



Digital Records Forensics Project

DIGITAL RECORDS FORENSICS: A NEW SCIENCE AND ACADEMIC PROGRAM FOR FORENSIC READINESS

3rd Australian Security and Intelligence Congress (secAU 2010)

1 December 2010

Security Research Center,

Edith Cowan University

Perth, Australia

Luciana Duranti, The University of British Columbia

Barbara Endicott-Popovsky, University of Washington

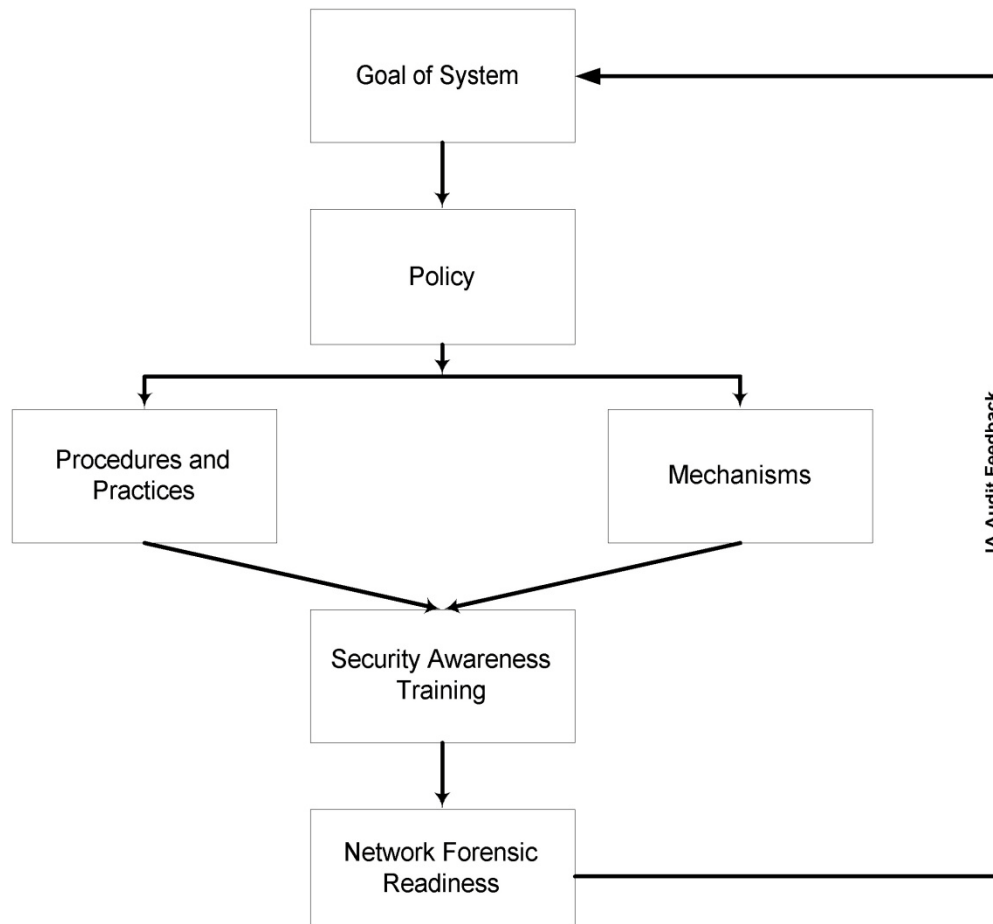


Digital Records Forensics Project

Incorporating Network Forensic Readiness

INFORMATION ASSURANCE

Digital Records Forensics Project



Digital Records Forensics Project

In a typical incident response....

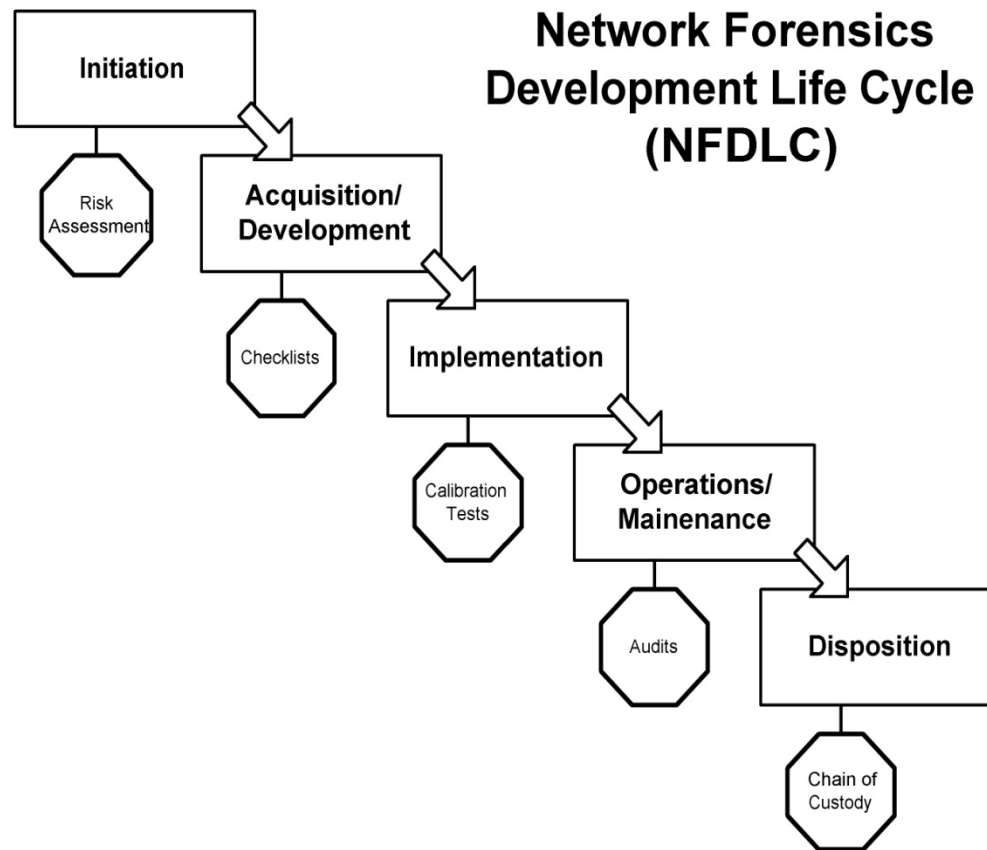
- Technicians must choose:
 - Expend effort collecting forensically sound data, or
 - Simply restore network as quickly as possible
 - » Evidentiary files altered in the process
 - » Forensic value limited
- Expediency wins...and so do attackers!

Digital Records Forensics Project

New Zealand vs. Russian Cases

Characteristics	NZ Hacker Case	Russian Hacker Case
Type of attack	Typical script kiddie intrusion scenario	Online criminal automated auction scam
Damages	\$400,000	\$25 million
Investigator time	417 hours	9 months
Consequences	Community service	3 & 4 years in Federal prison

Digital Records Forensics Project



Digital Records Forensics Project

ISDLC (Life Cycle) Phases	NFDLC Additional Procedures
Initiation Phase: preliminary risk assessment	Determine what aspects of a network warrant digital forensic protection
Acquisition/ Development Phase	Adhere to Rules of Evidence in system requirements
Implementation Phase	Perform baseline testing Perform network/mechanism verification/calibration tests
Operation/ Maintenance Phase	Conduct verification/calibration audits
Disposition Phase	Incorporate chain of custody/ evidence preservation procedures



Digital Records Forensics Project

Collecting evidence across the lifecycle of forensic data

- Gather
- Store
- Retrieve
- Make available
- Secure
- Create repeatable process

Digital Records Forensics Project

Survivability Strategy	Tools
Resistance Ability to repel attacks	• Firewalls • User authentication • Diversification
Recognition 1) Ability to detect an attack or a probe 2) Ability to react or adapt during an attack	• Intrusion detection systems • Internal integrity checks
Recovery 1) Provide essential services during attack 2) Store services following an attack	• Incident response • Replication • Backup systems • Fault tolerant designs
Redress 1) Ability to hold intruders accountable in a court of law. 2) Ability to retaliate	• Computer Forensics • Legal remedies • Active defense



Digital Records Forensics Project

First Principles

IA VS. ARCHIVAL SCIENCE

Digital Records Forensics Project

Underlying Principles

IA Principles	Archival Principles
Integrity	Integrity and reliability
Availability	Useability
Authentication	Authenticity
Non-repudiation	
Confidentiality	

Digital Records Forensics Project

Linkages and context

- **content** - facts about the activity are accurate and complete,
- **context** - circumstances of its creation and use and
- **structure** - relationships between data/information/records must be transparent



Digital Records Forensics Project

Archival Science essential is a Legal Science

HISTORY OF ARCHIVAL SCIENCE

Digital Records Forensics Project

Archival concepts are grounded in Roman Law

- Archives as a place—trusted custody
- Authenticity based on a chain of trusted custody
- Reliability based on antiquity and on form (Justinian Code)

Archival methods are born out of legislative acts

- Swedish Law of 1766—freedom of information act
- Decree 25 July 1793—public records belong to the people
- Decree of 1841—principle of respect des fonds

Archival science is at its heart a legal science

Digital Records Forensics Project

Authenticity and reliability needed to be tested using scientific methods, beyond Valla's textual criticism

Diplomatics (1681), a new science studying the nature, genesis, formal characteristics, structure, transmission and legal consequences of records, gave origin to **Palaeography, Sigillography, Heraldry, Philology, Exegesis, Semiotics, etc.**

The **Bella Diplomatica** gave origin to the **Law of Evidence**: by mid 18th century all faculties of law in Europe taught these “forensic” disciplines

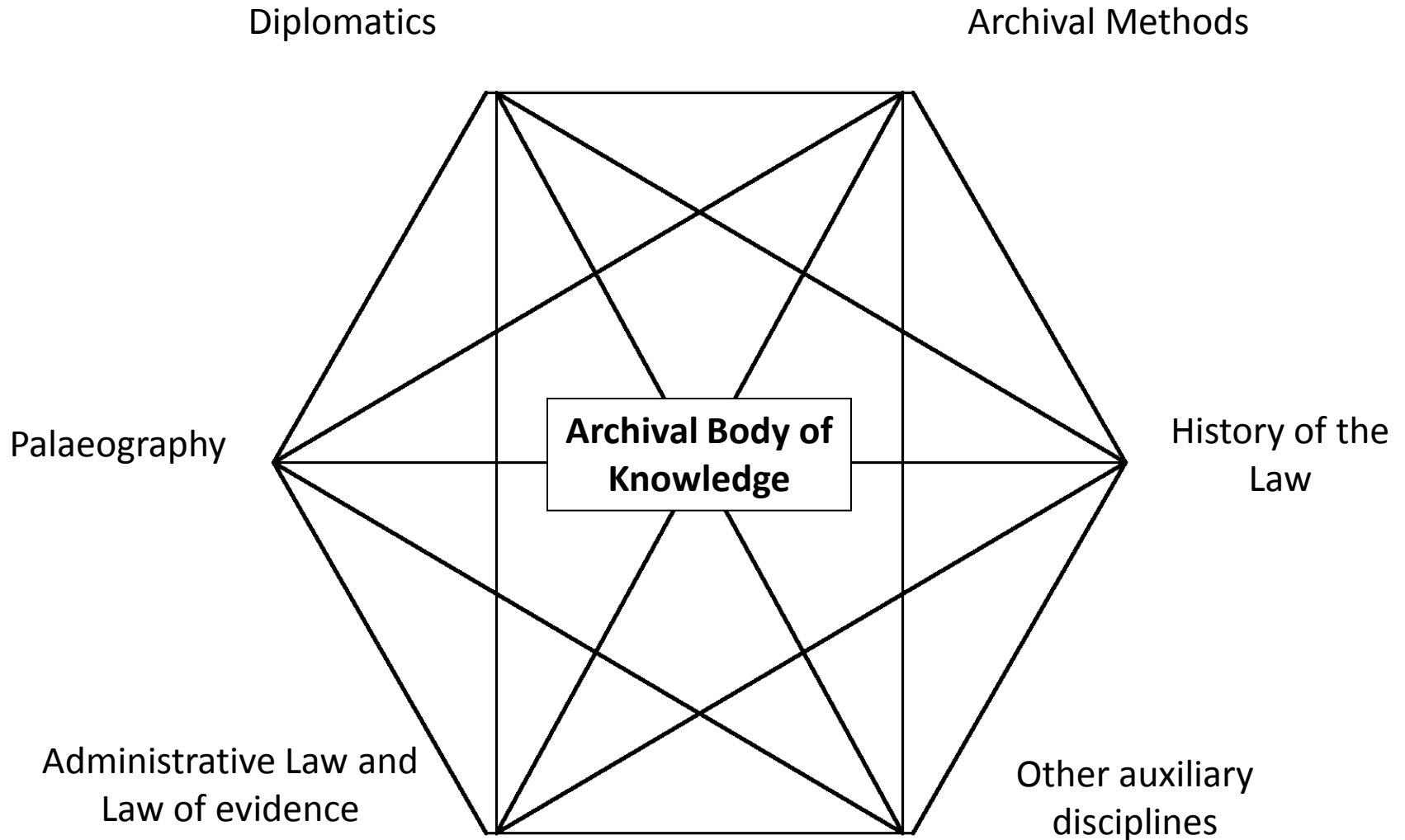


Digital Records Forensics Project

Comparing Bodies of Knowledge

DIGITAL FORENSICS VS. ARCHIVAL SCIENCE

Archivists



Digital Records Forensics Project

Today:

Archivists are called to act as forensics experts, e.g. assessing the identity and integrity of records stored in a variety of obsolete or nearly obsolete hardware/software and/or formats, or on portable media, and attesting to it

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.

Digital Records Forensics Project

Digital forensic experts need archival knowledge on

- Records Trustworthiness
- Concept of Record and Recordkeeping

Archivists need digital forensics'

- Understanding of integrity
- Processes of access, identification and acquisition

Digital Records Forensics Project

Records Trustworthiness: The Digital Forensics View

Reliability: Dependable, consistent and undeviating, created by a competent authority following established procedures -- trustworthy as to content and systems.

Accuracy: The degree to which data, information, documents or records are precise, correct, truthful, free of error or distortion, or pertinent to the matter

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 (=reliability). It implies integrity, but integrity does not imply authenticity.

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 computer integrity

Digital Records Forensics Project

The Daubert Rules

Extended from scientific to technical evidence (to assess demonstrative evidence, not substantive—capability rather than intentionality):

- the theory, procedure or process for making or keeping the record has been tested or cannot be tampered with
- it has been subjected to peer review or publication (standard)
- the known or potential error rate is acceptable
- it is generally accepted within the relevant scientific community

In a system, digital forensic experts look for **repeatability, verifiability, objectivity** and **transparency**

Digital Records Forensics Project

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

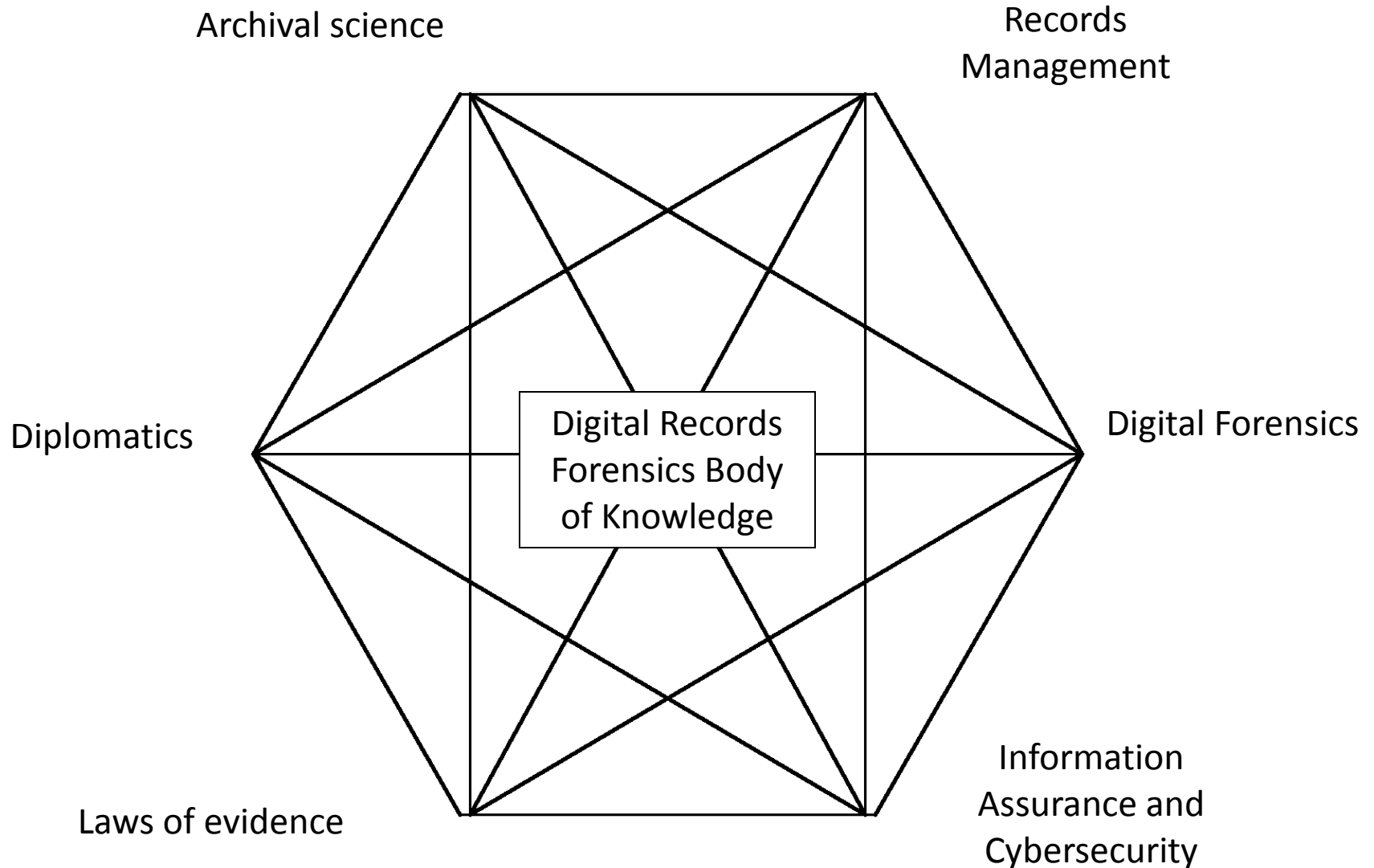
- British Columbia Rail case: the judge pointed out that legislation speaks of preserving “records,” and the Liberal MLA Ralph Sultan asked “What is the definition of a record?” referring “to the controversy over to what extent e-mails qualify” (Vancouver Sun, January 29, 2010).
- The Supreme Court of Canada is deciding whether hyperlinks in a text are akin to footnotes or make of the material to which they connect the reader a component of the document being read (Vancouver Sun, April 2, 2010).

Digital Records Forensics Project

The trustworthiness of digital records is equally problematic:

- The law prefers that the original of any document, regardless of medium or form, be used as evidence at trial, but in the digital environment, we no longer have originals.
- We cannot keep digital records. We can only maintain our ability to reproduce or even to re-create them as needed, or image the container of the records at a given point in time.
- As a consequence, the **authenticity** of digital records is difficult to establish on the records themselves and becomes ***an inference that one draws from the circumstances surrounding the creation, maintenance and preservation of the records.***
- This is a problem not limited to law enforcement, but affecting any human activity based on the trustworthiness of records, including research, therefore, it is an archivists' concern.

Digital Records Forensic Expert



Digital Records Forensics Project

Digital Records Forensics Science BOK

- The Law of Evidence
- Diplomats (specifically Digital Diplomats)
- Digital Forensics
- Archival Science
- Information Technology
- Organizational Information Assurance

Digital Records Forensics Project

Transition Required

- From an investigative and response mechanism to one of prevention, compliance and assurance (Barbin and Patzakis)
- Proactively influencing system design and the active life of the record



Digital Records Forensics Project

Collaboration between UBC and UW

DIGITAL RECORDS FORENSICS PROJECT

Digital Records Forensics Project

New Professional Master's Degree:

- Integration of MSIM at UW and MS Archival Science UBC
- Professionals educated in core theoretical and methodological knowledge that identifies their profession
- Learn international standards as well as specific, local and unique aspects of the local juridical-administrative environment in which they will work
- Educated in the scholarly and practical nature of their work.

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

<http://www.digitalrecordsforensics.org/>

Digital Records Forensics Project

“people need to understand what exactly a record is. And then understand the manner in which it’s maintained. So you’d have to have the knowledge of what it is you’re trying to maintain and then the knowledge of the systems that are maintained. So, yes, there’s some very specific knowledge needed”

Mark Johnstone, Sergeant, Forensics Services Division, Financial Crime Unit, Vancouver Police Department



Digital Records Forensics Project

QUESTIONS?