NIST
National Institute of Standards and Technology
U.S. Department of Commerce

FORENSICS @ NIST | #NISTForensics

Digital & Multimedia Forensics Introduction

Barbara Guttman

Information Technology Lab

What Does Digital Forensics Need?

- Tools that work well
- Admissible results
- Efficiency
- Knowledge about software

Is directed by a law enforcement steering committee

What is Happening at NIST?

- National Software Reference Library (NSRL)
  - Core, Mobile Apps, Games
  - Alternative Matchers
- Computer Forensic Tool Testing (CFTT)
  - Specs & Tests
  - Federated Testing: Do our testing in your own lab
  - Tool Catalog
- Computer Forensic Reference Dataset (CFReDS)

NSRL – Background

- Widely used in criminal, civil, corporate forensics
  - Alert/Ignore
  - Can build special sets
- Used for computer security
  - Systems management
  - NVD
- Largest publicly known repository of software
  - Cultural heritage

From http://bowtielaw.wordpress.com/Special Guest Blogger Pete Coons, D4, VP

"Can't you just DeNIST the data and get rid of all the junk files…?" This is a question I am often asked. It usually comes after an individual attends an eDiscovery conference and the magical phrase "DeNIST" was uttered at some point. The individual is led to believe, or rather wants to believe, it is a supernatural process that separates all the wheat from the chaff. Well, that's only half the story…

CFTT– Background

- Develop Specification for Forensic Functions

  Disk Imaging, Write Blocking, Forensic Disk Re-Use, Deleted File Recovery, File Carving, String Searching, Registry Analysis, Mobile Device Forensics

- Develop Test Plan and Test Material
- Perform Testing
- DHS publishes reports
- Add Functional Area to Federated Testing

Hacking Tools Get Peer Reviewed, Too

A government-led effort paves the way for data extracted from electronic devices to be accepted as evidence in court.

> In addition to setting standards for digital evidence-gathering, the reports help users decide which tool they should use, based on the electronic device they're looking at and the data they want to extract. They also help software vendors correct bugs in their products.

The Atlantic, March 20, 2017

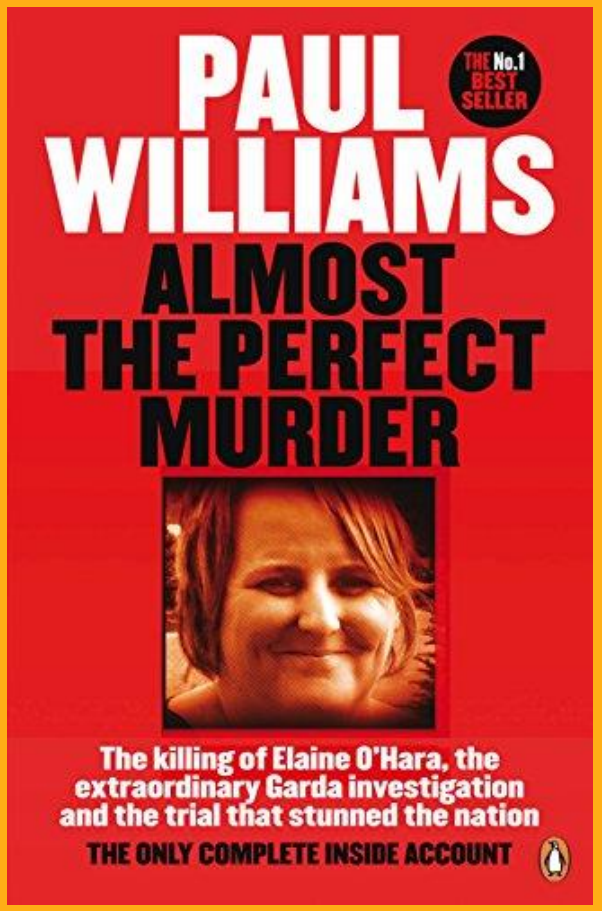
Murder of Elaine O'Hara

"…This began very late on the evening of day 16, and the judge ended testimony that day shortly before 4PM, so I had some time overnight to research the tool in question (Photorec) to see if it had been tested individually. I was absolutely delighted to find your excellent and detailed tests of the tool on NIST/CFTT.

When I came to court the next day, I was armed with both NIST reports on PHOTOREC and that avenue was rapidly closed off, and the text messages (which proved to be central in this highly circumstantial case) were admitted into evidence

Thank you so much for your excellent work, and I have asked Jim to buy you a pint on my behalf!"

Paul Durbin



Agenda

- The NSRL and Video Games – Why I get to buy video games at the Office: Austin Snelick
- Approximate Matching – Testing how well matchers work: Monika Singh
- Drone Forensics and other new additions to CFReDS: Ben Livelsberger
- Going deeper and deeper in Cell Phones: Jenise Reyes Rodriguez