Digital Records Forensics: Continuing in Mabillon's Footsteps - The Concepts

Luciana Duranti

Association of Canadian Archivists
Annual Conference
10 June 2010
Halifax, NS, Canada

Digital Records Forensics Project

Baldassarre Bonifacio (1632)

Records are "much better than navy yards, much more efficacious than munitions factories, as it is finer to win by reason rather than by violence, by right than by wrong“

Archival concepts are grounded in Roman Law

- Authenticity based on a chain of trusted custody—wax tablets
- Reliability based on antiquity and on form (Justinian Code)

Archival methods are born out of legislative acts

- Decree 25 July 1793—public records belong to the people
- Decree of 1841—principle of respect des fonds

Archival science is at its heart as a legal science

Dom Jean Mabillon (1632-1707)

First forensic scientist of the modern era

Diplomatics (1681) studied the nature, genesis, formal characteristics, structure, transmission and legal consequences of records, gave origin to **Palaeography, Sigillography, Heraldry, Philology, Exegesis, Semiotics, etc.**

The **Bella Diplomatica** gave origin to the **Law of Evidence:** by mid 18th century all faculties of law in Europe taught these “forensic” disciplines

Digital Forensics

Digital Forensics is the use of scientifically derived and proven methods toward the 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, or helping to anticipate unauthorized or inappropriate actions

Archivists and Forensic Scientists

Archivists are called to act as forensics experts, e.g. assessing the identity and integrity of records stored in a variety of obsolete or nearly obsolete hardware/software and/or formats, or on portable media, and attesting to it, and acquiring such records without altering them in the process

Digital forensic experts are called to act as archivists, e.g. identifying what digital materials fall under the definition of business records, and keeping them intact for as long as needed. They are also called to attest to and sometimes provide quality assurance for digital system that produce and/or contain records.

Records Managers and Forensic Knowledge

The issue of **what is a record in the digital environment** keeps coming up at trials and in political discussions.

- British Columbia Rail case: the judge pointed out that legislation speaks of preserving “records,” and the Liberal MLA Ralph Sultan asked “What is the definition of a record?” referring “to the controversy over to what extent e-mails qualify”
- The Supreme Court of Canada is deciding whether hyperlinks in a text are akin to footnotes or make of the material to which they connect the reader a component of the document being read

What Specific Knowledge?

Digital forensic experts need archival knowledge on

- Records Trustworthiness
- Concepts of Record and Recordkeeping

Archivists need digital forensics'

- Understanding of integrity
- Processes of access, reproduction, identification and extraction

Records Trustworthiness

- Creators cannot keep digital records. They can only maintain the ability to reproduce or even to re-create them as needed
- The trustworthiness of digital records cannot be established on the records themselves and becomes ***an inference that one draws from the circumstances surrounding the creation, maintenance and preservation of the records***

The Digital Forensics View

Problematic because of best evidence rule

Reliability: the trustworthiness of a record content based on its *source*, defined in digital forensics in a way that points to either a reliable person or a reliable software.

Accuracy: A component of authenticity and, specifically, integrity. Digital entities are guaranteed accurate if they are repeatable.

The Digital Forensics View (cont.)

Authenticity: The data or content of the record are what they purport to be and were produced by or came from the source they are claimed to have been produced by or come from (=reliability). It implies integrity, but integrity does not imply authenticity.

Authentication: Proof of authenticity provided by a **witness** who can testify about the existence and/or substance of the record, or **a computer programmer** showing computer integrity. In the absence of both, **chain of custody.**

Record

- A document made or received in the usual and ordinary course of business and kept for the purposes of such business at a time close to the fact at issue by a person responsible for doing so (law of evidence)
- A document made or received in the course of activity as a by-product of or instrument for it and kept for action or reference (diplomatics/archival science)

The Digital Forensics View

Problematic in relation to the hearsay rule: in common law, documents are hearsay because they contain human statements made outside the court—if they are records they fall under the business records exception to the rule

- **Computer Stored Documents:** They contain human statements and are considered hearsay (they can be tested for truthfulness and accuracy under the business records exception to the hearsay rule): e.g. e-mail messages, word processing documents, and Internet chat room messages.

The Digital Forensics View (cont.)

- **Computer Generated Documents**: They do not contain human statements, but they are the output of a computer program designed to process input following a defined algorithm (they can be tested for authenticity on the basis of the functioning of the computer program): e.g. server log-in records from Internet service providers, ATM records.
- **Computer Stored & Generated:** e.g. a spreadsheet record that has received human input followed by computer processing (the mathematical operations of the spreadsheet program).

Substantive Evidence vs Demonstrative Evidence

Integrity
Archival/ Diplomatics View

- The quality of being complete and unaltered in all essential respects. With identity, a component of authenticity
- The same for data, documents, records, copies, systems

Integrity
Digital Forensics View

Data integrity: the fact that data are not modified either intentionally or accidentally "without proper authorization."

Duplication integrity: the fact that, given a data set, the process of creating a duplicate of the data does not modify the data (either intentionally or accidentally) and the duplicate is an exact bit copy of the original data set. Digital forensics experts also link duplication integrity to time and have considered the use of time stamps for that purpose.

Integrity
Digital Forensics View (cont.)

Computer integrity: the computer process produces accurate results when used and operated properly and it was so employed when the evidence was generated.

System Integrity: a system would perform its intended function in an unimpaired manner, free from unauthorized manipulation whether intentional or accidental

Integrity
Digital Forensics View (cont.)

The assessment is based on **repeatability, verifiability, objectivity** and **transparency**

Inference of system integrity derives from the fact that:

- the theory, procedure or process on which the system design is based has been tested or cannot be tampered with
- it has been subjected to peer review or publication (standard)
- its known or potential error rate is acceptable
- it is generally accepted within the relevant scientific community

Integrity
Digital Forensics View (cont.)

Non-interference: the method used to gather and analyse [or acquire and preserve] digital data or records does not change the digital entities

Identifiable interference: if the method used does alter the entities, the changes are identifiable

These principles, which embody the ethical and professional stance of digital forensics experts, are consistent with the traditional impartial stance of the archivist, as well as with his/her new responsibility of neutral third party, of trusted custodian

Conclusion

Clear evidence of complementary knowledge

Ours for them: Records, Recordkeeping, Preservation

Theirs for us: Authentication and Integrity; Access, Extraction, Reproduction, Identification Processes

This is why we need an integrated body of knowledge.

www.digitalrecordsforensics.ca

Thank you!

www.digitalrecordsforesnics.org