From Records Manager to Digital Records Forensic Expert: Practicing an eXtreme Profession

Luciana Duranti

ARMA Chapter

Winnipeg, 17 June 2010

Digital Records Forensics Project

Common Law 12th-13th cc.

Responding to increase in forgeries, it developed

- the **best evidence rule**: an original record must be submitted as evidence whenever possible
- the **authentication rule**: either direct or circumstantial evidence must be presented that a record submitted as evidence of a fact at issue is what it purports to be

Diplomatics 17th c.

A new discipline studying the nature, genesis, formal characteristics, structure, transmission and legal consequences of records. It

- provided the tools for assessing the conformity of a record's elements of form to established procedures, thereby establishing its authenticity
- paved the way for the development of the concept of evidence as inference , and
- for a fundamental exception to another basic rule of evidence at common law, the **hearsay rule**

The Hearsay Rule and Its Exception

All documents are hearsay as they contain statements made outside a court of law

On the grounds of circumstantial probability of trustworthiness, **business records** are considered an exception and can be entered as evidence in a court of law because their creation process makes them inherently reliable.

Business Records

- Legal definition: Documents made or received in the usual and ordinary course of business, at or near the time of the event recorded in or attested by them, by a person competent and with the authority to make or receive and keep them
- A definition very close to the diplomatic/archival definition of records: Documents made or received in the course of activity and kept for action or reference

Digital Records

We cannot preserve digital records, but only our capacity to reproduce them time after time, in a continuing effort to beat technologic obsolescence. They challenge the application of

- the best evidence rule: no original
- the authentication rule: no evidence on the record
- the business records exception to the hearsay rule: the complexity and variety of digital information systems and the often uncontrolled way in which they are used make it difficult to distinguish business records from documents or data and to identify the business activities to which they are linked

Records Managers and Archivists Why should you care?

- Records managers have to maintain recordkeeping systems that offer reliability, integrity, compliance, comprehensiveness and systematization in order to create and maintain records that have integrity and are authentic, reliable and useable
- Archivists are increasingly assuming responsibility for unprecedented quantities and numbers of formats of digital material that could be introduced in litigation
- Your voices are needed to participate in the monitoring of existing rules and in the elaboration of new rules

Uniform Electronic Evidence Act (UEEA) 1998

The Uniform Law Conference of Canada (ULCC) adopted the *UEEA* as a model legislation that proposed reform of the traditional common law evidentiary requirements for proof of authentication and best evidence

http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2

In terms of general acceptance, a great success

UEEA Adoption
Criminal Matters

As the Canadian federal system confers legislative jurisdiction over criminal matters on the Parliament of Canada, the *Canada Evidence Act,* which includes the *Uniform Electronic Records Act's* provisions in sections 37.1-37.6, extends its application to all Provinces and Territories

UEEA Adoption
Civil Matters

- Four jurisdictions declined to adopt the *UEEA*: British Columbia*, New Brunswick, Newfoundland and Labrador, and Quebec
- PEI and Yukon enacted it as a distinct statute
- The remaining jurisdictions incorporated it in their evidence acts (*Manitoba Evidence Act)*

* It influenced provisions of the *British Columbia Evidence Act* relating to the requirements for proof for electronic court records

Application of UEEA

- The *UEEA* has received very little judicial consideration or application in the past twelve years
- Its limitations have resulted in continuing reliance on traditional, narrow common law rules rather than broader new statutory rules

UEEA Limitations

- focus on authentication and the best evidence rule
- scant attention paid to the hearsay rule and the business records exception
- absence of provisions related to the search and seizure of electronic records in both civil and criminal cases
- no attention to the protection of privacy; retention and preservation of electronic records on the part of law enforcement offices, legal offices and the courts; spoliation, or purposeful destruction of electronic records to escape prosecution; and e-discovery

UEEA Definition of Record

Paragraph 1(b): "'electronic record' means data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data."

It defines a document rather than a record (in fact, the *Manitoba Evidence Act*, section 51.1, replaces the term with 'electronic document') and does so on the basis of method of inscription and capacity of access

UEEA Best Evidence

Paragraph 1(b): “This Act focuses on replacing the search for originality, proving the reliability of systems instead of that of individual records, and using standards to show systems reliability.”

Section 6 replaced the identification of individual records by a witness or other foundation evidence with proof of compliance of the system with recognized records management standards, procedures, usages or practices.

UEEA Definition of System

Paragraph 1 ©: “an ‘electronic records system’ includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and storage of electronic records”.

Section 4 contradicts this early emphasis on records management by saying that “records retention policies, for paper or electronic records, are beyond its scope.”

UEEA and Records Management

Section 4 defies the statutory and common law rules relating to proof of authenticity by “chain of custody,” duties of preservation of evidence, destruction or spoliation of evidence, etc.

It conflicts with section 6 of UEEA, which requires a presiding judge to take into account in applying any rule of law governing admissibility of records a “standard, procedure, usage or practice,” thereby making records management pivotal in a judge’s decision as to admissibility, a decision that becomes part of the law of evidence.

Attempts to Correct UEEA

- Some jurisdictions have added definitions of additional terms to their enactment of the *Act*.
- For example, Canada and Manitoba add a definition of "computer system" to their legislation: a "computer system" is "a device that, or a group of interconnected or related devices one or more of which, a) contains computer programs or other data, and b) pursuant to computer programs, performs logic and control, and may perform any other function."

  Canada, *Canada Evidence Act,* section 31.8; Manitoba, *The Manitoba Evidence Act*, section 51.1.

Critical Gaps

- a definition of integrity, essential to the applicability of both the authentication and the best evidence rule, is not provided
- “a standard, procedure, usage or practice”, important to admissibility, is not defined
- the concept of authentication is legally incomplete as it only refers to the identification of the source of the record

As a consequence, the courts are not applying the UEEA, but rely on the old act and on digital forensic experts

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

Its methods are based on conceptual assumptions about records, trustworthiness, and recordkeeping

Records Managers, Archivists and Digital Forensics Experts

Records Managers and Archivists are called to act as forensics experts, e.g. ensuring the identity and integrity of digital records through time and attesting to it, and acquiring such records, often from obsolete systems or portable media, 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, to assess whether spoliation has occurred, to fulfill e-discovery requirements.

We Need Each Other's Knowledge

Digital forensic experts need our knowledge on

- Records Trustworthiness
- Concepts of Record and Recordkeeping

We need digital forensic experts'knowledge on

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

Digital Record: Our View

- **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**

Fixed Form

- An entity has fixed form if its binary content is stored so that the message it conveys can be rendered with the **same documentary presentation** it had on the screen when first saved (different digital presentation: Word to .pdf)
- An entity has fixed form also if the same content can be presented on the screen in several different ways in a **limited series of possibilities:** we have a different documentary presentation of the same stored record having stable content and fixed form (e.g. statistical data viewed as a pie chart, a bar chart, or a table)

Stable Content

- An entity has stable content if the data and the message it conveys are **unchanged and unchangeable**, meaning that data cannot be overwritten, altered, deleted or added to

- **Bounded Variability**: when changes to the documentary presentation of a determined stable content are limited and controlled by fixed rules, so that the same query or interaction always generates the same result, and we have different views of different subsets of content, due to the intention of the author or to different operating systems or applications

The Parts of a Digital Record

- **Formal Elements:** constituent parts of the record documentary form as shown on its face, e.g. address, salutation, preamble, complimentary close
- **Metadata:** the attributes of the records that demonstrate its identity and integrity
- **Digital Components:** stored digital entities that either contain one or more records or are contained in the record and require a specific preservation measure

Stored and Manifested Record

- **Stored record:** it is constituted of the digital component(s) used in re-producing it, which comprise the data to be processed in order to manifest the record (content data and form data) and the rules for processing the data, including those enabling variations (composition data)

- **Manifested record:** the visualization of the record in a form suitable for presentation to a person or a system. Sometimes, it does not have a corresponding stored record, but it is re-created from fixed content data when a user's action associates them with specific form data and composition data (e.g. a record produced from a relational database)

Static and Interactive Records

Static Records: They do not provide possibilities for changing their manifest content or form beyond opening, closing and navigating: e-mail, reports, sound recordings, motion video, snapshots of web pages

Interactive Records: They present variable content, form, or both, but the rules governing the content and form of presentation are fixed. Ex. Interactive web pages, online catalogs, records enabling performances

Digital Record: 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.

Digital Record: 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

Records Trustworthiness: Our View

Reliability: The trustworthiness of a record as a statement of fact, *based on* the competence of its author and the controls on its creation

Accuracy: The correctness and precision of a record's content, *based on* the competence of its author, and the controls on content recording and transmission

Authenticity: The trustworthiness of a record that is what it purports to be, untampered with and uncorrupted, *based on its* identity, integrity and the reliability of the system in which it resides

Authenticity: Our View

Identity: The whole of the attributes of a record that characterize it as unique, and that distinguish it from other records (e.g. date, author, addressee, subject, identifier).

Integrity: A record has integrity if the message it is meant to communicate in order to achieve its purpose is unaltered (e.g. chain of custody, security, technical changes).

Records Trustworthiness. The Digital Forensics View: Reliability

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

This would be an open source software, because the processes of records creation and maintenance can be authenticated either by describing a process or system used to produce a result or by showing that the process or system produces an accurate result

Records Trustworthiness. The Digital Forensics View: Accuracy

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

Repeatability, which is one of the fundamental precepts of digital forensics practice, is supported by the documentation of each and every action carried out on the evidence.

Open source software is the best choice for assessing accuracy, especially when conversion or migration occurs, because it allows for a practical demonstration that nothing could be altered, lost, planted, or destroyed in the process

Records Trustworthiness. The 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. Again, the term “source” is used to refer to either a person (physical or juridical), a system, software, or a piece of hardware.

Like in diplomatics, authenticity implies integrity, but the opposite is not true, that is, integrity does not imply authenticity.

Integrity: Our 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

Authentication: Our View

A means of declaring the authenticity of a record at one particular moment in time -- possibly without regard to other evidence of identity and integrity.

Example: the **digital signature**. Functionally equivalent to medieval seals (not signatures): verifies origin (identity); certifies intactness (integrity); makes record indisputable and incontestable (non-repudiation)

But, medieval seals were associated with a person; digital signatures are associated with a person and a record

Records Trustworthiness. The Digital Forensics View: 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 that *the computer process or system produces accurate results when used and operated properly and that it was so employed when the evidence was generated.*

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.

Other Means of Authentication

A chain of legitimate custody is ground for inferring authenticity and authenticate a record.

Digital chain of custody: the information preserved about the record and its changes that shows specific data was in a particular state at a given date and time.

A declaration made by an expert who bases it on the **trustworthiness of the recordkeeping system** and of the procedures controlling it (quality assurance).

Other Means of Authentication (cont.)

Biometric identification systems and cryptography **are not** considered the prevalent means of authentication.

Inference of system integrity: Circumstantial evidence that a system would perform its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

Other Relevant Concepts

- Copy vs. Image (a bit by bit reproduction of the storage medium)
- Chain of Custody vs. Chain of Documentation (the conditions under which the evidence is gathered, the identity of all evidence handlers, duration of evidence custody, security conditions while handling or storing the evidence, and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs)
- Prevention vs. Preparation (for detection and response)
- Identification and Acquisition vs. Search and Seizure
- Cryptography vs. Steganography (a covert form of information hiding)

What for?

Among other things:

- **Discovery**: the compulsory disclosure of pertinent facts or documents to the opposing party in a civil action, usually before a trial begins. The **discovery process** is the process of identifying, preserving, collecting, reviewing, analyzing and producing information during legal actions.
- **E-discovery:** the extension of the discovery process to information stored electronically (ESI), including email, instant messages, word processing files, spreadsheets, social networking content, and anything else stored on desktops, laptops, file servers, mainframes, smartphones, employees' home computers or on a variety of other platforms.

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.

Digital Records Forensics Project

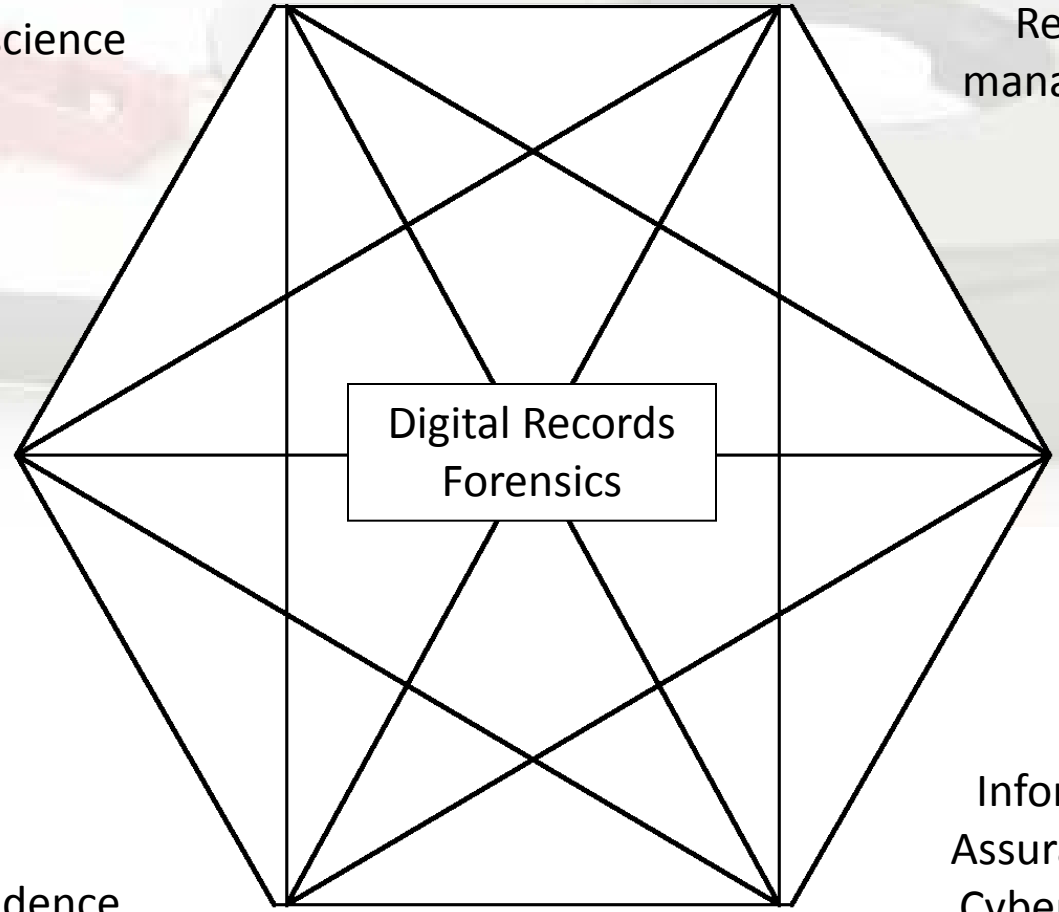
The DRF Project (2008-2011) is a collaboration between

- The UBC Archival Studies programs in the School of Library, Archival & Information Studies
- The UBC Law of Evidence Department in the Faculty of Law
- The University of Washington Information Assurance and Cybersecurity program in the School of Information, and
- the Computer Forensics Division of the Vancouver Police Department

Objectives of the Digital Records Forensics Project

- to carry out an analytical comparison and integration of the concepts and methods of Diplomatics/Records Management, Archival Science and Digital Records Forensics
- to further enrich this integrated body of knowledge with the Law of Evidence, and Information Assurance and Cybersecurity concepts and methods
- to identify, develop and organize the content of a new discipline called “Digital Records Forensics”
- to develop the intellectual components of a program of education for Digital Records Forensics experts, as a specialization of archival programs

Digital Records Forensics



Methodology

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

Bibliographic Database

- Provides an overview of diplomatic, records management, archival, legal and digital forensic literature on digital records
- Searchable by discipline, keyword, author, etc.
- Provides brief annotations on each citation, highlighting relevant issues

Case Law Database

- Authentication
- Discovery and Disclosure
- Forensic Experts
- Preservation Orders
- Privacy
- Probative Value
- Spoliation
- Unintelligible Evidence
- Digital Evidence

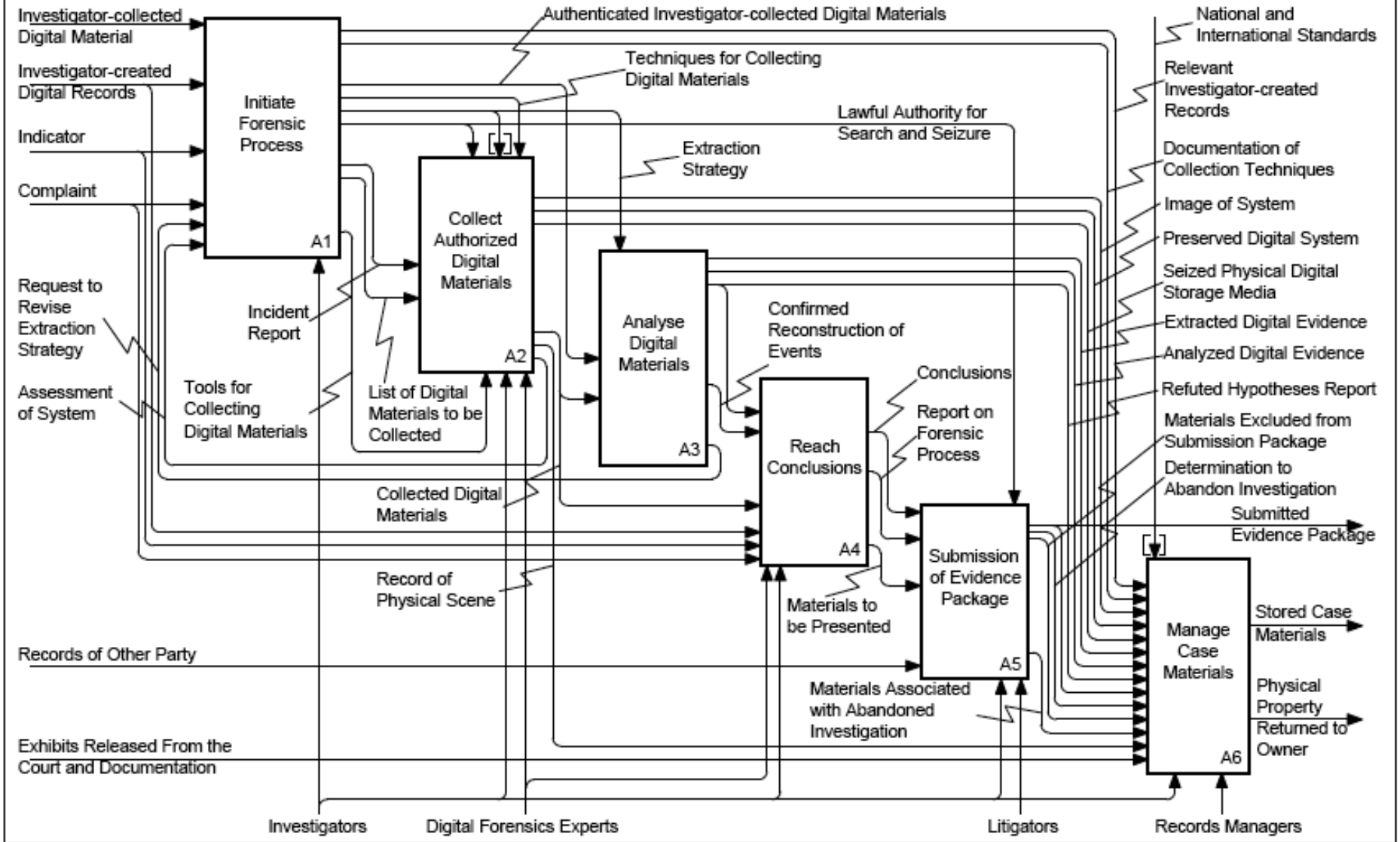
Terminology Database

- **Purpose**: To support multi-disciplinary communication
- **Scope**: terms are taken from articles, dictionaries & glossaries of various fields
- **Structure**: names the term, identifies the part of speech, provides a definition for each discipline, and the source of the definition.

Interviews

- Interviews to date and scheduled:
  - Lawyers
  - Judges
  - Court clerks
  - Records managers (in law enforcement)
  - Police investigators
  - Forensics experts

USED AT:	AUTHOR:	DATE: 14-Nov-2008		WORKING	READER	DATE	CONTEXT:
	PROJECT: DRF Model	REV: 05-Jun-2010		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION			A-0



NODE:	TITLE:	NUMBER:
A0	Conduct Digital Forensics	

Preliminary Findings

- Professions involved with documentary evidence have a disciplinary perspective that affects:
  - What is considered a record
  - How authenticity is determined
  - How reliability is determined
  - What constitutes evidence and its admissibility

Preliminary Findings (cont.)

- Chain of Custody: a common thread throughout professions
  - Either establishes or demonstrates authenticity
- Context is a key driver in understanding domain differences, e.g.
  - Lawyers do not require a definition of record because the context defines the entity
  - Archivists build context into the definition of record

Preliminary Findings (cont.)

- 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

Preliminary Findings (cont.)

Case Study: Vancouver Police Department

- Chain of custody is the basis for presumption of reliability and authenticity.
- At moment of seizure, investigator takes on the role of trusted custodian
- Complete reliance on EDRMS to make explicit all links between records
- Implementing a Storage Area Network - ahead of the curve

Preliminary Findings (cont.)

	Concept of digital record	Establishment of authenticity	Maintenance of authenticity over time	Challenges to authenticity, preservation	Challenges to digital records as evidence
Archivists	Established definition	Specific requirements-identity & integrity	Trusted custodian	Creation; lack of procedures; Obsolescence	Archival theory addresses evidentiary capacity
IM (law enforce-ment)	Generated in electronic format	Chain of custody	Chain of command	Silos; different SW/HW, collaborative, multi-users	Retention, integrated units, migration
Lawyers	Anything on digital media; context dependent	Context; proper forensic process; source	Not an issue	Process; multi-user systems	Unallocated clusters / forensic process
Judges	Anything in a computer	Authentication	Not a concern	Proof of reliability	Proof of reliability; chain of custody; alterations; completeness
Forensics experts	Anything stored in or generated by a computer	Hash values; chain of documentation; trusted 3rd party	Maintenance of integrity and chain of custody	Lack of understanding of technology	N/A
Police investi-gators	Archival and/or legal definition (business records)	Provenance (source)	Chain of custody	Obsolescence; corruption;no interoperability	Show chain of custody

Next Steps

- Complete interviews
- Develop a model of a digital records forensics process
- Develop series of concept papers
- Develop educational program

Stay Tuned...

Thank you!

www.digitalrecordsforensics.org

Addendum on E-Discovery and Spoliation

Case Law 2010

E-Discovery-Negligence

Regardless of whether the actions resulted “from a pure heart and an empty head” (Judge Scheindlin), simple negligence is:

- failure to obtain records from all employees,
- failure to take all appropriate measures to preserve ESI (electronically stored information),
- the failure to assess the accuracy and validity of selected search terms, or
- the failure to collect evidence.

E-Discovery-Gross Negligence

- the failure to issue a written legal hold;
- the failure to identify the key players and ensure that their electronic and paper records are preserved;
- the failure to cease the deletion of e-mail or to preserve the records of former employees that are in a party's possession, custody or control;
- and the failure to preserve backup tapes when they are the sole source of relevant information or when they relate to key players, if the relevant information maintained by those players is not obtainable from readily accessible sources.

E-Discovery-Misconduct

Willful, wanton or reckless misconduct includes an intentional act, indifferent to the consequences, which "make[s] it highly probable that harm would follow."

For example, the intentional destruction of relevant ESI or paper documents, especially if the conduct occurred after the final relevant *Zubulake opinion was issued in July 2004.*

Zubulake opinion

Cost-sharing is only to be considered when electronic discovery imposes an "undue burden or expense" on the responding party, based on

- the extent to which the request is specifically tailored to discover relevant information;
- the availability of such information from other sources;
- the total cost of production, compared to the amount in controversy;
- the total costs of production, compared to the resources available to each party;
- the relative ability of each party to control costs and its incentive to do so;
- the importance of the issues at stake in the litigation; and
- the relative benefits to the parties of obtaining the information.

Implications for Canada

- Manitoba rules of procedure are based on BC, Ontario and, partly, Alberta rules. These, on turn, tend to follow the Peruvian Guano principle by which both parties have access to each other's documentation, and the "train of inquiry" clause makes the process virtually unlimited. BC is looking at the Zubulake opinion, correcting it by stating that the proceeding should be conducted in ways that are proportionate to:

  (a) the amount involved in the proceeding;

  (b) the importance of the issues in dispute; and

  (c) the complexity of the proceeding.

Other issues

- Duty to preserve: it arises when a party reasonably anticipates litigation
- Burden-shifting: it is the responsibility of the innocent party to prove spoliation, including culpable state of mind and relevancy
- Ignorance is no longer bliss and there is decreasing protection for preservation mistakes, oversights or intentional destruction activities.
- Written legal holds should be issued as soon as litigation is anticipated.

Legal Hold

A recent study by Kroll Ontrack found that only 57% of U.S. corporations have an identified means to preserve potentially relevant data when litigation or a regulatory investigation is anticipated.

Corporations are unable to comply with their duty to preserve potentially relevant information if they lack an appropriate means to suspend the expulsion of potentially responsive data. By failing to implement measures necessary to issue a legal hold, a company's ESI readiness policy cannot be effective and the company is at risk for costly motions and sanctions.

Legal Hold (cont.)

Furthering the precariousness of the legal hold process is the divide between corporate legal and IT departments, which share an increasing amount of responsibility for creating ESI strategy and enforcement. This is due to:

- role confusion,
- terminological barriers and
- budgetary ownership

Forensic Readiness

- Implement a recordkeeping system
- Develop Applications Inventory and Data Map
- Periodic updates should intertwine with technology asset management processes, storage planning, information security assessments and other peripheral processes
- When applications or systems are retired, information should be included as to where the final set of data/docs/rec is kept and what process will be required to restore if necessary
- Implement a written legal hold sooner rather than later if litigation appears to be on the horizon. To increase defensibility, parties should maintain detailed notes of the preservation protocol: when the hold was issued, what details were included in it, to whom it was issued and the efforts taken to continually monitor compliance.

More on the Hold

- It should contain the purpose for the hold, a description of the lawsuit or investigation, and the guidelines for determining what data should be preserved and by whom.
- Counsel should then work jointly with IT to notify legal opponents and any relevant third parties of their duty to preserve potentially responsive information.
- Internal automatic destruction must also be suspended, which includes halting defragmentation software and other forms of automatic or routine drive “cleanup” activities

More on Hold (2)

- Counsel should actively monitor internal suspension measures and ensure compliance: sending update notices to keep key players and new employees informed, reminding them of their preservation obligations.
- Detailed and accurate records should be kept of what data have been preserved and how, should the opposing party bring preservation methods into question.
- Counsel should ensure the legal hold is in effect until final judgment, a settlement has been reached and a formal release has been signed by all parties, or the case is dismissed and no related claims remain outstanding.
- To lift the legal hold, counsel should circulate an explicit notice that serves to officially resume scheduled disposal. Care must be taken to ensure the hold is not lifted prematurely on particular data that may be concurrently under hold for another matter.