Digital Records Forensics:
Conducting a Gap Analysis to Measure Legal Risk

Alexandra Allen
Corinne Rogers

Session T15 - ARMA Canada 2010

London, ON, Canada

June 1, 2010

Digital Records Forensics Project

Outline

- Present research in the develpment of a new discipline - digital records forensics
- Discuss issues concerning digital evidence from the archival, forensic and legal points of view
- Identify gaps in digital recordkeeping that are areas of concern in the new discipline

Digital Records Landscape

- > 90% of all information is being created in electronic format
- Records are being created and must be maintained and preserved in a rapidly changing technological context
- Documentary evidence called in legal proceedings is increasingly in electronic format

Why the fuss?

The most challenging issues presented by digital technology:

1. The identification of ‘records’ among complex digital objects
2. the determination of their authenticity

Digital Records Forensics Project*

a collaboration between:

- The UBC School of Library, Archival & Information Studies
- The Faculty of Law, and
- the Computer Forensics Division of the Vancouver Police Department

*Funded by SSHRC

Objectives

- to develop concepts and methods that will allow the records management, archival, legal, judicial, law enforcement and digital forensics professions to recognize records among all digital data objects produced by complex digital technologies once they have been removed from the original system
- to develop concepts and methods to determine the reliability, accuracy and authenticity of records no longer in the original digital environment

Objectives cont.

- to identify, develop and organize the content of a new science and discipline called “Digital Records Forensics”
- to develop the intellectual components of a new program of education for Digital Records Forensics experts.

Methodology

- Literature review
- Digital Records Forensics Activity Model
- Case Law Database
- Terminology Database
- Questionnaires and Interviews
- Ethnographic study with the Vancouver Police Department

http://www.digitalrecordsforensics.org/

Define your terms

Why do these matter?

- Digital Record
- Digital Diplomatics
- Digital Forensics
- Digital Evidence
- Hearsay & Law of Evidence

"What is a Record?"

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

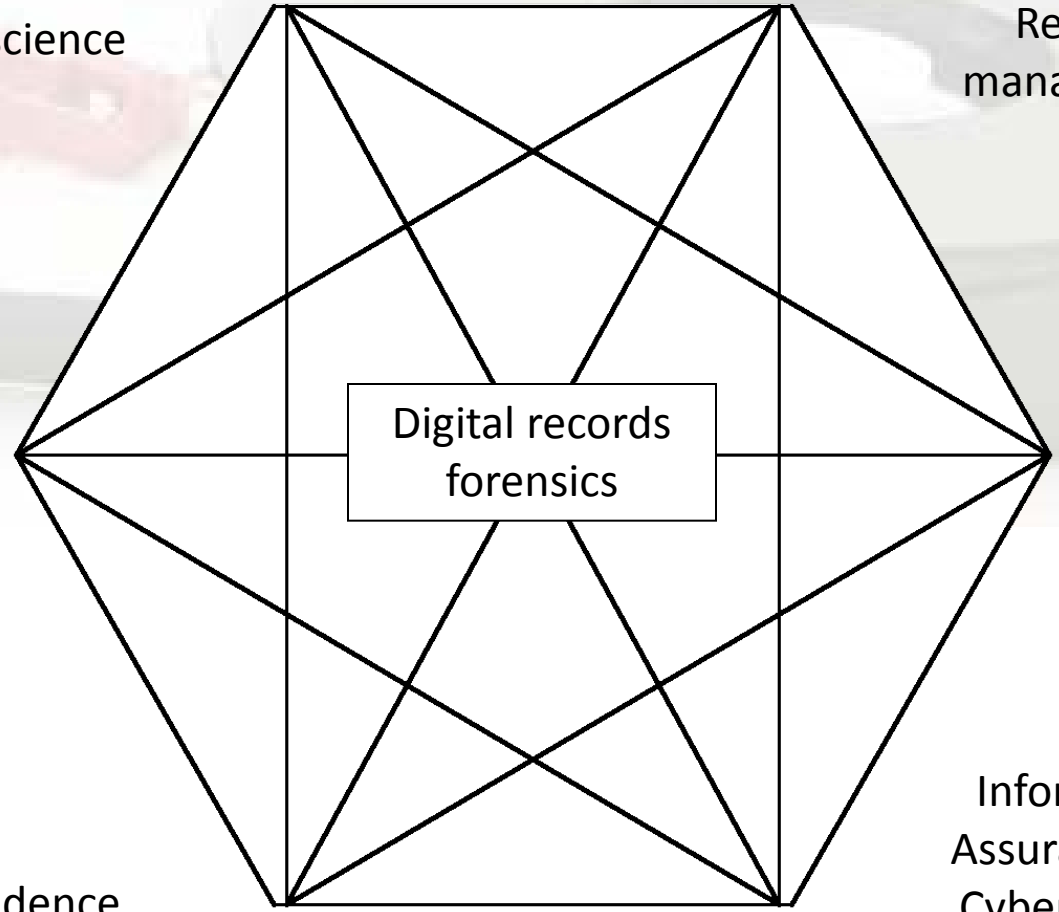
Digital Diplomatics

Studies the nature, genesis, formal characteristics, structure, transmission and legal consequences of records

Digital forensics

- Forensic analysis is often required to identify, retrieve and present digital materials
- It has developed as a technical activity
- There is an increasing call for exploration of theoretical underpinnings
- Recognition of contributions from complementary disciplines

Digital Records Forensics



Records - the archival / diplomatic view:

Any document made or received in the course of a practical activity by a natural or juridical person and kept for action or reference

Records - The Digital Forensics View

- **Computer Stored:** contain human statements
- **Computer Generated**: output of a computer program run without human intervention
- **Computer Stored & Generated:** human input followed by computer processing

Records - The Digital Forensics View

- **Static:** manifest content & unchanging form
- **Interactive:** variable content &/or form
  - **Non-dynamic**: rules of presentation fixed; content from a finite set of data
  - **Dynamic**: rules governing content & presentation may vary (not records in archival sense)

Digital *records* forensics

- Archival concepts of authenticity and reliability can be brought to bear on admissibility and weight (relevance) of *evidence* respectively
- Archival theory places *records* in context
- Diplomatic theory examines *records* as individual items

Reconciling the archival and forensic views

- Essential in light of the application of the hearsay rule to computer generated records, and of the determination of whether they constitute substantive evidence (revealing intentionality) or demonstrative evidence (showing capability)
- This reconciliation must be made in relation to the concept of trustworthiness as it is understood by the two fields in order for the legal system to establish at any given time whether it is concerned with issues of reliability or authenticity

At common law

- Admissibility of documentary evidence is at discretion of presiding judge
- Rests on matters of law: relevance & authenticity
- Documents are hearsay but may be admissible under exceptions
- What does “best evidence” mean in the digital environment?

Law of Evidence

- Documents are hearsay - under what exceptions are they admissible?
  - Business records exception: created in usual and ordinary course of business, and it was the regular practice of the business activity to create them

Law of Evidence

- Best evidence rule - calls for original
  - Satisfied on proof of the integrity of the system in which the record was produced or stored, or on presumptions regarding secure electronic signatures

Admissibility & weight

- Admissibility determined by the judge & rests on authenticity
- Relevance (weight) determined during trial and relates to reliability

And furthermore,

- Are computer-generated records direct evidence or hearsay?
- How do the courts address the issue of authentication of computer-generated evidence?
- When is a hard drive a record and when is it a collection of records?

Digital Forensics View

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.
- authenticity implies integrity, but the opposite is not true, that is, integrity does not imply authenticity.

Digital Forensics View

Authentication :

- Proof of authenticity provided by a witness who can testify about the record on the basis of familiarity with it, or,
- by a computer programmer showing that the computer process or system operated properly when the evidence was generated.

Chain of Custody

A chain of legitimate custody is grounds for inferring authenticity and authenticates a record.

Digital chain of custody:

- the information preserved about the data and its changes that shows specific data was in a particular state at a given date and time

Metadata

The strength of circumstantial digital evidence could be increased by metadata which records:

1. the exact dates and times of any messages sent or received
2. which computer(s) actually created them, and
3. which computer(s) received them.

System Integrity

Authentication (cont.)

A declaration made by an expert who bases it on the trustworthiness of the system containing the record and of the procedures controlling it is a prevalent method.

System Integrity: The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

The assessment of system integrity is based on the rules used for scientific evidence

How does digital forensics support admissibility?

Digital forensic experts look for **repeatability, verifiability, objectivity** and **transparency** of the ***process***

Daubert Guidelines

- Testing
- Error rate
- Publication
- Acceptance

Challenges to digital evidence

- "Digital forensic evidence is challenged by identifying that, by intent or accident, content, context, meaning, process, relationships, ordering, timing, location, corroboration, and/or consistency are made or missed by the other side…"

Frederick B. Cohen

"Fundamentals of Digital Evidence"

Organizational Risk Management

- "…the systematic application of policies, procedures and practices to the tasks of identifying, analysing, evaluating, treating, and monitoring risk." DIRKS

What are the risks?

- Loss of authenticity, reliability of records
  - Version control
  - Unauthorized change
- Loss of physical & intellectual control over records
  - Search & access
- Loss of records
  - Hardware/software failure
  - Technical obsolescence
  - Invasive attack

Types of Risk

- Operational/Administrative
  - Affect business decisions
  - Intellectual property
- Regulatory
- Legal
  - In 2005 American businesses spent $6 billion in discovery

Types of Risk Management

- Event-based
  - Reactive, after the fact
- Records and Information-based
  - Proactive

Forensic readiness

- Forensic investigations are “post-event”
- Forensic readiness anticipates an information security incident or litigation hold
- Forensic readiness is the process of maximizing potential to use digital evidence & minimizing disruption and cost of investigation

Digital Evidence Maps

Digital records ~ Digital Evidence ~ ESI

- Digital evidence maps identify the location of e-mail, log files, backup tapes and other critical data sources
- Digital forensics experts see this as an IT function
- Records managers should be part of the conversation

Risk Management - where are your gaps?

- Know what you are creating! Create digital records with stable content and fixed documentary form
- Can the digital components of your records be separately maintained and reassembled?
- Have you addressed reliability, accuracy and authenticity expressly and separately?
- Do you embed preservation capacity in all creation and maintenance activities to maintain and preserve digital evidence?

Risk Management - where are your gaps?

- Do you have established policies & procedures for records management?
- Does technology serve your business functions in records creation & maintenance?
- Have you established cross-jurisdictional control based on legal requirements of the creator's jurisdiction?

Risk Management - where are your gaps?

- Use a trusted record-making system for reliability
- Use a trusted record-keeping system for accuracy and authenticity
- Use a trusted custodian to take physical and legal custody of inactive records
- Document all decisions
- Explicitly identify 3rd-party intellectual property rights and privacy rights within the record
- Remember that reproductions of a records carry the same weight as the first manifestation

In practice…

- Identify the risk
- Consider the consequences
- Identify your risk mitigation strategy
- Identify the person responsible

You need…

- Cooperation from top management
- Policies that can be enforced and monitored
- Clearly defined business processes and an understanding of the records that result
- Training

- View your records as evidence of transactions
- Don’t rely on technology alone to preserve your digital records

DRF Project - Some preliminary interview findings

- Preservation requirements and/or expectations are longer, becoming indefinite, but the means are unclear
- The courts still have paper minds
- Lack of consistency in understanding of digital issues
- Records are whatever is presented as evidence

In a Local Context - Vancouver Police Department

- Chain of custody is the basis for presumption of reliability and authenticity.
- Complete reliance on EDRMS to make explicit all links between records
- Retention schedules exists but are not fully implemented

Thank you!

Alexandra Allen, MAS

akallen_186@hotmail.com

Corinne Rogers, MAS

Doctoral student

cmrogers@interchange.ubc.ca