# Digital Records Forensics Project

A collaboration between University of British Columbia's School of Library, Archival and Information Studies,
Faculty of Law, & Vancouver Police Department

Corinne Rogers, UBC

authenticity available concepts develop digital diplomatics

The Digital Records Forensics Project integrates archival diplomatics, computer forensics and the law of evidence to develop concepts and methods:

- to recognize records produced by and removed from complex digital systems;
- to determine their authenticity, reliability & accuracy;
- to maintain records acquired from crime scenes or created by police to pursue crime over the long term so that their authenticity will not be questioned;
- to identify & develop a new discipline of *digital records forensics*;
- to identify intellectual components of an education program.

issues knowledge law legal methodology methods original practices preservation

## Research Methods & Products:

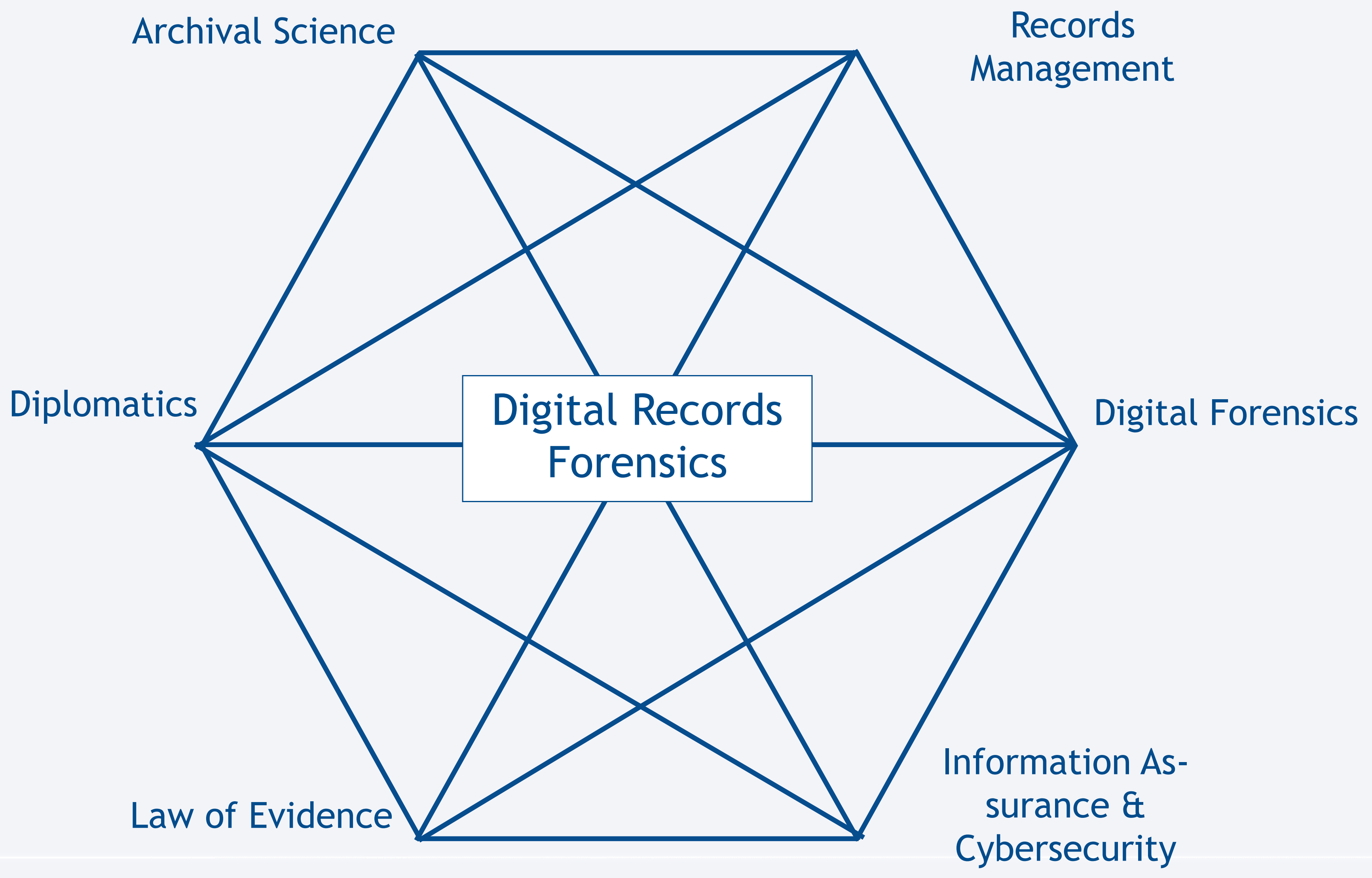
- interdisciplinary literature review - law, digital forensics, archival diplomatics
- analysis of North American case law
- interviews & questionnaires
- ethnographic study of the Vancouver Police Department
- case law database
- terminology database
- digital records forensics activity model
- white papers
- educational curricula

document electronic environment evidence

## This research benefits:

- law enforcement professionals
- the legal profession - lawyers & judges
- records professionals
- records users - journalists, scholarly researchers and citizens
- records creators - public and private sectors, individuals or organizations

preservation principles professionals purpose records



### Record types

- computer stored
- computer generated

### Where found

- hard drives
- photocopiers
- PDAs
- cell phones
- digital cameras
- swipe card logs
- appliances
- gaming systems

### Archival issues

- what is a record
- context
- authenticity
- reliability
- maintenance
- preservation

### Law of Evidence

- best evidence rule
- hearsay rule
- business exception to the hearsay rule
- Daubert guidelines
- case law v. statutory law

### Evidence Issues

- evidence
- authentication
- authenticity
- reliability
- integrity
- accuracy
- identity

### Forensics Issues

- repeatability
- verifiability
- objectivity
- transparency
- data integrity
- duplication integrity
- computer integrity
- system integrity

### Terminology

- record v. document
- information v. data
- lifecycle
- authenticity
- authentication
- classification
- privilege
- image v. copy
- preservation
- storage
- archive

### Interviews

- lawyers
- judges
- court clerks
- records managers
- police investigators
- forensics experts

### Commonalities

- chain of custody
- context
- e-discovery
- electronically stored information
- risk

www.digitalrecordsforensics.org

## Vancouver Police Department Case Study

- VPD is "ahead of the curve";
- Implementing a Storage Area Network (SAN);
- At the moment of siezure, the investigator assumes role of trusted custodian;
- There is reliance on VPD's EDRMS to make explicit all links between records.

## 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 |
|---|---|---|---|---|---|
| **Archivists** | Established definition based on theory & practice | Specific requirements - identity & integrity | Critical - trusted custodian | Circumstances of creation; tampering; obsolescence | Archival theory addresses evidentiary capacity |
| **Information managers (law enforcement)** | Anything generated in electronic format | Chain of custody | Chain of command | Silos; different SW/HW; multiple creators/owners | Retention; integrated units; migration |
| **Lawyers** | Anything on digital media; context-dependent | Context; proper forensic process; source | Not an issue (interviews to date) | Process; multi-user systems | Unallocated clusters; forensic process |
| **Judges** | Any record on a computer | Authentication | Not a concern (interviews to date) | Proof of reliability | Proof of reliability; chain of custody; alterations; completeness |
| **Forensics experts** | Anything created electronically | Hash values; digital signatures; trusted 3rd party | Maintain integrity | Lack of understanding of technology | N/A |
| **Police investigators** | Archival definition (evidential value) | Provenance (source) | Chain of custody | Obsolescence; corruption; interoperability | Show chain of custody |

## Next Steps

- Complete interviews
- Develop a model of the digital records forensics process
- Conduct survey questionnaires
- Develop a series of concept papers
- Develop education curriculum

UBC

Digital Records Forensics Project

Social Sciences and Humanities Research Council of Canada
Conseil de recherches en sciences humaines du Canada

Luciana Duranti, Principal Investigator; Anthony Sheppard, Co-investigator. Graduate Research Assistants: Alexandra Allen; Donald Force; Adam Jansen; Cindy McLellan; Corinne Rogers.