UNSW SYDNEY | Australia's Global University

sec edu

security
engineering
capability

COMP6445 – Digital Forensics

Term 3 2019 - Week 3 part 1

1 October 2019

Topics for this lecture

Digital forensic concepts

1. Quick tours of historical waypoints in digital forensics
2. Different disciplines of “digital” forensics

General forensic concepts

- The adjective forensic comes from the Latin word *forensis*, meaning “in open court” or “public.”

- Forensic science (often shortened to forensics) is the application of a broad spectrum of sciences to answer questions of interest to the legal system. The study and application of science to matters of law.

Locard’s principle

- Alphonse Bertillon, a French criminal investigator, developed one of the earliest systems of documenting personal evidence on criminals in the late 19th century. Called Bertillonage, the procedure was a relatively simple way of recording physical measurements onto identification cards and then filing them in order along with photographs of the individual.

- One of the most important figures in the history of forensic science was a student of Bertillon, Edmond Locard, who would carry many of his teacher's influences with him. Locard worked as a medical examiner during World War I and was able to identify causes and locations of death by looking at stains or dirt left on soldier's uniforms. In 1910, he opened the world's first crime investigation lab in Lyons, France

- Locard also wrote a highly influential seven-volume work on forensic science, titled "Traité de criminalistique," and in it and his other works as a forensic scientist, he developed what would become known as Locard's exchange principle.
  - *Il est impossible au malfaiteur d’agir avec l’intensité que suppose l’action criminelle sans laisser des traces de son passage.*
  - *It is impossible for a criminal to act, especially considering the intensity of a crime, without leaving traces of this presence*.

- Another form: "with contact between two items, there will be an exchange and traces will be created."

Computers turn this on its head

- A “trace” is only created if a computer is designed to record and store it

- The trace is the observing computer’s interpretation of the interaction
  - Some things that are interpreted (sometimes wrongly):
    - Number format
    - Character set and language
    - Time
    - Other examples….

Waypoints in the history of computer forensics

- Earliest computer forensic efforts said to be in 1965 in US involving Bank of Minnesota
- 1976 Donn Parker's *Crime by Computer*

- 1980's and 1990's saw marked increase in activity, aligned with X.25 and Internet
  - Increase in **computer misuse** followed by investigative practices and legislation
  - 1986 is when computer offences started appearing in Australian legislation
  - 1990 Cliffiord Stoll's *The Cuckoos Egg*
  - In Australia, 1991 arrest and 1996 trial of Julian Hawkins (aka Julian Assange) saw the first concerted Australia efforts
  - Operation Long Arm in 1992 was first globally coordinated child pornography investigation (my first CP investigations)
  - 1993 saw the introduction of the SEARCH course at FLETC (hosted at FBI Academy)
  - 1995 International Organization on Computer Evidence (IOCE) founded

Waypoints in the history of computer forensics (cont)

- Budapest Treaty on Cybercrime[1] (signed 2001)
  - Digital Forensic Research Working Group established to assist with harmonizing practices. Landmark conference in 2001
  - Driver for many countries, including Australia to re-visit their legislation, including investitive procedures
  - Driver for HB 171 – *Guidelines for management of IT evidence* first published in 2003
  - Driver for national bodies such as NIST/NIJ in US e.g. US DOJ Handbook – *Examination of digital evidence* (2004)

- RFC 3227 - *Guidelines for Evidence Collection and Archiving* (2002)
- ISO 17025 - *General requirements for the competence of testing and calibration laboratories* (2005)
- NIST 800-86 - *Guide to Integrating Forensic Techniques into Incident Response* (2006)
- BSI 10008 - *Evidential weight and legal admissibility of electronic information (2008)*
- ISO 27037 - *Guidelines for identification, collection, acquisition and preservation of digital evidence* (2012 with drafting from 2008)

1. See https://www.coe.int/en/web/cybercrime/the-budapest-convention (also in readings)

Principles for dealing with digital evidence

International Organisation for Computer Evidence (IOCE)

1. When dealing with digital evidence, **all of the general forensic and procedural principles** must be applied.
2. Upon seizing digital evidence, actions taken **should not change that evidence**.
3. Where changes occur during any of the phases of the digital forensic process, **the nature, extent and reason for such changes** shall be properly documented
4. When it is necessary for a person to access original digital evidence, that person **should be trained for the purpose**.
5. All activity relating to the seizure, access, storage or transfer of digital evidence must **be fully documented, preserved and available for review**.
6. **An individual is responsible** for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.

1. The IOCE is no longer functioning. Some activities have been taken over by Scientific Working Group on Digital Evidence and others by NIST (under NIJ)

Definition of Digital Forensics and Network Forensics

Digital Forensics

The use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purposes of facilitating or furthering the reconstructions of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations.[1]

Network Forensics

The use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities[1]

1. A roadmap for Digital Forensic Research DFRWS 2001 See http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

DFRWS – Network forensic challenges

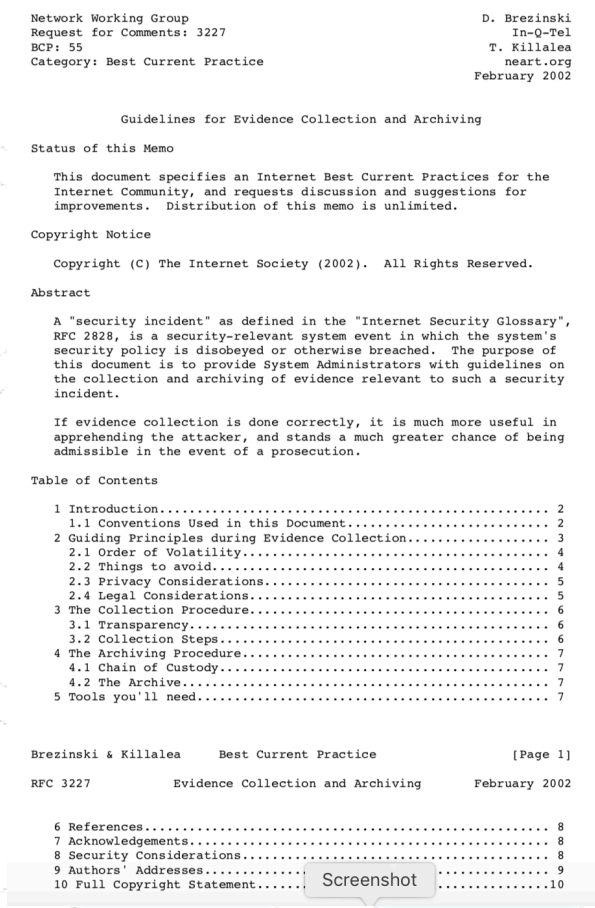
- Time
- Performance
- Complexity
  - Tools across multiple environments
  - Correlation
- Collection
  - Who, when and what
- Paradigms
  - Intelligence, network operations, law enforcement
- Collaboration
- Legal hurdle
- Emerging technologies

We are going to discuss these later

RFC 3227 - Guidelines for Evidence Collection and Archiving (2002)[1]

- Order of volatility
  1. registers, cache
  2. routing table, arp cache, process table, kernel statistics,
  3. memory
  4. temporary file systems
  5. disk
  6. remote logging and monitoring data that is relevant to the
  7. system in question
  8. physical configuration, network topology
  9. archival media

- Legal considerations
  - Admissible
  - Authentic
  - Complete
  - Reliable
  - Believable



Network Working Group
Request for Comments: 3227
BCP: 55
Category: Best Current Practice

D. Brezinski
In-Q-Tel
T. Killalea
neart.org
February 2002

Guidelines for Evidence Collection and Archiving

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

A "security incident" as defined in the "Internet Security Glossary", RFC 2828, is a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. The purpose of this document is to provide System Administrators with guidelines on the collection and archiving of evidence relevant to such a security incident.

If evidence collection is done correctly, it is much more useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution.

Table of Contents

Screenshot

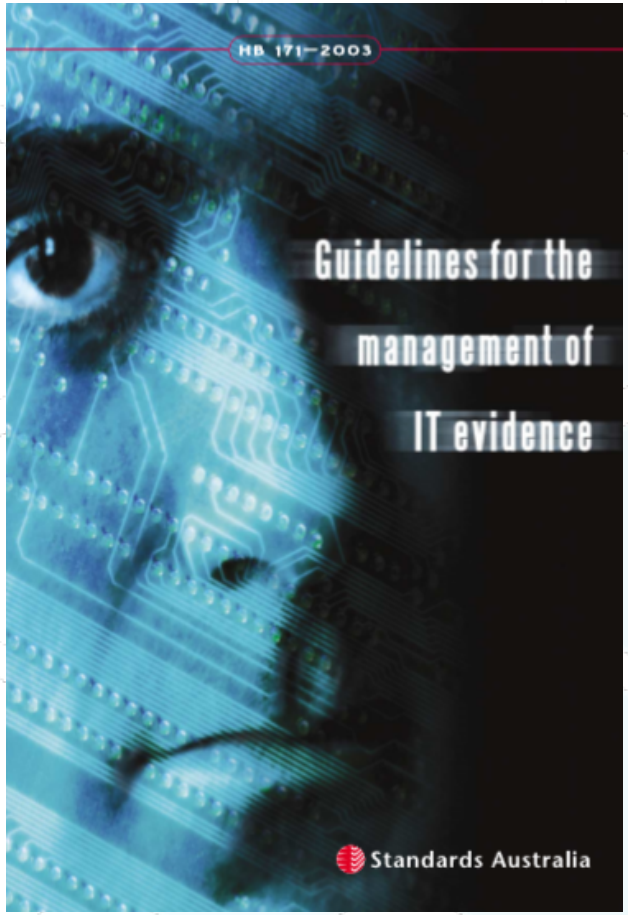
1. Available at https://www.ietf.org/rfc/rfc3227.txt (also in readings)

HB171 – Guidelines for Management of IT Evidence (2003)[1]

- Jointly sponsored by AFP and Attorney-General

- Six stages:
  1. Design for evidence
  2. Produce records
  3. Collect evidence
  4. Analyse evidence
  5. Reporting and presentation
  6. Determine evidentiary weight

- Withdrawn after 3 cycles
  - Content is now included in ISO27037, ISO2704x and ISO27050 series

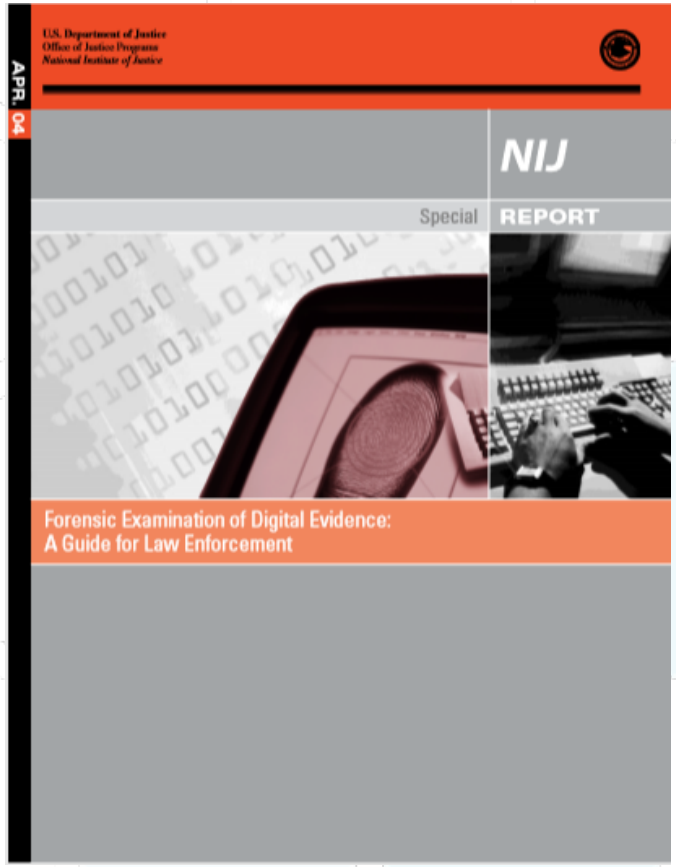


1. No longer published (handbooks are published for 10 years and then may be upgraded to standards)

Forensic Examination of Digital Evidence[1] (2004)

- US Department of Justice
  - Prosecutor's advise to practitioners
  - US-centric, but still relevant at a macro-level

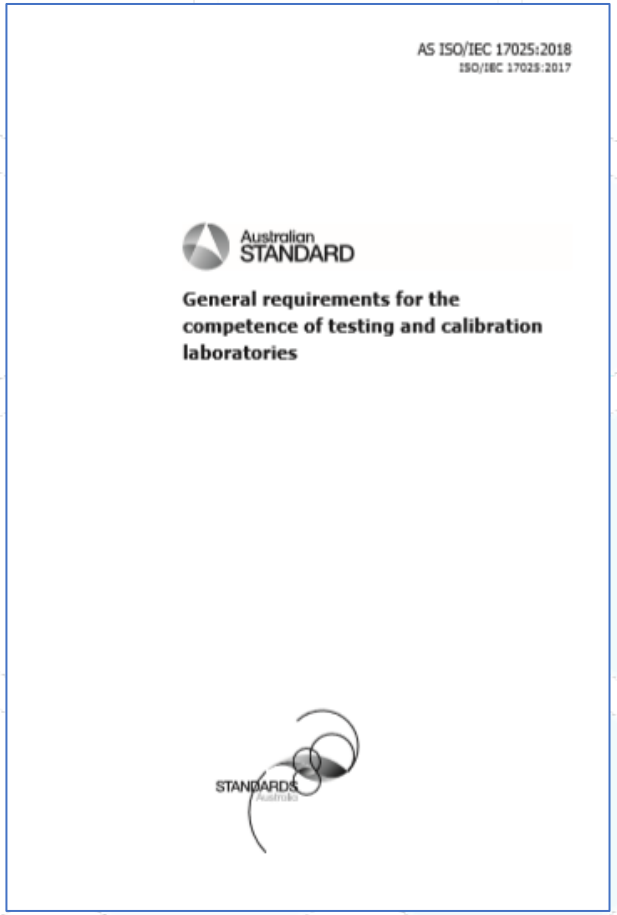
- Process:
  1. Policy and Procedure Development
  2. Evidence Assessment
  3. Evidence Acquisition
  4. Evidence Examination
  5. Documenting and Reporting



1. Available from https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (also in readings)

ISO 17025 - General requirements for the competence of testing and calibration laboratories (2005)

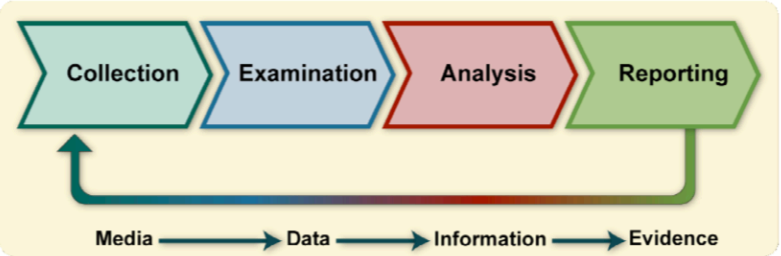
- Applies to all types of laboratories
  - Supported by an JAS/ANZ accreditation scheme[1]
- A number of interesting requirements e.g.:
  - Personnel (e.g. training)
  - Verification and validation
  - Measuring uncertainty
  - Selection and reporting of sample sizes



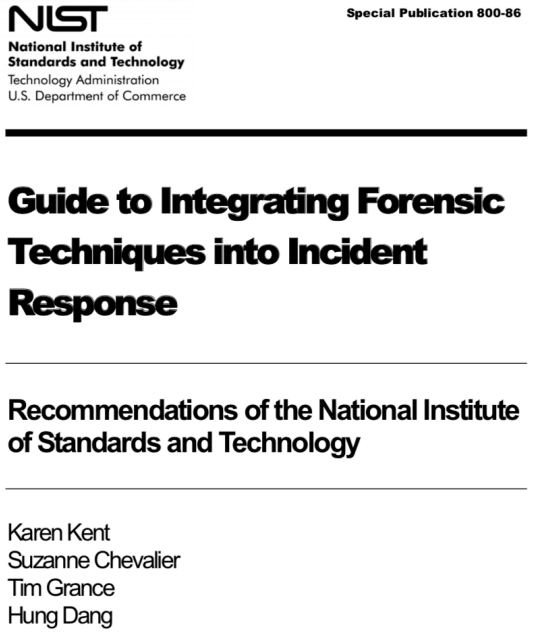
1. See http://www.jas-anz.org/ (also from UNSW subscription to SAI Global standards library)

NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response[1] (2006)

- Forensic process



- Forensic tookit
  - Preparation
  - Collection plan
  - Toolkit


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

Special Publication 800-86

Guide to Integrating Forensic Techniques into Incident Response

Recommendations of the National Institute of Standards and Technology

Karen Kent
Suzanne Chevalier
Tim Grance
Hung Dang

1. Available at https://csrc.nist.gov/publications/detail/sp/800-86/final (also in readings)

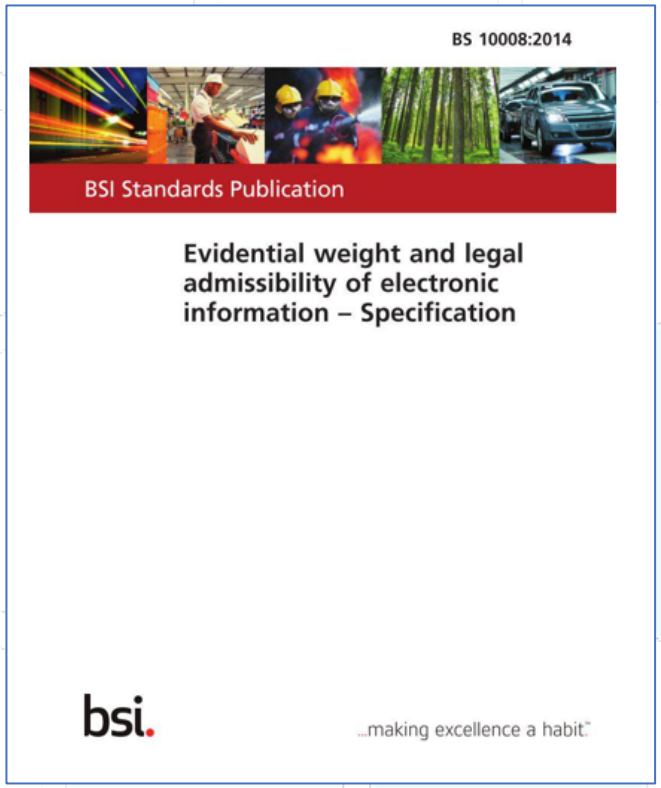
BSI 10008 - Evidential weight and legal admissibility of electronic information (2008)

- Updated in 2014
  - UK centric and based on British law

- Causing headache for UK Police
  - Reasonableness for recovering deleted items from a phone and deleted messages coming to light just before or after prosecution

⇩

    - Capability to do extraction/recovery
    - Volume of material to review
    - Duty to discover incriminating and exculpatory material



The Telegraph

HOME | NEWS | SPORT | BUSINESS | ALL SECTIONS

News

UK | World | Politics | Science | Education | Health | Brexit | Royals | Investigations | Matt | More

News

All rape and serious sexual assault cases are being reviewed after trials collapse, CPS reveals

share

Save

Director of Public Prosecutions, Alison Saunders has confirmed a national review following a string of disclosure failings

MORE STORIES

1 Why Hollywood won't give Liam Neeson a second act

2 Julian Edelman's award as Super Bowl MVP only served to highlight NFL's appalling failure to...

3 The only 8 beauty products you need according to Marie Kondo...and they're perfect for women over 40

4 After meeting Martin Selmayr, I know why the EU is confused about Brexit

See https://www.telegraph.co.uk/news/2018/01/26/rape-serious-sexual-assault-cases-reviewed-trials-collapse-cps/

ISO 27037 - Guidelines for identification, collection, acquisition, and preservation of digital evidence [1] (2012)

- First published in 2012 and re-published in 2018
- Requirements for evidence handling
  - Auditability
  - Repeatability
  - Reproducibility
  - Justifiability
- Digital evidence handling process
  1. Identification
  2. Collection
  3. Acquisition
  4. Preservation
- Supported by other ISO standards:
  - ISO/IEC 27041 (2015): Guidance on assuring suitability and adequacy of incident investigative method
  - ISO/IEC 27042 (2015): Guidelines for the analysis and interpretation of digital evidence
  - ISO/IEC 27043 (2015): Incident investigation principles and processes
  - ISO/IEC 27050 (in 4 parts from 2016): Electronic discovery


INTERNATIONAL STANDARD

ISO/IEC 27037

First edition
2012-10-15

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

Reference number
ISO/IEC 27037:2012(E)

© ISO/IEC 2012

1. Students can get ISO standards from UNSW subscription to SAI Global standards library (see instructions provided with readings)

Short break – 10 mins

And then Week 3 part2:

- Windows memory forensics