI international conferences on computer evidence, were symposia devoted to computer crime (Noblett et al. 2000). Others were long-established gatherings that began to include sessions on computer forensics, such as INTERPOL's International Forensic Science Symposia (Internet / Home - INTERPOL n.d.).

Mark Pollitt's frequent reports and presentations to international law enforcement in the 1990s give a clear picture of the state of development of the discipline. Through observation and experience, Pollitt developed one of the first high-level models of the computer forensic process, reflecting the common principles that guide the conduct of an examination. His "three-tiered approach" consists of principles, methodologies (practices), and procedures. With this three-tiered model he formulates a basis for standards development. Moving from the general to the specific, he identifies universal principles: that evidence should not be altered; that examination results should be accurate; and that the results are verifiable and repeatable (Pollitt 1995a, b). This model was further developed in a later article (Noblett et al. 2000) and has been the foundation of many subsequent models.

Digital evidence was recognized as a principle type of evidence at INTERPOL's International Forensic Science Symposium in 1998 (Pollitt 2001) and each subsequent conference has received a report on the status of digital evidence collection and analysis, as well as areas of growth and challenge. The reports outline the growth of community through working groups, professional organizations, and scientific bodies (DiClemente et al. 2004); challenges and concerns such as increased workload, and need for accreditation and certification balanced by professional maturity and methodology; and the increasing complexity of computer crime with its parallel demands on computer forensics, and the spread beyond its original stakeholders (Reedy et al. 2007). In 2010 a sobering picture was presented of a 'coming digital forensic crisis' caused by rapidly increasing storage capacity, data volume on networks, an expanding variety of computing devices, growing case loads, and limited resources (Garfinkel 2010, S66:).

5 Definitions, standards, and the building of community

Early in the evolution of digital forensics practice, the need for standards to guide and regulate the discipline and increase the acceptance of digital material offered as evidence in court became an important subject of discussion. Standards were recognized as instruments that ensured quality and served as a guarantee of reliable results, dictated a minimum acceptable level of performance, ensured proper training of examiners, and limited liability for the actions of both examiner and examining organization (Pollitt 1995a). However, some questioned the ability to develop standards for digital forensics because of the variety and pace of change of technology. The challenge was to build in sufficient flexibility to balance meaningful standards with rapid change and individual investigative approaches. Digital forensics working groups sought to develop universal principles that could be applied irrespective of the media under investigation.

In 1998 the US Federal Crime Laboratory Directors group established the Scientific Working Group on Digital Evidence (SWGDE), with a mandate to explore digital evidence as a forensic discipline (Pollitt 2003). Shortly after it was formed, the SWGDE proposed draft definitions and, on the principle that digital evidence must be ‘collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence’, a draft standard was presented to the International Hi-Tech Crime and Forensics Conference in October 1999 (SWGDE and IOCE 2000). The draft defined digital evidence as information of probative value stored or transmitted in digital form, and identified that its acquisition begins when information and/or physical items are collected or stored for examination purposes. The process of collecting evidence should be conducted according to the rules of evidence in the relevant jurisdiction. Data objects are defined as information of potential probative value that are associated with physical items, and may occur in different formats without altering the original information. The draft standard also distinguished original digital evidence from duplicates or copies. Original digital evidence is defined as the physical items and data objects associated with such items at the time of acquisition or seizure. Duplicate digital evidence is an accurate digital reproduction of all data objects contained on an original physical item, while a copy is an accurate reproduction of information contained on an original physical item, independent of the original physical item.

Other organizations were also pursuing the development of standards and best practices. In the United Kingdom, the Association of Chief Police Officers (ACPO) drafted good practice guidelines for search, seizure and examination of digital evidence. The original four principles of digital forensics examination still stand today, in the fifth edition of their guidelines (Association of Chief Police Officers (ACPO) 2012). They require that no action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court; that in exceptional circumstances, a competent person may need to access original data held on a computer or on storage media and must be able to give evidence explaining the relevance and the implications of their actions; that an audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved, and an independent third party should be able to examine those processes and achieve the same result; and that the person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to. Standards and practice guidelines continue to be updated as the field matures.

With standards and principles drafted for forensic investigations related to law enforcement, the discipline was ready to explore a more theoretical focus and build a multi-disciplinary community. In 2001 the first Digital Forensics Research Workshop (DFRWS) was convened in Utica, New York. The conference represented the nucleus of a multi-disciplinary digital forensics community that included law enforcement, military and civilian partners; participants included academics and digital forensic practitioners, with keynote speakers from law enforcement, military operations, infrastructure protection, industry, academia and government. These domains each employed a difference paradigm for forensic analysis—prosecution (law enforcement), security and continuity of operations (military), and availability and security of service (business and industry) (Palmer 2001). The report from that conference provides an important benchmark of the profession—a synchronic snapshot of digital forensic science at that moment, and a blueprint for future research. It provides a base from which much of the subsequent literature derives.

Participants agreed that to be considered a discipline, digital forensics must be characterized by a combination of theory, abstractions and models, elements of practice, a corpus of literature and professional practice, and confidence and trust in results. They also agreed that these areas had not all yet been adequately addressed. The keynote speakers expressed strong concern for development of the profession that goes well beyond the solely technical aspects. This "full-spectrum" approach does not rest on technology alone, but draws on the procedural, social and legal realms to create a holistic body of knowledge that both informs and supports the primary objectives of forensic analysis and leads to an integration of "forensic hooks" into live computer and network systems and away from the "current band aid approach that produces point solution tools." Lack of standardization of analytical procedures, protocols and terminology; issues of accuracy, efficiency and retention of extracted material; the conflict between individual privacy rights and data collection requirements were all identified as holding back the development of the profession.

Participants agreed that future research should build on collaboration. Important foci included work to define terms and develop taxonomies and ontologies that would make communications more effective and research more applicable, increasing opportunities for training and certification, and continuing to work on standards and standardized procedures, among many more specific goals.

6 Towards a theory of digital forensics

Theory develops through contemplation of practice intended to uncover general or abstract concepts, which are modeled and tested, and eventually transcend the specific, returning to inform and guide practice. In relation to disciplined knowledge creation, theory 'denotes systematic ideas to explain or account for observed facts or phenomena' (Eastwood 1994, 123). Digital forensics is practiced in an investigative context, regardless of the domain of the investigation. The roots for the development of a theory of digital forensics, then, may be found in the early practice guidelines and principles developed by law enforcement and technical working groups (Mocas 2004).

The call for development of a theory of digital forensics was first broadly articulated in the DFRWS report (Palmer 2001; Carrier and Spafford 2004). The framework proposed by the DFRWS modeled a typical investigation: identification, preservation, collection, examination, analysis, presentation and decision (Palmer 2001). Models have been proposed that elaborate on the stages of investigation, outline incident response, frame the process through a particular lens, or define the discipline through abstracted concepts (c.f. Pollitt 1995a; Noblett et al. 2000; Palmer 2001; Reith et al. 2002; Carrier 2003a; Carrier and Spafford 2004; Ciardhuáin 2004; Beebe and Clark 2005; Ieong 2006; Selamat et al. 2008; Blackwell 2011). They share similarities as they present more or less detailed abstractions of investigative steps.

There is no consensus about the maturity of the models that have been proposed, or a universally accepted theory. Perhaps there can never be, as process models are subjective, and must be evaluated with respect to scalability for future technologies and applicability to different types of investigations (Carrier and Spafford 2004). They are descriptive in nature, presenting in greater or lesser detail the elements of an investigation in linear detail as it unfolds.

Proposed theoretical foundations begin to enter the literature with the search for functional requirements that a process model must meet. Carrier and Spafford propose five requirements: that the model be practical and follow the steps of an investigation, that it be technology-neutral, but allow enough specificity to support technology requirements for each phase, that it be based on existing theory for physical crime investigations, and that it must apply across domains to law enforcement investigations, corporate investigations and incident response.

They approach the development of a model from a particular perspective—that the computer or system under investigation is analogous to a physical crime scene. This offers a way of organizing the steps of the process into five categories: readiness phases; deployment phases; physical crime scene investigative phases; digital crime scene investigative phases; and review phase. This model contributes to developing knowledge in several ways. Its foundation in the theory of physical crime scene investigation is intended to enhance credibility in the eyes of the court. Considering the digital environment as a crime scene rather than simply an object of physical evidence supports a richer and more holistic analysis, and identifies interaction between the physical and digital investigation. The model is abstract enough to be generalized to any investigative situation (Carrier and Spafford 2003, 2004).

6.1 Digital forensics concept models and functional requirements

Descriptive process models, however, are necessarily limited in their ability to suggest a theory of digital forensics that identifies concepts and functional requirements of the discipline. The goal is to develop a conceptual model that is based on more than "investigative experiences and biases" (Carrier and Spafford 2006). A model that succeeds in this will conceptualize the requirements for "forensic soundness," and support the development of procedural methods and tools (Casey 2007).

Rather than propose a model for the forensic process, Sarah Mocas defined a set of organizing principles for the development and evaluation of digital forensics research (2004). She identified five abstractions, or properties, through which the researcher can frame questions, model behaviors and evaluate procedures. Integrity, authentication, reproducibility, non-interference, and minimization also define what properties are necessary and/or sufficient for evidence to be viable in a specific investigative context. These properties are considered within that context, including reasons for the investigation, constraints on its scope, and a set of potential and desired outcomes that provides the framework for the model. The Reasons-Constraints-Outcome framework and the necessary/sufficient digital forensics properties, she claims, can be adapted to any domain.

Michael Andrew has proposed further theoretical considerations (2007). He outlines the overall forensic process as Acquisition-Preservation-Analysis, and focuses in particular on formalizing the analysis phase. Starting with basic system concepts (that the whole is more than the sum of its parts, the whole determines the nature of the parts, the parts cannot be understood if considered in isolation from the whole, and the parts are dynamically interrelated or interdependent), he argues in favour of analysis in context, rather than isolating information items. Starting with two principles of well designed systems – the principle of consistent results (a well designed system will produce consistent results from any given action unless corrupted by an outside force) and the principle of static storage (data at rest will remain at rest unless accessed for a directed purpose), he poses five requirements (stated as laws): association (data must be correctly associated with the processes that created it and the source that initiated the process), context data can only be interpreted correctly in context, internal and external), access (it must be demonstrated that the individual had access to the device at the time the data was created), intent (it must be demonstrated that the data was created as the result of an intentional action taken by the user), validation (the integrity, authenticity, and accuracy of the data must be validated before it can be presented as evidence in support of conclusions and opinions). The parallels with archival science are clear, and discussed below.

6.2 Interdisciplinarity

Legal theory, computer security and information assurance, and computer science (systems architecture and computer history models) have all driven the development of digital forensics. Several writers, however, look beyond digital forensics' traditional partners to find similarities and mutual affordances in other disciplines: information theory (Hama and Pollitt 1996), records management (Irons 2006), archival diplomatics (Duranti 2009; Cohen 2015), and archival science (Kirschenbaum et al. 2010; Duranti and Endicott-Popovsky 2010; John 2012; Dietrich and Adelstein 2015).

Alistair Irons made explicit the parallels and complementarity of digital forensics and records management in his analysis of the principles of computer forensics in the context of record characteristics of authenticity, reliability, integrity and usability. 'Computer forensics', states Irons, 'should be based around the characteristics of good records, levels and nature of access and an indication of the completeness of the records'. (Irons 2006, 107) Likewise, computer forensics techniques can help the records manager monitor the integrity, authenticity, reliability and completeness of records. Irons also proposed that computer forensics could benefit through the application of theoretical models of the record.

In *Digital Forensics and Born Digital Content in Cultural Heritage Collections,* Michael Kirschenbaum, Richard Ovenden, and Gabriela Redwine examine the relevance of digital forensics for archivists, curators, and others working in the field of cultural heritage. One purpose of the report was to promote interdisciplinarity between fields increasingly recognized as having converging interests (2010).

The Digital Records Forensics Project, conducted at the University of British Columbia from 2009 to 2011 and funded by the Social Sciences and Humanities Research Council of Canada studied the challenges presented by digital technology to the records management, archival and legal professions, including the identification of records among all the digital objects produced by complex digital systems, and the determination of their authenticity when they are removed and stored outside of their originating systems. The interdisciplinarity explored by the project is represented in Fig. 1 (Rogers 2010).

One of the research objectives of the DRF project was to develop the theoretical and methodological content of a new discipline, called Digital Records Forensics, resulting from an integration of archival diplomatics,[1] digital forensics, and the law of evidence (Duranti 2009; Rogers 2013). The project also led to a new proposed academic curriculum that weaves the complementary knowledge from archival science and digital diplomatics with digital forensics and information assurance (Duranti and Endicott-Popovsky 2010). A course entitled Digital Diplomatics and Digital Records Forensics (ARST 556H) taught in the Master of Archival Science program at UBC addresses the convergence of digital forensics and archival science for the purpose of furthering digital archival work.

7 Digital forensics and archival diplomatics – pulling it all together

Archival science and digital forensics are, first and foremost, applied sciences. Both evolved out of practice and grew into established professional disciplines by developing theoretical foundations, which then returned to inform and standardize practice. They have roots in law and legal practice, and professionals in both fields are trusted to attest to the identity and integrity of the materials for which they are responsible – they are regarded as experts in the acquisition, interpretation, description and presentation of that material. A significant challenge to both fields, therefore, is the identification of records (archival focus) and evidence (digital forensics focus) in digital systems, establishing their contexts, provenance, relationships, and meaning.

The digital archivist is concerned with identifying records among all the digital objects present in digital media, and assessing their reliability, authenticity, and accuracy. When an archivist acquires records contained in a digital storage device for appraisal and accessioning (ingest) into a repository, it is critical that she be able to identify the records on the device, analyze them to ascertain their provenance, assess their authenticity and accuracy, establish whether there are issues regarding intellectual property or copyright, privileged communication, or personal information that will be subject to redaction, data privacy protection, or access restrictions. The digital forensics investigator is similarly concerned with identifying digital objects that may serve as

[1] Diplomatics is a discipline first developed in the seventeenth century to assess the authenticity of documents, taught in faculties of law and archival science in Europe, and subsequently applied to modern office documents and digital records (Duranti and Thibodeau, 2006).

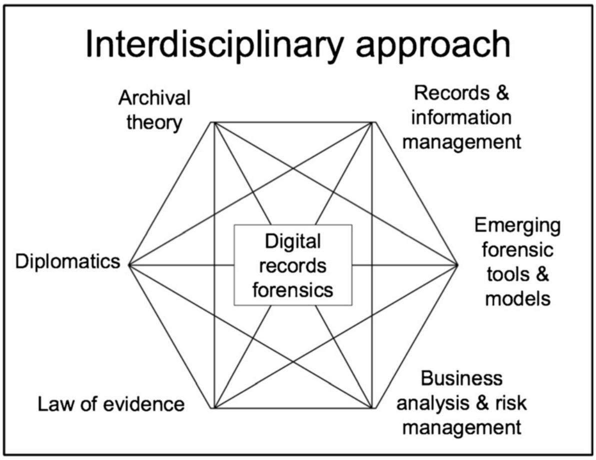
Interdisciplinary approach
Archival theory
Records & information management
Emerging forensic tools & models
Business analysis & risk management
Law of evidence
Diplomatics
Digital records forensics

Fig. 1 Interdisciplinary approach

evidence of criminal or other activity, and analyzing those objects for their evidentiary capacity, that is, their attribution, integrity, and verifiability. Privileged information must also be identified and protected from unauthorized disclosure (Rogers 2013).

Archivists and digital forensics practitioners share the challenges of appraising and analyzing large volumes of digital material. The core archival functions are appraisal and acquisition, arrangement and description, retention and preservation, management and administration, reference and access (Duranti and Giovanni 2015). The ability to preserve digital records that are authentic and reliable over time and across technological change also depends on the circumstances of records creation and record keeping, thereby extending the archival functions across the entire life of the records. This compares with the functions of digital forensics practice: identification, preservation, collection, examination, analysis, presentation and decision (Palmer 2001). At the root of each is investigative research into the material in question – namely the story revealed by analyzing the digital objects and traces of activities, and the relationships of those objects and traces to the actors and actions that gave rise to them.

The archival first principle is *respect des fonds*, essentially equivalent to the principle of provenance and the principle of original order. These principles demand that the records of one creator are maintained separately from another creator, and that a creator’s records are kept in the same order in which they were created and used. When they are respected and articulated through archival description, the authenticity of the record aggregations is protected (MacNeil 1995, 2005; Millar 2006). A presumption of authenticity derives from the context of creation and chain of custody, and the processes of establishing intellectual, administrative, and usually, physical control – appraisal, accessioning and archival arrangement. Description is the primary means of illuminating provenancial and contextual relationships that are at the heart of the principles.

Archival description is the expression of the essence of the archivist’s accountability, which confers authority, and in court, affords the status of expert witness. Records offered in evidence must be authenticated, and the archivist who is responsible for the records has that authority. By exerting intellectual control over the records through archival description, the archivist becomes accountable for the records and can speak with authority to their identity and integrity—to their trustworthiness. The archivist is recognized as a trusted custodian and confers trustworthiness on the records by virtue of his or her accountability.

The digital forensics practitioner, confronted with a digital crime scene, may be compared with the archivist, who, when processing a new acquisition by the archives, must approach the task of arrangement and then description of these records, which have been removed intellectually and physically from their creator, that is from their functional, documentary and technological context, and placed in the context of the investigation. We have seen that accountability is intertwined with responsibility, authority, and trust (Millar 2006). Just as the archivist acquires the status of trusted custodian through accountability for the records, digital forensics practitioners are called upon as expert witnesses to account for and report their investigative process.

Digital forensics practitioners act as expert witnesses because of their accountability to the investigative process. They are bound, however, by a different set of demands than archivists: theirs is scientific testimony given to justify their tools and techniques in identifying and authenticating digital evidence. Scientific testimony may be tested for credibility in a *Daubert* hearing.

Digital objects are examined not as documentary residue of business activity, 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 forensics practitioner.

The authority conferred upon these professionals has different roots deriving from the particular ontological view of the evidence they seek to authenticate. However, despite the different vantage points of the archival and digital forensic analysis of digital evidence, the goals are the same: to identify and authenticate digital evidence. To that end, the 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. As Cohen has shown, there can be a crosswalk drawn between the concepts of diplomatics and the elements of forensic examination (Cohen 2011).

Records are considered trustworthy if they can be shown to be authentic (by establishing their identity and assessing their integrity), reliability, and accuracy. In the digital environment, archivists benefit from also incorporating concepts from digital forensics: concepts of authentication, reproducibility, non-interference, and minimization (Mocas 2004), and laws of association, context, access, intent, and validation (Andrew 2007).

References

Andrew, M. (2007). Defining a process model for forensic analysis of digital devices and storage media. In Northwest security institute and pacific northwest national laboratory (Eds.), *SADFE* 2007*: Second International Workshop on Systematic Approaches to Digital Forensic Engineering: Proceedings: 10–12 April* 2007*, Seattle, Washington, USA*, 16–30. Los Alamitos, Calif: IEEE Computer Society.

Association of Chief Police Officers (ACPO). (2012). G*ood practice guide for computer-based electronic evidence, v. 5*. Retrieved from https://www.7safe.com/about-7Safe/downloads/acpo-guidelines.

Beebe, N., & 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. In G. Peterson & S. Shenoi (Eds.), *Advances in digital forensics VII* (pp. 23–34). IFIP AICT 361. IFIP International Federation for Information Processing.

Carrier, B. (2003a). Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of Digital Evidence, 1*(4), 1–12.

Carrier, B. (2003b). Open source digital forensics tools: The Legal Argument. www.digital-evidence.org/papers/opensrc_legal.pdf.

Carrier, B., & Spafford, E. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence, 2*(2), 1–20.

Carrier, B., & Spafford, E. (2004). An event-based digital forensics investigative framework. Presented at DFRWS 2004, Baltimore, MD. http://www.digital-evidence.org/papers/dfrws_event.pdf. Accessed 6 Jan 2017.

Carrier, B., & Spafford E.H. (2006). Categories of digital investigation analysis techniques based on the computer history model. *Digital Investigation*, 3, (Supp 1), 121–130.

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

Charters, I. (2009). The evolution of digital forensics: Civilizing the cyber frontier. http://www.guerilla-ciso.com/wp-content/uploads/2009/01/the-evolution-of-digital-forensics-ian-charters.pdf. Accessed 21 April, 2018.

Ciardhuáin, S. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence, 3*(1), 1–22.

Cohen, F. (2011). Digital forensic evidence examination. 3rd ed. Livermore, CA: Fred Cohen & Associates.

Cohen, F. (2015). Digital Diplomatics and forensics: Going forward on a global basis. *Records Management Journal, 25*(1), 21–44. https://doi.org/10.1108/RMJ-03-2014-0016.

Collier, P. A., & Spaul, B. J. (1992). A forensic methodology for countering computer crime. *Artificial Intelligence Review, 6*, 203–215.

Diamond, E. (1994). The archivist as forensic scientist—seeing ourselves in a different way. *Archivaria, 38*, 139–154.

DiClemente, A., Horvath, M., & Pollitt, M. (2004). Digital evidence-a review: 2001–2004. *Proceedings of the 14th International Forensic Science Symposium*, 412–549. Lyon, France. https://pdfs.semanticscholar.org/6d39/4c44dc354e90986ed14c56cbf13e66905a7d.pdf. Accessed 21 April, 2018.

Dietrich, D., & Adelstein, F. (2015). Archival science, digital forensics, and new media art. *Digital Investigation, 14*, 137–145. https://doi.org/10.1016/j.diin.2015.05.004.

Duranti, L. (1996). *Archival science. Encyclopedia of Library and Information Science* (pp. 1–19). New York, Basel, Hong Kong: Marcel Dekker.

Duranti, L. (2009). From digital Diplomatics to digital records forensics. *Archivaria, 68*, 39–66.

Duranti, L., & Endicott-Popovsky, B. (2010). Digital records forensics: A new science and academic program for forensic readiness. *Journal of Digital Forensics, Security and Law, 5*(2), 1–12.

Duranti, L., & Giovanni, M. (2015). The archival method: Rediscovering a research tradition. In A. Gilliland, S. McKemmish, & A. Lau (Eds.), *Research in the archival multiverse* (pp. 75–95). Melbourne: Monash Publishing.

Duranti, L., & Thibodeau, K. (2006). The concept of record in interactive, experiential and dynamic environments: The view of InterPARES. *Archival Science, 6*(1), 13–68.

Eastwood, T. (1994). What is archival theory and why is it important? *Archivaria, 37*, 122–130.

Garfinkel, S. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*, 64–73. https://doi.org/10.1016/j.diin.2010.05.009.

Hama, G., & Pollitt, M. (1996, August). Data reduction - refining the sieve. Presented at *International Conference on Computer Evidence*. Melbourne, Australia: IOCE. www.digitalevidencepro.com/Resources/Sieve1.pdf. Accessed 21 April, 2018.

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

Internet / Home - INTERPOL. (n.d.). Accessed March 1, 2018. https://www.interpol.int/.

Irons, A. (2006). Computer forensics and records management – compatible disciplines. *Records Management Journal, 16*(2), 102–112. https://doi.org/10.1108/09565690610677463.

John, J. (2012). Digital forensics and preservation. Digital preservation coalition. http://www.dpconline.org/component/docman/doc_download/810-dpctw12-03pdf. Accessed 21 April, 2018.

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, 13*, www.vjolt.net/vol6/issue3/v6i3-a13-Kenneally.html.

Kirschenbaum, M., Ovenden, R., & Redwine, G. (2010). *Digital forensics in born digital cultural heritage collections*. Washington, D.C.: Council on Library and Information resources.

Lee, C. (2012). Archival application of digital forensics methods for authenticity, description and access provision. *Comma, 2012*(2), 133–140. https://doi.org/10.3828/comma.2012.2.14.

MacNeil, H. (1995). Metadata strategies and archival description: Comparing apples to oranges. *Archivaria, 39*, 22–31.

MacNeil, H. (2005). Picking our text: Description, authenticity, and the archivist as editor. *The American Archivist, 68*(2), 264–278.

Marsico, C. (2005). Computer evidence v. Daubert: The coming conflict. Purdue University. https://www.cerias.purdue.edu/apps/reports_and_papers/view/2819/.

Menne-Haritz, A. (1994). Appraisal or documentation: Can we appraise archives by selecting content? *The American Archivist, 57*(3), 528–542.

Millar, L. (2006). An obligation of trust: Speculations on accountability and description. *The American Archivist, 69*(1), 60–78.

Mocas, S. (2004). Building theoretical underpinnings for digital forensics research. *Digital Investigation, 1*(1), 61–68.

Noblett, M. G., Pollitt, M., & Presley, L. A. (2000). Recovering and examining computer forensic evidence. *Forensic Science Communications, 2*(4) http://www.ncjrs.gov/App/publications/abstract.aspx?ID=186015. Accessed 16 Feb 2019.

Palmer, G. (2001). A road map for digital forensic research. DFRWS Technical Report. http://www.dfrws.org/2001/dfrws-rm-final.pdf.

Pollitt, M. (1995a). Principles, practices, and procedures: An approach to standards in computer forensics. Presented at *Second International Conference on Computer Evidence.* Baltimore, Maryland: IOCE. www.digitalevidencepro.com/Resources/Principles.pdf. Accessed May 17, 2018.

Pollitt, M. (1995b). Computer forensics: An approach to evidence in cyberspace. In Wakid, S. and Davis, J., Eds. *Proceedings of the 18th International Systems Security Conference*, (pp. 487–91). Baltimore, Maryland: NIST. https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1995/10/10/proceedings-of-the-18th-nissc-1995/documents/1995-18th-NISSC-proceedings-vol-1.pdf. Accessed 21 April 21, 2018.

Pollitt, M. (2001). Report on digital evidence. Lyon, France. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.304.8748&rep=rep1&type=pdf. Access 21 April, 2018.

Pollitt, M. (2003). Who Is SWGDE and what is the history? https://www.swgde.org/pdf/2003-01-22%20SWGDE%20History.pdf. Accessed 21 April, 2018.

Pollitt, M. (2010). A history of digital forensics. *IFIP Advances in Information and Communication Technology, 337*, 3–15. https://doi.org/10.1007/978-3-642-15506-2_1.

Reedy, P. Diplock, B., & Dunlop, M. (2007). Digital evidence-a review: 2004–2007. *Fifteenth International Forensic Science Symposium* (pp. 414-36). Lyon, France.

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence 1*(3). https://utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf. Accessed 21 April, 2018.

Rogers, C. (2010, June). *Digital records forensics: Preliminary findings. Presented at the Association of Canadian Archivists*. Canada: Halifax.

Rogers, C. (2013). Digital records forensics: Integrating archival science into a general model of the digital forensics process. *Proceedings of the Second International Workshop on Cyberpatterns: Unifying Design Patterns with Security, Attack and Forensic Patterns*, C. Blackwell (Ed.), 4–21. Oxford, UK: Oxford Brookes University.

Rogers, C., & John, J. (2013). Shared perspectives, common challenges: A history of Digital Forensics & Ancestral Computing for digital heritage. In *In The Memory of the World in the Digital Age: Digitization and Preservation (pp. 314–36). Vancouver, BC: UNESCO* http://iibi.unam.mx/archivistica/UNESCO%202013%20MOW%20vancouver%20declaration.pdf. Accessed 21 April, 2018.

Selamat, S., Yusof, R., & Sahib, S. (2008). Mapping process of digital forensic investigation framework. *IJCSNS International Journal of Computer Science and Network Security, 8*(10), 163–169.

Stoll, C. (1989). The cuckoo's egg: Tracking a spy through the maze of computer espionage. Doubleday. http://bayrampasamakina.com/tr/pdf_stoll_4_1.pdf. Accessed 21 April, 2018.

SWGDE, & IOCE. (2000). Digital evidence: Standards and principles. *Forensic Science Communications 2*(2). http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/. Accessed 21 April, 2018.

Whitcomb, C. (2002). An historical perspective of digital evidence: A forensic Scientist's view. *International Journal of Digital Evidence 1*(1). http://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf. Accessed 21 April, 2018.