



The Return of Diplomats As A Forensic Discipline

Luciana Duranti

Director, InterPARES & DRF Projects

Naples, 1 October 2011



Digital Records Forensics Project

The Use of Diplomatics

Diplomatics came about as a methodology for establishing the authenticity of records attesting to patrimonial rights

It developed as a study of the nature, genesis, formal characteristics, structure, transmission and legal consequences of records for the purpose of understanding their true nature and meaning

Diplomatics' interpretation of authenticity based on form (its extrinsic and intrinsic elements) and transmission is the foundation of the law of evidence and perfectly consistent with the legal principles we know today

However, diplomatists as a profession have increasingly used their knowledge to support purposes related to historical research turning away from the “bella diplomatica” that made them so popular a few centuries ago

Digital Records Forensics Project

Back to the Future

Record keepers are increasingly called to ensure the protection of the identity and integrity of digital records through time and attesting to it while **archivists** are called to acquire records, often from obsolete systems or portable media, without altering them in the process

Digital forensic experts are called to

- attest to the integrity of digital systems
- provide quality assurance for digital systems that produce, contain or preserve records,
- assess whether fraudulent disposal has occurred
- ensure that e-discovery requirements are fulfilled

They all need to be educated in diplomatics, but diplomatists need to go back to the forensic origins of their discipline and start using their knowledge to assess, maintain and attest authenticity

Digital Records Forensics Project

A Need for Interdisciplinary Growth

- Digital technology has separated the content and structure of documents from their form (content, form and composition data are linked but not inextricably)
- Manifested and stored versions of the same record cohesist
- Interactive records may not have a stable manifestation
- Evidence of transmission is no longer linked to the document but contained in systems logs
- Authenticity can no longer be determined on the document, which is composite and permanently new, but must be an inference drawn from the digital environment.
- For this we need help from Digital Forensics

Digital Records Forensics Project

Digital Forensics

Digital Forensics is defined as “the use of scientifically derived and proven methods toward the collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events, or helping to anticipate unauthorized or inappropriate actions”

Its methods are based on conceptual assumptions about records, trustworthiness, and recordkeeping

Digital Records Forensics Project

What Knowledge We Should Share

Digital forensic experts need our knowledge on

- Concepts of Archival Document (or Record) and Recordkeeping
- Concept of Trustworthiness

We need digital forensic experts' knowledge on

- Types of integrity
- Processes of access, reproduction, identification and extraction

Today I will focus on Trustworthiness and Integrity

Digital Records Forensics Project

Records Trustworthiness: Our View

In classic diplomatics, trustworthiness was all wrapped up in the concept of authenticity so that an authentic document was also reliable and accurate. This is no longer true

Reliability: The trustworthiness of a record as a statement of fact, must be *based on* the competence of its author, its completeness, and the controls on its creation

Accuracy: The correctness and precision of a record's content, must be *based on* the above, and on the controls on content recording and transmission

Authenticity: The trustworthiness of a record that is what it purports to be, untampered with and uncorrupted, must be *based on its* identity and integrity, and on the reliability of the records system in which it resides

Digital Records Forensics Project

Authenticity: Our View

Identity: The whole of the attributes of a record that characterize it as unique, and that distinguish it from other records (e.g. date, author, addressee, subject, identifier).

Integrity: A record has integrity if the message it is meant to communicate in order to achieve its purpose is unaltered (e.g. text and form fidelity, absence of technical changes).

Context: The administrative-juridical, provenancial, procedural, documentary and technological environment in which the record was created and used overtime

Digital Records Forensics Project

Digital Forensics View: Linked to Type of Documents

- **Computer Stored Documents:** Contain human statements; if created in the course of business, they are records; e.g. e-mail messages, word processing documents, etc. Used as **Substantive Evidence**
- **Computer Generated Documents:** Do not contain human statements, but are the output of a computer program designed to process input following a defined algorithm; e.g. server log-in records from Internet service providers, ATM records. Used as **Demonstrative Evidence**
- **Computer Stored & Generated:** A combination of the two: e.g. a spreadsheet record that has received human input followed by computer processing (the mathematical operations of the spreadsheet program). Used both or either way.

Digital Records Forensics Project

Records Trustworthiness: Digital Forensics View. Reliability

Reliability: the trustworthiness of a record as to its *source*, defined in digital forensics in a way that points to either a reliable person (for computer stored documents) or a reliable software (for computer generated documents), or both.

The software should be open source, because the processes of records creation and maintenance can be authenticated either

- by describing a process or system used to produce a result or
- by showing that the process or system produces an accurate result

Digital Records Forensics Project

Records Trustworthiness: Digital Forensics View: Accuracy

A component of authenticity and, specifically, integrity. Digital entities are guaranteed accurate if they are repeatable.

Repeatability, which is one of the fundamental precepts of digital forensics practice, is supported by the documentation of each and every action carried out on the evidence.

Open source software is again the best choice for assessing accuracy, especially when conversion or migration occurs, because it allows for a practical demonstration that nothing could be altered, lost, planted, or destroyed in the process

Digital Records Forensics Project



Records Trustworthiness: Digital Forensics View: 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. Again, the term “source” is used to refer to either a person (physical or juridical), a system, software, or a piece of hardware.

Like in diplomatics, authenticity implies integrity, but the opposite is not true, that is, integrity does not imply authenticity (as identity must also be certain).

Digital Records Forensics Project



Integrity: Our View

The quality of being complete and unaltered in all **essential** respects. We were never fussy about it. What if a letter had holes, or was burned on the side or the ink passed through?

The same for all documents, records, copies, records systems

As long as it was good enough...but how good is good enough in the digital environment?

Digital Records Forensics Project



Integrity

Digital Forensics View

Data integrity: the fact that data are not modified either intentionally or accidentally “without proper authorization.”

Based on **Bitwise Integrity**

Digital Records Forensics Project



Integrity

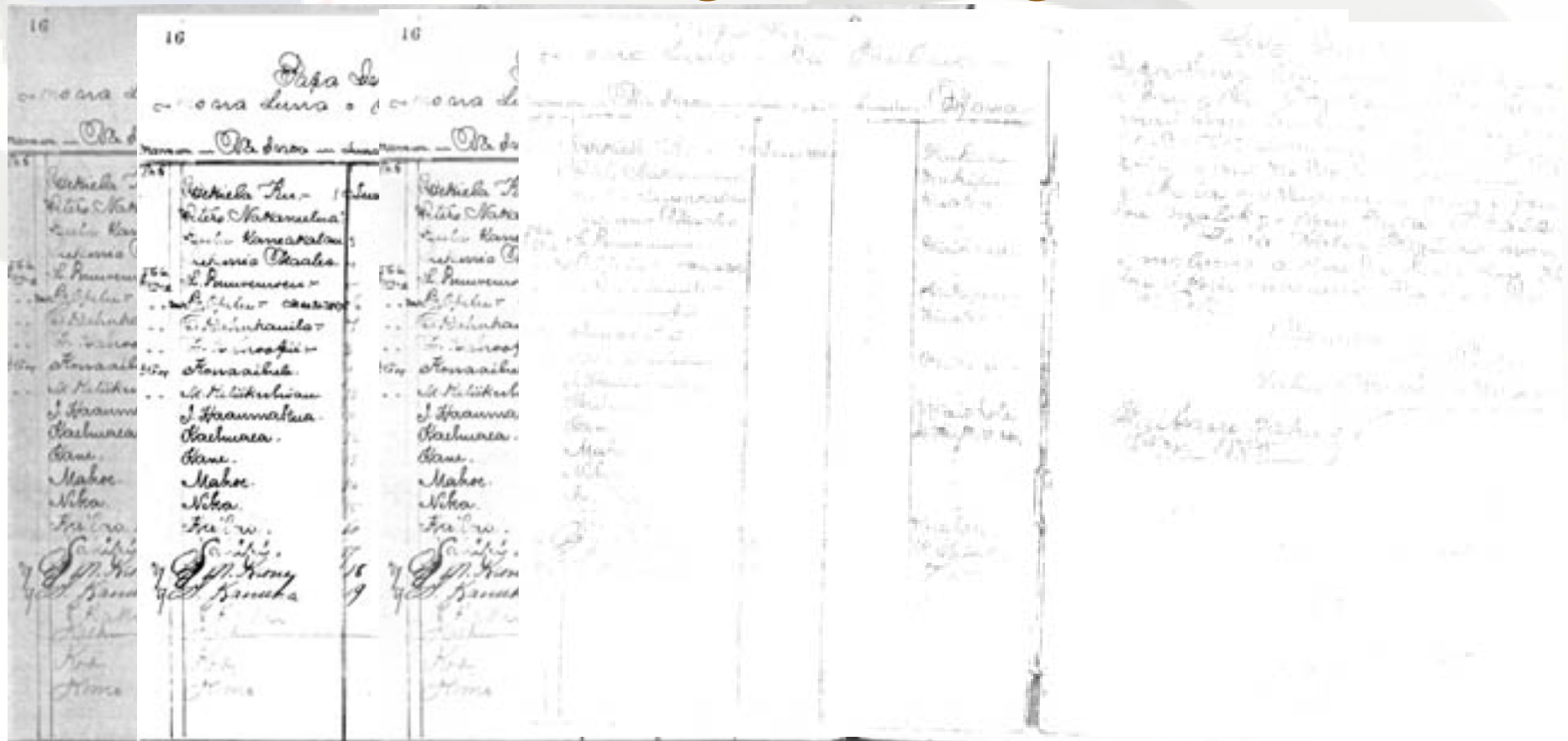
Digital Forensics View (cont.)

Bitwise Integrity

- The original bits are in a complete and unaltered state from the time of capture
- Exact and same order and value of the bits
- Small change in a bit means a very different value presented on the screen or action taken in a program or database.

Digital Records Forensics Project

Loss of Fidelity: Analog vs. Digital



Digital Records Forensics Project

Loss of Fidelity (cont.)

- If Original Bits 101
- Change state to 110
- Continues to a 011

- Same bits, but
Different value

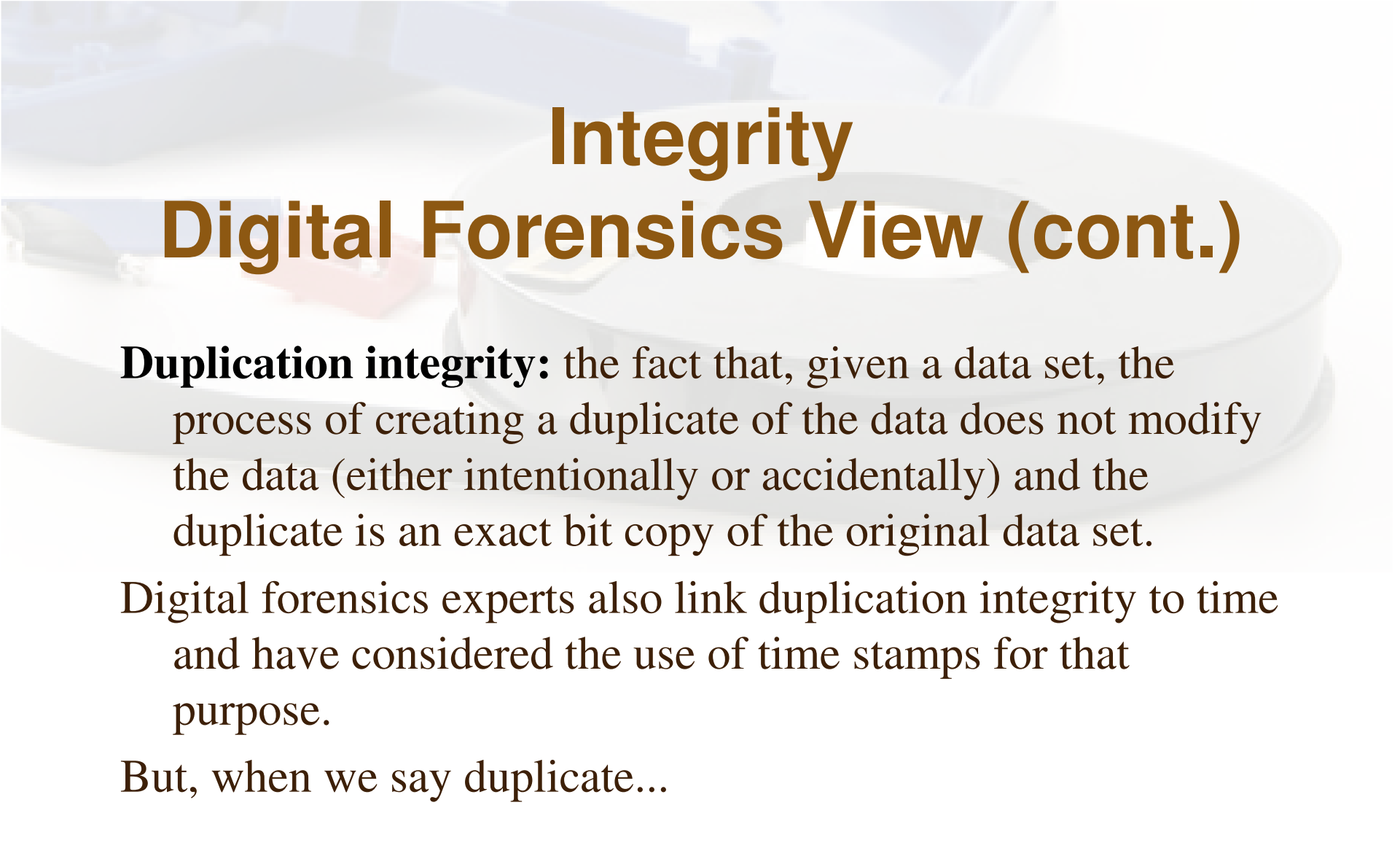
A pixelated black number 3 on a white background.

Determining Data Alteration

To determine whether a record has been altered, maliciously or otherwise we

- Cannot rely on file size, dates or other file properties
- Need audit logs and strong methods like Checksum and HASH Algorithms

Digital Records Forensics Project



Integrity

Digital Forensics View (cont.)

Duplication integrity: the fact that, given a data set, the process of creating a duplicate of the data does not modify the data (either intentionally or accidentally) and the duplicate is an exact bit copy of the original data set.

Digital forensics experts also link duplication integrity to time and have considered the use of time stamps for that purpose.

But, when we say duplicate...



Digital Records Forensics Project

Diplomatic Concept: Copy

Copy: selective duplicate of files

- You can only copy what you can see
- Rarely includes confirmation of completeness
- Moved as individual files
- Provides incomplete picture of the digital device

Digital Records Forensics Project



Forensic Duplicate: Disk Image

Image: a bit by bit reproduction of the storage medium.

A full disk copy of the data on a storage device – regardless of operating system or storage technology -- made prior to performing any forensic analysis of the disk.

Creating a disk image is important in forensics to:

- ensure that disk information is not inadvertently changed.
- reproduce forensic test results on the original evidence.
- capture information normally invisible to the operating system when in use (including deleted files)

Digital Records Forensics Project



Integrity

Digital Forensics View (cont.)

Computer integrity: the computer process produces accurate results when used and operated properly and it was so employed when the evidence was generated.

System Integrity: a system would perform its intended function in an unimpaired manner, free from unauthorized manipulation whether intentional or accidental

Both imply **hardware and software integrity**

Digital Records Forensics Project

Computer or System Integrity

Inferred from:

- Sufficient security measures to prevent unauthorized or untracked access to the computers, networks, devices, or storage.
- Stable physical devices that will maintain the value they were given is maintained until authorized to change.
 - Users/permissions
 - Passwords
 - Firewalls
 - **Logs**

Digital Records Forensics Project

System Logs and Auditing

Sets of files *automatically* created to track the actions taken, services run, or files accessed or modified, at what time, by whom and from where

- Web logs (Client IP Address, Request Date/Time, Page Requested, HTTP Code, Bytes Sent, Browser Type, etc.)
- Access logs (User account ID, User IP address, File Descriptor, Actions taken upon record, Unbind record, Closed connection)
- Transaction logs (History of actions taken on a system to ensure Atomicity, Consistency, Isolation, Durability; Sequence number; Link to previous log; Transaction ID; Type; Updates, commits, aborts, completes)

Digital Records Forensics Project

Auditing Logs

- Increasing **required by law to demonstrate integrity of the system**
- Properly configured, restricted, provide checks and balances
- Ability to determine effective security policies
- Ability to trap errors that occur
- Provide instantaneous notification of events
- Monitor many systems and devices through ‘dashboards’
- Allow to determine accountability of people
- Provide the necessary snapshot for post-event reconstruction (‘black-box’)
- Answer Who-What-Where-When, but only if retained for sufficient time (space vs. money vs. risk vs. knowledge)

Digital Records Forensics Project

Assessment of Computer/System Integrity

The assessment is based on **repeatability, verifiability, objectivity** and **transparency**

An **inference** of system integrity can be made based on the facts that:

- the theory, procedure or process on which the system design is based has been tested or cannot be tampered with
- it has been subjected to peer review or publication (standard)
- its known or potential error rate is acceptable
- it is generally accepted within the relevant scientific community

Digital Records Forensics Project

Process Integrity

Process Integrity: Formalized legal requirements for the collection, recovery, interpretation and presentation of digital evidence.

Principle of non-interference: the method used to gather and analyse [or acquire and preserve] digital data or records does not change the digital entities

Principle of identifiable interference: if the method used does alter the entities, the changes are identifiable

These principles, which embody the ethical and professional stance of digital forensics experts, are consistent with our traditional impartial stance

Digital Records Forensics Project

Authentication: Our View

A means of declaring the authenticity of a record at one particular moment in time -- possibly without regard to other evidence of identity and integrity.

Example: the **digital signature**. Functionally equivalent seals (not signatures): verifies origin (identity); certifies intactness (integrity); makes record indisputable and incontestable (non-repudiation)

But, seals are associated with a person; digital signatures are associated with a person and a record

Digital Records Forensics Project



Authentication: The Digital Forensics View

Proof of authenticity provided by showing that *the computer process or system produces accurate results when used and operated properly and that it was so employed when the evidence was generated.*

The strength of circumstantial digital evidence could be increased by metadata which records (1) the exact dates and times of any messages sent or received, (2) which computer(s) actually created them, and (3) which computer(s) received them.



Digital Records Forensics Project

Other Forensic Means of Authentication

A **chain of legitimate custody** is ground for inferring authenticity and authenticate a record.

Digital chain of custody: the information preserved about the record and its changes that shows specific data was in a particular state at a given date and time.

A declaration made by an expert who bases it on the **trustworthiness of the recordkeeping system** and of the procedures controlling it (quality assurance).

Digital Records Forensics Project

Why should you care?

The documentary world is becoming completely digital. It is vital to governments, businesses, citizens, the courts, and the scholars of the future to be able to trust the documentary by-product of activities conducted in the digital environment

Classic diplomatics theoretical core is the foundation of its subsequent development as a methodology of analysis in the digital environment, but both theory and methodology need to be integrated with other knowledge and be further developed to be able to meet the digital challenge

If not you, who can do it?

If not now, when?

Digital Records Forensics Project



www.digitalrecordsforensics.org

Director, Luciana Duranti
luciana.duranti@ubc.ca



Digital Records Forensics Project