Digital Investigation 14 (2015) S137–S145

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

DFRWS 2015 USA

Archival science, digital forensics, and new media art

Dianne Dietrich [a, *], Frank Adelstein [b]

[a] Cornell University Library, Ithaca, NY, USA
[b] Cayuga Networks, Ithaca, NY, USA

Keywords:
Archives
Archival forensics
New media art
Complex born-digital material
Case study
Intent vs. integrity

ABSTRACT

Digital archivists and traditional digital forensics practitioners have significant points of convergence as well as notable differences between their work. This paper provides an overview of how digital archivists use digital forensics tools and techniques to approach their work, comparing and contrasting archival with traditional computer forensics. Archives encounter a wide range of digital materials. This paper details a specific example within archival forensics—the analysis of complex, interactive, new media digital artworks. From this, the paper concludes with considerations for future directions and recommendations to the traditional forensics community to support the needs of cultural heritage institutions.

Introduction

Digital forensic analysts conduct digital investigations using various tools and techniques following the principles of Forensic Science. Digital archivists also use many of the same tools and techniques to conduct digital investigations as part of archival activities following the principles of Archival Science. A large overlap exists between these two fields. Both seek to understand the intent behind the artifacts they find, although the interpretations of intent as well as interactions with properties such as bitwise fidelity can be very different. This paper compares the commonalities and differences between archival and traditional forensics approaches to handling digital material, and considers these in light of a case study focusing on analysis of new media digital artworks.

The paper is organized as follows. The next section, Archival science, describes the essential principles of archival science, its goals, and the tools and technology used by digital archivists and where these converge and diverge with digital forensics. Following that, we present a case study from the analysis of a collection of digital New Media Digital Art from the mid 1990s to early 2000s, focusing on the analysis of three specific works, highlighting the challenges these works presented. The final section concludes the paper with a discussion of recommendations for tool developers and potential future work.

Archival science

The phrase “digital forensics” invokes an image of law enforcement officers conducting criminal investigations. The breadth of digital forensics practices goes far beyond this narrow definition. Civil cases use forensic analysis. Large corporations and organizations use their own forensics groups to investigate internal issues, compliance, and insider threats that are rarely publicly released. Governments have forensic resources that are applied in many areas, such as military intelligence.

In addition, a well-established area of forensic investigation that is rarely considered or mentioned by other forensics groups involves the use of digital forensics practices by digital archivists. There is a significant overlap between the goals and approaches of digital archivists and traditional forensics practitioners; further, archivists working

* Corresponding author.
E-mail addresses: dd388@cornell.edu (D. Dietrich), frank@notfrank.com (F. Adelstein).

http://dx.doi.org/10.1016/j.diin.2015.05.004

with digital materials often use utilities developed from traditional forensics fields (Kirschenbaum et al., 2010). (In this paper, we will use the term "traditional forensics" to denote non-archival forensics.) In this section, we introduce archival science, and then compare and contrast it to traditional forensics groups, considering high-level goals and objectives, as well as lower-level use of specific forensics technologies and techniques.

Archival science and archivists

In order to understand the work that digital archivists do, one must understand the framework that underpins their work—that is, the goals and aims of the archival profession as a whole. The Society of American Archivists defines archival science as a "systematic body of theory that supports the practice of appraising, *acquiring, authenticating, preserving, and providing access* [emphasis added] to recorded materials" (Pearce-Moses, 2005). This has many similarities to McKemmish's definition of *forensic computing* as the "process of identifying, preserving, analyzing and presenting digital evidence" (McKemmish, 1999). The above definition of archival science serves to support the creation and curation of archives. Archives generally contain primary source documentary materials, or records, that have been "preserved because of the enduring value contained in the information they contain or as evidence of the functions and responsibilities of their creator (Pearce-Moses, 2005)." Types of archives range widely and include university archives, government archives, corporate archives, and others. Not all archives house records only: some archives also collect rare materials (e.g., first editions of important novels or political ephemera) that are of interest to the institution or its user community. In general, though, archival practice draws from the core principles of archival science.

Archival science goals and objectives

Archivists provide access to trustworthy records, irrespective of their original format. Trustworthiness depends on a number of factors, including reliability and authenticity. In considering how archivists draw from forensic practice to approach handling digital material, we highlight two key characteristics of archival materials, as identified by the International Council on Archives.

- Records must have *integrity*, meaning they are complete and free from corruption. And,
- Records must be *usable*, stored in a way that allows others to retrieve, examine, and analyze them.[1]

Ensuring the *integrity* of digital materials means that archivists must have the appropriate tools and policies to prove that digital material has not been corrupted or inadvertently altered, either through decay or transfer to other storage environments or repositories.

Like all materials, the physical media containing the digital material is subject to decay. For example, manufacturers of so-called archival CD-Rs purport that this media can last up to 100 years, but the true lifespan of the media can be dependent on a variety of factors (Iraci, 2005) and research on optical media longevity is still ongoing (Library of Congress and National Institute of Standards and Technology, 2007). Unlike physical material, exact copies of digital materials can be produced (e.g., backups of files). Unless archivists take care when copying digital material, this process has the potential to introduce subtle changes that might go undetected, such as altering metadata (e.g., timestamps) or altering the data itself (e.g., inadvertently copying a file into a lossy format or failing to copy both forks of a file on an HFS file system). Archivists often try to avoid actions that change the material in any way, but if this is not possible (e.g., a degrading VHS tape needs to be digitized, or a rare book needs to be rebound), it is important to fully document what conservation actions were done in case these changes have implications for future users of the material.

In order to properly manage digital materials, archivists must define metadata that sufficiently describes the creation and context of complex digital material and the digital material itself. Long-term preservation ensures the ongoing accessibility and usability of records by users. In the following sections, we describe how archivists maintain record integrity and accessibility, highlighting where these activities and goals parallel those of and diverge from those of digital forensic investigators.

Ensuring integrity of materials

Archivists need to ensure that digital material has integrity, meaning it has not been inadvertently altered or changed in any way from acquisition through preservation actions, including transfer to and from storage environments and repositories. The following describes how archivists ensure material integrity at various stages in processing, with comparisons to similar activities in traditional forensics.

Integrity is closely related to, though not the same as, the archival concept of authenticity: the International Research on Permanent Authentic Records in Electronic Systems (InterPARES) project defines an authentic record as "a record that is what it purports to be and is free from tampering or corruption" (MacNeil et al., 2001). The topic of authenticating data—for example, verifying an email has been sent by the person identified in the header—is out of scope for this paper. It was not needed in the work described in our examples because the artworks were either provided by the original artists or purchased from vendors who supplied credible provenance information.

Ensuring that records have not been inadvertently altered or corrupted begins with *accessioning* (Pearce-Moses, 2005), the process by which the archives assumes control and responsibility for materials, and acquisition, and continues through all subsequent processing steps. Archivists keep records regarding the details of the acquisition process. During acquisition, as well as afterwards, archivists must ensure that no inadvertent changes have been made to digital material or its respective metadata.

[1] http://www.ica.org/125/about-records-archives-and-the-profession/discover-archives-and-our-profession.html