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.

Research Methods & Products:
- Interdisciplinary literature review - law, digital forensics, archival diplomatics
- analysis of North American case law
- interviews & questionnaires
- archival diplomatics database
- digital records forensics activity model
- white papers
- educational curricula

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

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

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

Vancouver Police Department Case Study
- VPD is “ahead of the curve”;
- Implementing a Storage Area Network (SAN);
- At the moment of seizure, the investigator assumes role of trusted custodian;
- There is reliance on VPD’s EDRMS to make explicit all links between records.

Preliminary Interview Data

<table>
<thead>
<tr>
<th>Researcher</th>
<th>Concept of digital record</th>
<th>Establishment of authenticity</th>
<th>Maintenance of authenticity over time</th>
<th>Challenges to authenticity &amp; preservation</th>
<th>Challenges to digital records as evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archivists</td>
<td>Established definition based on theory &amp; practice</td>
<td>Specific requirements - identity &amp; integrity</td>
<td>Critical - trusted custodian</td>
<td>Circumstances of creation; tampering; obfuscation</td>
<td>Archival theory addresses evidentiary capacity</td>
</tr>
<tr>
<td>Information managers (law enforcement)</td>
<td>Anything on a computer; context-dependent</td>
<td>Chained to custody</td>
<td>Chain of command</td>
<td>Cross-platform/ multi-environment foreclosure, integrated units; migration</td>
<td></td>
</tr>
<tr>
<td>Lawyers</td>
<td>Anything on digital media; context-dependent</td>
<td>Content, proper forensics process; source</td>
<td>Not an issue; interviews to date</td>
<td>Proven process; multi-user systems</td>
<td>Unreferenced; clustered; forensic process</td>
</tr>
<tr>
<td>Judges</td>
<td>Any record on a computer</td>
<td>Authentication</td>
<td>Not a concern; interviews to date</td>
<td>Proof of reliability; proof of reliability; chain of custody; alterations; completeness</td>
<td></td>
</tr>
</tbody>
</table>

Forensics experts
- Anything created electronically; hash values; digital signatures; trusted third parties
- Proof of reliability; proof of reliability; chain of custody; alterations; completeness

Police investigators
- Archival definition (adversarial value); chain of custody | Preservation; source | Chain of custody | Obfuscation; corruption; interdependency | Show chain of custody