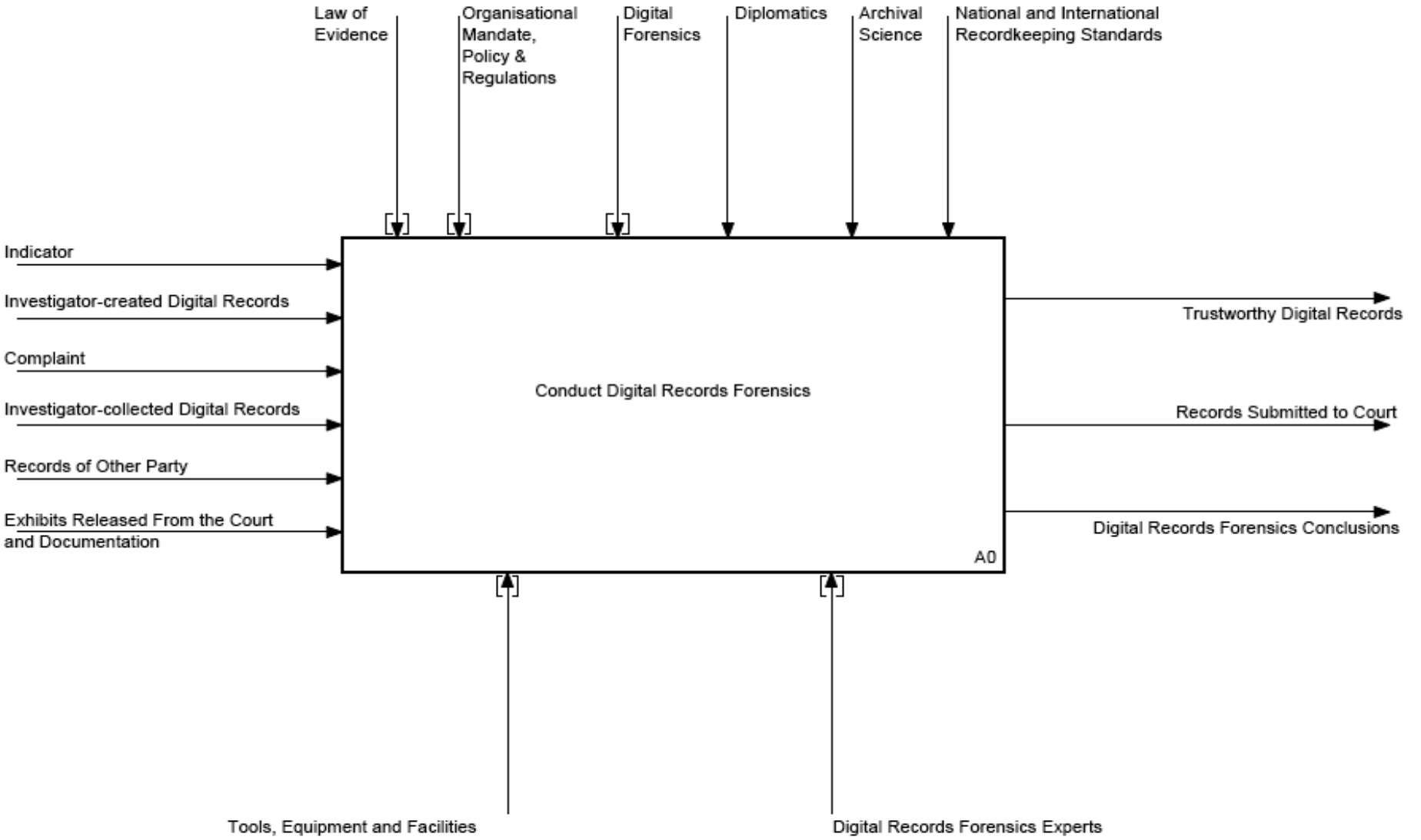
Digital Records Forensics: Preliminary Findings

Corinne Rogers

Association of Canadian Archivists
Annual Conference
10 June 2010
Halifax, NS, Canada

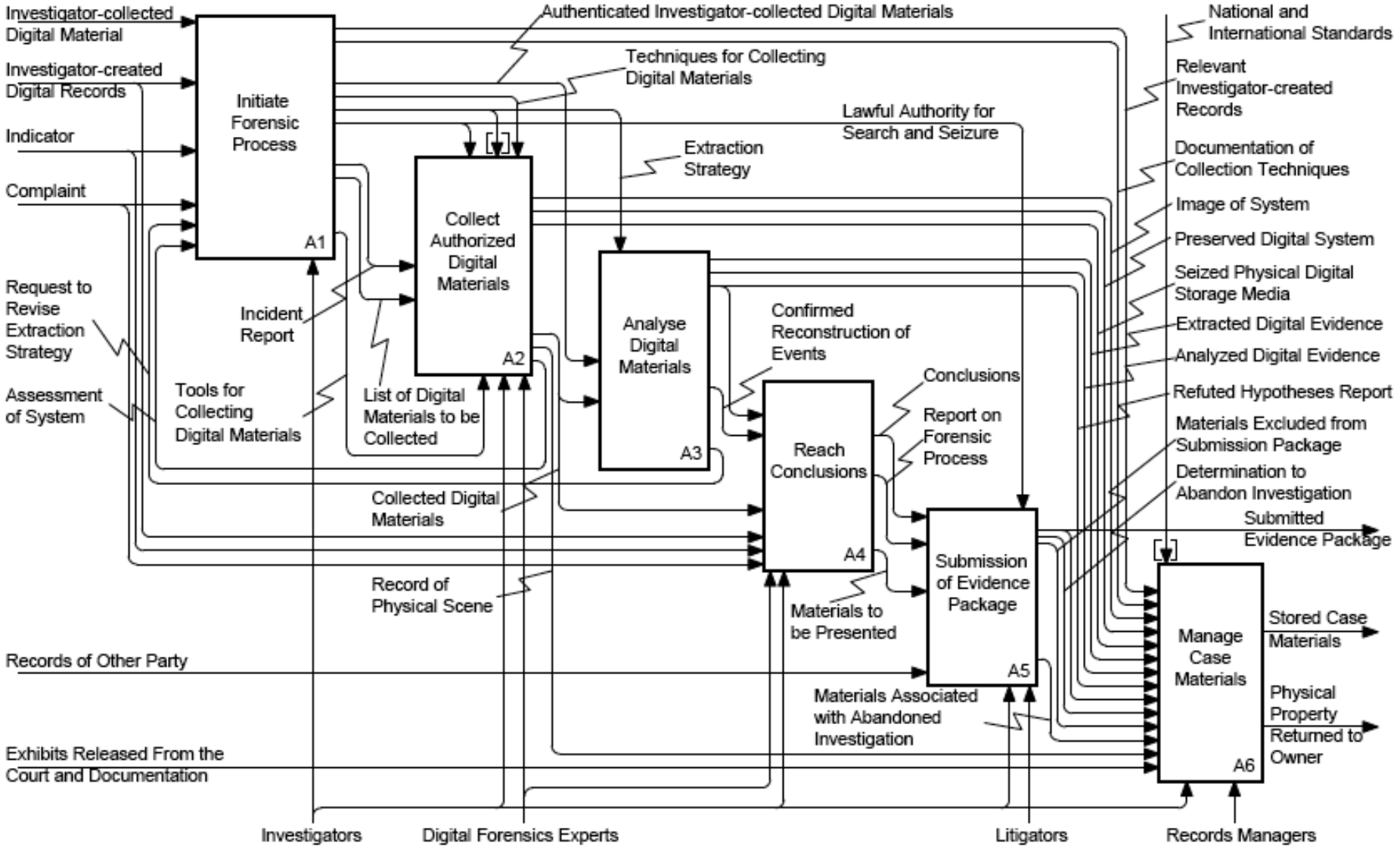
Digital Records Forensics Project

USED AT:	AUTHOR:	DATE: 03-Nov-2008		WORKING	READER DATE	CONTEXT:
	PROJECT: DRF Model	REV: 09-Feb-2009		DRAFT		TOP
				RECOMMENDED		
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION		



NODE:	TITLE:	NUMBER:
A-0	Conduct Digital Records Forensics	

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	

Interviews

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

Perspectives of digital evidence

- 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

Common threads

- 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 distinct definition of record because application of context defines purpose
  - Archivists build context into the definition of record

Terminology

- Definitions are domain-specific & terminology is often conflicting across domains
  - Record
  - Lifecycle
  - Classification
  - Privilege
  - Image v. copy
  - Bit image copy v. file system copy
  - Preservation v. storage v. archive
  - Archive, noun or a verb?

Paper v. digital

- 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

Case study

Vancouver Police Department

- Chain of custody is the basis for presumption of reliability and authenticity.
- At moment of seizure, investigator assumes 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 interview data

	Concept of digital record	Establishment of authenticity	Maintenance of authenticity over time	Challenges to authenticity, preservation	Challenges to digital records as evidence
Archiv-ists	Established definition	Specific requirements-identity & integrity	Critical-trusted custodian	Creation; Tampering; 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	Any record on a computer	Authentication	Not a concern	Proof of reliability	Proof of reliability; chain of custody; alterations; completeness
Forensic s experts	Could be anything	Hash values; digital sig; trusted 3rd party	Maintain integrity	Lack of understanding of technology	N/A
Police investi-gators	Archival definition (evidential value)	Provenance (source)	Chain of custody	Obsolescence; corruption; interoperability	Show chain of custody

Digital forensics to digital *records* forensics

- Is there specific knowledge needed?

"Absolutely"

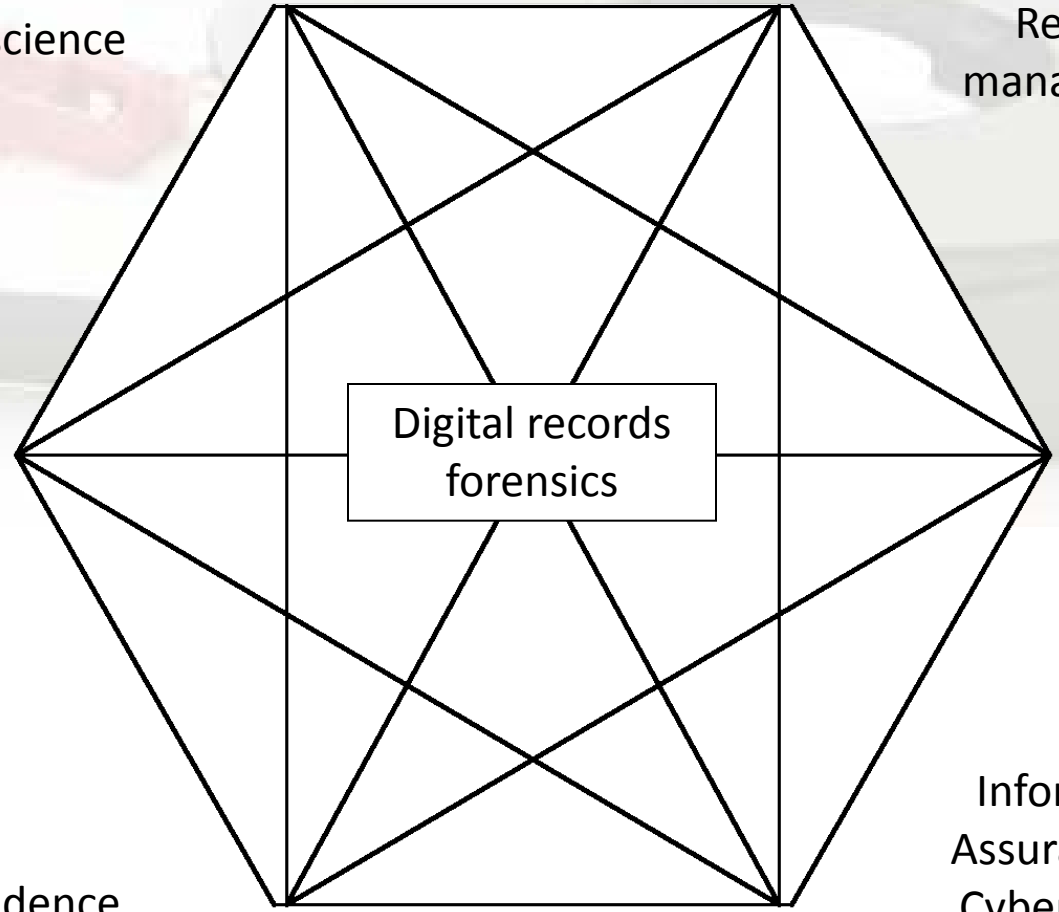
- Technological
- Archival/Diplomatic
- Legal

} *Digital Records Forensics*

Next Steps

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

Digital Records Forensics



Thank you!

www.digitalrecordsforesnics.org