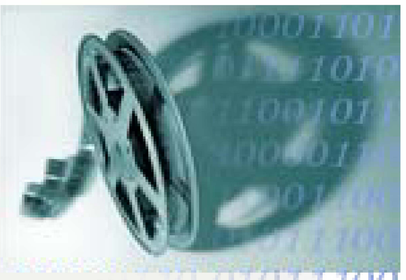


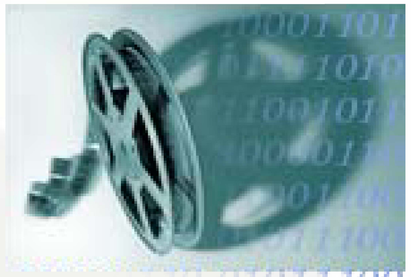
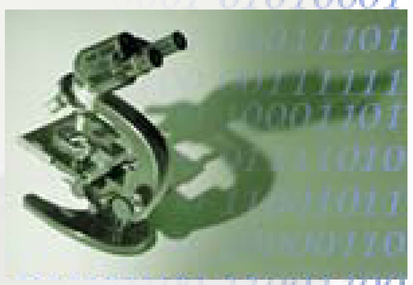

Preserving the Authenticity of Digital Evidence

Luciana Duranti
Adam Jansen
Barbara Endicott-Popovsky
Fred Cohen

Seventh Annual IFIP WG 11.9 International. Conference on Digital Forensics
1 Feb 2011, Orlando, FL, USA

Adam Jansen
Doctoral Candidate
Library, Archival and Information Studies (SLAIS)
The University of British Columbia
Vancouver, British Columbia

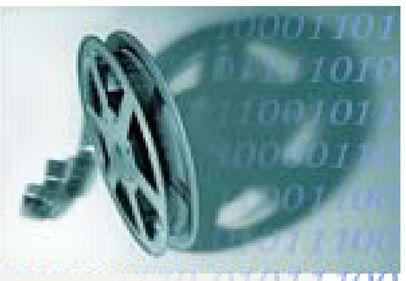
EXPANDING PRESERVATION



Seventh Annual IFIP WG 11.9 International. Conference on Digital Forensics
1 Feb 2011, Orlando, FL, USA

Expanding the View of ‘Preservation’



Preservation a key focus of the forensic process

“Preservation must be a guarded principle across “forensic” categories” (DRFWS *Road Map for Digital Forensic Research*)

Imaging technologies, chain of custody, time sync

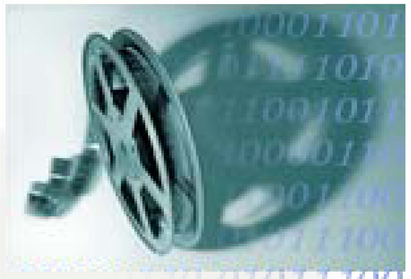
Strong focus on ‘freezing’ the immediate environment to maintain integrity

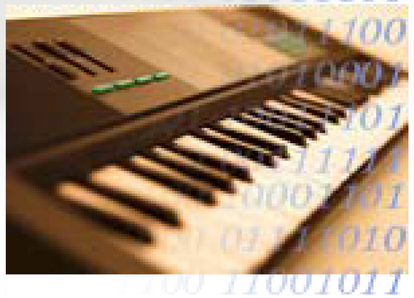
Expand the focus to incorporate authenticity

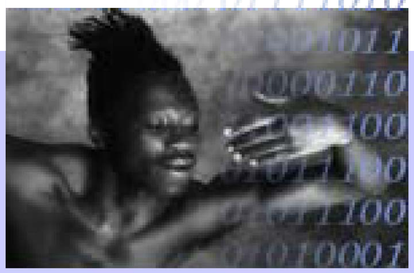
Integrity = complete and unaltered, but not genuine!

Authentic = is what it purports to be

Understanding Authenticity in the Digital Age







Integrity is a necessary part of authenticity, but it is not the whole meaning there is something more…

Authenticity requires distinct identity:

Determine one version from another

Sender from receiver, draft from final

For a record to be "what it purports to be" requires understanding of intent and context of creation, collection and handling (chain and process of custody)

Identity of a Digital Record

Act: an action in which the records participates or which the record supports (naturalness and impartiality)

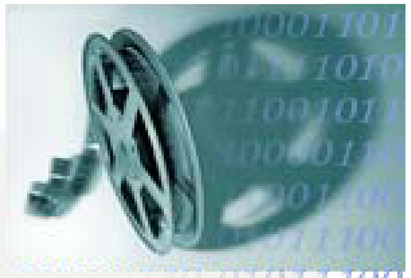
Persons Concurring to Its Creation: author, writer, originator, addressee, and creator

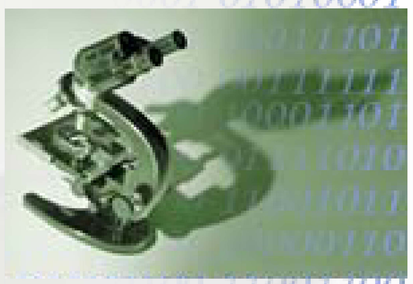
Archival Bond: explicit linkages to other records inside or outside the system (uniqueness)

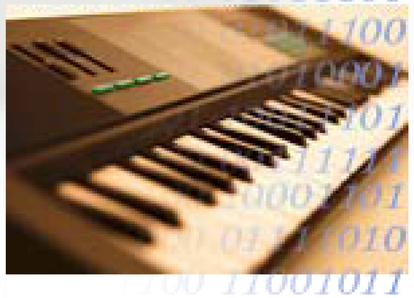
Identifiable Contexts: juridical-administrative, provenancial, procedural, documentary, technological (interrelatedness)

Medium: necessary part of the technological context, not of the record

Fixed Form and Stable Content







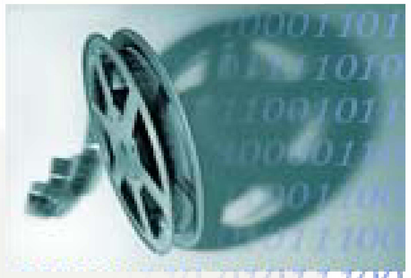
Understanding ‘Fixed Form’

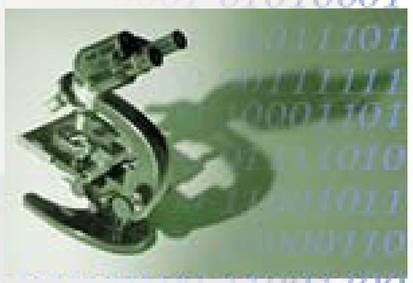
It is **not possible to preserve digital records, only the ability to reproduce the representation** of the record as it was sent to the addressee.

Requires:

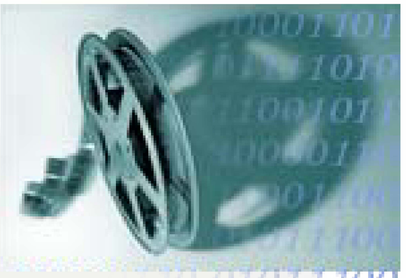
The binary content, including indicators of the documentary form, are stored in a manner that ensures it will remain complete and unaltered

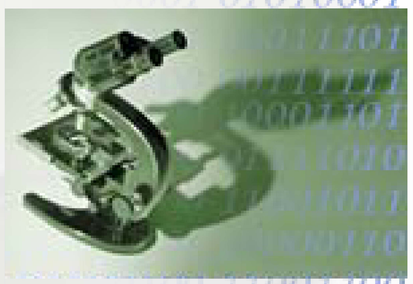
Technology maintained and procedures defined so that the record can be rendered with the same documentary form as when set aside





Authenticity of a Digital Record



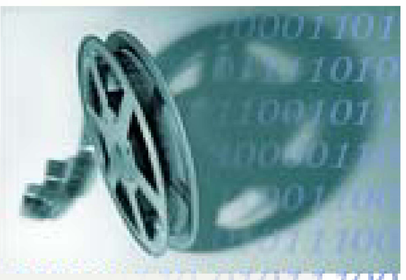


As digital records undergo repeated conversion to new formats and migration to new systems in order to be preserved over the long term, their trustworthiness cannot be established on the records themselves

It becomes an **inference** that one draws from the data maintained about their the creation, and those generated about their maintenance and preservation:

Done through Identity Metadata and Integrity Metadata

Record Profiles

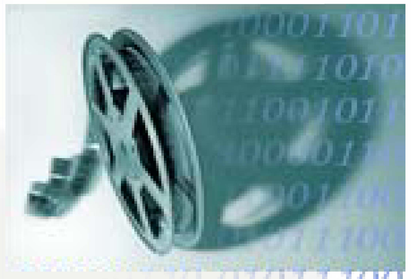


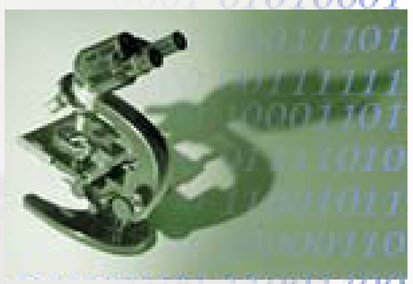
Can be used to document the identity of digital records by representing the conceptual juncture between the administrative-documentary procedures and the intellectual form, where the components of the intellectual form converge together.

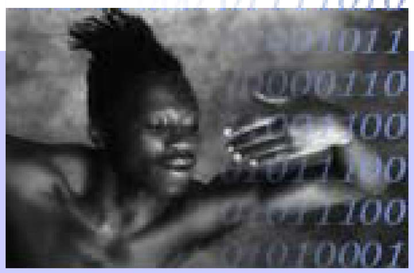
Profile should contain the **necessary components to uniquely identify the record** and place it in relation to other records

Identity and Integrity

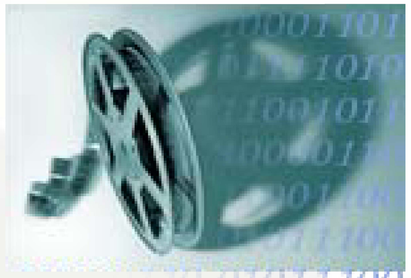
Identity	Integrity
Name of person creating	Name of person handling
Date of Creation	Name of custodian
Matter or Action	Indication of annotation
Relationship to other records	Technical changes
Documentary form	Presence of digital signature
Digital Signature	Location of duplicates
Name of person responsible	Hash value







Questions?



Contact Information

- Luciana Duranti
  luciana@interchange.ubc.ca
- Adam Jansen
  adam@dkives.com
- Barbara Endicott-Popovsky
  endicott@uw.edu
- Fred Cohen
  fc@all.net