NOTE

- The text used to prepare this presentation is that of FDIS27037
- Do be aware:
  "This document is not an ISO International Standard. It is subject to change without notice and may not be referred to as an International Standard".
- Standardization Process milestones:
  - Ballot for FDIS (Currently Underway)
  - Assuming successful FDIS ballot, publish as ISO International Standard
    - Target date is late October, 2012
WHY?

- To make it easier for digital evidence collected in one jurisdiction to be used in another jurisdiction
  - Because our interconnected world enables a victim to be in one nation while the offender is in another

http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

SC 27 RELATED PROJECTS

Diagram courtesy of Eric Hibbard of HDS
GOAL

“...provide guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential evidence between jurisdictions.”

-- 1 Scope

• Establish a minimal baseline of acceptable good practice for dealing with digital evidence

CAVEAT

• A standard does not override applicable law
• So what good is it?
  • Law stops at national boundary
    • “The root problem is that there is no such thing as international law. It’s nothing more than a series of bilateral treaties, conventions and governments claiming jurisdiction over certain laws. It’s up to individual countries to decide whether they want to comply with another country’s laws.”
      -- Jonathan Birk, Adjunct Professor of Internet Law, Rutgers. Quoted in S. Greengard, Law and Disorder, CACM 55:1, January, 2012, p.23
• Standards provide a common ground of requirements and practice for cooperation across national boundaries
TWO ROLES DEFINED

- **DEFR – Digital Evidence First Responder**
  - “authorized, trained and qualified to act first at an incident scene in performing digital evidence collection and acquisition with the responsibility for handling that evidence”
  - Properly and adequately trained to handle digital devices that may contain digital evidence
  - Demonstrate and maintain skills and competency
  - Responsibility of both the DEFR and her employer to ensure he is adequately trained and competencies maintained

- **DES – Digital Evidence Specialist**
  - “can carry out the tasks of a DEFR and has specialized knowledge, skills and abilities to handle a wide range of technical issues”
  - e.g., network/RAM/SAN acquisition, etc.

POTENTIAL DIGITAL EVIDENCE?

- A rather odd term (originally used in Charles Nemeth’s *Law and Evidence*) which reflects the fact that *generally* a piece of evidence does not become “evidence” until admitted as such in a court or other legal proceeding
  - Opposing counsel can (and often does) challenge such admission
GENERAL REQUIREMENTS

- Digital evidence must be:
  - Relevant – contains information of value in assisting the investigation of the incident and there is good reason for its collection/acquisition
  - Reliable – processes should be auditable and repeatable. Process results should be reproducible.
    - In the US, “authentic” is more often used than “reliable”
    - Sufficient – assure enough evidence was gathered to support a proper investigation

EFFECTIVE HANDLING REQUIREMENTS

- Auditable – an independent assessor can evaluate the steps taken by a DEFR or DES
- Repeatable – produce the same results using the same tools on the same items under the same conditions
- Reproducible – produce the same results when using different but equivalent processes
- Justifiable – DEFR/DES can justify all actions and methods used for handling digital evidence

Note that volatile data may have implications for both repeatability and reproducibility
- For example, two successive images of the RAM on a running server will be different (because of the running system clock if for no other reason)
  - However, operations on those images must be both repeatable and reproducible
- The DEFR/DES must be able to justify methods/tools
GENERAL RULES

- Minimize handling of original digital evidence
- Account for any changes and document actions taken
- Comply with local rules of evidence
- DEFR/DES must not exceed their competence

DE HANDLING PROCESSES

- Identification – the search for, recognition and documentation of potential digital evidence
  - DE includes both its physical and logical forms
  - Includes prioritization based on volatility
    - May invalidate the classic seize/image (collect/acquire) dichotomy
VOLATILE OR NOT?

- Volatile data is “data that is especially prone to change and can be easily modified”
- Volatile data can be easily destroyed or lost forever if due care to protect it is not applied (e.g., preserve it before interrupting power)
  - Active network connections
  - List of running processes
  - ...
- Non-Volatile data remains on the media even when the power supply is disconnected

PRIORITIZATION

- Depends on the reason the digital evidence is being collected/acquired
- Generally, the DEFR should maximize the amount of evidence acquired/preserved
  - However, the laws of physics do still apply 😐
- Volatility should be considered only if required by the specific circumstances of the case
  - Active malware
  - Memory-only malware
  - Intrusion, data exfiltration, etc.
- When volatile information is identified and is relevant, the DEFR should take quick actions to collect/acquire the data with validated methods
LIVE ACQUISITION

- Live acquisition may be required due to active encryption and/or the criticality of the system (i.e., it cannot be shutdown)
  - Live acquisition will change the state of the system and imposes the duty on the DEFR (in consultation with the DES) to use validated tools and be able to account for the changes

DECISION MAKING
DE HANDLING PROCESSES

- Devices that potentially contain digital evidence are gathered and may be moved to another facility for later acquisition and analysis.
COLLECT A POWERED-OFF DEVICE

- Producing an image of a source of potential digital evidence and documenting the steps used
ACQUIRING A POWERED-ON DEVICE

ACQUIRING A POWERED-OFF DEVICE
DE HANDLING PROCESSES

- Safeguarding of potential digital evidence and devices that may contain potential digital evidence

PRESERVATION

- Protection, as far as possible, from loss, tampering or spoliation
  - Maintains the integrity and authenticity of the potential digital evidence and its chain of custody
  - Includes packaging, storage, transport, process and documentation