Digital Records Forensics Project

A Framework for Digital Heritage Forensics

Luciana Duranti, The University of British Columbia

Digital Records Forensics Project

Archival concepts are grounded in Roman Law

- Archives as a place—trusted custody
- 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

- Swedish Law of 1766—freedom of information act
- 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

Digital Records Forensics Project

The rule of law was easily circumvented, authenticity and reliability needed to be tested using scientific methods, beyond Valla's textual criticism

Diplomatics (1681), a new science studying 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 Records Forensics Project

In addition to Jurists, other professionals were educated in forensic disciplines:

1811 Naples—Scuola per Archivisti

1821 Paris—Ecole des Chartes

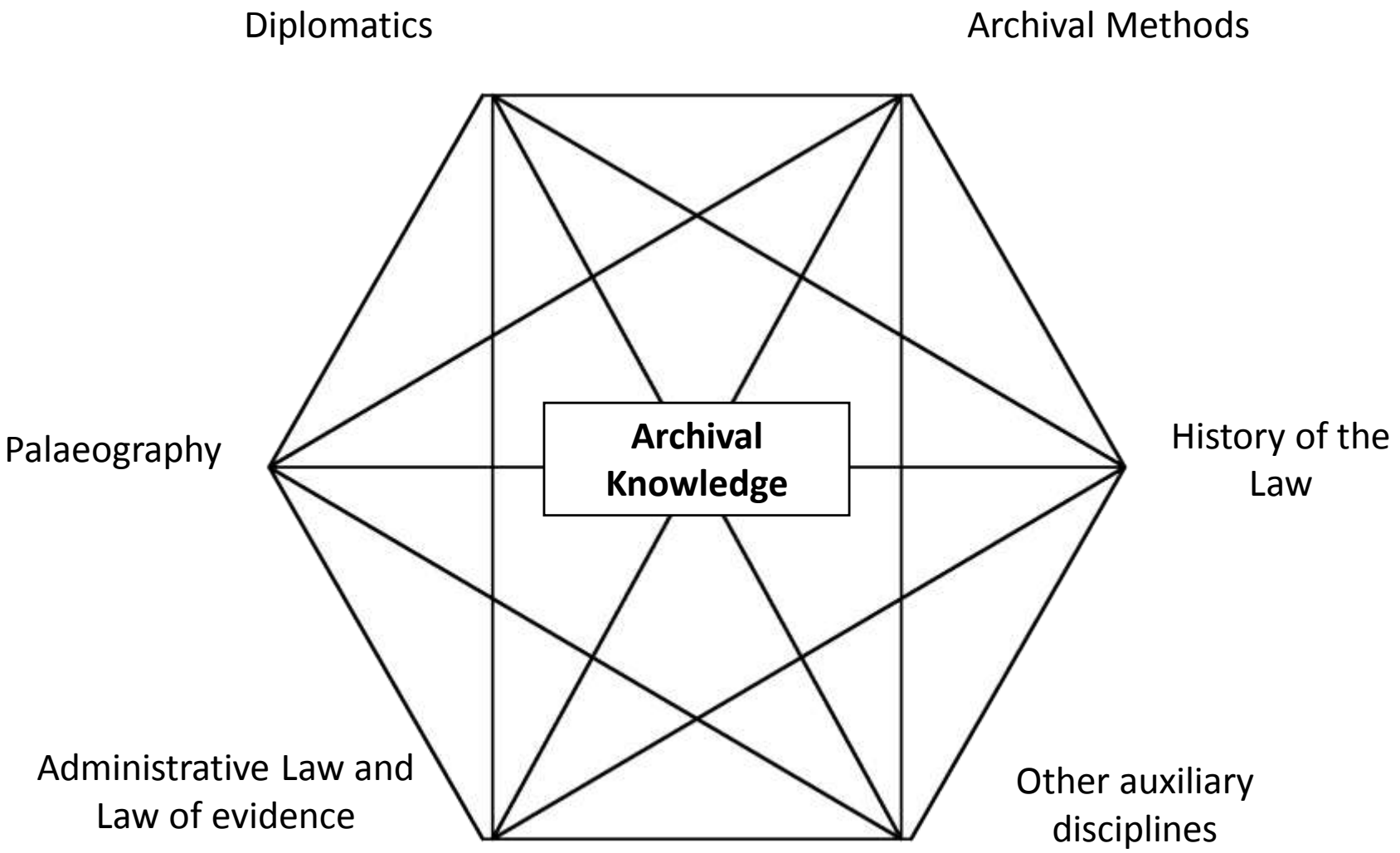
1821 Marburg—Archivschule

1854 Vienna—School on Auxiliary Disciplines of History

1925 Roma—Scuola Speciale per Archivisti e Bibliotecari

They all taught the forensic disciplines, legislation, and the archival methods rooted in legislation

Archivists


Diplomatics
Archival Methods
Palaeography
Archival Knowledge
History of the Law
Administrative Law and Law of evidence
Other auxiliary disciplines

Digital Records Forensics Project

Today:

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

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.

Digital Records Forensics Project

Digital forensic experts need archival knowledge on

- Records Trustworthiness
- Concept of Record and Recordkeeping

Archivists need digital forensics'

- Understanding of integrity
- Processes of access, identification and acquisition

Digital Records Forensics Project

The trustworthiness of digital records is problematic to digital forensics because:

- The law prefers that the original of any document, regardless of medium or form, be used as evidence at trial, but in the digital environment, we no longer have originals
- Creators cannot keep digital records. They can only maintain the ability to reproduce or even to re-create them as needed
- As a consequence, the **authenticity** 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***

Digital Records Forensics Project

Records Trustworthiness: The Digital Forensics View

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.

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 on the basis of his/her familiarity with it, or, in the absence of such person, by **a computer programmer** showing computer integrity

Digital Records Forensics Project

What is a Record is equally problematic—Digital Forensics View

A document made or received in the usual and ordinary course of business and kept for the purposes of such business

- **Computer Stored:** They contain human statements and, in common law, are considered hearsay (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.
- **Computer Generated**: They do not contain human statements, but they are the output of a computer program designed to process input following a defined algorithm (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).

Digital Records Forensics Project

But we can learn from digital forensics about integrity

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.

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

Digital Records Forensics Project

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

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

Digital Records Forensics Project

Forensic Principles for Protecting Integrity

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

Digital Heritage Forensic Expert