Shared Perspectives, Common Challenges

A History of Digital Forensics & Ancestral Computing for Digital Heritage

Corinne Rogers[1] & Jeremy Leighton John[2/1]

[1]*School of Library, Archival and Information Studies, University of British Columbia, cmrogers@mail.ubc.ca;*

[2]*Department of Digital Scholarship, The British Library*

Abstract

Although the field of computer forensics might appear distinct from the curation and preservation of cultural objects, these disciplines have overlapping histories and legacies deriving from shared challenges and theoretical perspectives. A convergence of practice of the digital forensic investigator and the digital archivist is gaining momentum as collecting institutions are faced with growing accessions of digital media. Shared theoretical perspectives include issues relating to authorship and identity, informational pattern and change over time, evidential reliability, and digital materiality. Shared challenges include the volume of a person's life information spread across myriad devices, the complexity of diverse applications and locations, the necessary versatility of tools and techniques required to capture, investigate, and describe digital information, planning to ensure sustainability and long-term preservation, and issues of security, privacy and other digital rights. This paper offers a historical overview of digital forensics mapped to current issues in digital curation and preservation in cultural heritage domains.

Authors

Corinne Rogers comes from a senior administrative background in non-profit organizations with an interest in policy and governance. Currently a doctoral student at UBC's School of Library, Archives and Information Studies, her research interests focus on legal and ethical issues associated with digital materials offered as evidence at trial. She is a research assistant under the direction of Dr. Luciana Duranti in InterPARES and the recently completed Digital Records Forensics Project. Corinne is also a researcher with the Veterans Transition Program at UBC where she is establishing an oral history project.

Dr Jeremy Leighton John has been Curator of eMANUSCRIPTS at the British Library since 2003, previously having been Specialist Scientific Curator. In 1996 he completed a DPhil in Zoology at Merton College, University of Oxford. He is a Fellow of the Linnean Society of London and of the Royal Geographical Society. As Principal Investigator of the Digital Lives Research Project funded by the UK Arts & Humanities Research Council, he promoted archival digital forensics. Currently, a member of the Committee of the Section for Archives and Technology within the Archives and Records Association of UK & Ireland; previously, a member of the Library Committee of the Royal Society.

1. Introduction

The field of forensics and investigation might at first glance seem quite separate from the curation and preservation of cultural objects; yet these disciplines have overlapping histories and legacies deriving

1 The authors made similarly substantial contributions to the paper

from similar goals, common challenges, and shared theoretical perspectives. A convergence of perspectives and methods of the digital forensic investigator and the digital archivist is gaining momentum as collecting institutions are faced with growing accessions of digital media and objects (John 2008; Kirschenbaum, Ovenden, and Redwine 2010). The conceptual underpinnings of digital (or computer) forensics[2] can be interpreted through the lens of information and archival science, to illuminate parallels between these disciplines and reveal avenues of further research to their mutual benefit. This paper outlines points of convergence between these disciplines, offers a historical overview of digital forensics, and discusses its relevance to ancestral computing and issues of digital curation and preservation in cultural heritage domains. The role of an archivist may be as a record keeper, caring for the documentary legacy of an organization, or as a curator of a personal archive of a writer, scientist or political figure. Both functions are embraced by this paper.

2. Similar Goals

2.1 Archival Function

At the most basic level, both digital archivists and digital forensics practitioners are concerned with discovering, understanding, describing and presenting information inscribed on digital media.

The core archival functions "upon which archivists build their scientific, professional and educational profiles" (Duranti and Michetti 2012) can be identified as appraisal and acquisition, arrangement and description, retention and preservation, management and administration, and reference and access. Furthermore, research may be considered the foundation of each archival activity, "a professional function if not the core of all functions" (Duranti and Michetti 2012).

Archival research has focused historically on records, defined as documents created or received in the course of practical activity, and set aside for further action or reference (Duranti and Thibodeau 2006), as the primary objects of investigation. Records serve as evidence of actions and transactions, and lose much of their meaning in isolation or removed from their juridical or institutional context. In their analysis, the archivist strives to determine the purpose and functions of their creator, and the means and methods of their documentation. The informational content of records may in some cases be less important to this analysis than the circumstances of their creation and use. Personal archives may be investigated for their content as when a series of drafts leading to a final published novel is critically examined for evidence of literary creativity. Archivists are thus concerned with establishing the evidentiary capacity of documents, and analysing their evidential value, whether they are preserved primarily as records (as with a public organisation) or for their informational value as personal memory or legacy (as with a personal archive). According to Menne-Haritz, "Evidence 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" (Menne-Haritz 1994).

Although archival theory originated in legal and administrative doctrine reaching back many centuries to Roman times, modern archival scholarship has its roots in the 17th and 18th centuries, when it

[2] Early practitioners referred to the practice of computer forensics. As digital devices become ubiquitous and diverse, the term "digital" has begun to replace "computer" (see for example 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, and is particularly appropriate in the context of ancestral computing and legacy hardware and software.

became closely aligned with historical scholarship, adopting and adapting methods of historical research and the philological disciplines to archival research into documents in the prevailing world of print. Today we live in a digital world. Computer technology has changed the way we communicate, conduct business, present our public face(s), and document our private lives. As digital communications supplant print-based culture, a new literacy is evolving. Digital culture is challenging the viability and legitimacy of many well-established social and cultural norms and their associated legal frameworks (Doueihi 2011).

One aspect of this evolution can be observed in our concepts of trust in digital information and our reconception of what it means for a digital object to serve as documentary evidence, which relies on our ability to assess its authenticity and integrity. We are tempted to consider the records, documents, and information that we create and disseminate over the Internet as being equivalent to similar forms in our traditional, analogue world. Because of an assumption of functional equivalence of digital and analogue documents and data, the authenticity and trustworthiness of these new digital creations are often judged by the same standards. However, "Virtual authenticity is not to be explained by a transfer of a well-known and ultimately problematic category from one model to another; it is not to be restricted to a shift from the real to the virtual" (Doueihi 2011). Archivists are embracing the new digital literacy, re-examining traditional concepts of retained information – records, documents, data – and the attributes by which we have traditionally assessed evidentiary capacity and evidential value. Archival methodologies, developed originally over centuries in a print-based culture, are being adapted to address digital material, and are embracing new disciplinary knowledge in order to do so.

2.2 Digital Forensic Function

The new discipline of digital forensics was developed originally for the purposes of law enforcement in order to investigate computer crime and bring digital evidence to trial. It applies scientific principles and methodologies in reconstructing past events and artefacts, and has developed technologically in intimate association with the advancement of forensic tools. It is defined as:

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence[1] 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).

Throughout its history there have been calls for digital forensics to be situated within a broader social and theoretical framework (Palmer 2001). Drawing on computer science theory and forensics theory from physical forensics disciplines, digital forensics practitioners and researchers are actively developing process models that can be used to help standardize digital forensics investigations and form the basis of new theory. These process models identify core digital forensics activities, and from these, we can draw close parallels with archival functions. Beebe and Clark (2005) have proposed one such model, and mapped their framework to similar, previous frameworks commonly cited in the literature.[3] The core functions of the Beebe and Clark model are preparation and incident response, data collection, data analysis, presentation of findings, and incident closure. The first three may be compared with archival

[3] The models compared by (Beebe and Clark 2005) are: the DFRWS model (Palmer 2001; US Department of Justice 2001; Reith, Carr, and Gunsch 2002; Carrier and Spafford 2003; Mandia et al. 2003; Nelson et al. 2004, O'Ciardua'in 2004; Casey and Palmer 2004).

functions of appraisal and acquisition, while data analysis parallels arrangement and description, and elements of presentation of findings (also evident in arrangement and description) may be seen in reference and access, and elements of incident closure may be compared with archival retention and preservation.

2.3 Convergent Utility of Evidence

Digital forensics thus offers digital archivists another way of conceptualizing digital objects and assessing their integrity and authenticity that can complement and be complemented by existing archival methodologies (Duranti and Endicott-Popovsky 2010; Duranti and Rogers 2011). Digital forensic tools and techniques are also being applied in service of information security, including incident investigation and forensic readiness, or incident prevention (Endicott-Popovsky, Frincke, and Taylor 2007; Endicott-Popovsky and Frincke 2007; Taylor, Endicott-Popovsky, and Frincke 2007). They are increasingly being tested in trusted digital repositories to assist archival processes of acquisition, selection, appraisal, description, and preservation of cultural and scientific heritage materials (John 2008; Kirschenbaum 2008; Kirschenbaum, Ovenden, and Redwine 2010).

There is an increasing desire in both the archival and the digital forensics communities to look to knowledge in complementary disciplines to investigate the challenges to theory and practice presented by digital technologies. Social and natural sciences, humanities, law and digital forensic discipline, and the information disciplines are all evidence-based disciplines, and so have a stake in the trustworthiness of digital material and its preservation, and each brings unique theoretical perspectives to bear.

3. Common Challenges

3.1 Digital Diversity, Volume & Complexity

Some of the biggest challenges faced by digital forensic scientists and practitioners are the diversity of digital media, the sheer volume of digital material, and the complexity of the problems of capture and analysis. This similarly confronts those who are responsible for digital archives and cultural heritage repositories, for these may contain representatives of digital objects and media that come from almost anywhere. At the same time the size of the digital universe[4], and the rate of technological change are far outpacing the capacity of archivists and forensic examiners to keep up.

3.2 Versatility of Tools & Techniques for Digital Forensic Analysis and Curation

"Just as it has been said that 'one software tool does not a computer examiner make', only possessing one investigative process model is equally as limiting. Computer forensics examiners need a repertoire of tools and just as important a repertoire of examination and investigative approaches" (Rogers et al. 2006). To address the profusion of digital objects and media in countless situations it is necessary to have a variety of tools and not to rely on any single technology or methodology. Equally the workflows and procedures need to be receptive to change, to be designed for flexibility and adaptability so that new functions can be quickly embraced and integrated.

This novelty, diversity and complexity of tools and digital objects in turn calls for a careful and extensive marshalling of metadata and documentation. This is a requirement that may draw on the rapidly increasing experience and expertise of the digital archive and data curation communities.

[4] http://www.emc.com/leadership/programs/digital-universe.htm

Historically, much of the analysis software used by digital forensics practitioners has been proprietary and commercial or custom-built for local use. Increasingly, open source solutions are being sought and developed. This benefits forensics analysts, supports admissibility requirements of digital evidence at trial, and enhances capacity for archival processing and long-term preservation in digital repositories (Altheide and Carvey 2011).

3.3 Long Term & Lifecycle Considerations for Digital Preservation

The long-term sustainability of digital objects and the information that these bear, and their continuing accessibility and usability over time has been a primary driver, a *raison d'être*, for the digital preservation community. It is increasingly a concern for the digital forensic community too, which has made some important steps including the development of the Advanced Forensic Format, a new open source format for storing disk images (Cohen, Garfinkel, and Schatz 2009; Garfinkel 2006; Garfinkel et al. 2006; Garfinkel 2009). Although the timeframes of legal and archival activities are different, with archives generally holding material indefinitely if not 'forever', in the legal context too it is often necessary to care for artefacts for periods longer than digital media and objects can be expected to survive without due care and attention.[5] It is an area that could benefit significantly from the attention of digital preservation developers and practitioners.

3.4 Security, Privacy, and Digital Rights

The ease with which digital material can be altered, intentionally or accidentally, and the ease with which it can be disseminated, shared, combined, and repurposed, has driven security, privacy, and rights concerns across domains and disciplines. Information and network security, measured in various types of integrity analysis and control, is foundational to digital forensics, while protection of privacy and management of digital rights are at the forefront of archival concerns. While digital forensics addresses privacy and security in the context of intrusion detection and incidence response, digital archivists and curators must be aware of privacy and rights requirements in order to manage description of and access to material entrusted to their care.

4. Shared Theoretical Perspectives

The ensuing portrayal of shared perspectives does not negate the differences in outlook and purpose between forensic examiners operating in a legal context and those adopting the techniques for the purposes of curation and preservation. In the context of law enforcement, there is a perpetrator and a victim, and digital forensics is employed to uncover and present evidence that will be material in the case at issue. Once a legal case has been completed or is closed, the evidence tends to be put aside and stored without further access or management (unless there is an appeal). Long-term preservation of supporting material, including migration to ensure continued accessibility, is often not undertaken. Scholarly examination of archival material, on the other hand, continues indefinitely, and is repeated over time as new and varying research goals are adopted. The archivist who secures digital material and initially interprets it through archival analysis and description expects to be followed by historians who investigate the archive decades and centuries later. These purposes are quite different, even if the elimination of

[5] Personal communication, Tony Sammes and Brian Jenkinson, October 2011

hypotheses is a critical approach in each discipline (Fraser and Williams 2011; Fraser 2010), and lead to different applications and requirements of digital forensic tools and techniques.

4.1 Authorship & Identity

There has been a longstanding interest in the identification of forgeries specifically and in ascertaining the origin of all documents generally. Forgeries were rife in medieval and classical times, requiring vigilance with respect to their authenticity at the time and their authentication subsequently by historical scholars. Examination and investigation of handwriting (palaeography) and document analysis have long played a prominent role in identifying authors (Nickell 2005).

The science of diplomatics developed since the 17th century to establish the authenticity, and indirectly, the reliability, of archival documents, in order to determine rights and to identify and eliminate forgeries. Diplomatics is concerned with proving that a document is what it purports to be through the study of its genesis, forms, and transmission, and the relationships of the documents with the actions and persons and with its juridical context. Diplomatic criticism has evolved to analyse and evaluate individual documents in terms of a recognized system of formal elements, through which those documents can be shown to have been "written according to the practice of the time and place indicated in the text, and signed with the name(s) of the person(s) competent to create them" (Duranti 1998).

In the digital environment, the absence of such elements of proof of authorship and identity as handwritten signatures have led to an erosion in trust. This has been addressed over the past 13 years in the InterPARES (International Research on Permanent Authentic Records in Electronic Systems, 1999-2012) Projects, in which the theory and methodology of traditional diplomatics and the principles of archival knowledge were refined and tested to provide a framework for assessing the authenticity of digital records through the development of a new body of knowledge, digital diplomatics. Digital diplomatics offers archivists a powerful methodology for analysing digital records. However, according to Duranti, digital diplomatics alone may not be sufficient to understand the challenges posed to information inscribed by increasingly complex digital systems (Duranti 2009).

Traditional concepts of provenance and identity are severely undermined by the default of anonymity on the Internet. The identity of creator, author, writer or originator may be obscured and separated from the inscribed message by virtue of the layers of technology that mediate between physical person and transmitted document. "Establishing who is behind the keyboard at a given time is perhaps the single most commonly litigated issue involving electronic evidence" (Scanlan 2011). Just as archival principles have been combined with diplomatic concepts to provide a methodology to analyse traditional digital objects, new knowledge from digital forensics may extend digital diplomatics to illuminate growing challenges to issues of provenance, identity, and integrity in increasingly complex digital environments.

4.2 Integrity and Change over Time

Philology, textual criticism, decipherment, stemmatics, phylogenetics and cladistics, historical relatedness, semiotics, and more recently fuzzy hashing, all share an interest in how objects change with the passage of time. The key concept is relatedness. Historically, it has been much concerned with the development of some writing or work, and contemplates the relationship between objects, entities, existing contemporaneously (e.g. today) or longitudinally through time.

The 17th and 18th centuries saw the deepening of critical scholarship with the development of systematic investigation of literary style, poetic harmony and formal measures, chronological inconsistencies and aberrations, historical incongruities, and the presence and absence of independent, long lasting evidence (Levine 1989). The parallels in stemmatics and phylogenetics and their use in forensics, historical reconstruction, and conjectural criticism is an active area of research today (John 2009; Kraus 2009).

Integrity, once presumed from the controls on the procedures dictated by the creator of a record, now may be assessed in the absence of or further to provenance and explicit identity, and at both the physical (bits) and logical (meaning) layers of the record. Digital forensics offers another way of conceptualizing digital objects and assessing their integrity that can complement and be complemented by digital diplomatics in understanding and assessing the elements of authenticity of digital objects (Duranti and Endicott-Popovsky 2010; Duranti and Rogers 2011).

4.3 Procedures for Establishing Authenticity and Reliability of Evidence

Curation and forensics share a concern with provenance and the application of tested and certifiably reliable protocols and tools: the collection of a set of digital objects, the evidence (legal or historical), and its subsequent demonstrable authentication, once it is in the care of the responsible institution (and its evidence custodian).

Three central requirements of digital forensics match those of archivists: capturing the information without changing it, demonstrating that the information has not been changed or that the changes can be identified, and analysing and auditing the analysis of the information, again without changing it (see John 2008).

Some of the functionality of forensic software can be found in assorted tools that exist independently of the forensic community, some of it freely available on the internet. An important distinction is that forensic software is routinely subject to appraisal and peer examination (not to mention the daily scrutiny of the law courts) as well as increasingly rigorous formal testing conducted according to specified protocols and overseen by independent bodies such as the National Institute of Justice and the National Institute of Standards and Technology in the USA.[6]

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. The assessment of reliability and integrity is based on procedures that are repeatable, verifiable, objective, and transparent. Digital forensics tools are subject to a demonstration that they have been tested, that the error rate is known and within acceptable limits, that the tool or procedure has been published and subjected to peer review, and that it is generally accepted in the relevant scientific community (Carrier 2003). Admittedly, there is much more testing to be done and its implications remain to be comprehensively implemented and consolidated across practicing organizations.

4.4 Digital Materiality, Virtualisation & the Importance of Ornament

Just as curators and scholars attach significance to the materiality of objects, to their look and feel and behaviour, in the fullest of detail, so forensic examiners have come to realise the importance of these qualities, with for example the emergence of virtual forensic computing, involving the use of virtual

[6] http://www.cftt.nist.gov/; http://www.nsrl.nist.gov/.

machines, emulators and 3D virtual reality. This has led to the development of tools such as Virtual Forensic Computing (VFC) produced by MD5 (UK) and based on work conducted at Cranfield University in the UK (Penhallurick 2005). At the end of forensic examination and analysis it is necessary to present the material in a manner that matches (to varying degrees) the original computer environment as well as the real landscape setting itself (Schofield 2009). An example of a textbook that provides general practical advice for the presentation of digital evidence in court is that of Sammes and Jenkinson (2007).

5. Looking Back to Look Forward

5.1 The Forensics of Ancestral Computers

The rapid pace of technological change means that forensic researchers are continually having to explore new techniques and develop new tools to support security and counter criminality. Over time the modern forensics community tends to become less focused on earlier computing technologies and forensic techniques. To forensics experts concerned with staying ahead of criminal activity in cyberspace, the progress of the previous decade is becoming less relevant (Garfinkel 2010). However, the tools and techniques created to analyse older technology remain crucial to scholars such as historians and archivists, who increasingly rely on digitized and born digital material in a variety of ancestral and legacy formats. In the archival context, it is unlikely that computing in, say, the 1990s will cease to be of any interest to digital scholars. This requirement will motivate continuing research into the forensics of ancestral computers and other digital devices.

In principle, there are two major kinds of ancestral computer forensic techniques, tools and knowledge bases: (i) those developed by earlier generations of practicing computer forensic experts; and (ii) those developed subsequently as a retrospective research activity by contemporary classic computer enthusiasts, computer history conservationists, and, increasingly, digital scholars and curators. A third and emerging source of expertise might be the current generation of researchers and developers operating in the field of personal information management (PIM) and the research output of this and related fields such as software development.

Future researchers of ancestral computer forensics would benefit from being able to look back over many decades and examine the way the forensic capabilities have changed. With early disks, for example, the low track density resulted in greater space between each track, and the head would wander over the floppy disk or platter. Deletion and overwriting would be incomplete and data potentially could be retrieved from earlier writes (Nelson et al. 2004) in ways that would be more forbidding with comparable technology today.

5.2 Digital Forensics: Knowledge Retention

An important requirement from the curatorial point of view is to document digital forensics knowledge even before it ceases to be of strong relevance to the wider forensics community. The earlier experiences of the forensics community represent an important resource, to match that of the original developers and usability designers of the hardware and software. This knowledge is already being lost, according to several forensics experts (Charters 2009; Garfinkel 2010; Pollitt 2010), and there are efforts to preserve it, at least from the perspective of the forensics community, for the purposes of better understanding future directions (Charters 2009) rather than supporting its use with obsolete media. The British Library has

initiated discussions with forensic practitioners about documenting early computer forensic experiences and tools, with the aim to record interviews in due course.

5.3 History of Digital Forensics: Introduction

In the past three years three short historical retrospectives have been written that capture early development and identify future directions of digital forensics practice (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 intelligence community, law enforcement and academic perspectives. 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.

Charters' background is in IT security and information assurance spanning more than 20 years in the United States' Intelligence Community. Like Pollitt's informant, Charters believes that by "looking at the way forensics evolved in the past, with an eye to the pressures that guided its evolution, we could get a better understanding of how forensics would evolve in the near future." He explains the development of computer forensics in three stages of evolution – the Ad Hoc Phase, the Structured Phase, and the Enterprise Phase.

The twin lenses that Charters focuses on the development of digital forensics are those of policy and procedure, and forensic tool development. The Ad Hoc Phase was characterized by lack of structure, goals, Appropriate Use policy and procedures, and challenges to the accuracy of forensic tools. This phase appears to be cyclical and transcend computer technology – it happened in the mainframe era and again in the microprocessor era. (Charters wonders if it is doomed to happen again in the wake of new technologies.) The resulting confusion led 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 – 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 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.

These phases map neatly to the concept of epochs, with which Pollitt outlines the salient characteristics of the profession. Pollitt begin with "pre-history" (pre-1985 characterized by mainframe computing, an ad hoc and individualized approach to digital forensics), and, adopting a lifecycle model, moves from "infancy" (stand-alone PCs and dial-up internet, forensics in service of law enforcement, development of the first forensics groups and task forces[7]), through "childhood and adolescence" (rapid development of diverse technologies, broadband, increasing professionalization[8]), with "maturity" (characterized by greater opportunities for academic training, certification, standardization, and research) 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

[7] For example, the FBI, IACIS (International Association of Computer Investigative Specialists), and IOCE (International Organization on Computer Evidence.

[8] Including establishment of SWGDE (Scientific Working Group on Digital Evidence), DFRWS (Digital Forensic Research Workshop), and IFIP (International Federation for Information Processing) Working Group on Digital Forensics.

years as a Special Agent of the Federal Bureau of Investigation, approaches the history through the lens 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 (Pollitt, 2010). These epochs are particularly relevant in an analysis of digital cultural heritage and the application of ancestral computing.
Garfinkel, 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, 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 (2010). He argues that we are coming to the 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. We are facing an impending crisis, however, brought on by advances and fundamental changes in the computer industry – specifically increased storage capacity, proliferation 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. This article is particularly important for its suggestion that research ought to focus on a completely new approach to understanding forensic data through the development of new abstractions for data representation. If this is supported by standards and procedures that use these abstractions for testing and validation of research products, the result will be lower costs and improved quality.

5.4 History of Digital Forensics: Organisations

The birth of the digital forensics field can be dated from the early 1980s. In 1984, the FBI established its Magnetic Media Program, which subsequently became the Computer Analysis and Response Team (CART). In 1985 Scotland Yard founded the Computer Crime Unit (CCU), which provided training courses at Interpol. The Federal Law Enforcement Training (FLETC) programs played a key role in dispensing an understanding of the recovery of digital data.

The literature is sparse for this early period in the development of investigative techniques for crimes involving computers. Most of the literature devoted to computer crime, found in computing and accounting journals, focuses on proactive security intended to prevent criminal acts by reducing opportunity (Collier and Spaul 1992). In 1986, however, an article appeared in the journal *Computers & Security* that addressed the problem from the perspective of the investigation of a crime after the fact (Stanley 1986).

Possibly the first published use of the term "computer forensics" in the academic literature appeared six years later in an article entitled "A forensic methodology for countering computer crime" (Collier and Spaul 1992). Collier and Spaul proposed the term "computer forensics" as a label for "existing but very limited activities amongst the police and consultancy firms" 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. Although the term appears not to have existed formally in print prior to this publication, it had long been used informally (Sommer 1998; see also Sommer 1992)

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, Pollitt, and Presley 2000). Others were long-established gatherings that began to include sessions on computer forensics, such as Interpol's International Forensic Science Symposia.

It was not until the 1990s that standardisation and dissemination began in earnest. In the UK the Computer Misuse Act was introduced in 1990, and was specifically designed to deal with criminal activities associated with computer systems, which in turn motivated greater attention towards evidence handling and other procedures.

The Royal College of Military Science (later the Defence Academy of the UK) commenced courses soon afterwards: initially as short courses, subsequently at MSc and PhD levels. The Interpol European Working Party on Information Technology Crime was established in 1993, and quickly followed by the formation of the International Organisation on Computer Evidence in 1995.

Computer forensics has been defined as "the application of science and engineering to the legal problem of digital evidence," and the admissibility of digital evidence has been related to the legal requirements of comparable paper-based evidence (Pollitt 1995). Pollitt compares the document paradigm (traditional, paper-based) with the (then) new digital paradigm in order to situate digital evidence within the legal process. He summarizes the investigative process for traditional document in four phases: acquisition -> identification -> evaluation -> admission of evidence. This has become the basis for all subsequent process models.

A handbook entitled *Computer Evidence*, produced by Edward Wilding, 1997, outlined techniques for PCs using DOS and the use of DIBS (Digital Image Backup System) and included details about the handling of evidence (Wilding 1997). This was followed by *Forensic Computing*, by Tony Sammes and Brian Jenkinson (2000), which combined first principles with practical investigation and incorporated a pioneering section on electronic organisers (a second edition appeared in 2007). It contains some of the original source references used by the forensic community at the time. Other influential texts such as *File System Forensic Analysis* by Brian Carrier and *Forensic Discovery* by Dan Farmer and Wietse Venema, both published in 2005, are listed at the end of this paper (Carrier 2005; Farmer and Venema 2005).

5.5 History of Computer Forensics: Software

Tools were produced by government agencies such as the Royal Canadian Mounted Police (RCMP) in Ottawa and the US Internal Revenue Service (IRS); but over the years, many advances in the field have been due to individual law enforcement officers and to computer technicians in the private sector (Sommer 1998).

Some investigators wrote their own tools in C and assembly language; examiners carried out their work from the DOS command prompt and through the use of hexadecimal editors. The Windows environment was avoided due to its propensity to alter data and to write to the drive.

A tool called X-Tree Gold arose in the 1980s, useful for recognising file types and retrieving lost or deleted files. Norton Disk Edit soon followed, and became a preferred tool. Later still came an expanded set of Norton Utilities as well as PC Tools. Of distinctive interest are the GammaTech Utilities for inspection and data recovery of computers with OS/2 (Wilding 1997; Nelson et al. 2004).

In the 1990s prominent suites of command line utilities became available: Maresware Forensic Processing Software Suite; and The Coroner's Toolkit (TCT). Designed for the forensic analysis of compromised Unix systems, TCT suffered from not being portable between systems and from its inability to cater for file systems other than those of Unix. It has since evolved into Sleuth Kit and Autopsy. Also noteworthy from this period were DriveSpy, Image and PDBlock of Digital Intelligence.

Around this time, ASR Data created Expert Witness for the Macintosh, the GUI forerunner of EnCase. The two GUI tools that would come to dominate computer forensics both arose in the late 1990s: EnCase of Guidance Software and Forensic Tool Kit of AccessData. For the purpose of viewing and handling a wide variety of file types, it was common for forensics experts to adopt existing viewing software such as QuickView Plus, Outside In, LView Pro, Magellan, ACDSee, ThumbsPlus and IrfanView.

A brief example of how software evolves, and how one developer picks up where another left off, is provided by file carvers which assist in the recovery of deleted files, acting independently of the file system by simply seeking to identify files through their file signatures and other identifiers. The carving tool Foremost was originally created in March 2001 by Jesse Kornblum and Kris Kendall from the United States Air Force Office of Special Investigations for analysing and recovering deleted files. It was itself inspired by the program called CarvThis that had been developed in 1999 by Defense Computer Forensics Lab although it was never released to the general public. Foremost is now open source, and the code is maintained by Nick Mikus (Spenneberg 2008).

Another tool known as Scalpel was derived from Foremost 0.69 by Golden G. Richard III, and Scalpel became highly regarded, said to be recommended by Foremost developers themselves. In recent years, Foremost has received yet more attention: "Although Scalpel was far superior to its predecessor in 2005 - with the ability to analyse images around 10 times faster - Foremost has caught up recently thanks to Nick Mikus, and it is actually superior to its derivative for some tasks"(Spenneberg 2008).

5.6 History of Computer Forensics: Legacy Machines

Nelson and colleagues have recommended that forensic practitioners retain legacy equipment for as long as possible — both software and hardware — suggesting that there are some forensic tasks using current operating systems and hardware, that cannot be performed with modern tools: "To be an effective computing investigator and forensic examiner, you should maintain a library of old operating systems and application software"(Nelson et al. 2004).

Even as the more universal and forensically dedicated tools were becoming firmly established, practitioners were reminding colleagues of the need to retain earlier computers and tools, as Microsoft, Apple and Unix/Linux became predominant. Computers such Commodore 64, Osbourne I or Kaypro running CP/M may be needed; or even a Pentium I or 486 PC for accessing an early IDE disk (Nelson et al. 2004).

5.7 Data Recovery

Alongside the development of security and forensic computing, other professions were already conducting many of the activities that are today embraced by forensics (Kane and Hopkins 1993, with a 3.5 inch floppy disk that "Contains 16 life saving utilities"). There is a multitude of publications on data recovery each catering for the diverse early computer systems as well as current ones. Data recovery companies today include: MjM data recovery, Disklabs, Xytron Data Recovery, DPTS, eMag Solutions). Professional associations include: Global Data Recovery Alliance9; and International Professional Data Recovery Association (IPDRA).[10]

[9] http://www.globaldra.org
[10] http://ipdra.org

5.8 Reverse Engineering for Interoperability

Reverse engineering was being conducted not only by those seeking to understand software or computer programs (including malware) (Eilam 2005) but in order to understand file formats and so be able to address interoperability on behalf of publishers. For example, InterMedia (UK) produced a floppy disk conversion system so that files on an extensive variety of disks could be copied to a publisher's own editing system (see John 2008). A longstanding tool in reverse engineering continuing today is IDA, an interactive disassembler and debugger[11] (Eagle 2008).

6. Classic, Retro, Vintage Computing & Gaming

6.1 Rosetta Machines

Digital scholars have invoked the concept of the Rosetta machine, any computer that is peculiarly preadapted for the interflow of information between generations of computers and storage media, citing the Macintosh Wallstreet edition of the G3 PowerBook as the holotype for this kind of technology: manufactured in 1998 it came with swappable CD, DVD, and floppy drives capable of reading 800K and 400K disks, an ethernet port, a PCMCIA slot permitting the addition of USB ports and access to an external hard drive; a swappable zip drive was also available (Kirschenbaum, Ovenden, and Redwine 2010).

A possible candidate as a Rosetta machine is the Cat Mac, a system that was designed to allow individuals to build their own Apple Macintosh computers (Brant 1991). The guide to the system also highlights the possibility of running DOS on a Mac, and an Apple OS on a PC or Atari. In addition to matching specific models it was possible to mix and match some of the components; and it might in this way be possible to build a number of dedicated and versatile Rosetta machines - if the necessary components could be found. It accepted hard drives including a removable version by Wetex, floppy drives, Iomega's Bernoulli design (predecessor of the Zip disk), SyQuest's and Ricoh's removable cartridges, optical drives (Magneto Optical, MO; Erasable Optical, EO; Write Once Read Many, WORM; Read Only, CD-ROM); tape drives including data cassettes, akin to audio cassettes but significantly different internally, and DAT 4mm cartridges; limited networking is also feasible.

6.2 Enthusiast Computing

Due to their 'universal computer' nature, computers lend themselves to self design and manipulation. Personal computing was famously driven by hobbyists experimenting at home. Apple I was a circuit design and board rather than a complete computer and even with later finished models, enthusiasts were invited to build their own – a tradition that continues to this day (Owad 2005). Subsequently this was discouraged by Apple but remained commonplace with PCs. Customers were encouraged to upgrade their computers themselves, and often needed to install their own drivers and generally tinker.

This 'universality' led, of course, to numerous types of computing devices; but it also yielded a large community of enthusiasts, many of them associated with games and gaming: in time, gradually evolving into a classic and retro computing community - with much of the activity being directed at the capture, emulation and preservation of computer games (John 2008; McDonough et al. 2010, see also

[11] http://www.hex-rays.com/products/ida/overview.shtml

recent news concerning the Princess of Persia source code)[12]. The role of ancestral computing enthusiasts has been outlined previously (John 2008); further examples are a web site dedicated to the Spectrum computer[13] and another that is concerned with the capture of Apple II disks (with a link to a video on how to clean the disk drive).[14]

Computer experts with an interest in games and other early computer technologies specialised in this area and made it possible to capture and interpret a wide variety of floppy disk formats, notably Disk2FDI which produces disk images in an open file format and has been used to process a major collection of games for the BnF, Bibliothèque nationale de France.[15]

6.3 Specialist Modern Technology

As Doug Reside has observed, ancestral (obsolete) equipment, such as a computer with a 5.25" floppy disk drive, requires considerable attention and care; and in the long run modern specialist replacement technology is the sustainable option (Reside 2010; Reside 2011).

The Software Preservation Society,[16] a group derived from an interest in gaming and initially the Amiga computer, has made available the KryoFlux and accompanying software, a device for reading floppy disk drives via a USB connector. It works as standard with 3.5" and 5.25" floppy disks and has been made to work recently[17] with 8" floppy disks with the help of the FDADAP floppy disk adapter.[18] The recently formed company has been exploring a number of business models, selling the basic setup to individuals at a lower price while charging institutions a higher fee, with support provided. There is a GUI emerging as an advanced form of DTC (DiskTool Console), and a forensic version of the KryoFlux has been promoted.

An important consideration is the nature of the information that the KryoFlux yields; there are detailed log files that document the capture with hash values calculated. There are two kinds of capture output: fundamentally the stream files that represent the magnetic flux transitions; and interpreted sector disk images. The stream files are not intended for long term preservation as their encoding is optimised for the transfer of the binary stream "over the wire while a track is being read". Software Preservation Society state: "Long term storage of disk data should be kept in the DRAFT format". However, DRAFT (Data Recording Archival Flux Format) is not yet complete.[19] There is another format known as IPF, Interchangeable Preservation Format, and the forum for KryoFlux indicates that the company has long reflected on how best to licence the IPF library source code; it has released the IPF decoder library under a modified MAME licence.[20]

Visualisation tends to be seen as a tool that is useful at the end of the curatorial or forensic lifecycle but it can also be used at other stages. A new software tool for use with the KryoFlux demonstrates the value of visualising the condition and formatting of floppy disks at the level of the magnetic flux

[12] http://www.wired.co.uk/news/archive/2012-04/23/prince-of-persia-source-code, and https://github.com/jmechner/Prince-of-Persia-Apple-II

[13] http://www.worldofspectrum.org/emulators.html; and http://www.worldofspectrum.org/TZXGuide.pdf for converting tapes

[14] http://adtpro.sourceforge.net/

[15] http://www.joguin.com; http://www.oldskool.org/disk2fdi/

[16] http://www.softpres.org

[17] http://forum.kryoflux.com/viewtopic.php?f=3&t=159

[18] http://www.dbit.com/fdadap.html

[19] http://www.softpres.org/kryoflux:stream; http://www.softpres.org/glossary:draft

[20] http://forum.kryoflux.com/viewtopic.php?f=2&t=136; http://forum.kryoflux.com/viewtopic.php?f=2&t=265; http://en.wikipedia.org/wiki/MAME#License

transitions: in identifying unformatted, healthy and degraded disks and much else besides. For further details see the KryoFlux website.

Other useful tools for working with floppy disks include the Catweasel, Disc Ferret and FC5025 controller.[21]

6.4 Reconfigurable Hardware, Emulation Software

Despite these important advances, digital capture is still dependent on the original disk drives. Perhaps an enterprising group will create a modern version of disk drives, using reconfigurable hardware. A step in the right direction is the C-One which is a modern computer (motherboard) designed to be reconfigured to behave like one or more earlier computers.[22]

The ultimate in reconfigurability, of course, lies in the virtualisation of machines and components. Much of the understanding and the techniques being developed in the design of emulators and universal virtual machines are truly forensic in approach and standard. Important projects in this area include Dioscuri, Qemu, KEEP, POCOS and Planets.[23]

7. Software Licensing & Preservation

The curation of personal archives where the original look and feel are critical for scholarship currently relies on the use of ancestral software. Most especially, the booting from an original disk image entails the use of the original software residing on the disk. What are the implications for curatorial examination, for access, for long-term preservation? (In July 2012, The Court of Justice of the European Union ruled that it is legal to trade 'used' software provided the reseller makes his or her own copy unusable following the sale, a decision that seems to have potentially beneficial implications for digital preservation24.)

A prototype, somewhat procrustean, policy might be that the originators agree to forego further use of the software so that the curators may inherit the right to use it on behalf of the repository institution. In fact software licensing is extremely diverse and complex. Some of the issues of software preservation generally have received attention in recent years (Matthews et al. 2008), not least in the context of computer games and virtual worlds (McDonough et al. 2010; see also John et al. 2010) A Technology Watch paper from the Digital Preservation Coalition by Andrew Charlesworth has examined Intellectual Property.[25]

8. Lessons for Mobile Forensics?

Challenges in the forensics of handheld and mobile devices arise primarily from the diversity of approaches taken by systems with many idiosyncratic qualities, which differ from those that are familiar from desktop and laptop forensics: platforms, encodings, operating systems, memory systems, interface

[21] http://www.jschoenfeld.com/home/indexe.htm; http://discferret.com/wiki/DiscFerret; http://mith.umd.edu/vintage-computers/fc5025-operation-instructions; http://www.deviceside.com/

[22] http://www.c64upgra.de/c-one; for a brief introduction see (John 2008).

[23] http://dioscuri.sourceforge.net/dioscuri.html; http://wiki.qemu.org/Main_Page; http://www.keep-project.eu/ezpub2/index.php; http://www.pocos.org/index.php/pocos-symposia; http://planets-suite.sourceforge.net/opf/

[24] see Press Release Number 94/12, Luxembourg, 3 July 2012, http://curia.europa.eu/jcms/upload/docs/application/pdf/2012-07/cp12009en.pdf

[25] See http://www.dpconline.org/advice/technology-watch-reports. Member login required at present but will be available by time of publication of this paper.

methods, storage technologies, software agents and APIs (Application Programming Interface), timestamps all may differ in special and frequently proprietary ways; and products from the same vendor can differ significantly. It is reminiscent of the early days of personal computing except that mobile devices change even more frequently. Exemplars of the devices as well as a stockpile of power and data connectors and cables will be invaluable in the years ahead.

Is it possible that experiences with early computing can provide lessons for the present in this respect?

9. Tools & Software Repository

Planets[26] initiated a registry of software tools suitable for digital preservation, and the Digital Lives Synthesis promoted the notion of corpora for the digital curation of personal digital objects that can serve for archival testing. In addition to collecting software, ancestral software as a matter of urgency, it would be beneficial for some centres to collect forensic tools and software, especially those used during the early history of computer forensics.

There are tools for changing metadata (inappropriately) such as date-time; but these have the (fortunate) weakness that few are truly certified in their ability to do what they claim to do and may be incomplete in their actions. On the other hand it means that an understanding and documentation of just what these tools do may be necessary in order to detect forgery.

10. Knowledge Reuse & Documentation

The field of digital forensics may be young, but it is rich and complex. From its beginnings as a technical support to law enforcement, it has developed into an accepted forensic science, and its tools and techniques are valuable in both reactive and proactive and preventative endeavours. At least within the close confines of the legal forensics community, there is an emerging tradition of case files, anecdotes and instances from which to draw experience and judicious insights. Curatorial and archival forensics and digital scholarship have only just begun in the field of forensic and ancestral computing.

Documentation is a persistent problem. As Linus Torvalds replied on being asked – around the time when Linux 3.0 became available – to state the toughest technical problem during the development of Linux so far: “The two areas where we’ve had serious problems was documentation and help from hardware manufacturers”. [27]

A potential area of collaboration among institutions and across forensic and preservation disciplines is in the archiving of manuals, datasheets, for hardware as well as software, and in approaching computer companies. Ronald van der Knijf warns that existing embedded systems will have been replaced within a decade: “There is a high demand for cooperation with the industry because a lot of time is spent building knowledge about the working and behaviour of systems that are designed and built by people who already have most of that knowledge but are not allowed to share it” (van der Knijff 2012).

[26] The successor of the digital preservation project Planets which was originally funded by the European Union is http://www.openplanetsfoundation.org/

[27] Interview of Linus Torvalds, Linux Magazine, issue 131, October 2011, pp 16-18

11. Virtualisation of Ancestral Computers

The virtual experience is highly portable, meaning that it can be made available on workstations with restricted access, a single reading room or, where appropriate and permitted, on the web. The usual way to interact with the original system is to 'restore' the original disk (as a clone, a hard drive) from the disk image, and boot up this clone. An alternative, more flexible, approach is to make use of virtual computing tools whereby virtual hard drives are accessed by a virtual machine (Barrett and Kipper 2010)

The possibility of using a disk image to virtually boot disks derived from personal archives was discussed in John (2008). The initial but still evolving approach at the eMSS Lab in the British Library may be outlined. The software Mount Image Pro of GetData [28] may be used to mount multiple 'dd' disk image files as well as virtual file systems such as those of VMware; it also works with the AFF image file and the proprietary one of EnCase. Having mounted the disk image as an emulated physical disk, a suitable virtual machine can be created (e.g. VMware) and the 'raw disk' can be added to the virtual machine, which is booted up using the original operating system that resides in the 'raw disk' [29]. Virtual machines may be configured manually or quasi-automatically although some tweaking is often necessary. One of the key advantages of using a virtual environment (instead of booting a physical clone of a physical disk) is that it allows for highly repeatable, controlled and referable experiences suitable for the scholar or scientist who is required to study the subject in an academically accountable way.

A common approach is to build a virtual environment from scratch: first the operating system, then the necessary application software and then add the files for viewing. Frequently it requires careful configuration and testing. A significant advantage of capturing entire disks - or at least capturing the software (and profiles of the hardware and services) along with the focal files is that the captured disk 'image' comes ready made (in many cases) with the appropriate settings and preferences of the archive's originator, notably with the application software satisfactorily tuned with the operating system; moreover, the captured system is authenticated by means of the hash values, and software can be identified in detail by means of hash libraries.

It enables scholars to explore and immerse themselves in an environment that matches that of the creator, with a virtualised equivalent of the original folder structure and computer desktop arrangement in place and files available for examination. It is even possible, depending on availability and condition to set up this environment on the original computer with a new hard drive. Where a person retains system snapshots (or shadow volumes) of the entire contents of a computer throughout its life, it will be possible for the researcher to follow its evolution through time.

Sometimes the originator's setup will be awry and the system prone to malfunction; in which case some accountable tinkering or in depth manipulation of a replicate of the archival disk image may be necessary to produce an access version of the system.

Another issue is the speed of response under emulation: for some scholarly purposes it may be too slow. A possible solution would be to offer an option for a realistic pace and behaviour, and another option for a more responsive interaction, depending on the requirements of the scholar. An ultimate goal would be to engineer a combination of high performance searching and exploration with the option to switch where desired to high fidelity viewing.

[28] http://www.getdata.com; http://www.mountimage.com; other useful tools include LiveView, VirtualBox, Xen, VMware and VMware Fusion, and Parallels.

[29] Sometimes it is helpful to first create a virtual disk (eg using VMware) and then to clone the 'raw disk' to this virtual disk (see Penhallurick 2005).

Scholarly note taking may be enhanced through the retention of VM snapshots or through video capture of screen activity. A challenge remains in devising a widely accepted means of referencing the virtual experience for academic research.

12. Open Source Emulators of Ancestral Computers

It is possible to use emulators of ancestral computers for the same purpose. For example, the open source emulator SheepShaver has be used by the British Library to mount and boot a forensically sound disk image of a hard drive from a G3 PowerPC Apple Macintoshwith OS 8.[30] The computer in question is from the archive of the evolutionary biologist W. D. Hamilton. Each time the disk image is booted within the SheepShaver emulator, one of a number of desktop pictures (e.g. the forest and river system of Amazonia) becomes apparent along with the numerous 'objects' on the virtual desktop; if the emulated computer is left inactive for a while, a screen saver from the original computer appears. Files can be opened using the original software that resides on the G3 hard drive including Microsoft Word 4, Acrobat Reader and Photoshop 4. Most excitingly, it is possible to run C++ programs using the CodeWarrior software that exists on the original disk, with dynamical graphs of the program output; moreover, users may potentially change the parameters of the original program and run a modified version for themselves. The archival technical team at Emory University has demonstrated a similar arrangement for the digital archive of Salman Rushdie, and as Naomi Nelson observed: "The emulated environment is as close as we can get to recreating Rushdie's desktop for the researcher".

"Instead of isolated files on floppies, we have the entire context in which he worked. We can see how he used technology and the growing Web as part of his creative process".[31]

13. Reservation, Redaction, Confinement

Tools for manipulating disk images and virtual machines are useful in several ways but most critically for editing disk images in order to comply with privacy requirements; some files may be embargoed for a number of years or decades. Following selection of digital objects that have been agreed and accepted for accession by the repository, Winimage, for instance, can be used to delete folders and files from access versions to cater for privacy agreements while retaining bootable functionality. An important aspect for future research is for the security of this editing and deletion process to be accountable and demonstrably secure.

14. Conclusion

Descriptive process models, however generalized, are necessarily limited in their ability to suggest a theory of digital forensics that identifies concepts and functional requirements of the discipline. Beebe and Clark hint at this in their articulation of digital investigative principles (Beebe and Clark 2005). 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" of the resulting analysis and support the development of procedural methods and tools (Casey 2007).

[30] http://www.emaculation.com/doku.php/sheepshaver
[31] Naomi Nelson, http://web.library.emory.edu/node/358

At the most basic level, abstracted models of digital forensics activities are based on three major functions: acquisition, analysis, and presentation (Carrier 2003). The theoretical concepts to be embedded in and realized through any abstract model are revealed in principles of practice that protect the authenticity, integrity, and reliability of digital material for the immediate purpose, whether that be presentation of digital evidence at trial or investigation of intrusion. Increasingly, a fourth function could be proposed – that of long-term preservation as required, or at least the possibility of long-term preservation.

This can be compared with key archival functions, articulated in a wealth of scholarly archival literature, and central to the work of digital heritage preservation: appraisal and acquisition, arrangement and description, retention and preservation. Preservation of digital heritage for use by current and future scholars depends on tools and methodologies that protect the authenticity, integrity, and reliability of digital material, and ensure its accessibility and usability over time and across technological change. Well-established for documents and records in traditional media, the affordances of digital technologies are forcing archivists to take up new tools and techniques from the digital forensics toolkit[32].

The future, for cultural heritage, depends on digital forensics knowledge from the past.

References

Altheide, Cory, and Harlan Carvey. 2011. *Digital Forensics with Open Source Tools*. 1st ed. Syngress.

Barrett, Diane, and Greg Kipper. 2010. *Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments*. 1st ed. Syngress.

Beebe, Nicole Lang, and Jan Guynes Clark. 2005. "A Hierarchical, Objectives-based Framework for the Digital Investigations Process." *Digital Investigation* 2 (2): 147–167. http://www.sciencedirect.com/science/article/B7CW4-4G7JXTM-1/2/aa0ba8969e75dd766b77a09b1e38967e.

Brant, Bob. 1991. *Build Your Own Macintosh and Save a Bundle*. Windcrest Books.

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

———. 2005. *File System Forensic Analysis*. 1st ed. Addison-Wesley Professional.

Carrier, Brian, and Eugene Spafford. 2003. "Getting Physical with the Digital Investigation Process." *International Journal of Digital Evidence* 2 (2): 1–20.

Carrier, Brian, and Eugene H. Spafford. 2006. "Categories of Digital Investigation Analysis Techniques Based on the Computer History Model." *Digital Investigation* 3 (Supplement 1): 121–130. http://www.sciencedirect.com/science/article/B7CW4-4KCPVBY-5/2/affc23432b1b89386dda701e2b554791.

[32] There is a pending Digital Preservation Coalition Technology Watch report by Jeremy Leighton John entitled: Digital Forensics and Preservation.

Casey, Eoghan. 2007. “What Does ‘forensically Sound’ Really Mean?” *Digital Investigation* 4 (2): 49–50. http://www.sciencedirect.com/science/article/B7CW4-4NWNCSP-1/2/36717bc8a1dc225cfec6a4c835866999.

Charters, Ian. 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.

Cohen, Michael, Simson Garfinkel, and Bradley Schatz. 2009. “Extending the Advanced Forensic Format to Accommodate Multiple Data Sources, Logical Evidence, Arbitrary Information and Forensic Workflow.” *Digital Investigation* 6 (Supplement 1): S57–S68. http://www.sciencedirect.com/science/article/B7CW4-4X1HY5C-9/2/5c0d842b6ee8802cfe11230246fc9772.

Collier, P.A., and B.J. Spaul. 1992. “A Forensic Methodology for Countering Computer Crime.” *Artificial Intelligence Review* 6: 203–215.

Doueihi, Milad. 2011. *Digital Cultures*. Cambridge, Massachesetts: Harvard University Press.

Duranti, Luciana. 1998. *Diplomatics: New Uses for an Old Science*. Lanham: Scarecrow Press.

———. 2009. “From Digital Diplomatics to Digital Records Forensics.” *Archivaria* 68 (Fall): 39–66.

Duranti, Luciana, and Barbara Endicott-Popovsky. 2010. “Digital Records Forensics: A New Science and Academic Program for Forensic Readiness.” *Journal of Digital Forensics, Security and Law* 5 (2): 1–12. http://www.jdfsl.org/subscriptions/JDFSL-V5N2-Duranti.pdf.

Duranti, Luciana, and Giovanni Michetti. 2012. “Archival Method”. Vancouver, BC.

Duranti, Luciana, and Corinne Rogers. 2011. “Educating for Trust.” *Archival Science* 11 (3-4) (September 24): 373–390. doi:10.1007/s10502-011-9152-3. http://www.springerlink.com/index/10.1007/s10502-011-9152-3.

Duranti, Luciana, and Kenneth Thibodeau. 2006. “The Concept of Record in Interactive, Experiential and Dynamic Environments: The View of InterPARES.” *Archival Science* 6 (1): 13–68.

Eagle, Chris. 2008. *The IDA Pro Book: The Unofficial Guide to the World’s Most Popular Disassembler*. No Starch Press.

Eilam, Eldad. 2005. *Reversing: Secrets of Reverse Engineering*. 1st ed. Wiley.

Endicott-Popovsky, Barbara, and Deborah Frincke. 2007. “Embedding Hercule Poirot in Networks: Addressing Inefficiencies in Digital Forensic Investigations.” In *Foundations of Augmented Cognition*, 364–372. http://dx.doi.org/10.1007/978-3-540-73216-7_41.

Endicott-Popovsky, Barbara, Deborah A. Frincke, and Carol Taylor. 2007. “A Theoretical Framework for Organizational Forensic Readiness.” *Journal of Computers* 2 (3): 1–11. www.academypublisher.com/ojs/index.php/jcp/article/download/.../291.

Farmer, Dan, and Wietse Venema. 2005. *Forensic Discovery*. 1st ed. Addison-Wesley Professional.

Fraser, Jim. 2010. *Forensic Science: A Very Short Introduction*. Oxford University Press.

Fraser, Jim, and Robin Williams, eds. 2011. *Handbook of Forensic Science*. Willan.

Garfinkel, Simson L. 2006. "AFF: A New Format for Storing Hard Drive Images." *Communications of the ACM* 49 (2) (February): 85–87. http://vnweb.hwwilsonweb.com/hww/jumpstart.jhtml?recid=0bc05f7a67b1790e939d3f3af5fcffbb4fe36e4feca9cd3be8b83614f440a32063db8c63b3ca06c6&fmt=C.

———. 2009. "Providing Cryptographic Security and Evidentiary Chain-of-Custody with the Advanced Forensic Format, Library, and Tools." *International Journal of Digital Crime and Forensics* 1 (1): 1–28. http://simson.net/clips/academic/2009.IJDCF.AFFLIB.pdf.

———. 2010. "Digital Forensics Research: The Next 10 Years." *Digital Investigation* 7: 64–73. doi:doi.101016/j.diin.2010.05.009. www.elsevier.com/locate/diin.

Garfinkel, Simson L., K Malan, C Dubec, C Stevens, and C Pham. 2006. "Advanced Forensic Format: An Open, Extensible Format for Disk Imaging." In *Research Advances in Digital Forensics Second Annual IFIPWG 11.9 International Conference on Digital Forensics,*. Springer.

John, JL. 2008. "Adapting Existing Technologies for Digitally Archiving Personal Lives: Digital Forensics, Ancestral Computing, and Evolutionary Perspectives and Tools." In *The Fifth International Conference on the Preservation of Digital Objects (iPRES)*.

———. 2009. "The Future of Saving the Past." *Nature* 459 (June 11): 775–776.

John, JL, I Rowlands, P Williams, and K Dean. 2010. *Digital Lives: Personal Digital Archives for the 21st Century - An Initial Synthesis*. Digital Lives Research Paper. http://britishlibrary.typepad.co.uk/files/digital-lives-synthesis02-1.pdf.

Kane, Pamela, and Andy Hopkins. 1993. *The Data Recovery Bible, Preventing and Surviving Computer Crashes/Book and Disk*. Pap/Dis. Brady.

Kirschenbaum, Matthew G. 2008. *Mechanisms: New Media and the Forensic ImaginationC*. Cambridge, MA: MIT Press.

Kirschenbaum, Matthew G., Richard Ovenden, and Gabriela Redwine. 2010. *Digital Forensics in Born Digital Cultural Heritage Collections*. Washington, D.C.: Council on Library and Information resources.

van der Knijff, R. 2012. "Embedded Systems Analysis." In *Handbook of Digital Forensics and Investigation*, ed. Eoghan Casey. London: Elsevier Academic Press.

Kraus, Kari. 2009. "Conjectural Criticism: Computing Past and Future Texts." *Digital Humanities Quarterly* 3 (4). http://digitalhumanities.org/dhq/vol/3/4/000069/000069.html.

Levine, J. 1989. "'Et Tu Brute?' History and Forgery in 18th-century England." In *Fakes and Frauds: Varieties in Deception in Print and Manuscript*, ed. R Myers and M Harris. Winchester: St. Paul's Biographies.

Matthews, Brian, Brian McIlwrath, David Giaretta, and Esther Conway. 2008. *The Significant Properties of Software: A Study*. JISC.

McDonough, Jerome P, Robert Olendorf, Matthew Kirschenbaum, Kari Kraus, Doug Reside, Rachel Donahue, Andrew Phelps, Christopher Egert, Henry Lowood, and Susan Rojo. 2010. "Preserving Virtual Worlds Final Report." http://hdl.handle.net/2142/17097.

Menne-Haritz, Angelika. 1994. "Appraisal or Documentation: Can We Appraise Archives by Selecting Content?" *The American Archivist* 57 (3) (July 1): 528–542. http://www.jstor.org/stable/40293851.

Nelson, Bill, Amelia Phillips, Christopher Steuart, and F Enfinger. 2004. *Computer Forensics and Investigations*. Boston, MA: Thomson Learning.

Nickell, Joe. 2005. *Detecting Forgery: Forensic Investigation of Documents*. The University Press of Kentucky.

Noblett, M.G., Mark M. Pollitt, and L.A. Presley. 2000. "Recovering and Examining Computer Forensic Evidence." *Forensic Science Communications* 2 (4). http://www.fbi.gov/hq/lab/fsc.

Owad, Tom. 2005. *Apple I Replica Creation: Back to the Garage*. 1st ed. Syngress.

Palmer, G. 2001. *A Road Map for Digital Forensic Research*. DFRWS Technical Report. http://www.dfrws.org/2001/dfrws-rm-final.pdf.

Penhallurick, MA. 2005. "Methodologies for the Use of VMware to Boot Cloned/mounted Subject Hard Disk Images." *Digital Investigation* 2: 209–222.

Pollitt, Mark M. 2010. "A History of Digital Forensics." *IFIP Advances in Information and Communication Technology* 337: 3–15. doi:10.1007/978-3-642-15506-2_1. http://www.springerlink.com/content/gr3v34n5248r7x28/.

Reith, Mark, Clint Carr, and Gregg Gunsch. 2002. "An Examination of Digital Forensic Models." *International Journal of Digital Evidence* 1 (3). http://www.worldcat.org/wcpa/oclc/223384589?page=frame&url=http%3A%2F%2Fwww.ijde.org%2F%26checksum%3D85756f448e9f3f33b58f16d99aa26bcf&title=&linktype=digitalObject&detail=.

Reside, Doug. 2010. "Digital Forensics, Textual Criticism, and the Born Digital Musical." In London, England. http://dh2010.cch.kcl.ac.uk/academic-programme/abstracts/papers/html/ab-739.html.

———. 2011. "Howard Ashman and Our Digital Future." http://www.nypl.org/blog/2011/04/07/howard-ashman-and-our-digital-future.

Rogers, Marcus K., J Goldman, R Mislan, T Wedge, and S Dabrota. 2006. “Computer Forensic Field Triage Process Model.” In *Conference on Digital Forensics, Security and Law*, 27–40.

Sammes, A J, and Brian Jenkinson. 2007. *Forensic Computing*. 2nd ed. Springer.

Scanlan, Daniel M. 2011. *Digital evidence in criminal law*. Aurora, Ont.: Canada Law Book.

Schofield, D. 2009. “Graphical Evidence: Forensic Examinations and Virtual Reconstructions.” *Australian Journal of Forensic Sciences* 41: 131–145.

Sommer, Peter. 1992. “Computer Forensics: An Introduction.” In *Compsec Proceedings 1992*. Elsevier. http://www.bookdepository.co.uk/Compsec-Proceedings-1992-Monk/9781856171687.

———. 1998. “Digital Footprins: Assessing Computer Evidence.” *Criminal Law Review* Special Edition: 61–78. http://www.pmsommer.net/page7.html.

Spenneberg, Ralf. 2008. “Undeleted: Carving Tools Help You Recover Deleted Files.” *Linux Magazine* (93) (August): 30–33.

Stanley, Philip M. 1986. “Computer Crime Investigation and Investigators.” *Computers & Security* 5: 309–313. http://www.sciencedirect.com/science/journal/01674048.

Taylor, Carol, Barbara Endicott-Popovsky, and Deborah A. Frincke. 2007. “Specifying Digital Forensics: A Forensics Policy Approach.” *Digital Investigation* 4 (Supplement 1): 101–104. http://www.sciencedirect.com/science/article/B7CW4-4NYD8T4-2/2/42ca628dc0b4d15097058816a107e2b9.

US Department of Justice. 2001. *Electronic Crime Scene Investigation: A Guide for First Responders*. NIJ Special Report. Washington, DC. www.ojp.usdoj.gov/nij.

Whitcomb, Carrie Morgan. 2002. “An Historical Perspective of Digital Evidence: A Forensic Scientis’ts View.” *International Journal of Digital Evidence* 1 (1). http://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

Wilding, Edward. 1996. *Computer Evidence: a Forensic Investigations Handbook*. Sweet & Maxwell.