Building Bridges:
Digital Forensics & Archival Science

Live Ibict: "Forense Digital e a autenticidade dos documentos arquivísticos digitais"

Corinne Rogers, PhD
University of British Columbia

October 4, 2021

Agenda

- Connections between digital forensics, archival theory & practice
- Digital forensic and archival workflows - practice and purpose
- Archival theory - what it means for digital records
- InterPARES - expanding archival theory for digital records and archival practice
- Digital forensic theory and archival theory integrated…?
- Current and future directions in archival science

Whose workflow? What purpose?

- Acquisition -> Identification -> Evaluation -> Admission
  (Digital Forensics - Pollitt 1995)

- Identification -> Preservation -> Collection -> Examination -> Analysis -> Presentation -> (Decision) (Digital Forensics - DFRWS 2001, 2002)

- Appraisal/Acquisition -> Arrangement/Description -> Retention/Preservation -> Presentation (Access) (Archival workflow)

  Ingest -> Verify -> Identify -> Characterize -> Package -> Describe -> Normalize -> Arrange -> Store and/or Present (Archival workflow-Archivematica)

- Digital forensics is **inter-disciplinary** - this extends to archives and records management (c.f. Irons, 2006; Ferguson-Boucher & Endicott-Popovsky, 2008)

- Digital archival practice draws on digital forensics tools and knowledge (c.f. BitCurator; Digital Records Forensics-UBC; Kirschenbaum, 2010; Lee, 2012; Duranti & Rogers, 2013)

Overlapping goals, overlapping principles

- Digital forensics: concerned with identifying digital objects and traces that may serve as evidence of criminal activity, and analyzing those objects for their evidentiary capacity - attribution (provenance, identity), integrity, verifiability
- Digital archivist: concerned with identifying digital objects and traces that have been created as records of actions and transactions, facts and events, and assessing thier reliability, authenticity, and accuracy in order to guarantee trustworthy memory and historical accountability
- Can we harmonize concepts of trustworthiness of digital records (archival focus) and digital artifacts/traces (digital forensic focus)?

Digital forensics & digital archival practice: common challenges

- Diversity, volume, complexity of material
- Identifying & locating digital material
- Versatility and proliferation of tools & techniques
- Long term & lifecycle considerations for preservation
- Risks to security, privacy, digital rights

Digital forensics & digital archival practice: shared theoretical perspectives

- Establishing authorship & identity
- Ensuring integrity & tracking change over time
- Establishing and verifying authenticity, reliability, context
- Describing, presenting / providing access

Digital evidence

- Regardless of discipline, we believe that digital records/artifacts/traces stand in relation to past events, regardless of how they were created or preserved
- Their capacity to serve as evidence does not come from any intrinsic nature or value, but **from their relationship to events**
- In order to understand them, we must establish (identify, describe, prove) the relationships between the record/artifact/trace and event

The archival mindset

- The history of archives is traced to ancient legal and administrative principles expressed in the Justinian Code
- The archivist asks of a record: “What is this?” as opposed to “What is this about?”
- The archivist’s professional function is to clarify the meaning of the record
- Not concerned primarily with *information*, or *narrative,* but with the documents in which information is contained, their structure (form and formal elements) and contexts

Fundamental archival principles

- Principle of provenance
- Principle of original order
- Principle of the archival bond

The object of archival theory: the record & its aggregations

- Definition: a **record** is a document (recorded information) created (made or received) in the course of practical activity and kept for further action or reference
- Corollary 1: a record arises in the context of some action, as a means or a byproduct of that action
- Corollary 2: a record is created by/for one or more agents (human or machine) - the information in the record is intended to be transmitted
- Inference 1: more than one record may be created in the context of that action
- Inference 2: records created in the context of an action are related through their role in executing or documenting that action

Qualities of records*

- Impartiality
- Authenticity
- Naturalness
- Inter-relatedness
- Uniqueness

*Sir Hilary Jenkinson

The object of diplomatics: the document as conceptual system

- The context of a document's creation is manifest in its physical and intellectual form
- Elements of form can be examined separately from content
- The document is a conceptual system of internal and external elements consisting of
  - Acts
  - Persons
  - Procedures
  - Documentary form

InterPARES - archival diplomatic theory in the digital environment

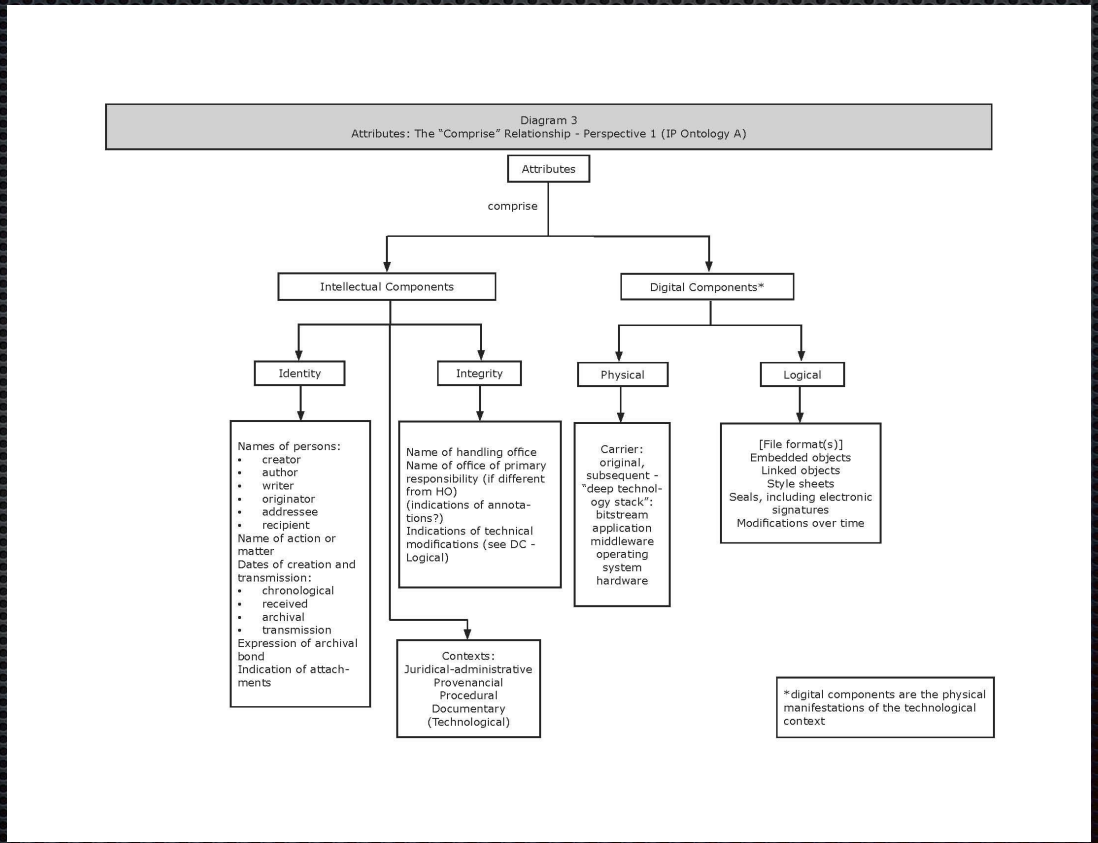
- Archival and diplomatic theory, developed over centuries for paper/parchment records, foundation of laws governing admissibility of documentary evidence and taught in European faculties of law, now tested in the digital environment in service of determining/assessing/preserving evidentiary capacity Benchmark requirements supporting the presumption of authenticity
- Hypothesis: all records can be analyzed, understood, and evaluated in terms of a system of formal elements, the circumstances of their creation and status of transmission, regardless of technology
- As digital technology has separated content and structure from form, we can no longer determine authenticity on the object-record, which is composite and permanently new, but must make an inference of authenticity from its environment.

Outcomes

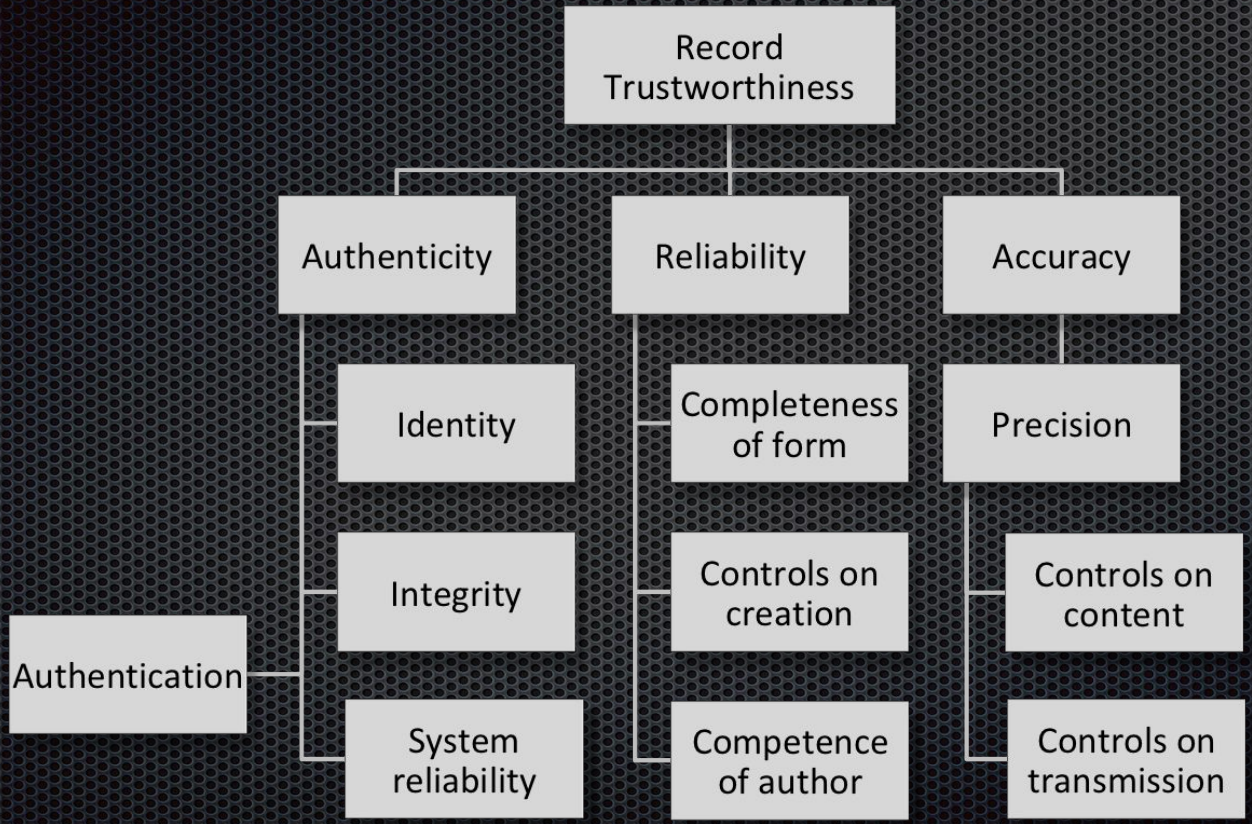
- Benchmark requirements for the creation of authentic records; Baseline requirements supporting the production of authentic copies
- Chain of Preservation (CoP) model - extension of concept of chain of custody
- Preservation as a Service for Trust (PaaST) - executable functional requirements for digital preservation
- Ontologies - digital record, trustworthiness (authenticity, reliability, accuracy)
- Templates for contextual, and diplomatic analyses of digital material

Model of a digital record

- Required attributes:
  - Stable content/fixed form
  - Persons/agents
  - Links to related records
  - Action
  - Contexts



Trust framework



How does this relate to digital forensics?

- Best practice guidelines (e.g. ACPO)
- Standards (e.g. SWGDE, IOCE, ISO 17025, ISO 27001, ISO 27037)
- Scientific measurements of reliability
- Case law governing scientific testimony (U.S.: Frye 1923, Daubert 1993, Kumho Tire 2000; Canada: R. v. Mohan 1994, R. v. J.J. 2000, R. v. D.D. 2000)

Qualities of the domain of digital forensics?

- "…most digital information is an accurate representation of what it purports to be (subject to the well-known volatile nature of data where a file date is, for example, inadvertently modified by someone who opens the file to read it and then saves it when closing it)."
- "A suitable theory to serve as scientific grounds for a digital forensic science… needs to satisfy the demands imposed by science and justify the facts derived as evidence using theory."
- Domain of digital forensics - definition:
  "a digital artefact is a sequence of bits that has (or represents) meaning… often (but not always) determined by context."

(Olivier 2016)

Key principles - relevant to both disciplines

- maintain the integrity of the material
- document all processes
- ensure archival / forensic competence of the analyst
- ensure compliance with regulations / laws
- adhere to scientific measurements of reliability: repeatability, objectivity, verifiability, transparency

InterPARES: contextual analysis template

- Purpose is to enable systematic documentation of information relevant to the context of the investigation
- Section 1: analysis of administrative context (including legal status, provenance, controls, policies)
- Section 2: administrative/managerial framework in which relevant digital objects are created (including access controls, procedures, computations)

Diplomatic criticism of digital material

Criticism of the formal elements of material under investigation to determine its identity and integrity

Although criticism is dependent on the context of the investigation, the concepts and procedures can apply to any investigation

Observe/examine the physical / technological environment, the digital and documentary presentation of the material

Investigate the presence/absence of required attributes of digital records: fixed form, stable content, persons/agents, action/intent, archival bond, hierarchy of contexts (juridical/administrative, provenancial, procedural, documentary, technological)

- locate presence/evidence of attributes in conceptual/logical layers of abstraction
- examine and qualify relationships between material and action, persons/agents, other entities

If attributes are absent, further analysis should explain the status of the material

If attributes are present, more detailed analysis will determine the trustworthiness of the material

Relating diplomatic criticism & digital forensic examination

- Map diplomatic criticism to elements of generally accepted digital forensic process models, e.g. Gladyshev (2004), Carrier (2004), Cohen (2011, 2013)
- Map to proposed theoretical frameworks of digital forensics, e.g. Mocas (2004), Andrew (2007), Olivier (2016)
- These models or frameworks include theoretical and methodological requirements:
  - Analysis of the object(s) (necessary and sufficient properties for viable digital evidence)
  - Validation of the methodology (tool development & testing; results testing)

Questions

- Can diplomatic criticism provide a framework for the examination/analysis phase of a digital forensic investigation focusing on digital artefacts/traces as the domain investigation?
- Will such a framework satisfy scientific requirements?

What? (Diplomatics)	Where? Abstraction layer	How? Tools & their validation
Admin/Investigative context	-	-
Creation of digital entities		
ID digital entities		

Process: Digital forensics* to *Archives*

. Get search authority : *authority to acquire material*
. Establish chain of custody
. Use imaging/hashing functions } : *acquire*
. Use validated tools
. Analyze : *describe*
. Ensure repeatability : *follow archival principles*
. Report : *produce finding aids and descriptions*
. Prepare for possible expert presentation : *provide access*

*Zatyko 2007

Abstraction

- Abstraction is a process of understanding complex objects by hiding all of the detail expect those essential features of a particular task, concept, or object
- The divisibility of digital data into smaller components, or levels, where each component or level will contain its own unique set of characteristics and functionality
- All models use abstraction, but it is particularly relevant in digital systems
- Computer science uses abstraction extensively – how can we use it to understand digital records?

An abstracted view of digital records

Conceptual: an object as it is recognized and understood by a person

Logical: an object that is recognized and processed by hardware & software

Physical: an inscription of signs on a physical medium

Logical layer

Application software: word processing, spreadsheets, multimedia, databases, etc.

System software: operating system, utilities, compilers, etc.

Hardware: hard drive, optical disk, tape, solid state, etc.

Olivier: A scientific theory of digital forensics

- "A suitable theory to serve as scientific grounds for a digital forensic science… needs to satisfy the demands imposed by science and justify the facts derived as evidence using theory."

- A scientific theory of digital forensics needs to:

  Consider the domain of digital forensics: identified as the digital artefact - "a sequence of bits that has (or represents) meaning… often (but not always) determined by context."

Olivier 2016

Mocas: Theoretical underpinning for DF research

- Integrity
- Authentication
- Reproducibility
- Non-interference
- Minimization

Mocas 2004

Andrew: Digital analysis process model

- Two principles: form the foundation for analysis
  - Principle of consistency
  - Principle of stability
- Five ‘laws’: areas of examination that must be addressed in qualifying data in support of conclusions and opinions
  - Association: process & source
  - Context: internal & external
  - Access: general & specific
  - Intent: intentional; not corrupted or controlled
  - Validation: integrity; authenticity; accuracy

Andrew 2007

Bridge building…

Archival theories
- Original order
- Provenance
- Archival bond

Archival/Diplomatic Principles
- Qualities of archives/
- Necessary attributes of records
- Elements of trustworthiness

Scientific measurements of reliability
- Repeatability
- Objectivity
- Verifiability
- Transparency

Admissibility of documentary evidence
- Relevancy
- Authentication
- Hearsay exclusion
- Best evidence/system integrity

Digital forensics principles - Andrew
- Principle of stability
- Principle of consistency
- Law of association
- Law of context
- Law of access
- Law of intent
- Law of validation

Digital forensics workflow & principles
- Do not change evidence
- Maintain chain of custody
  - Integrity
  - Authentication
  - Reproducibility
  - Non-interference
  - Minimization (Mocas, 2004)

Admissibility of scientific/expert testimony
- Frye/Daubert/Kumho
  - Testing, reviewed, known error rate, generally accepted
- R v Mohan
  - Relevant, necessary, qualified, scientific

Current and future digital forensic applications in archival science

- Developing clear, objective, and executable criteria for formulating and evaluating concepts in archival science (Thibodeau) - example: Preservation as a Service for Trust (PaaST)
- Integrating digital forensic tools into archival processing where digital collections can be analyzed at multiple levels of representation to help ensure authenticity, provenance (Lee) - example: BitCurator, Archivematica
- Development of “Computational Archival Science” - an interdisciplinary field concerned with the application of computational methods and resources to large-scale records/archives work; to apply collective knowledge of computer and archival science (Marciano, Lemieux et al)

Thank you!

corinne.rogers@ubc.ca

https://interpares.org

https://interparestrust.org

https://interparestrustai.org

Andrew, Michael W. 2007. “Defining a Process Model for Forensic Analysis of Digital Devices and Storage Media.” In SADFE 2007: Second International Workshop on Systematic Approaches to Digital Forensic Engineering: Proceedings: 10-12 April 2007, Seattle, Washington, USA, edited by Northwest Security Institute and Pacific Northwest National Laboratory (U.S.). Los Alamitos, Calif: IEEE Computer Society.

Cohen, Fred. 2012. Digital Forensic Evidence Examination. Place of publication not identified: Asp Press.

———. 2015. “Digital Diplomatics and Forensics: Going Forward on a Global Basis.” Records Management Journal 25 (1): 21–44. https://doi.org/10.1108/RMJ-03-2014-0016.

Diamond, Elizabeth. 1994. “The Archivist as Forensic Scientist – Seeing Ourselves in a Different Way.” Archivaria 38 (Fall): 139–54.

Duranti, Luciana. 2009. “From Digital Diplomatics to Digital Records Forensics.” Archivaria 68 (Fall): 39–66.

Duranti, Luciana, and Corinne Rogers. 2013. “Memory Forensics: Integrating Digital Forensics with Archival Science for Trusting Records and Data.” eForensics Magazine 2 (15): 96–111.

Eastwood, Terry. 1994. “What Is Archival Theory and Why Is It Important?” Archivaria 37 (Spring): 122–30.

———. 2004. “Jenkinson’s Writings on Some Enduring Archival Themes.” American Archivist 67 (1): 31–44.

Ferguson-Boucher, K. A., and Barbara Endicott-Popovsky. 2008. “Digital Forensics and Records Management: What We Can Learn from the Discipline of Archiving,” 1–6.

Irons, Alastair. 2006. “Computer Forensics and Records Management – Compatible Disciplines.” Records Management Journal 16 (2): 102–12. https://doi.org/10.1108/09565690610677463.

John, Jeremy Leighton. 2012. “Digital Forensics and Preservation.” Digital Preservation Coalition. http://www.dpconline.org/component/docman/doc_download/810-dpctw12-03pdf.

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.

Lee, Christopher. 2012. “Archival Application of Digital Forensics Methods for Authenticity, Description and Access Provision.” Comma 2012 (2): 133–40. https://doi.org/10.3828/comma.2012.2.14.

Marciano, R., V. Lemieux, M. Hedges, M. Esteva, W. Underwood, M. Kurtz, and M. Conrad. 2018. “Archival Records and Training in the Age of Big Data.” Submission Draft. http://dcicblog.umd.edu/cas/wp-content/uploads/sites/13/2016/05/submission_final_draft.pdf.

Mocas, Sarah. 2004. “Building Theoretical Underpinnings for Digital Forensics Research.” Digital Investigation 1 (1): 61–68.

Olivier, Martin. 2016. “On a Scientific Theory of Digital Forensics.” In Advances in Digital Forensics XII, edited by Gilbert Peterson and Sujeet Shenoi, 484:3–24. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-46279-0_1.

Pollitt, Mark M. 1995. “Computer Forensics: An Approach to Evidence in Cyberspace.” In , II:487–91. Baltimore, Maryland: NIST. www.digitalevidencepro.com/Resources/Approach.pdf.

Rogers, Corinne. 2015. “Diplomatics of Born Digital Documents: Considering Documentary Form in a Digital Environment.” Records Management Journal 25 (1): 6–20.

Rogers, Corinne, and JL John. 2013. “Shared Perspectives, Common Challenges: A History of Digital Forensics & Ancestral Computing for Digital Heritage.” In The Memory of the World in the Digital Age: Digitization and Preservation, 314–36. Vancouver, BC: UNESCO. http://www.unesco.org/webworld/download/mow/mow_vancouver_proceedings_en.pdf.

Zatyko, Ken. 2007. “Commentary: Defining Digital Forensics.” Forensic Magazine, January. http://www.forensicmag.com/node/128.182.