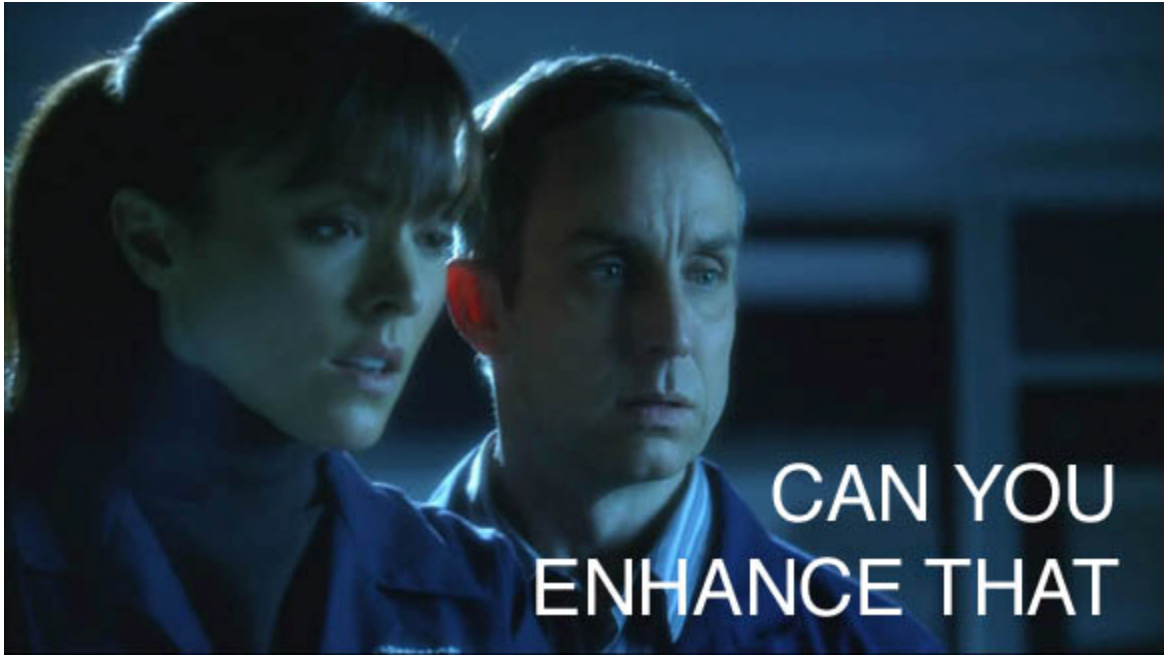


Enhance! Digital Forensics in the Library

Natalya Rattan & Steve Marks

January 29, 2015 - OLA Super Conference

What is digital forensics?

Digital forensics

From Wikipedia, the free encyclopedia

Digital forensics (sometimes known as **digital forensic science**) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.[1][2] The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.[1] With roots in the personal computing revolution of the late 1970s and early '80s, the discipline evolved in a haphazard manner during the 1990s, and it was not until the early 21st century that national policies emerged.

Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil (as part of the electronic discovery process) courts. Forensics may also feature in the private sector; such as during internal corporate investigations or intrusion investigation (a specialist probe into the nature and extent of an unauthorized network intrusion).

The technical aspect of an investigation is divided into several sub-branches, relating to the type of digital devices involved; computer forensics, network forensics, forensic data analysis and mobile device forensics. The typical forensic process encompasses the seizure, forensic imaging (acquisition) and analysis of digital media and the production of a report into collected evidence.

As well as identifying direct evidence of a crime, digital forensics can be used to attribute evidence to specific suspects, confirm alibis or statements, determine intent, identify sources (for example, in copyright cases), or authenticate documents.[3] Investigations are much broader in scope than other areas of forensic analysis (where the usual aim is to provide answers to a series of simpler questions) often involving complex time-lines or hypotheses.[4]

Forensic science

Physiological sciences
Forensic anthropology
Forensic dentistry
Forensic entomology
Forensic pathology
Forensic botany
Forensic biology
DNA profiling
DNA phenotyping
Bloodstain pattern analysis
Forensic chemistry

Social sciences
Forensic psychology
Forensic psychiatry

Forensic criminalistics
Ballistics
Ballistic fingerprinting
Body identification

Why is this useful in an library/archival context?

Collection risk factors:

- Media degradation
- File format obsolescence
- Post-facto integrity measurement
- Maintaining provenance

But also, access!

Thomas Fisher Rare Book Library, University of Toronto

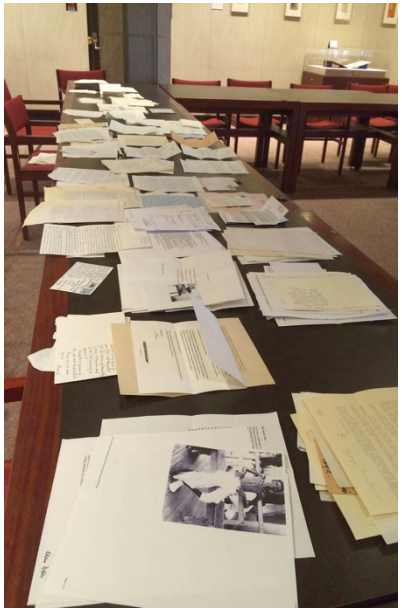
Who are we?

- Department of Rare Books and Special Collections established in 1955; moved to the Fisher Library building at 120 St. George Street in 1973
- Collection size: 733,629 volumes and 3,944 metres of manuscripts (since this statistic was recorded the collection has grown)
- Mandate: to foster the search for knowledge by supporting research and learning across all disciplines taught at the University of Toronto. The Library acquires, makes accessible and preserves comprehensive research collections of national and international significance. It serves the faculty, staff, students and alumni of the University, as well as the general public.

Manuscript Collections

- The Fisher houses over 600 manuscript collections covering a wide range of subject areas
- Includes collections of literary, historical and personal papers for individuals and organizations, with a focus on Canadiana.

Manuscript Collections



Case study: The Don Bailey Files

…until we received a donation of authors' papers that contained 160 floppy disks.

Case Study: The Don Bailey Files

- The collection belonged to **Donald (Don) Gilbert Bailey** (1942-2003), who was a novelist, poet, story writer, playwright, and television and film writer born in Toronto in 1942.
- Bailey dedicated a significant portion of his life to working closely with those in both foster care and correctional facilities.
- Bailey's work has been published in numerous magazines and literary journals. His plays have been broadcast on both CBC Radio and TV. His TV plays include *Nightfall*, *Shared Accommodation* and *All Sales Final*.
- The author of more than 15 books, Bailey won the Margaret Laurence Literary Award for Fiction for his last novel, *A Stranger to Myself*, at the Manitoba Literary and Publishing Awards in 2002.

Photograph of Don Bailey, from the Don Bailey Papers (MS Coll. 214, Box 18 - Folder 4) at the Thomas Fisher Rare Book Library, University of Toronto.

Case Study: The Don Bailey Files

We received this material from Don Bailey's son, Daniel Bailey about 10 years after his death. Adding to previous donations to the Fisher Library (or 67 boxes/8.5 metres), this accession included personal correspondence, audio-visual materials from his various productions, as well as **160 floppy disks, along with Don's old Powerbook 5300c.**

Initial attempts and the consequences

[Removed: image of letter written by Don Bailey on his Powerbook 5300c laptop to fellow writer, Jane Rule]

I have a new toy in the form of a lap-top computer. I have not mastered it so how this letter will appear is a mystery. In format I mean. the screen is quite small and I have to adjust to that. I obtained the lap-top from a guy ion the computer business. He leases, buys and sells. Two years ago I was persuaded by a film editor that what I was working with needed to up-gradeed. My ten year old machine was stone-age material. So I purchased a machine from him since he was about to upgrade again. The computer I got from him was capable of burning CD's which is really illegal as far as I am concerned. It's like someone scanning one of your novels and reproducing 50 copies on their desk top printing program. In the end I realized that this new piece of hardware offered far too many choices to someone who just wants to word process. So I put it away and went back to my old machine. But last week I saw an ad from this man who leases, buys, and sells and I called him. I told him the model that I had bought from the editor abnd explained that I would rather have a lap-top that I could take travelling with me. We met the next day and made a straight trade. So I am pleased but also having to learn the technique, and inherent mysteries of what is called a PowerBook.

Initial attempts and the consequences

Here's a what-not-to-do list for recovering floppy disk files for ***archival purposes***:

- Open floppy disks on Powerbook 5300c (it's tempting but don't do it!)
- Save file to "text" format then to Desktop (create separate folder for files)
- Once all of the files are on the desktop, insert PC floppy disk and drag desktop folder into PC floppy disk
- Insert PC floppy disk into external drive reader and from there right click on computer and open in Note ++
- Print files

What to remember when dealing with or analog/ born-digital materials

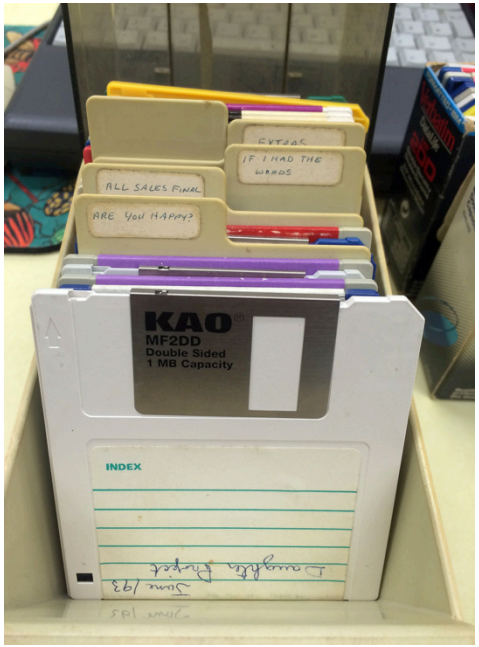
- The same archival concepts applied to textual documents, such as provenance, original order and authenticity, must be applied to born-digital materials

- The integrity of the materials must be ensured (that is, you must avoid accidentally altering the data or metadata, such as date/timestamps)

  •Electronic documents, such as drafts and correspondence, written on floppy disks and other data storage media will degrade faster than paper

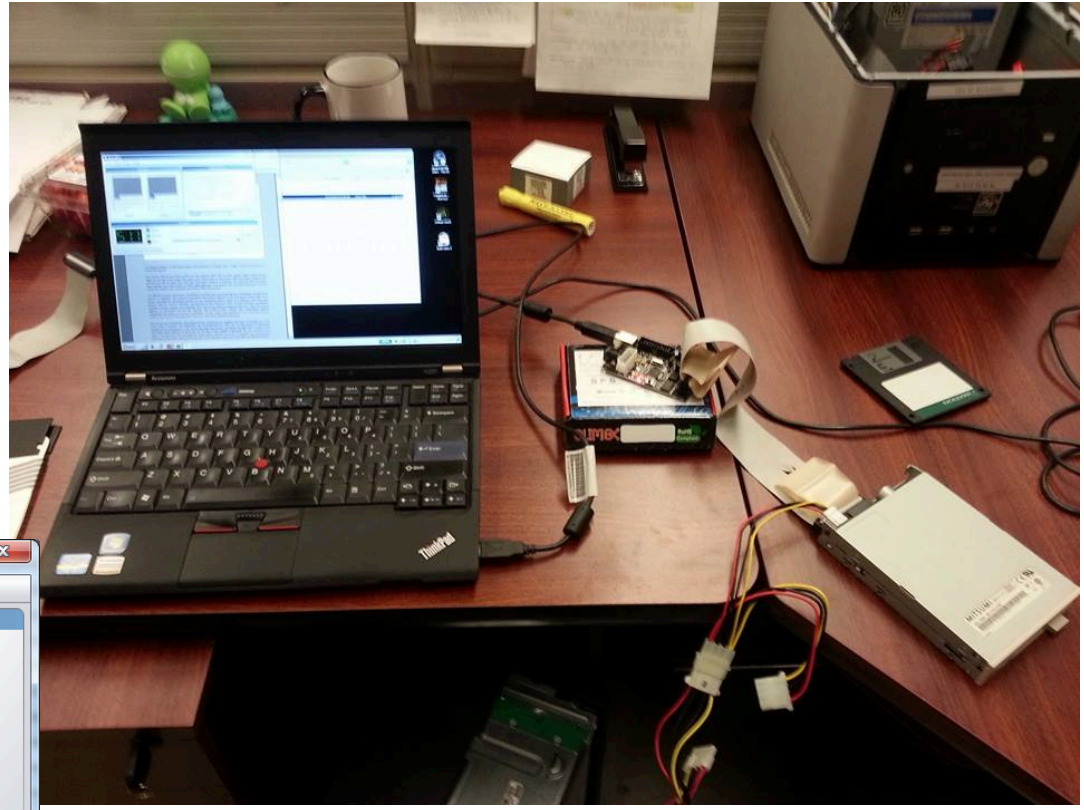
Case study: The Don Bailey Files

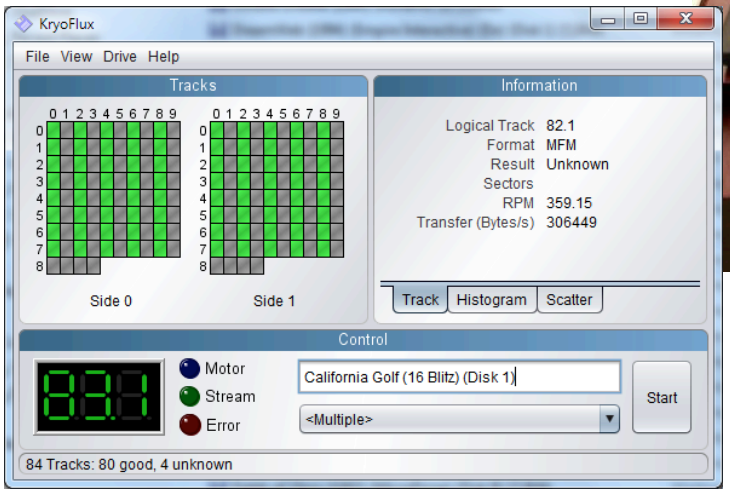
- Formatted in Macintosh File System (MFS) format[1]
- Not readable on modern machines



1: https://en.wikipedia.org/wiki/Macintosh_File_System

Case study




KryoFlux
File View Drive Help
Tracks
0 1 2 3 4 5 6 7 8 9
0 1 2 3 4 5 6 7 8
Side 0
Side 1
Information
Logical Track 82.1
Format MFM
Result Unknown
Sectors
RPM 359.15
Transfer (Bytes/s) 306449
Track
Histogram
Scatter
Control
Motor
Stream
Error
California Golf (16 Blitz) (Disk 1)
<Multiple>
Start
84 Tracks: 80 good, 4 unknown

Case study

Getting the data off

a) Total commander

i) but then there’s an issue of whether we have the right application

Case study

Emulation

Some resources

General forensics wiki: http://forensicswiki.org/wiki/Main_Page

BitCurator: http://wiki.bitcurator.net/index.php?title=Main_Page

Kryoflux:

- Official: http://forum.kryoflux.com/
- Non-official but a good intro: http://goughlui.com/2013/04/21/project-kryoflux-part-1-the-board-and-associated-hardware/

Classes!

- e.g. http://saa.archivists.org/events/digital-forensics-for-archivists-fundamentals-1643/649/

natalya.rattan@utoronto.ca

steve.marks@utoronto.ca