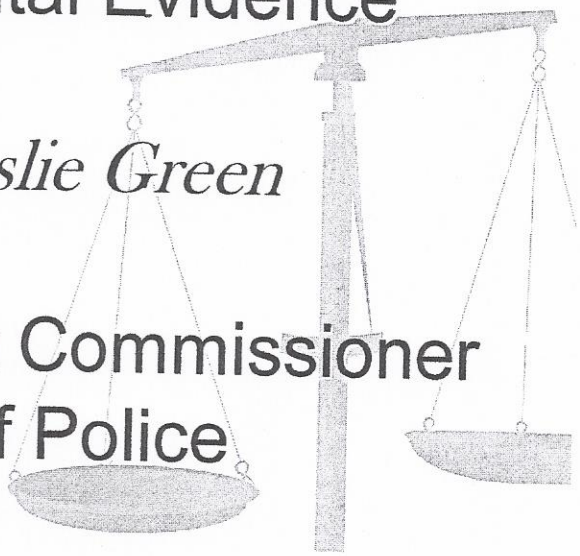
Gathering and Collecting of Digital Evidence

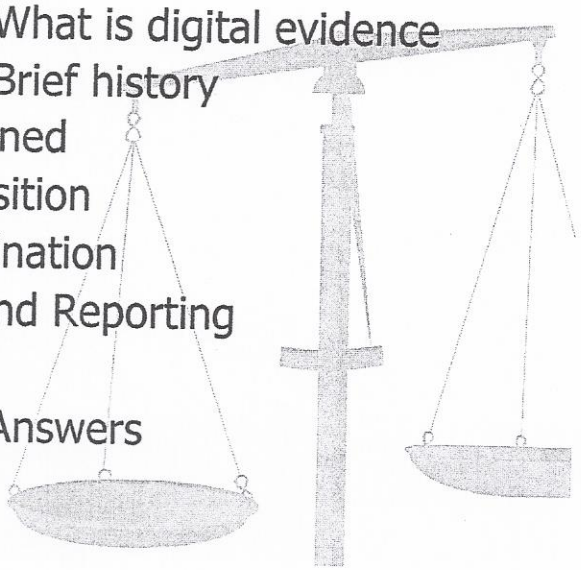


Leslie Green

Assistant Commissioner of Police

This Brief will cover

- Introduction -What is digital evidence
  -Brief history
- Key Terms Defined
- Evidence Acquisition
- Evidence Examination
- Documenting and Reporting
- Legal Authority
- Questions and Answers



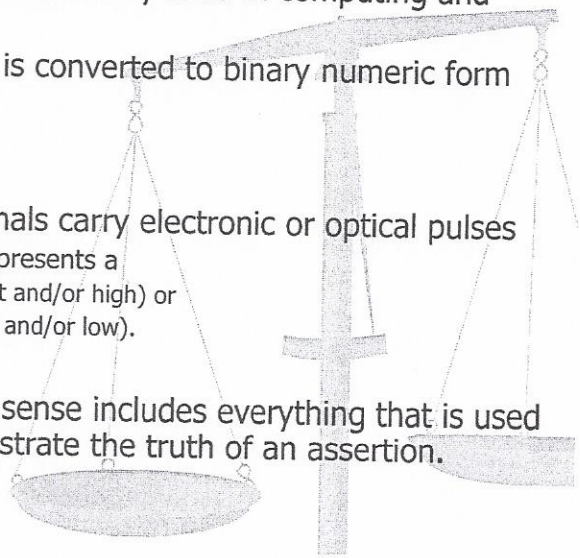
Key Terms Defined

The word ***digital*** is most commonly used in computing and electronics

- real-world information is converted to binary numeric form
  - digital audio
  - digital photography.

- Such data-carrying signals carry electronic or optical pulses
  - amplitude of each - represents a
    - logical 1 (pulse present and/or high) or
    - logical 0 (pulse absent and/or low).

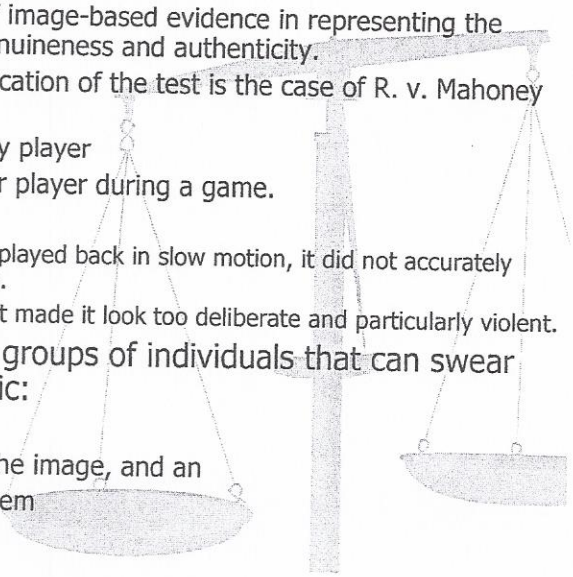
Evidence in its broadest sense includes everything that is used to determine or demonstrate the truth of an assertion.



Brief history

- Admission of image evidence - Common Law test (R. v. Creemer and Cormier) developed in 1968.
  - Assesses the accuracy of image-based evidence in representing the facts, and assesses its genuineness and authenticity.

  A good example of the application of the test is the case of R. v. Mahoney (1976).
  - The accused was a hockey player
  - trial for assaulting another player during a game.
  - Issue
    - The video evidence was played back in slow motion, it did not accurately portray the facts at issue.
    - the slowing of the assault made it look too deliberate and particularly violent.
- This test identifies three groups of individuals that can swear that an image is authentic:
  - Witness to the event,
  - Cameraperson who took the image, and an
  - Expert on the camera system

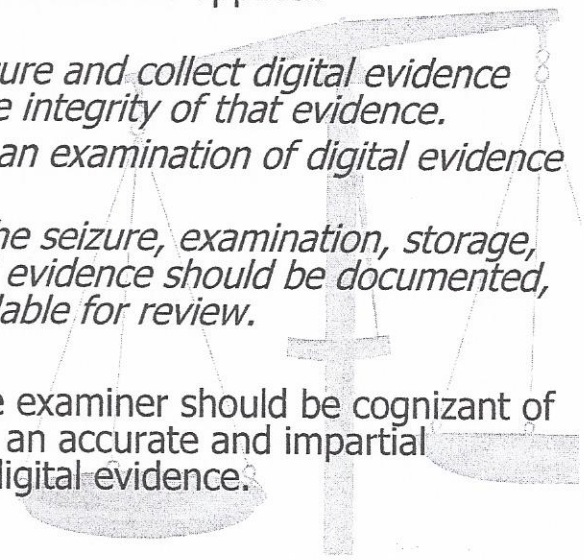


Introduction Cont'd

When dealing with digital evidence, the following 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.*
- *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 cognizant of the need to conduct an accurate and impartial examination of the digital evidence.



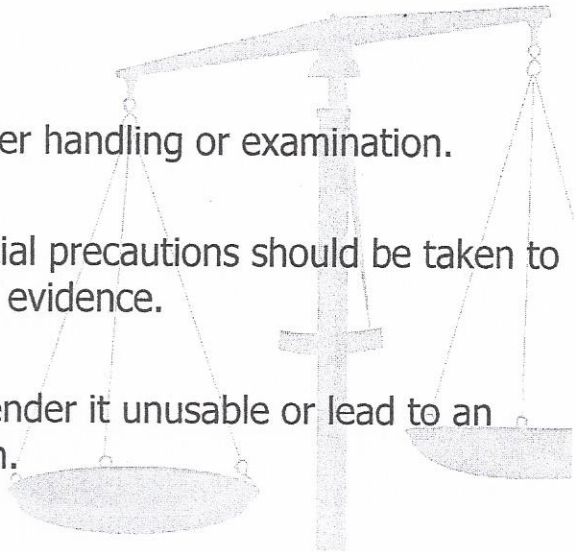
Evidence Acquisition

Principle: Digital evidence, by its very nature, is fragile and can be;

- altered,
- damaged, or
- destroyed by improper handling or examination.

For these reasons special precautions should be taken to preserve this type of evidence.

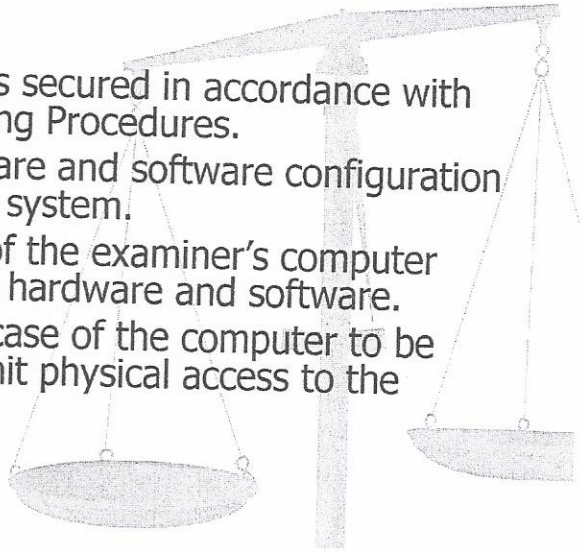
Failure to do so may render it unusable or lead to an inaccurate conclusion.



Procedure: Acquire the original digital evidence in a manner that protects and preserves the evidence.

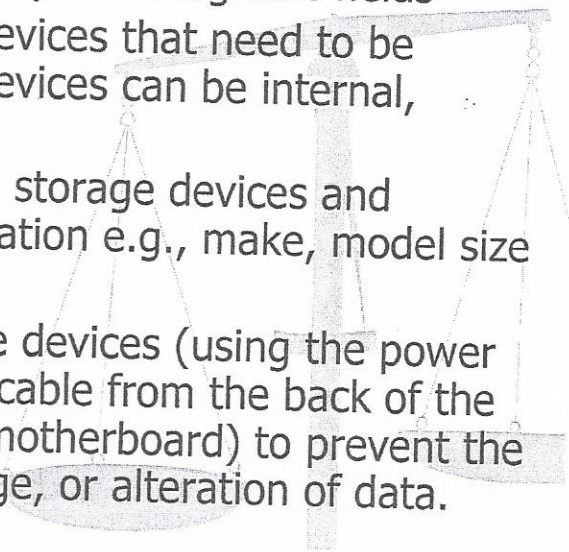
The basic steps:

- Digital evidence is secured in accordance with Standard Operating Procedures.
- Document hardware and software configuration of the examiner's system.
- Verify operation of the examiner's computer system to include hardware and software.
- Disassemble the case of the computer to be examined to permit physical access to the storage devices.



Evidence Acquisition cont'd

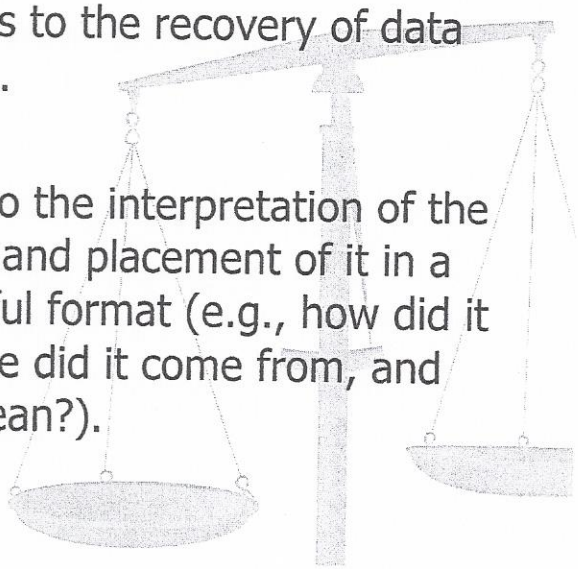
- Take care to ensure equipment is protected from static electricity and magnetic fields
- Identify storage devices that need to be acquired. These devices can be internal, external, or both.
- Document internal storage devices and hardware configuration e.g., make, model size etc.
- Disconnect storage devices (using the power connector or data cable from the back of the drive or from the motherboard) to prevent the destruction, damage, or alteration of data.



Extraction & Analysis of digital Evidence.

Extraction refers to the recovery of data from the media.

Analysis refers to the interpretation of the recovered data and placement of it in a logical and useful format (e.g., how did it get there, where did it come from, and what does it mean?).



Evidence Examination Cont'd

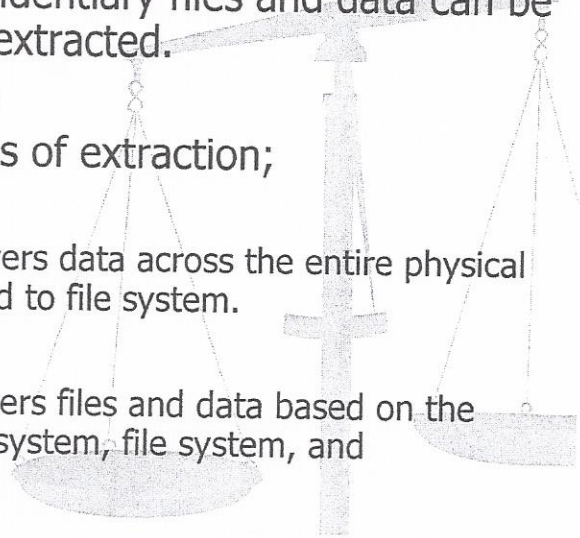
Step 1. Preparation

Prepare working directory/directories on separate media to which evidentiary files and data can be recovered and/or extracted.

Step 2. Extraction

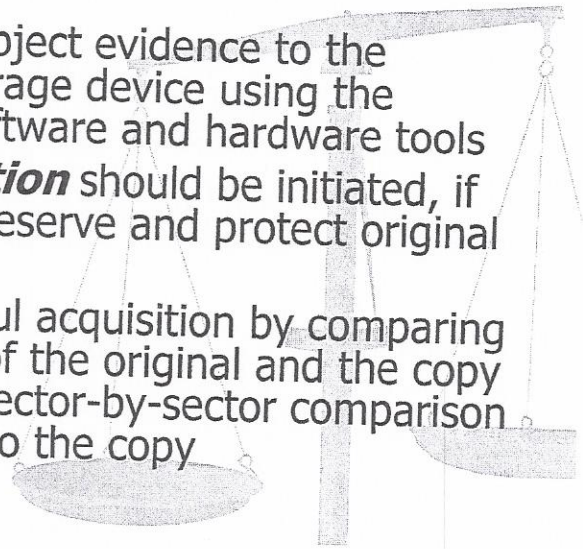
Two different types of extraction;

- Physical
  - identifies and recovers data across the entire physical drive without regard to file system.
- Logical.
  - identifies and recovers files and data based on the installed operating system, file system, and application(s).



Evidence Acquisition cont'd

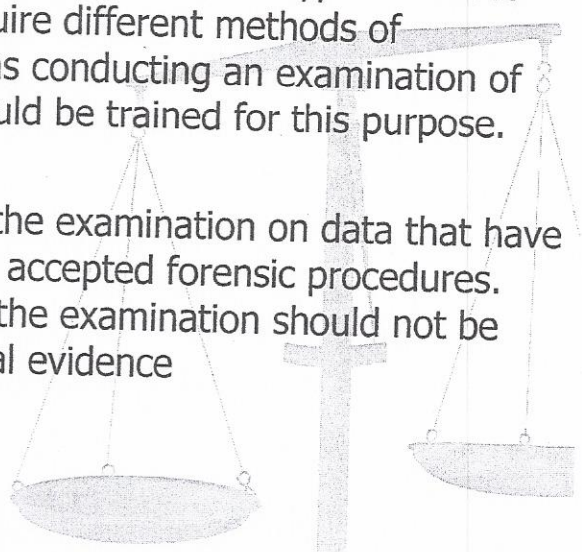
- Retrieve configuration information from the suspect's system through controlled boots
- Acquire the subject evidence to the examiner's storage device using the appropriate software and hardware tools
- ***Write protection*** should be initiated, if available, to preserve and protect original evidence
- Verify successful acquisition by comparing known values of the original and the copy or by doing a sector-by-sector comparison of the original to the copy



Evidence Examination

Principle: General forensic principles apply when examining digital evidence. Different types of cases and media may require different methods of examination. Persons conducting an examination of digital evidence should be trained for this purpose.

Procedure: Conduct the examination on data that have been acquired using accepted forensic procedures. Whenever possible, the examination should not be conducted on original evidence

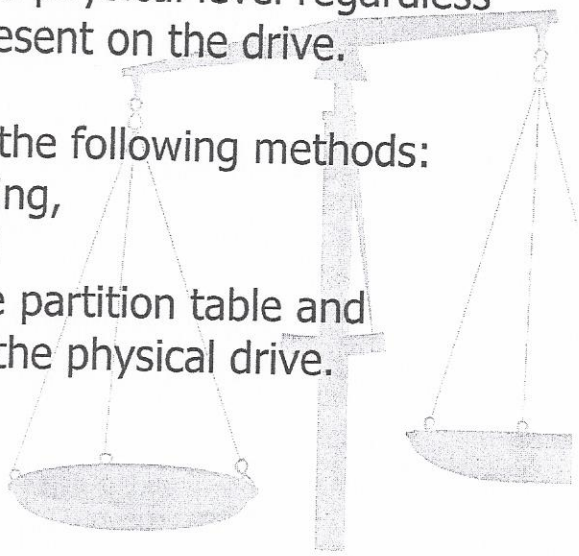


Physical extraction

the extraction of the data from the drive occurs at the physical level regardless of file systems present on the drive.

This may include the following methods:

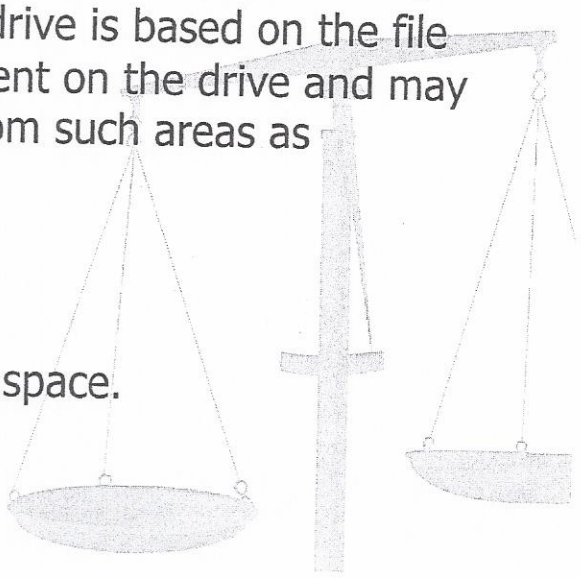
- keyword searching,
- file carving, and
- extraction of the partition table and unused space on the physical drive.



- **Logical extraction**

  During this stage the extraction of the data from the drive is based on the file system(s) present on the drive and may include data from such areas as

- active files,
- deleted files,
- file slack, and
- unallocated file space.



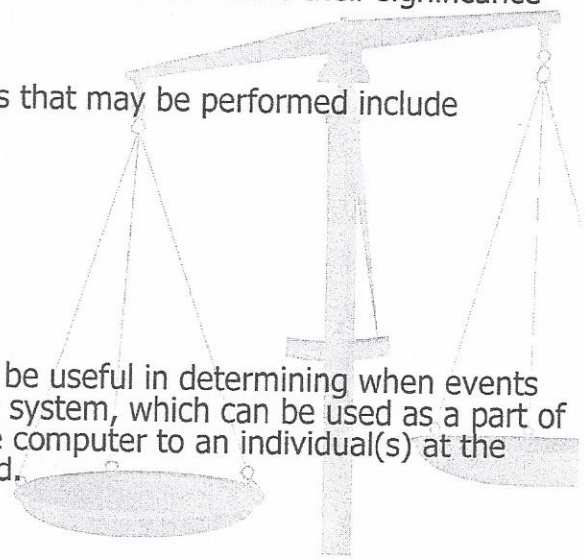
Evidence Examination Cont'd

Analysis of extracted data

- interpreting the extracted data to determine their significance to the case.

Some examples of analysis that may be performed include

- timeframe,
- data hiding,
- application and file, and
- ownership and
- possession.



Timeframe analysis

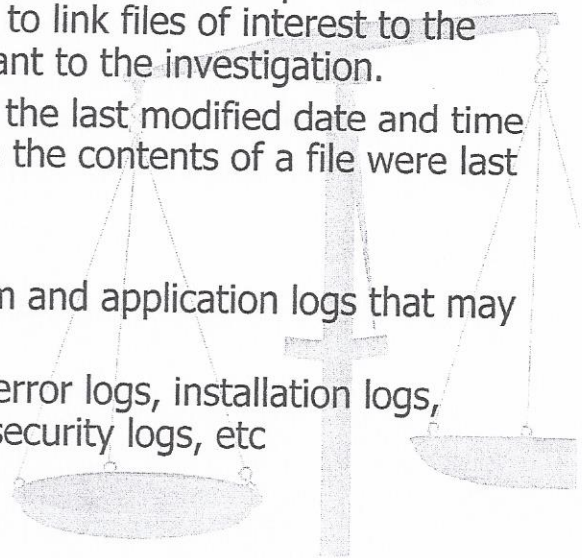
Timeframe analysis can be useful in determining when events occurred on a computer system, which can be used as a part of associating usage of the computer to an individual(s) at the time the events occurred.

Timeframe analysis cont'd

Two methods that can be used are:

- Reviewing the time and date stamps contained in the file system to link files of interest to the timeframes relevant to the investigation.

An example - using the last modified date and time to establish when the contents of a file were last changed.



- Reviewing system and application logs that may be present.

These may include error logs, installation logs, connection logs, security logs, etc

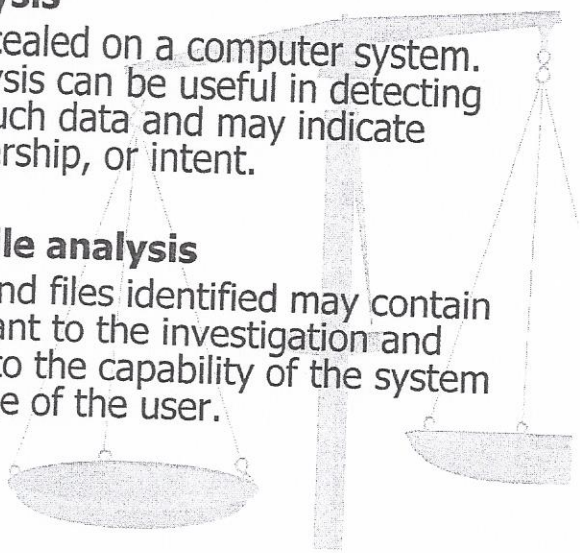
Evidence Examination Cont'd

Data hiding analysis

Data can be concealed on a computer system. Data hiding analysis can be useful in detecting and recovering such data and may indicate knowledge, ownership, or intent.

Application and file analysis

Many programs and files identified may contain information relevant to the investigation and provide insight into the capability of the system and the knowledge of the user.



Evidence Examination Cont'd

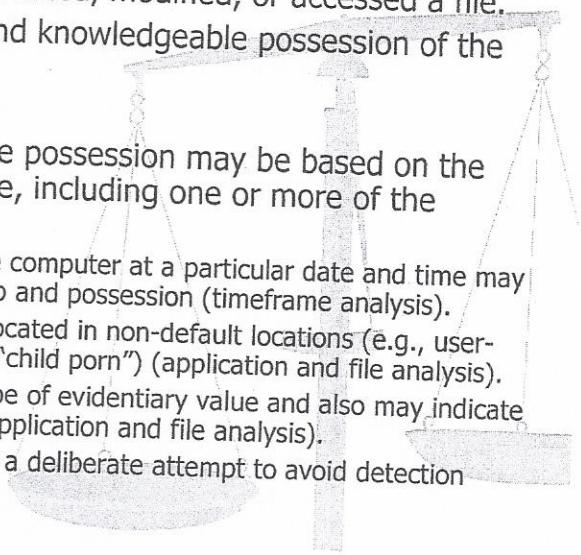
Ownership and possession

may be essential to identify

- the individual (s) who created, modified, or accessed a file.
- determine ownership and knowledgeable possession of the questioned data.

Elements of knowledgeable possession may be based on the analysis described above, including one or more of the following factors-:

- Placing the subject at the computer at a particular date and time may help determine ownership and possession (timeframe analysis).
- Files of interest may be located in non-default locations (e.g., user-created directory named "child porn") (application and file analysis).
- The file name itself may be of evidentiary value and also may indicate the contents of the file (application and file analysis).
- Hidden data may indicate a deliberate attempt to avoid detection (hidden data analysis).



Evidence Examination Cont'd

- passwords - encrypted and password-protected files are recovered, the passwords themselves may indicate possession or ownership (hidden data analysis).
- Contents of a file may indicate ownership or possession by containing information specific to a user (application and file analysis).

Conclusion

results obtained from any one of these steps may not be sufficient to draw a conclusion on their own.

When viewed as a whole, however, associations between individual results may provide a more complete picture.

As a final step in the examination process, be sure to consider the results of the extraction and analysis in their entirety.

Documenting and Reporting

Principle:

- The examiner is responsible for completely and accurately reporting findings and the results of the analysis of the digital evidence examination.
- Documentation is an ongoing process throughout the examination. It is important to accurately record the steps taken during the digital evidence examination.

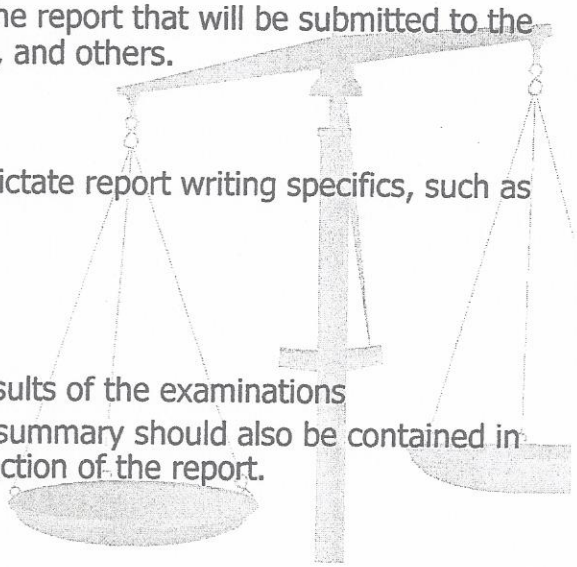
Procedure:

- All documentation should be complete, accurate, and comprehensive.
- The resulting report should be written for the intended audience.

Documenting and Reporting

Examiner's report

Guidance in preparing the report that will be submitted to the investigator, prosecutor, and others.



general suggestions;

departmental policy may dictate report writing specifics, such as its order and contents.

The report may include;

Summary of findings

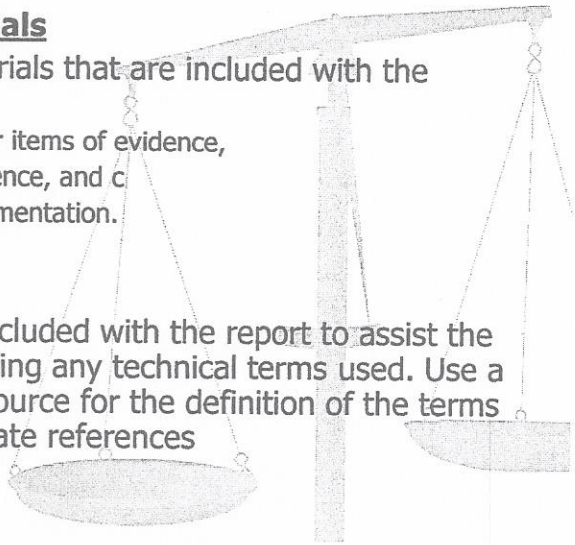
- Brief summary of the results of the examinations
- All findings listed in the summary should also be contained in the details of findings section of the report.

Details of findings

- Describe in greater detail the results of the examinations

Supporting materials

- List supporting materials that are included with the report, such as
  - printouts of particular items of evidence,
  - digital copies of evidence, and c
  - hain of custody documentation.



Glossary

A glossary may be included with the report to assist the reader in understanding any technical terms used. Use a generally accepted source for the definition of the terms and include appropriate references

Legal Authority

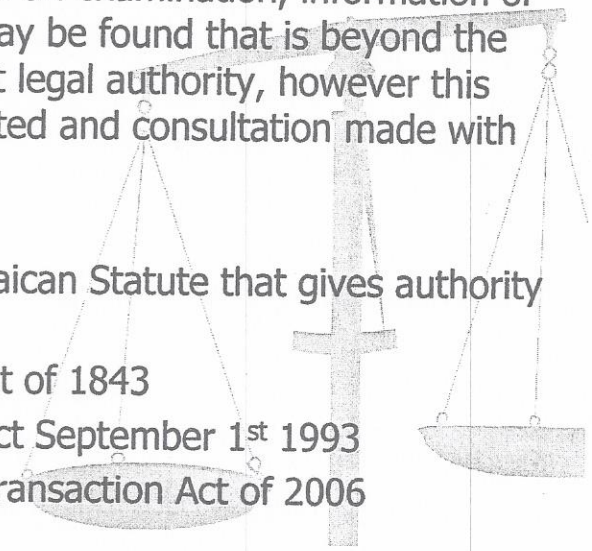
- During the course of an examination, information of evidentiary value may be found that is beyond the scope of the current legal authority, however this should be documented and consultation made with the DPP.

- Acts within the Jamaican Statute that gives authority are as follows-:

  The Evidence Act of 1843

  The Copyright Act September 1st 1993

  The Electronic Transaction Act of 2006



The End

Questions and Answers