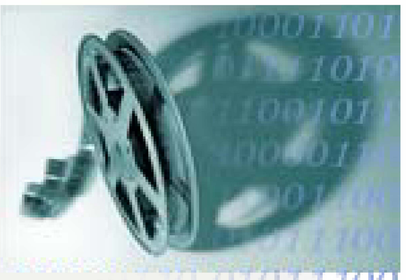


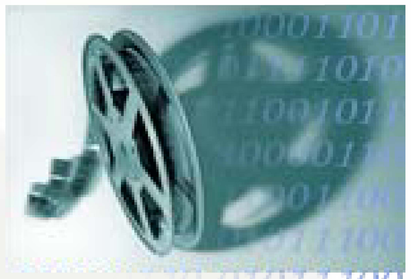

Preserving the Authenticity of Digital Evidence

Luciana Duranti
Adam Jansen
Barbara Endicott-Popovsky
Fred Cohen

Seventh Annual IFIP WG 11.9 International. Conference on Digital Forensics
1 Feb 2011, Orlando, FL, USA

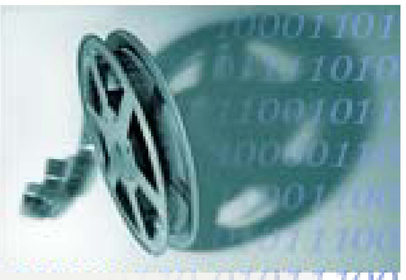
Dr. Barbara Endicott-Popovsky, Research Associate Professor Information School
Director, Center for Information Assurance and Cybersecurity
Academic Director, Master of Infrastructure Planning and Management
University of Washington
Seattle, Washington

AN INTERDISCIPLINARY APPROACH TO PROACTIVE FORENSIC READINESS




Seventh Annual IFIP WG 11.9 International. Conference on Digital Forensics
1 Feb 2011, Orlando, FL, USA

Typical Incident Response

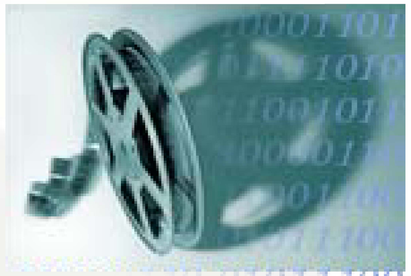
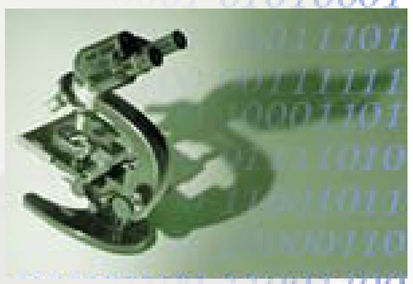


Technicians must choose:

- Expend effort collecting forensically sound data, or
- Simply restore network as quickly as possible
  - Evidentiary files altered in the process
  - Forensic value limited
- Expediency often wins

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

Transition Required

- From:

  - an **investigative and response mechanism**

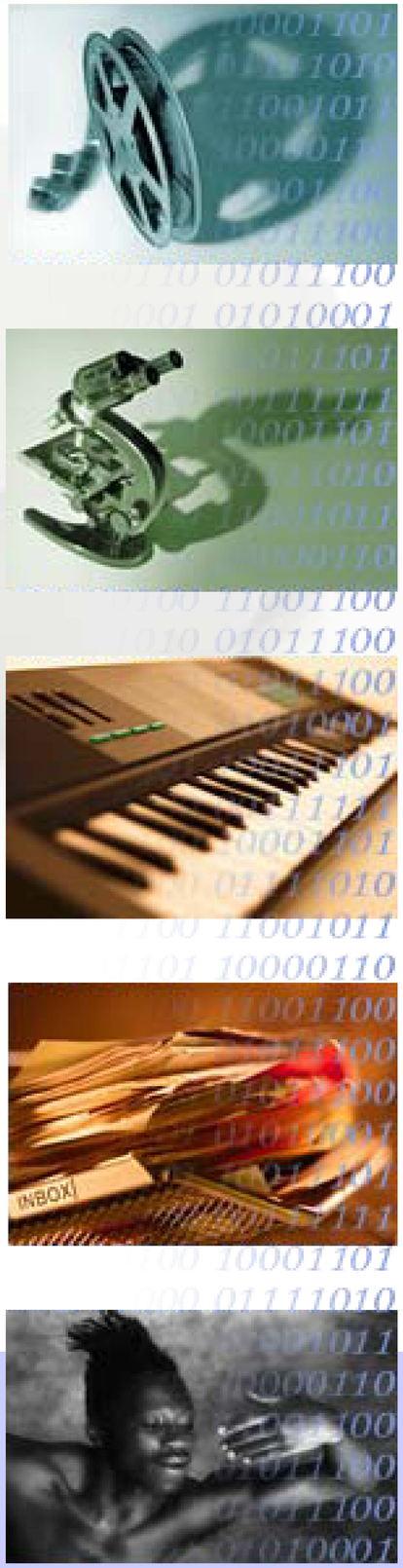
- To:

  - one of **prevention, compliance and assurance** (Barbin and Patzakis)

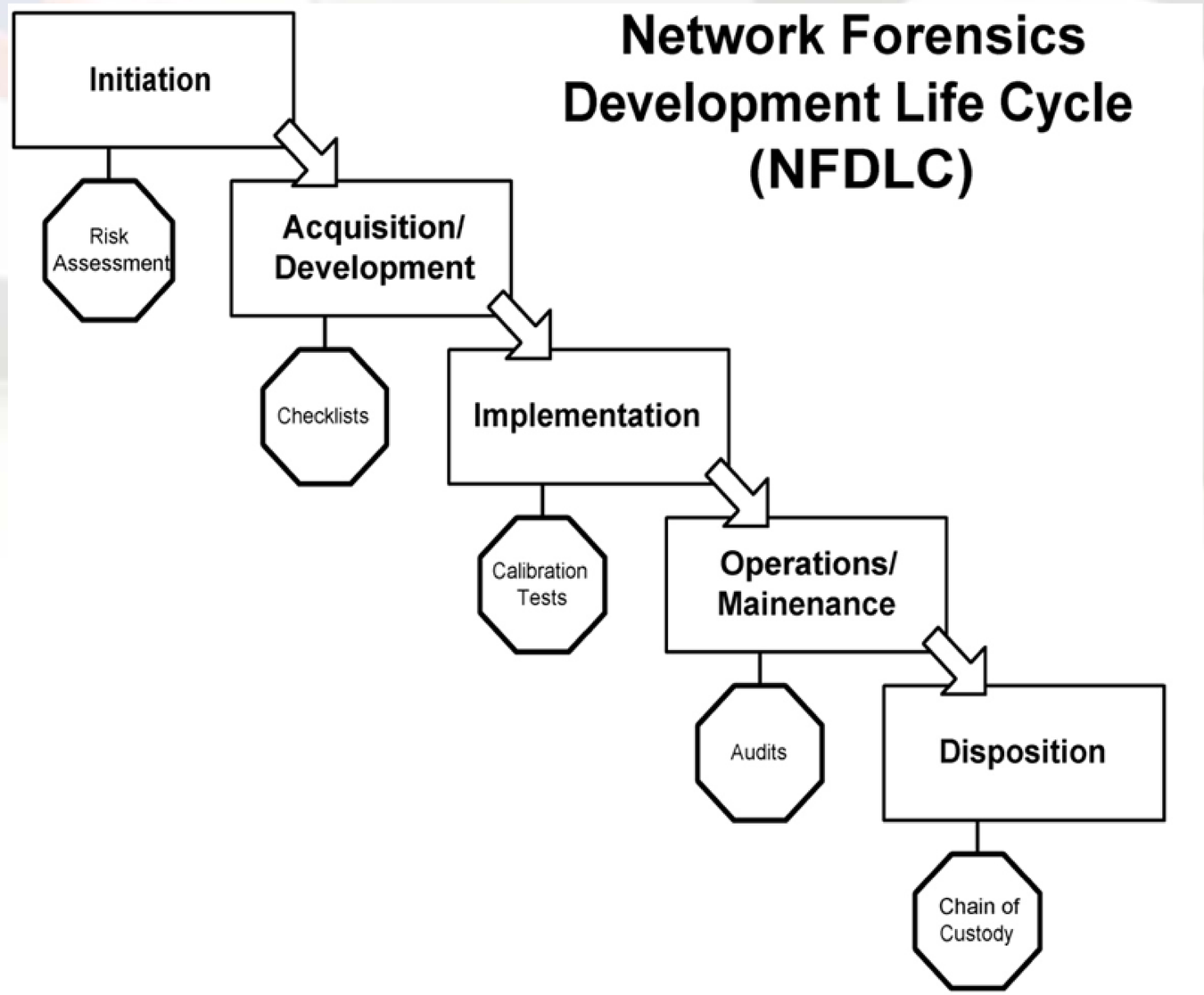
- **Proactively influencing**

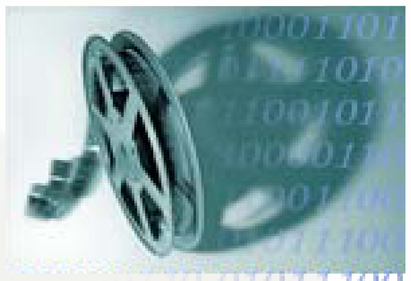
  - system design and

  - active life of the record



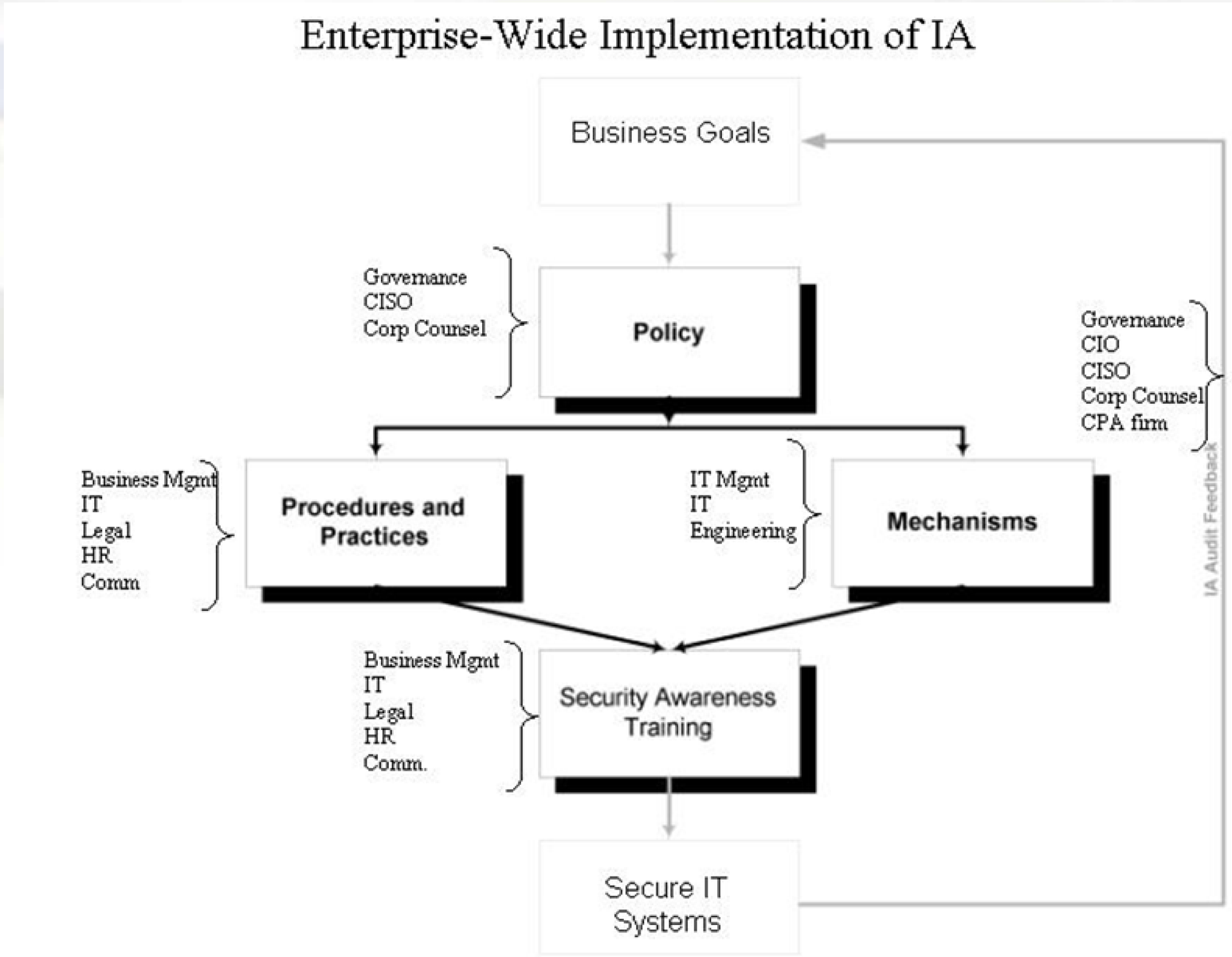
Embed Forensics in IT Systems

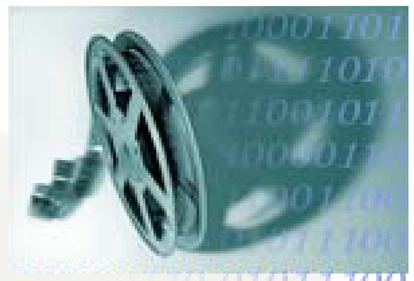




Seventh Annual IFIP WG 11.9 International. Conference on Digital Forensics
1 Feb 2011, Orlando, FL, USA

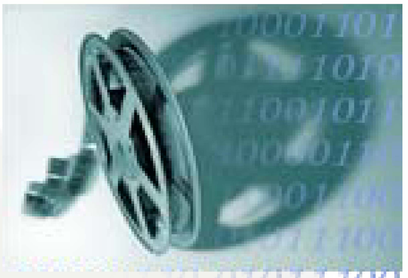
Embed Forensics in IA Programs





Seventh Annual IFIP WG 11.9 International. Conference on Digital Forensics
1 Feb 2011, Orlando, FL, USA

Complementary Needs of the Digital Forensics (IA) and Archival Disciplines

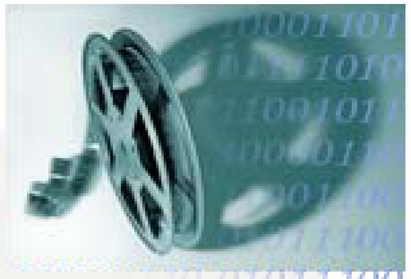
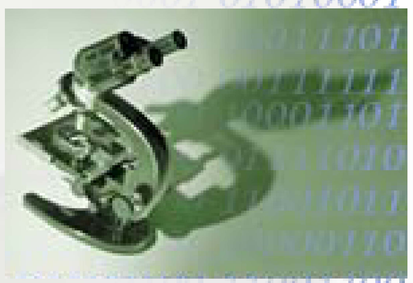


- Digital forensic (IA) experts need archival knowledge on:
  - Records Trustworthiness
  - Concept of Record and Recordkeeping

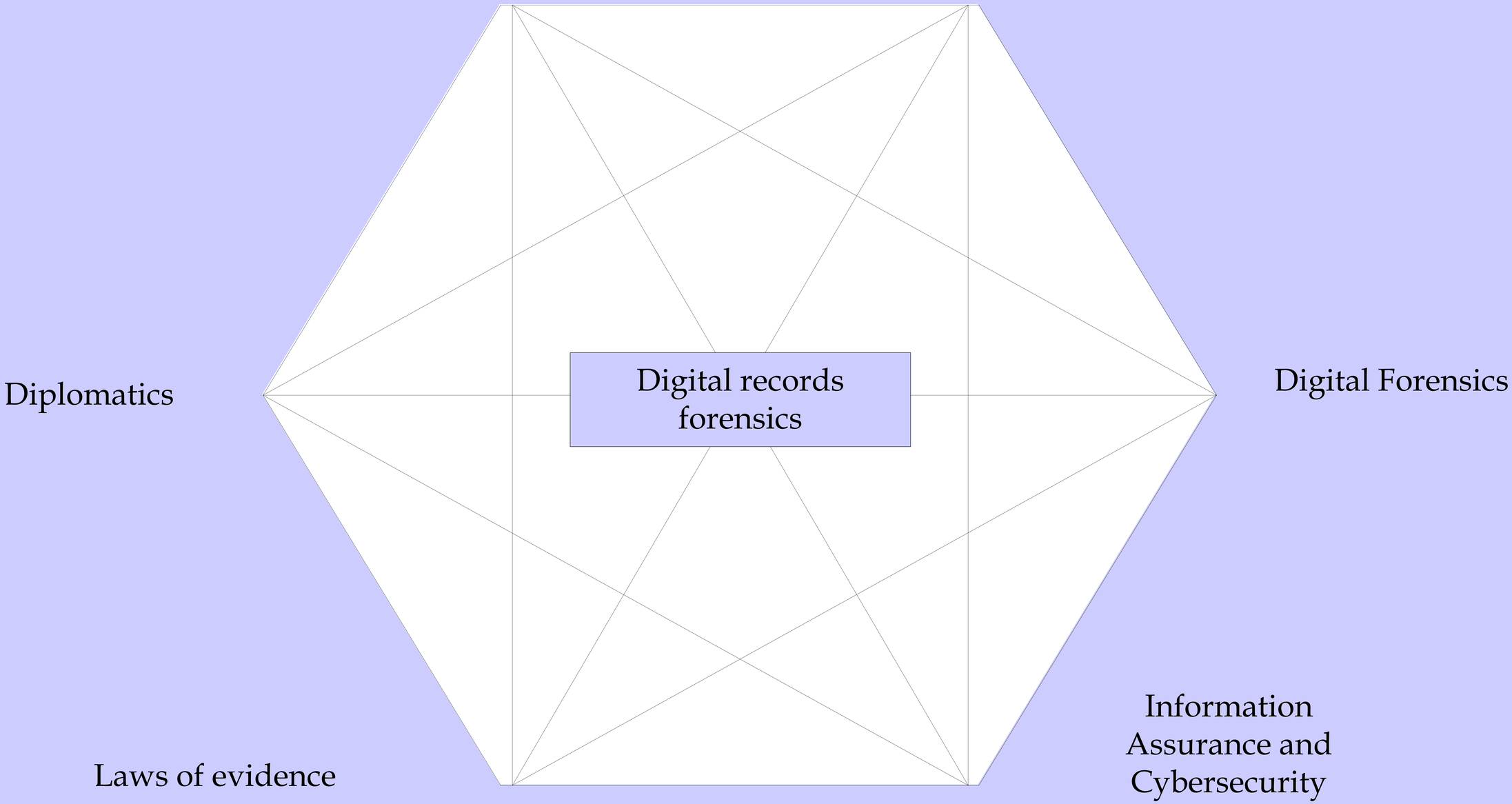
- Archivists need digital forensics knowledge for:
  - Understanding of integrity
  - Processes of access, identification and acquisition

Information Assurance and Archival Underlying Principles

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

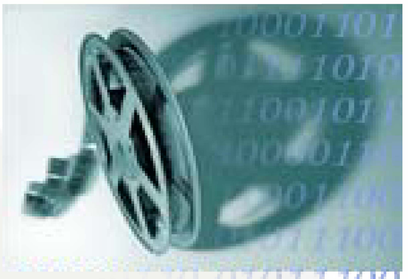



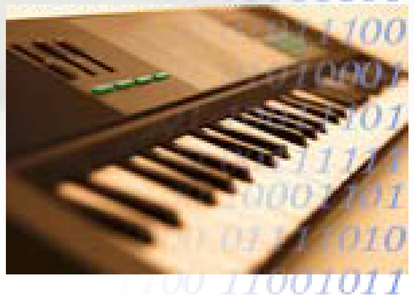
Digital Records Forensics



Seventh Annual IFIP WG 11.9 International. Conference on Digital Forensics
1 Feb 2011, Orlando, FL, USA

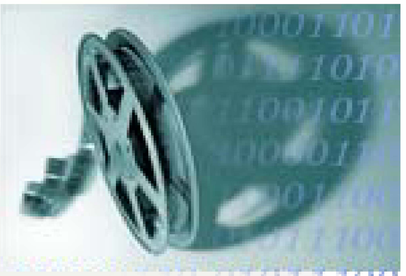
Digital Records Forensics Science BOK

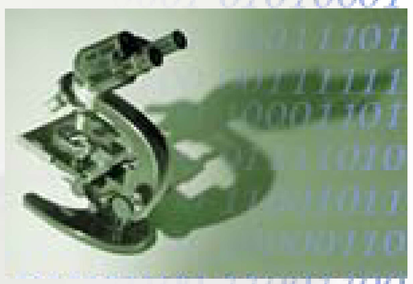




- The Law of Evidence
- Diplomatics (specifically Digital Diplomatics)
- Digital Forensics
- Archival Science
- Information Technology
- Organizational Information Assurance

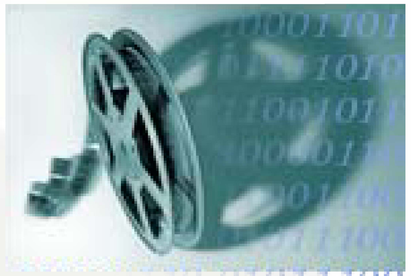
New Professional Master's Degree

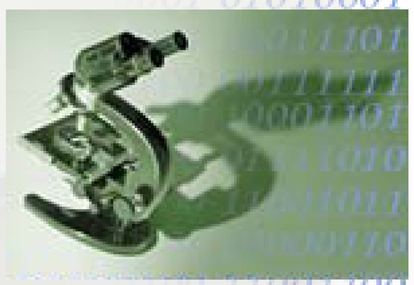




- Integration of
  - UW MSIM/IA and
  - UBC MS Archival Science
- Professionals educated in core theoretical and methodological knowledge that identifies their profession
- Learn international standards as well as specific, local and unique aspects of the local juridical-administrative environment in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

The DRF Project (2008-2011)



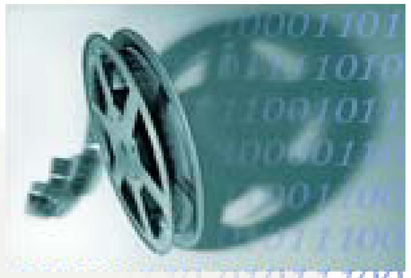


- Collaboration among:

  - UBC Archival Studies programs, School of Library, Archival & Information Studies
  - UBC Law of Evidence Department, Faculty of Law
  - UW Information Assurance and Cybersecurity program, Information School
  - Computer Forensics Division, Vancouver Police Dept.

http://www.digitalrecordsforensics.org/

Questions?



Contact Information

- Luciana Duranti
  luciana@interchange.ubc.ca
- Adam Jansen
  adam@dkives.com
- Barbara Endicott-Popovsky
  endicott@uw.edu
- Fred Cohen
  fc@all.net