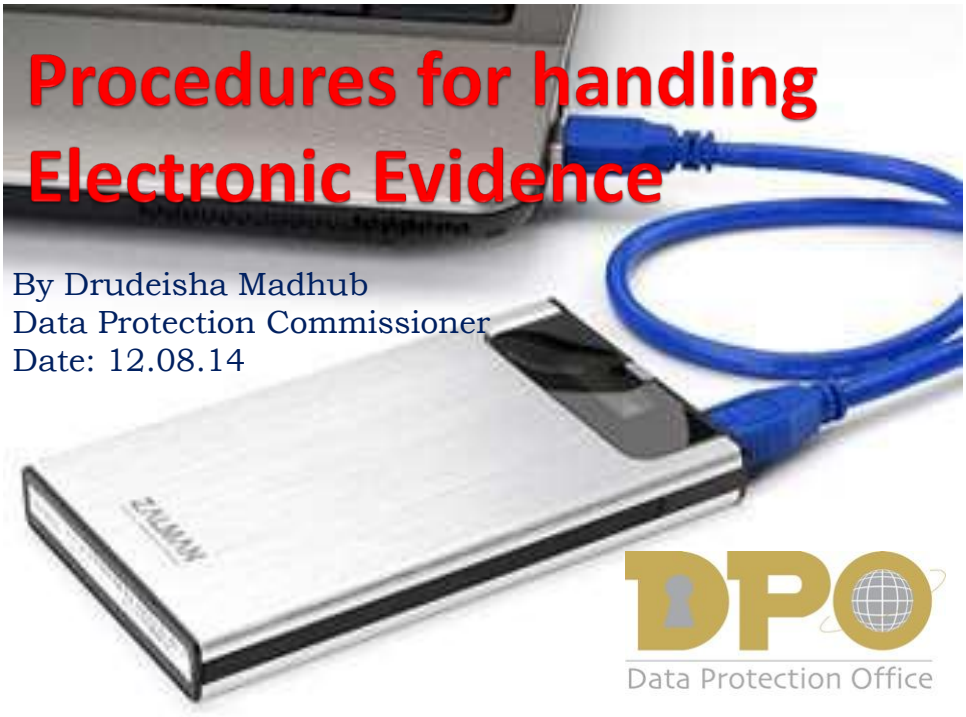

Electronic Evidence

Electronic Evidence requires

- Using high technology to investigate.
- Investigating high technology crimes.
- Creating a digital evidence forensic unit.
- Presenting digital evidence in the courtroom.

Examples

Some examples of data types:	Examples of digital forensic evidence:
• Standard computer systems • Networking equipment • Computing peripherals • Mobile devices • Consumer electronic devices • Various types of media	• Electronic mail messages • Video/photo/audio attachments • Unstructured data • Protocol information such as IP addresses • GPS data • Cell phone data • Metadata • Internet history • Deleted data residues in various types of IT devices.

Electronic Evidence

When dealing with digital evidence, the following general forensic and procedural principles should be applied:

- Actions taken to secure and collect digital evidence should not affect the integrity of that evidence.
- Persons conducting an examination of digital evidence should be trained for that purpose.
- Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review.
- Through all of this, the examiner should be cognisant of the need to conduct an accurate and impartial examination of the digital evidence.

Chain of Evidence

Maintaining source and content integrity of forensics information Electronic authentication, access control mechanisms, and audit trails are needed for:

- Control of forensic data
- To record generation of forensic data
- Access to forensic data
- Change management for forensic data.

Cryptographic technologies such as time stamped digital signature or signed hashes, can be employed to identify the source of forensic data, establish the time(s) at which each access to the data occurred and by whom, and whether or not modifications to the information has occurred (and, if so, at which point in the chain).

How is digital evidence processed?

1. **Assessment.** Computer forensic examiners should assess digital evidence thoroughly with respect to the scope of the case to determine the course of action to take.

2. **Acquisition.** Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. Examination is best conducted on a ***copy of the original evidence. The original evidence should be acquired in a manner that*** protects and preserves the integrity of the evidence.

How is digital evidence processed?

3. **Examination** The purpose of the examination process is to extract and analyze digital evidence. Extraction refers to the recovery of data from its media. ***Analysis refers to the interpretation*** of the recovered data and putting it in a logical and useful format.

4. **Documentation and reporting.** Actions and observations should be documented throughout the forensic processing of evidence. This will conclude with the preparation of a written report of the findings.

Training of Personnel

Computer forensics as a discipline demands:

- Specially trained personnel,
- Support from management,
- The necessary funding to keep a unit operating and
- Ongoing training plan due to the dynamic nature of the IT field

Partnering with other institutions

- The Data Protection Office is partnering with its Canadian Counterpart to assist the office in setting up a forensic lab.
- We rely on the council of Europe for guidance and training in Mauritius. The Action plan has already been scheduled to take all stakeholders on board i.e the Judiciary and Enforcement Departments.

Evidence handling and retention

- Guidelines are being established for receiving, processing, documenting, and handling evidence and work products associated with the examination.

  Note: Evidence identified as contraband, such as child pornography, may require special consideration, such as obtaining specific contraband-related seizure and search warrants.
- It is important to remember that other forensic disciplines might be able to recover other evidence, such as fingerprints on the hard drive, hair or fibers in the keyboard, and handwritten disk labels or printed material. In these instances, procedures should be developed to determine the order and manner in which examinations should be performed to reap full evidentiary value.

Case Processing

- Standard operating procedures (SOPs) are being developed for preserving and processing digital evidence.
  - SOPs should be general enough to address the basic steps in a routine forensic examination while providing flexibility to respond to unique circumstances arising from unforeseen situations.

Developing technical procedures

- Identifying the task or problem.
- Proposing possible solutions.
- Testing each solution on a known control sample.
- Evaluating the results of the test.
- Finalising the procedure.

Onsite considerations

- Consider safety of personnel at the scene.
- Always ensure the scene is properly secured before and during the search.

Onsite considerations

In some cases, the examiner may only have the opportunity to do the following while onsite:

- Identify the number and type of computers.
- Determine if a network is present.
- Interview the system administrator and users.
- Identify and document the types and volume of media, including ***removable media.***
- Document the location from which the media was removed.

Onsite considerations

- Identify offsite storage areas and/or remote computing locations.
- Identify ***proprietary software.***
- Evaluate general conditions of the site.
- Determine the operating system in question.

Onsite considerations

Whenever circumstances require an onsite examination to be conducted, attempt should be made to control the environment.

Assessment considerations might include the following:

- The time needed onsite to accomplish evidence recovery.
- Logistic and personnel concerns associated with long-term deployment.
- The impact on the business due to a lengthy search.
- The suitability of equipment, resources, media, training, and experience for an onsite examination.

Onsite considerations

- If evidence is located that was not authorised in the original search authority, determine what additional legal process may be necessary to continue the search (e.g., warrant, amended consent form).
- Contact legal advisors for assistance if needed.

Some Uses of Digital Forensics Techniques

- Investigating crimes and internal policy violations,
- Pre-trial e-discovery in civil litigations,
- Reconstructing computer security incidents,
- Troubleshooting operational problems, and
- Recovering from accidental system damage.

Computer Forensics Tool Testing (CFTT)

- Goal: Establish a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware.
- The Computer Forensics Tool Testing Project Handbook is now available in PDF format for downloading (http://www.cftt.nist.gov/CFTT-Booklet-Revised-02012012.pdf).

Thank You