



Digital Records Forensics Project

Conservare il digitale che non controlliamo

Luciana Duranti, University of British
Columbia

Digital Records Forensics Project

La regole fondamentali della conservazione digitale:

- La conservazione è un **processo continuo** che comincia con la produzione dei documenti
- Deve essere basata sul concetto di **sistema affidabile di gestione e tenuta dei documenti** e sul ruolo dell'archivista come **custode designato di fiducia**
- Deve incorporare la **selezione** pianificata dei documenti e la loro **descrizione, monitoraggio e autenticazione**
- Deve prevedere un **piano di conversione** sistematica e la **documentazione delle modifiche** determinate ²

Digital Records Forensics Project

Questa **Catena Ininterrotta di Conservazione** (vedi InterPARES COP model) è possibile — almeno in teoria — per i documenti digitali di istituti e enti pubblici e privati per cui esiste un'entità archivio designata esterna (ministero, tribunale) o interna (università, banca).

Come conservare i documenti digitali per cui non esiste un archivio storico designato?

Parliamo di archivi di persone, famiglie, studi (architetti, avvocati, dentisti), ditte, ecc.

Digital Records Forensics Project

Due possibili situazioni:

1. La sovrintendenza o l'archivio storico puo' intervenire quando i documenti sono ancora correnti e
 1. il produttore desidera collaborazione
 2. Il produttore accetta consigli senza interferenza
2. La sovrintendenza o l'archivio storico si trova di fronte a documenti non correnti, spesso su supporti esterni al sistema in cui sono stati prodotti

Digital Records Forensics Project

Situazione 1.1– Si stabilisce un rapporto di collaborazione che si sviluppa nelle fasi seguenti:

a) Si crea una infrastruttura

- stabilire la portata e gli obiettivi
- acquisire risorse
- focus sui documenti digitali
- dare consiglio su tecnologia e formati
- fornire esempi
- sviluppare policies e procedure, assegnare responsabilità
- sviluppare strategie di mantenimento

Digital Records Forensics Project



b) Si valutano i documenti archivistici

- Identificare i documenti tra gli oggetti digitali prodotti
- Identificare co-autori e proprietari multipli
- Determinare l'autenticità e documentarla
- Determinare problemi di privacy
- Monitorare i documenti da conservare
- Identificare tutte le componenti digitali
- Determinare la fattibilità della conservazione
- Sviluppare un piano di versamento

Digital Records Forensics Project

c) Versamento

- Migrare i documenti all'ambiente tecnologico dell'archivio
- Conservare il formato logico più vecchio ancora disponibile
- Evitare l'acquisizione di duplicati
- Documentare ogni attività a cui i documenti sono sottoposti

Digital Records Forensics Project

Situazione 1.2 - Il produttore accetta consigli senza interferenza

Si preparano linee guida chiare e comprensibili

- Un opuscolo generale
 - Come scegliere software e formati (standards)
 - Come organizzare i documenti
 - Come mantenere i documenti accessibili nel tempo (back-ups, system upgrade, conversione, dispersione)
 - Come prevenire la perdita di documenti

Cont.

Digital Records Forensics Project

- Un opuscolo specifico sulla gestione e tenuta dell'e-mail
 - Come organizzarla, anche in relazione ad altri documenti
 - Come trattare gli attachments
 - Come trattare i threads
 - Come conservarla in altri formati
 - Come selezionarla
- Un opuscolo su come donare i propri documenti digitali
 - Perchè donare, cosa donare, come, quando
 - Considerazioni sui diritti intellettuali, di privacy, sicurezza, accesso
 - Lista di persone/enti a cui rivolgersi per consigli e aiuto
- Lezioni e workshops su come proteggere le proprie foto, ecc.

Digital Records Forensics Project

Situazione 2. - Siamo di fronte a oggetti digitali non correnti, spesso su supporti esterni al sistema in cui sono stati prodotti

Regole da seguire:

- Si crea una copia o un'immagine (non sono la stessa cosa)
- Si analizza la copia o l'immagine e si determina se gli oggetti digitali sono documenti
- Se sono documenti, si determina la loro autenticità

Digital Records Forensics Project

Perchè è importante sapere quali sono documenti?

- Caso del British Columbia Rail: problema relativo alla conservazione di documenti archivistici. Il ministro liberale Ralph Sultan chiese “Qual’è la definizione di documento archivistico?” facendo riferimento alla controversia sull’e-mail (Vancouver Sun, January 29, 2010).
- La Corte Suprema del Canada sta ascoltando un caso di diffamazione basato sulla questione se hyperlinks in un testo costituiscano la ripetizione di un’affermazione diffamatoria (Vancouver Sun, April 2, 2010).
- Uso di banche dati, GIS, sistemi di registrazione

Digital Records Forensics Project

Materiali che ci potrebbero essere offerti:

Documenti generati da word processing
E-mail con word processing attachments
Foto, video e registrazioni musicali
Agende o calendari
Web portals, blogs & wikis
Registrazioni di videoconferenze &
webcasting
Databases
Flash drives & altre storage devices con
contenuti vari
Remote PDAs, Blackberrys, etc. etc. etc.

Digital Records Forensics Project

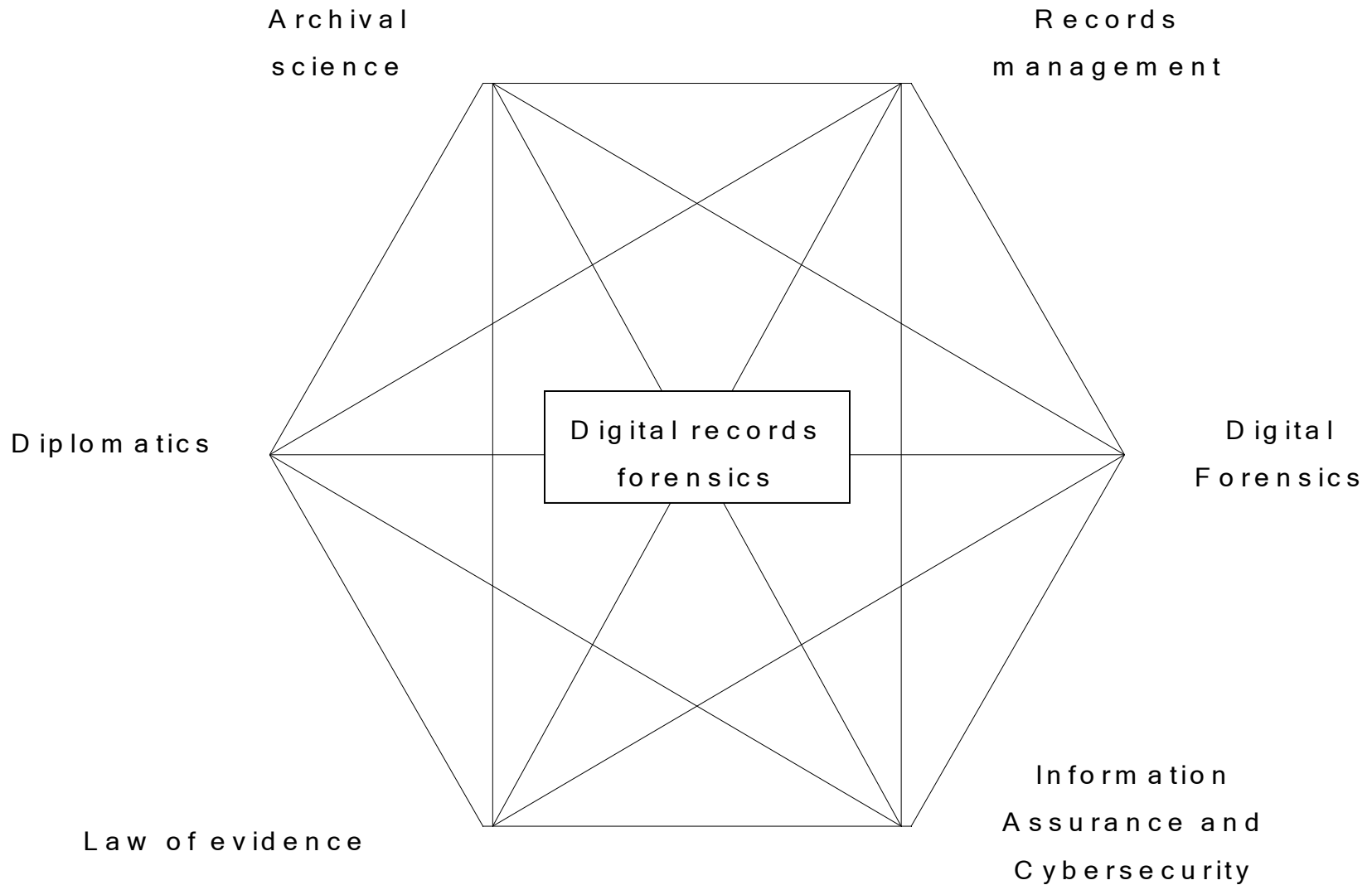
Quali conoscenze ci possono guidare?

Diplomatica Digitale: lo sviluppo e l'applicazione della diplomatica classica ai documenti digitali

Digital Forensics: l'uso di metodi scientifici per l'acquisizione, la validazione, l'identificazione, l'analisi, l'interpretazione, la documentazione e la presentazione di fonti digitali di prova allo scopo di facilitare la ricostruzione di eventi criminali o anticipare atti non autorizzati che possono danneggiare operazioni pianificate

In particolare, abbiamo bisogno di conoscenze interdisciplinari che, una volta integrate, potrebbero essere definite **“Digital Records Forensics”**.

Digital Records Forensics



Digital Records Forensics Project

Contributi della diplomatica

- Concetto di documento digitale
- Concetti di affidabilità, accuratezza, autenticità e autenticazione

Contributi di digital forensics:

- Processo affidabile di estrazione o riproduzione
- Principi di non-interferenza e interferenza identificabile
- Categorizzazione dei documenti digitali
- Distinzione tra integrità di documenti e di riproduzioni
- Regole per la determinazione dell'integrità di sistemi
- Principi per determinare autenticità
- Basi per l'autenticazione

Digital Records Forensics Project

Processo affidabile di estrazione e acquisizione

1. Produzione della copia delle entità logiche o dell'immagine dell'hard drive o supporto esterno
2. Identificazione degli oggetti di interesse potenziale
3. Analisi degli oggetti identificati
4. Valutazione e interpretazione dei risultati
5. Presentazione dei risultati in un rapporto che descrive in dettaglio le caratteristiche degli oggetti, l'interpretazione dei fatti e le opinioni di esperti
6. La revisione tecnica e amministrativa da parte di un soggetto neutrale

Digital Records Forensics Project

Principi di non-interferenza e interferenza identificabile:

Non-interferenza: il metodo usato per fare estrazione, upgrade, conversion o migration non cambia il contenuto e la forma documentaria del documento nativo

Interferenza identificabile: il metodo usato per fare estrazione, upgrade, conversion o migration altera il documento nativo ma i cambiamenti sono identificabili

Questi principi, che incorporano la posizione etica e professionale dell'archivista, caratterizzano anche il suo ruolo istituzionale di custode affidabile che esercita il controllo sul sistema di produzione e gestione dei documenti

Digital Records Forensics Project

Categorizzazione dei documenti digitali:

1. Documenti prodotti e tenuti in un computer
2. Documenti prodotti da un computer
3. Documenti prodotti da una persona fisica e un computer
4. Oggetti dinamici: nell'Internet

I primi sono esaminati e valutati come documenti
archivistici (business records)

I secondi sono esaminati e valutati come ogni prova
materiale

I terzi e i quarti devono passare entrambi i test

Digital Records Forensics Project

Distinzione tra integrità di documenti, di riproduzioni, di sistemi

Integrità dei documenti: il fatto che non siano modificati intenzionalmente o involontariamente senza l'autorizzazione necessaria

Integrità della riproduzione: il fatto che la produzione di un duplicato non modifichi il documento e che il duplicato sia una copia formalmente esatta del documento riprodotto. Per questo motivo è importante che la riproduzione sia connessa a dati temporali.

Cont.

Digital Records Forensics Project

Regole per la determinazione dell'integrità di sistemi (Daubert Rules):

La teoria, la procedura o il processo per produrre o gestire e mantenere il documento

- Devono essere stati testati e non possono essere stati manomessi
- Devono essere stati sottoposti alla valutazione di esperti e/o sono risultati in pubblicazione (e.g. standards)
- Devono essere generalmente accettati dalla comunità scientifica competente, e
- la ratio di errore conosciuta o potenziale che offrono deve essere accettabile

Digital Records Forensics Project

- Gli attributi di tale sistema sono **ripetibilità delle operazioni, verificabilità, oggettività e trasparenza**, che richiedono la documentazione accurata di qualunque operazione sul sistema e all'interno del sistema.
- **Open source software** è la scelta migliore per valutare integrità, specialmente in caso di estrazione, upgrade, conversione e migrazione, perchè permette la dimostrazione pratica che niente puo' essere alterato, perso, piantato o distrutto volontariamente o inavvertitamente

Digital Records Forensics Project

Principi per determinare autenticità

- **Autenticità** è la certezza dell'identità della fonte, persona o sistema. Autenticità implica integrità ma non viceversa.
- Autenticità si può basare sulla dichiarazione di un esperto che il sistema di gestione e tenuta dei documenti e le procedure che lo controllano sono affidabili, sulla base di
 1. uno schema di metadati di identità e integrità
 2. uno schema di classificazione (titolario)
 3. regole di selezione e scarto connesse al titolare
 4. un sistema di registrazione di protocollo
 5. un sistema di reperimento
 6. privilegi di accesso a documenti archiviati

Digital Records Forensics Project

Basi per l'autenticazione

- La firma digitale è uno strumento valido per garantire l'autenticità dei documenti attraverso lo **spazio... .. ma non nel tempo!**
- I sistemi giuridici nordamericani non la considerano il miglior metodo di autenticazione
- La firma digitale è soggetta a obsolescenza e quindi complica il problema della conservazione digitale
- Il metodo prevalente di autenticazione è **una catena di custodia legittima** in sistemi che passino i test di **ripetibilità, verificabilità, oggettività e trasparenza.**

Digital Records Forensics Project

Methodology of the Research

- Literature review
- Digital Records Forensics Activity Model
- Case Law Database
- Terminology Database
- Questionnaires and Interviews
- Ethnographic study with the Vancouver Police Department

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