

DRAFT

# Computer Forensics

*Part 2: Best Practices*

*Information Security and Forensics Society (ISFS)*  
[www.isfs.org.hk](http://www.isfs.org.hk)

*Date – May 2004*

# Table of Contents

## **Part 2:**

<b>Introduction and Scope</b> .....	<b>5</b>
Organization of this document.....	5
Audience.....	6
<b>Section 1: Introduction to Computer Forensics Best Practices</b> .....	<b>7</b>
<b>1. Important Perspective</b> .....	<b>8</b>
Professional Duties .....	8
1.1 Ethics in computer forensics.....	9
1.2 Evidence Handling Principles.....	10
1.3 Principles of forensics examination.....	11
1.3.1 Key Factors.....	11
1.3.2 Key Responsibilities .....	11
1.3.3 Conducting an examination .....	12
1.4 Chain of custody.....	13
1.4.1 Requirements for a chain of custody .....	13
<b>2. What are the aims of Computer Forensics best practices?</b> .....	<b>14</b>
2.1 The Objectives of Best Practices .....	14
<b>Section 2: Quality Computer Forensics</b> .....	<b>15</b>
<b>3. Establishing the foundation:</b> .....	<b>16</b>
3.1 People and facilities.....	16
3.1.1 Personnel .....	16
3.1.2 Cyber crime .....	17
3.1.3 Maintenance of Competence.....	17
3.2 Quality Process Documentation.....	18
3.2.1 For organizations conducting investigations.....	19
3.2.1.1. Standard Operating Procedures.....	19
3.2.1.2 Contacts .....	20
3.2.1.3 Conflicts and Complaint Resolution.....	20
Corrective Action Policy/Procedures.....	20
3.2.2. For organizations cooperating in investigations .....	20
3.3 Equipment and Procedures .....	20
3.3.1 Physical Work Space .....	21
3.4 Audit.....	21
<b>Section 3: Digital Evidence</b> .....	<b>22</b>
<b>4. Recovery, Handling, Tracking</b> .....	<b>23</b>
4.1 Foreword.....	23
4.2 Preparation.....	23
4.3 Searching the Scene.....	24
4.3.1 Prioritization .....	24
<b>Section 4: Gathering Evidence</b> .....	<b>25</b>
<b>5. General guidelines</b> .....	<b>26</b>
5.1 What to collect and from where?.....	27
5.1.1 How much to collect? .....	27

- 5.2 Collection considerations:.....27
  - 5.2.1 Evidence at all layers, from all places.....28
    - 5.2.1.1 Booby Traps.....28
- 5.3 Documentation of hardware and evidence.....29
  - 5.3.1 The importance of documentation .....29
  - 5.3.2 Documentation Guidelines .....30
    - 5.3.2.1 Hardware.....30
    - 5.3.2.2. Labeling of copied files .....30
    - 5.3.2.3 Photo Documentation .....31
    - 5.3.2.4 Level of detail .....31
  - 5.3.3 Back up .....31
- 5.4 Data Copies.....31
  - 5.4.1 Bit by bit mirror Imaging.....32
  - 5.4.2 Write protection and virus checks.....32
- 5.5 Preserve the chain of custody. ....32
  - 5.5.1 Evidence Handling.....32
  - 5.5.2 Packaging, Labeling and Documentation .....32
  - 5.5.3 Receivers .....33
- 6. First responder considerations..... 34**
  - 6.1 General rules for specific devices .....34
    - 6.1.0 Volatile memories.....34
    - 6.1.1 Mobile Telephones .....34
      - 6.1.1.1 Additional consideration for computer forensics professionals .....34
        - 6.1.1.1.1 Special Considerations.....35
    - 6.1.2 Electronic Paging Devices .....35
      - 6.1.2.1 Additional consideration for computer forensics professionals .....35
        - 6.1.2.1.1 Special Considerations.....36
    - 6.1.3 PDAs / Personal Digital Organizers / Handheld Computers.....36
      - 6.1.3.1 Additional consideration for computer forensics professionals .....36
        - 6.1.3.1.1 Special Considerations.....36
    - 6.1.4 Smart Cards .....37
      - 6.1.4.1 Additional consideration for computer forensics professionals .....37
        - 6.1.4.1.1 Special Considerations.....37
    - 6.1.5 Digital and Audio Systems .....38
      - 6.1.5.1 Devices that are active .....38
      - 6.1.5.2 Additional consideration for computer forensics professionals .....39
        - 6.1.5.2.1 Special Considerations.....40
- 7. Evidence Handling ..... 41**
  - 7.1 Receiving Digital Evidence .....41
    - 7.1.1 Additional considerations for Mobile Telephones, Smart Cards, PDAs, Handheld computers, Pagers, Smart Cards, Personal Data Organizers.....41
  - 7.2 Reconstruction and Reporting .....41
    - 7.2.1 Classification .....42
      - 7.2.1.2 Trustworthy and Untrustworthy.....42
    - 7.2.2 Handling of Mobile phones, pagers, PDAs, Smart Cards, etc. ....43
  - 7.3 Reconstruction .....43
    - 7.3.1 Final Report .....43
  - 7.4 Case File Review .....44
- Section 5: Considerations of Law..... 45**
- 8. Considerations of law..... 46**
  - 8.1 General principles.....46
    - 8.1.1. Authenticity .....46
    - 8.1.2 Best Evidence .....46

8.2 Electronic Records as Admissible Evidence.....	46
8.3. Evidence Considerations in Hong Kong.....	47
<b>Appendices.....</b>	<b>48</b>
<b>Appendix 1: Sample Statement of Findings.....</b>	<b>49</b>
<b>Appendix 2: Sources of Data .....</b>	<b>50</b>
Audio Devices .....	53
Video devices / Sources of digital image data .....	53
Applications, Users and Home Computers.....	53
Written Policies and Documents.....	54
<b>Appendix 3: Additional Evidence Considerations.....</b>	<b>55</b>
Appendix 3.1 Data categories.....	55
Appendix 3.1.1 Ad Hoc Data.....	55
Appendix 3.1.2 Data kept as part of a process.....	55
Appendix. 3.2 Admissibility of Digital Evidence.....	55
Appendix 3.2.1 Criminal Proceedings.....	56
Appendix 3.2.2 Civil Proceedings .....	56
Appendix 3.2.2.1 Evidence types .....	56
<b>Appendix 4: Selections from the Hong Kong Electronic Transactions Ordinance:.....</b>	<b>57</b>
ELECTRONIC TRANSACTIONS ORDINANCE - SECT 5.....	57
Requirement for writing .....	57
ELECTRONIC TRANSACTIONS ORDINANCE - SECT 6.....	57
Digital signatures.....	57
ELECTRONIC TRANSACTIONS ORDINANCE - SECT 7.....	57
Presentation or retention of information in its original form .....	57
ELECTRONIC TRANSACTIONS ORDINANCE - SECT 8.....	58
Retention of information in electronic records .....	58
ELECTRONIC TRANSACTIONS ORDINANCE - SECT 9.....	58
Admissibility of electronic records.....	58
<b>Appendix 5: Selections from the Hong Kong Evidence Ordinance:.....</b>	<b>59</b>
EVIDENCE ORDINANCE - SECT 22A .....	59
Documentary evidence in criminal proceedings from computer records.....	59
EVIDENCE ORDINANCE - SECT 22B .....	61
Provisions supplementary to sections 22 and 22A.....	61
EVIDENCE ORDINANCE - SECT 47 .....	62
Admissibility of hearsay evidence.....	62
EVIDENCE ORDINANCE - SECT 49.....	63
Considerations relevant to weighing of hearsay evidence .....	63
EVIDENCE ORDINANCE - SECT 53.....	63
Proof of statements contained in documents.....	63
EVIDENCE ORDINANCE - SECT 54.....	63
Proof of records of business or public body .....	63

## *Introduction and Scope*

---

### **Processes, procedures and other requirements**

### **Technological considerations**

### **Jurisdictional considerations**

---

The scope of Part 2 covers procedures and other requirements involved in the entire forensic process of digital evidence, from examinations at the scene of a crime to the preparation of reports for presentation in court.

Part 2 will also provide some explanation why certain procedures are performed.

This part will delve deeper into the technical details of computer forensics and though this document may repeat some topics covered in Part 1, Part 2 will cover these subjects in greater technical depth.

As with Part I, Part 2 is written in such a manner as to be as technologically- and as jurisdictionally-neutral as possible though it is written with Hong Kong readers in mind.

Nevertheless, readers are urged to keep in mind that:

1. Laws vary from country to country. Therefore professionals performing investigations in multiple legal jurisdictions need to determine the legal requirements of the jurisdictions they are operating in (especially the laws that pertain to collecting and protecting evidence, chain of custody, and sufficiency of evidence for prosecution) and implement the necessary procedures to meet those requirements.
2. Specialists need to account for variations in operating systems, applications, etc. as well as system configurations in performing forensics examinations and that no single set of guidelines can apply to all potential situations and contingencies.
3. This document is not intended to offer legal advice. *For matters of law, the ISFS recommends that readers seek proper qualified legal counsel in the relevant jurisdiction(s)*

### **Organization of this document**

This document is divided into five sections:

- *Section 1: Introduction to Computer Forensics Best Practices* provides some general overview of the aims and objectives of setting up a set of best practices
- *Section 2: Quality computer forensics:* is aimed at computer forensics professionals, persons involved in computer forensics, individuals contemplating a career in computer forensics or groups involved in the establishment of computer forensics teams

- *Section 3: Digital Evidence* provides guidelines on the collection and preservation of evidence. For most readers, this is the section that will be of most relevance to them.
- *Section 4: Considerations of Law* provides some perspective on the relevant legal issues concerning digital evidence in Hong Kong
- *Appendices*: provide handy reference materials including sample statements of findings, checklists and reprints of sections of relevant Hong Kong laws.

## **Audience**

The intended audience for this document are professionals involved in computer forensics including forensics specialists and law enforcement, persons who may work with or assist computer forensics professionals in the acquisition of evidence and others simply interested in learning more about the technical aspects of computer forensics.

Among those for whom this document is aimed are professionals:

- With overall authority and responsibility for the management and quality of the work carried out by forensics teams
- Trained to assess and identify digital evidence at the scene for collection, i.e. the first responders
- Responsible for directing the examination of evidence collected, interpretation of the findings, preparation of the necessary reports
- Providing evidence of fact and, if necessary, opinion for a court.
- With specialized technical competencies who may be called in to assist with a forensics examination
- Carrying out general casework examinations and/or technical work under supervision, who are able to provide information to assist with the interpretation of the analyses.

*Section 1: Introduction to Computer Forensics  
Best Practices*

## 1. Important Perspective

### Professional Duties

---

#### Collect all evidence

#### Preserve evidence

#### Ensure evidence is captured and preserved securely

---

Before discussing best practices, let us first consider the professional duty owned by the Computer Forensics specialist.

It is this professional's job to:

- Carefully identify and attempt to retrieve possible evidence that may exist on a subject computer or computing device(s) including all files on the subject system(s). This not only includes locating existing, normal files but also:
  - Retrieving deleted, temporary, hidden, password-protected or encrypted files
  - Revealing or recovering, to the extent possible, the contents of:
    - Discovered deleted files
    - Hidden files
    - Temporary files
    - Swap files used by application programs and the operating system.
    - Protected or encrypted files (if possible and if legally appropriate)
- Protect the subject system(s) during the forensic examination from any possible alteration, damage, data corruption, or contamination by a virus.
- Analyze all possibly relevant data found in special (and typically inaccessible) areas of a disk, notably:
  - The 'unallocated' space on a disk
  - The 'slack' space in a file
- Provide an overall analysis of the subject system(s), as well as a listing of all potentially relevant files and discovered file data. This may include offering an opinion of:
  - The system layout
  - The file structures discovered



- Any discovered data and authorship information
  - Attempts to hide, delete, protect, encrypt information and
  - Anything else that has been discovered and appears to be relevant to the overall examination
- Provide expert consultation and/or testimony, as required.

## 1.1 Ethics in computer forensics

---

**Objectivity**

**Accuracy**

**Completeness**

**Established and validated principles and procedures**

**Opinions of facts**

---

Given the crucial role a Computer Forensics specialist (or any other person involved in a forensics examination) plays, it is important that such an individual maintain strict ethical standards to ensure that the evidence gathered and analyzed meets the highest quality standards possible for:

- Integrity
- Authenticity and
- Accuracy.

It is critical that the persons involved in an investigation thoroughly examine and analyze case evidence conducting examinations based upon *established, validated principles*. These principles are elaborated upon in the next section.

## 1.2 Evidence Handling Principles

---

**Principle 1: No change of data**

**Principle 2: Only competent persons should access digital evidence**

**Principle 3: Documentation**

**Principle 4: Ownership**

---

According to the G8 recommendations relating to digital evidence, forensics specialists must follow four principles.

1. First, the general rules of evidence should be applied to all digital evidence. It is important that forensics specialists, upon seizing digital evidence, ensure that the evidence is not changed
2. If circumstances require access to original data held on a computer or on storage media, persons accessing this data must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
3. There must be full documentation of all activities related to the seizure, access, storage or transfer of digital evidence. The documentation should be preserved and available for review.
4. Finally, there must be ownership: that is the person in charge of the investigation must have overall responsibility for ensuring that these principles (and the law) are adhered to<sup>ii</sup>.

All practices employed in the recovery of digital evidence recovery should fall within a defined and accepted framework and must comply with the above principles.

And it goes without saying that you and all those involved with a digital forensics examination should always follow the law, particularly those who are first to respond to an investigation<sup>1</sup>.

---

<sup>1</sup> Ref: First responders guidelines for digital images and audio, IOCE 2000 conference, Rosny sous Bois, France

## 1.3 Principles of forensics examination

### 1.3.1 Key Factors

Four things are key to all forensics examinations; the:

- (1) Maintenance of data integrity as well as data authenticity,
- (2) Prevention of contamination of data,
- (3) Proper and comprehensive documentation and
- (4) Implementation of a systematic, scientific methodology

### 1.3.2 Key Responsibilities

All professionals involved in a forensics examination have both an ethical and a professional responsibility to:

- Maintain their objectivity.
- Present facts accurately and
- Not withhold any findings as such actions may distort or misrepresent the facts
- Render opinions only on the basis of what can be reasonably demonstrated.

It also goes without saying that these professionals *must never misrepresent their qualifications* and be willing to work with fellow specialists when the situation calls for such cooperation.

---

**Data Integrity**

- Completeness, wholeness and readability of information and
- Quality being unchanged from a previous state

**Data Authenticity**

- Validity
- Conformance
- Genuineness of information

**Freedom from contamination****Full documentation****Scientific methodology**

---

### 1.3.3 Conducting an examination

In conducting a forensics examination, the Computer Forensics specialist must:

- Apply all general forensics and procedural principles in dealing with digital evidence
- Not perform any actions that would change evidence held including data on media or in computers
- Ensure that only qualified persons access the digital evidence.

It may be necessary in exceptional circumstances to allow others access original data held on a target computer or other media. In such cases, it is vital that any and all persons accessing the data *are both competent to do so and competent to give evidence* explaining the relevance and the implications of their actions

- Document all activities related to the seizure, access, storage and transfer of digital evidence and preserve a record. An independent third party should be able to examine those documented procedures such that were this third party to repeat the process, it would achieve the same result
- Remember that as an individual in possession of digital evidence a Computer Forensics specialist is responsible for all actions taken with respect to this digital evidence. As a responsible party, he/she must ensure that these best practices principles of Computer Forensics are adhered to.

This applies to the possession of and access to, information contained in a computer. It is the duty of the Computer Forensics specialist in charge to ensure that anyone accessing evidence complies with these principles.

## 1.4 Chain of custody

Moreover, it is vital that a *verifiable chain of custody* is maintained for protection of potential evidence along with a detailed action and decision log indicating who made each entry.

This chain of custody is important as it tracks evidence from its original source to what is offered as evidence in court.

With digital evidence, a chain of custody is critical because the data can be altered or destroyed with relative ease.

### 1.4.1 Requirements for a chain of custody

Preserving a chain of custody requires the ability to prove that:

- (a) No information has been added or changed.
  - To do so, media should be write protected and virus checked all media
- (b) A complete copy was made;
  - To meet this requirement, the Compute Forensics specialist makes image copies A reliable copying process was used; and
- (c) All media was secured to assure that original copies are preserved.

To ensure that a reliable copy process was used, we can test for three critical characteristics.

- 1 First, did the process must meet industry standards for quality and reliability?

This includes the software used to create the copy and the media on which the copy is made. A good test for software as to whether it measures up is whether law enforcement agencies use and rely on the software.

- 2 Second, were the copies capable of independent verification?
- 3 Third, were the copies created tamper proof?

---

## 2. What are the aims of Computer Forensics best practices?

---

**Proper facilities, personnel**

**Quality process manual**

**Exhibit handling**

**Equipment:**

- Computer forensics examination environment
- Forensics computer
- Data storage

**Maintain chain of custody**

---

In creating a set of best practices for Computer Forensics one should first be very clear about the aims and objectives of this effort.

### 2.1 The Objectives of Best Practices

The aim of a set of best practices standards is to establish a benchmark of quality, quality principles and approaches for the detection, preservation, recovery, examination and use of digital evidence for forensic purposes.

Given the importance of forensics investigation in the discovery of evidence, high standards of quality and consistency are vital to retain the probative value of the evidence.

Best practices also serve to encourage professionals to adopt a consistent methodology to facilitate the interchange of data. This is particularly important given the growing need for local investigators to coordinate efforts with overseas counterparts.

In certain situations the evidence collected may be useful in defensive actions. For example, if an organization's computer had been used, inadvertently, to commit a crime, any evidence collected would be potentially valuable and may need to be shared if other organizations or entities initiate legal proceedings.

\*

*Section 2: Quality Computer Forensics*

### 3. Establishing the foundation:

In order to conduct a proper Computer Forensics examination a sound foundation must first be in place. This should include:

- **Skilled personnel:** who are competently trained to either conduct or assist in an examination.
- **Quality Assurance:** An important element is a computer forensics Quality Process Manual that will help to ensure consistency of process and provide a valuable reference resource for persons who may be involved in an investigation
- **Proper tools and facilities** (for organizations who may actually be conducting examinations themselves)

#### 3.1 People and facilities

##### 3.1.1 Personnel

\*\*

---

#### Computer Forensics Examiner/Specialist

- Hardware Operator
- Software user
  - Disk imaging
  - Data Search
  - Analysis
- Knowledge of computer systems (OS), database, Internet/web technology, etc.
  - Business, conceptual and/or operational knowledge
    - E.g. IT architect, business/system analysis, software engineer, programmer (OS, applications, assembler language, etc.) hardware engineer, etc.

---

The people involved in a digital forensics examination must not only have the required technical competencies in hardware, software, operating systems, applications, networks, etc. but must also be trained in the proper:

- Procedures for gathering and preserving digital evidence
- Use of the forensics tools they apply.

Given the variations among systems, implementations and technologies, these professionals must be able to adapt to different technological and situational requirements *without* compromising their professional or ethical standards.



### 3.1.2 Cyber crime

---

#### **A computer can be:**

- The object of a crime
- The subject of a crime
- Used as tool to commit a crime
- A symbol used to commit a crime (e.g. Loco London Gold Case, no transaction record found in the computers)

(Don Parker 1998)

#### **A source of digital evidence?**

---

As Computer Forensics specialists or others involved in an examination will likely interact with law enforcement, it is important that these individuals have at least some understanding of cyber crime terminology so as to expedite communications with law enforcement as well as have a better perspective of how digital media and computers may fit into an overall picture of a crime.

While it is beyond the scope of this document to discuss cyber crime, it is important that Computer Forensics specialists at least recognize that computers, networks and digital devices (e.g. PDAs), can be:

- The object or target of a crime, for instance when a criminal deliberately hacks into a computer to steal data
- Used as a tool to commit a crime: for example when a computer is used to commit a fraud
- Incidental to a crime – for example a computer may be used in money laundering or as a symbol to commit a crime – for example if a criminal syndicate were attempting to provide the illusion of a legitimate business operation, it might set up banks of computer systems to help further the illusion. (This was what happened during the noted Loco London gold case)
- A source of digital evidence

### 3.1.3 Maintenance of Competence

Finally, given the fast pace of change in the Information Technology world, Computer Forensics specialists must maintain their competence through regular proficiency testing and continuous study.

### 3.2 Quality Process Documentation

Given that a forensics examination is so critically dependent on both the completeness of the procedures followed and the quality of the work done, there should be a documented computer forensics Quality Process Manual covering all systems, processes and methods used in the examination and reporting of forensic digital evidence.

By providing detailed steps and procedures to be followed during an examination, such a Quality Process Manual would not only help ensure *consistency of process*, it could additionally serve as an important reference resource for personnel who may find themselves in a first responder situation.

This information can be particularly critical as first responders who are unaware of proper forensics procedures may inadvertently destroy valuable evidence.

---

#### Process Documentation:

- Standard operating procedures
- Contacts
- Evidence handling and tracking
- Corrective action policy/procedures
- Complaint and conflict resolution

---

Among other things, this Quality Process Manual should document organizational policy outlining the:

- Steps to be taken in the event a forensics examination is necessary (e.g. a criminal breach of the system),
- Procedures to follow (for specific systems if necessary),
- Persons to contact, etc.

Ideally, such information should also be included in a training program.

Whenever appropriate the Quality Process Manual should provide standardized form templates. It should be organized in an easily accessible, reference able and comprehensive format, be regularly reviewed and updated if necessary.

Readers should be aware that such standards documentation is common among firms that value quality, for instance organizations that are ISO 9000 certified. A Quality Process Manual also a good indicator to staff, investors and others of the importance of quality to the organization.

### 3.2.1 For organizations conducting investigations

For organizations that may be involved in conducting forensics examinations, their Quality Process Manual should also include procedures and information on:

- Standard Operating Procedures
- Contacts
- Complaints and conflict resolution
- Corrective Action Policy/Procedures
- Digital Evidence: Recovery Handling and Tracking Procedures

#### 3.2.1.1. Standard Operating Procedures

The Standard Operating Procedures section should cover:

1. **Incident identification** – Where an event is recognized as an incident and is classified accordingly. While this is not explicitly within the field of forensics, this step is significant because it impacts subsequent steps.
2. **Preparation** – Detailed procedures for the proper preparation of tools, techniques, monitoring authorizations and management support.
3. **Approach strategy** – Guidelines on how to dynamically formulate an approach based on potential impact and the specific technology or technologies in question in order to maximize the collection of untainted evidence while minimizing impact to the victim.
4. **Preservation** – Courses of action for isolating, securing and preserving the state of physical and digital evidence.
  - This includes preventing people from using the digital device or allowing other electromagnetic devices to be used within an affected radius.
5. **Collection** – Procedures and processes for recording the physical scene and duplication of digital evidence using standardized and accepted practices.
6. **Examination** – Guidelines on conducting an in-depth systematic search of evidence with particular focus on identifying and locating potential evidence, possibly within unconventional locations, as well as the production of detailed documentation for analysis.
  - Procedures for recording actions taken during an investigation including the acts performed, dates, times and persons involved should also be included.
7. **Analysis** – to determine the significance of data and draw conclusions based on evidence found.
8. **Presentation** – Guidelines on how to summarize, report and explain the conclusions reached
  - In this section, the document should remind the practitioner that reports should be written in a layperson's terms using abstracted terminology that references the specific details.
9. **Return of evidence** – Guidelines to ensure that physical and digital property is returned to proper owner as well as determining how and what criminal evidence must be removed.

Ideally, the Quality Process Manual should contain complete sets of checklists, to help ensure that investigators do not overlook key procedures or sources of data including cable connections, communications logs, screen shots, printouts, etc. (See Appendix 2 of a list of potential data sources)

An organization may wish to also include sample formats for reporting such as a sample Statement of Findings (See Appendix 1)

A competent Computer Forensics specialist should review the manual to ensure that it is complete and complies with relevant international practices, guidelines and standards.

#### **3.2.1.2 Contacts**

This Quality Process Manual should include a list of responsible persons, their contact details and alternate contacts.

#### **3.2.1.3 Conflicts and Complaint Resolution Corrective Action Policy/Procedures**

Ideally, an organization should have procedures dealing with complaints or anomalies. These procedures should cover the investigation of the complaints or anomalies, the taking of corrective actions, assuring that personnel are aware of their responsibilities and the reporting of findings.

### **3.2.2. For organizations cooperating in investigations**

Organizations that would not be conducting investigations themselves but might cooperate with investigators in the event some incident occurs may want to include procedures for handling incidents that might warrant forensics examinations (e.g. a suspicious attack) or create a separate Quality Process Manual

Among the items such documentation ought to contain are:

- Incident handling:
  - What to do
  - What NOT to do
- Contacts
- Procedures on working with investigators
- Event recording
- Corrective Action Policy/Procedures
- Complaints and conflict resolution

It must be stressed that such documentation should be created or at least reviewed by a qualified Computer Forensics expert.

### **3.3 Equipment and Procedures**

All equipment used during forensic casework should be appropriate for the purpose and be properly maintained for operational considerations.

- *Only properly evaluated tools, techniques and procedures should be used for a forensic examination of digital technology and*
- *All media used in making copies must be forensically sterile.*

---

### Equipment and Audits

- Suitable equipment
    - Properly validated
  - Proper working space
  - Regular audits
- 

Proper validation of equipment requires, as a minimum that:

- There is a minimum acceptable criteria for the technique or procedure;
- The critical aspects of the examination procedure and tools have been identified and the limitations defined wherever possible;
- The methods, materials and equipment used have been demonstrated to be fit for their respective purpose;
- There are appropriate quality control and quality assurance procedures in place for monitoring performance;
- The technique or procedure is documented;
- The results obtained are reliable and reproducible.

#### 3.3.1 Physical Work Space

Laboratories and/or forensic workspaces for the examination of digital technology items should be designed and equipped for efficient, secure, safe and effective use.

As a practical matter, designers of such workspaces must pay attention to the management electrical and other cables as well as environmental conditions.

### 3.4 Audit

Finally, audits and updates of the quality system, procedures and practices should be conducted in a timely manner to ensure that quality and competency standards are maintained.

## *Section 3: Digital Evidence*

## 4. Recovery, Handling, Tracking

### 4.1 Foreword

Any procedures, processes or practices employed in digital evidence recovery should fall within a defined and accepted framework for Computer Forensics investigation and must comply with the principles stated earlier.

In locating and recovering digital evidence, Computer Forensics specialists may need to attend the scene or may need to give advice to others attending the scene and recovering the evidence.

They should be aware of any relevant legal guidelines or constraints.

---

#### Collection of data:

- Preparation
  - Searching the scene
  - Prioritization
  - Evidence collection
- 

### 4.2 Preparation

Prior to any investigation, the Computer Forensics specialist must ensure that he/she has the proper tools on hand including *forensically sterile media*.

Ideally, all equipment, sampling materials and storage and transportation containers should be new, preferably disposable, or cleaned thoroughly before and after use.

Appropriate precautions should be taken to minimize any chance of accidental contamination of items, which may subsequently be required for later examination.

(Note: that in cases where law enforcement is conducting investigations, law enforcement personnel deciding what anti-contamination precautions need to be taken may base their considerations not only on the digital evidence, media and devices, but also on the other evidence that may potentially be available for other types of analysis (e.g. DNA analysis). However a discussion of this is beyond the scope of this document).

### 4.3 Searching the Scene

To reduce the risk of loss, movement or damage to digital evidence, all areas – indoor, outdoor or in vehicles -- should be protected at the earliest opportunity using procedures that follow all appropriate legal, technical and jurisdictional guidelines.

Areas should be searched systematically and thoroughly for digital evidence and related material. To increase investigative efficiency, areas should be targeted and prioritized according to how likely digital evidence may be found and the amount of digital data that may be recovered.

#### 4.3.1 Prioritization

In general, a Computer Forensics specialist conducting an investigation and will be pressed to complete his/her tasks as efficiently, as effectively and as quickly as possible both to quickly preserve vital evidence held on employees' or other parties' computers, devices, etc. and to minimize disruption to workplaces, businesses, etc.

Yet locating digital evidence from huge stores of data – that may be terabytes in size -- can be time consuming, disruptive, and costly.

Moreover, extracting data from computers in ways that reliably preserve evidence is not a simple undertaking, as data can easily be altered either intentionally or accidentally.

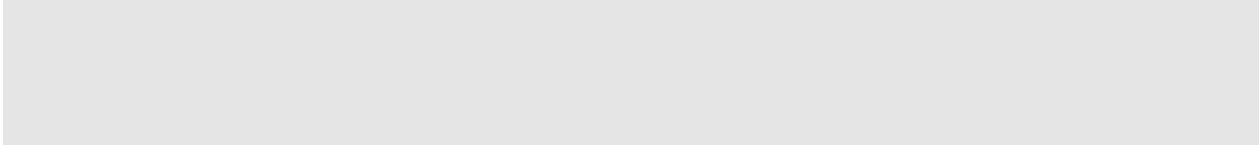
Therefore in conducting an examination for digital evidence, prioritizing the deployment of resources is critical.

Yet prioritization of activities is not easy, as the following must be considered before any activities are initiated:

- The urgencies and priorities
- The nature of the case
- Time constraints
- The other types of forensic examination that may have to be carried out on the same items (e.g. fingerprint analysis)
- The items that have the potential to provide the most information in response to the various propositions
- The items offering the best choice of target data, in terms of evidential value.

After an assessment of the relevant requirements, examination activities should be assigned to the appropriate qualified individual(s).





*Section 4: Gathering Evidence*



## 5. General guidelines

---

### What to do at the scene: General Guidelines

#### Collect evidence:

- All related evidence taken out of RAM

#### Shut off computer?

##### WHEN IN DOUBT:

- Leave system plugged in
- Unplug network cable
- Unplug modem
- When in doubt contact Computer Forensics specialists

#### Boot up with an OS that:

- Bypasses the existing OS
- Does not change data on hard drive

#### Make copies

---

When gathering digital evidence, four general principles apply:

1. All related evidence should be gathered including data from RAM, printouts, notes, etc. (See Appendix 2 of a list of potential data sources)
2. Leave the computer plugged in but if possible unplug modem, network or other communications links.<sup>2</sup>
  - *For those who are not computer forensics specialists, the ISFS recommends that when in doubt a computer forensics specialists should be consulted*
3. If the computer has been shut down, the subject system should be re-booted using another operating system that bypasses the existing one but does not change data in the hard drive
4. Copies of the digital evidence on the hard drive should be made.

Finally it goes without saying that examiners must follow the law!

---

<sup>1</sup>Generally speaking, the subject computer or device should be shut down (however, there may be circumstances that require that this not be done for example if it is clear that data is being deleted as part of an automated process).

## 5.1 What to collect and from where?

The first task is to gather as much evidence as possible in a systematic manner.

This involves the identification, retrieval, preservation and analysis of electronic data, usually to support an investigation or litigation.

During the collection of this evidence several questions are relevant:

- What relevant electronic and hard copy records exist?
- Where is the information located?
- What systems, media, smart cards or devices contain relevant data?
- Have appropriate preservation steps been taken to avoid overwriting data?
- Do backups exist, and if so, how and where are they maintained (e.g., tape, optical drives, on-site, off-site)?
- What (forensically recoverable) electronic logs and other "digital fingerprints" exist?
- Is the review of electronic data being done in an independent manner so as not to compromise the evidentiary value of the material?

### 5.1.1 How much to collect?

It is up to the judgment and discretion of the Computer Forensics specialist whether to copy all or just part of the data.

Again, as the list of potential sources may be very long it may be helpful for the Computer Forensics specialist to employ a checklist to ensure that nothing is overlooked. (See Appendix 2 of a list of potential data sources)

## 5.2 Collection considerations:

*It is vital* that all items collected during a forensic examination be preserved securely as soon as possible following appropriate jurisdictional practices. (Sources of data and examination will be covered in the following sections)

As noted previously, precautions should take adequate precautions to preserve evidence and materials from external factors such as electrical hazards, magnetic fields or static.

### 5.2.1 Evidence at all layers, from all places

---

#### **Digital evidence on the Internet:**

- OSI Model:
  - Application Layer
  - Presentation Layer
  - Session Layer
  - Transport Layer
  - Network Layer
  - Data-link Layer
  - Physical Layer

#### **Collecting and preserving hardware and digital evidence:**

- Copying everything or just the information needed?
    - Bit stream copies?
    - Two copies – empirical law of digital evidence collection and preservation
  - Evidence in RAM
  - Computer to be shut down? Discretionary
  - Booby Traps
    - Boot up using another OS to bypass the existing one
  - A copy of the digital evidence from the hard drive should be made
- 

In gathering evidence, *all sources* of data must be considered including RAM, devices, peripherals, non-printing information, etc. (refer to Appendix 2).

The Computer Forensics specialist must capture logs before they disappear because these logs may contain valuable information such as the time a document was created, the last time it was opened and the last time it was changed.

As most investigations may involve systems that are connected to networks, either in a local area network or through a direct connection to the Internet, data from applications, network programs, etc. must be collected.

In collecting evidence from networks, Computer Forensics specialists should keep the OSI Seven Layer network model in mind to ensure that no layer is overlooked.

#### **5.2.1.1 Booby Traps**

As a system might be booby trapped (e.g. the system may be programmed to erase data if someone attempts to re-boot it) the Computer Forensics specialist must be prepared for this contingency and take all necessary precautions.

## 5.3 Documentation of hardware and evidence

### 5.3.1 The importance of documentation

---

#### Shows evidence in original state to demonstrate authenticity and integrity

#### Documentation may help distinguish:

- Copies and originals
- Multiple systems from each other

#### Useful in reconstructing crime

---

As soon as the investigation starts, all activities must be fully documented. This documentation must contain the location and/or source of the original evidence, a log of actions taken, notes (such as aliases used by a suspect, Internet acquaintances), etc.

There are four reasons why such exacting documentation is necessary:

1. Documentation showing evidence in its original state can demonstrate that it is *authentic and unaltered*
2. As copies and originals are difficult to tell apart, documentation may be necessary to differentiate between copies and originals
3. In situations where several identical computers with identical configurations exist, documentation is critical in distinguishing between systems
4. Documentation the original location of evidence may be useful in reconstructing a crime

As a standard practice, everything should be documented as thoroughly as possible. Even cables should be individually labeled, as they are unplugged from a computer.

---

**Digital evidence guidelines:**

- Documentation of hardware and digital evidence:
    - Document the location/source of the source of the original evidence
      - Where the evidence was collected and from whom
      - Label cables
    - Photograph, videotape, capture screens, log or print the digital evidence
    - Keep a log record of actions taken
    - Calculate the message digest
    - Keep:
      - A list of possible aliases
      - Internet acquaintances
  - Hardware
    - Serial Numbers and other details
  - Media
    - Current date and time
    - Computer date and time (note discrepancies from actual date and time)
    - Person making copies
    - Program(s) / Command(s) used
    - Information believe to be contained in the media
    - List of files and properties
- 

### 5.3.2 Documentation Guidelines

#### 5.3.2.1 Hardware

When documenting hardware, serial numbers and other details should be noted.

All cables and attached peripherals must be labeled.

#### 5.3.2.2. Labeling of copied files

When evidence is copied onto another media, the media containing the copied files should be labeled to include the following information:

- Current data and time and the date/time on the computer (or device).
  - Any discrepancies between the date and time in the computer and actual date and time must be noted.
- The person making the copy
- The operating system
- The program(s) or command(s) used to copy the file

- Information believed to be contained on the files

### 5.3.2.3 Photo Documentation

In addition Computer Forensics specialists should photograph the scene including the computer, connections, screen shots, etc., -- preferably using film-based cameras.

A list of all files and their properties should be made and as a further integrity check message digests should be calculated using an appropriate hash algorithm.

### 5.3.2.4 Level of detail

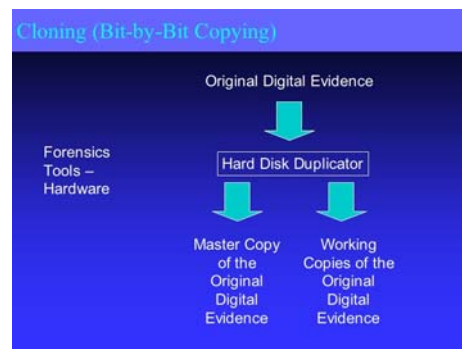
The exact requirements for recording casework information will depend on organizational policy and requirements. As a minimum, however, the records should be in sufficient detail to allow another Computer Forensics specialist, competent in the same area of expertise, to identify what has been done and assess the findings independently.

Case records should include both administrative and examination documentation. Whenever appropriate standardized forms should be used to document examinations.

### 5.3.3 Back up

Finally, documents should be backed up in case an original file is lost or destroyed.

## 5.4 Data Copies



---

**Chain of custody****Reconstruction****Which is the original?**

- No change or alteration

**Message digest and digital signature (MD5, SHA1) >>> Individualization**

---

**5.4.1 Bit by bit mirror Imaging**

*Computer Forensics examiners do not work with original data, rather they create working copies through a bit-by-bit mirror imaging of the original data. This bit-by-bit imaging is important as it ensures that all data, including residual, slack, etc. is included in the copy.*

**5.4.2 Write protection and virus checks**

After having obtained the data, the Computer Forensics specialist must maintain the integrity of the media received. The two key steps in doing this are write protection and virus checking.

- Write protecting prevents data from being added to the media, guaranteeing that the evidence gathered is not altered or erased while it is being worked on.
- Similarly, virus checking prevents evidence from being altered and is the second thing a Computer Forensics specialist should do with all media.

*A Computer Forensics specialist should create at least two working copies of data and make sure that he/she can track individual files and documents back to their original source.*

**5.5 Preserve the chain of custody.**

Finally, a chain of custody that tracks evidence from its original source to what is offered as evidence in court *must be preserved.*

**5.5.1 Evidence Handling**

Where practical, items should be examined in the laboratory or forensic workspace rather than at the scene.

The transportation of seized computers; peripherals and media must be done carefully to avoid heat damage or jostling.

**5.5.2 Packaging, Labeling and Documentation**



A record should be made, at the time that items are seized from the scene, from the suspect(s) or victim(s) that describes the exact locations where the items were recovered. The Computer Forensics specialist may mark the locations on a sketch/plan of the scene.

Organizational policy governing the handling of evidence and security must be followed

Evidence should be properly packaged and sealed when seized.

Each package should be labeled at the time of seizure. Such labeling should feature:

- A unique identifying mark;
- The name of the person and organization responsible for collecting and packaging the material
- Some description of the material (e.g. laptop computer, serial numbers)
- The location from where and from whom the material has been seized;
- The date and time the material was seized.

Where recovery of items for examination is not practical, the digital evidence may have to be copied at the scene according to standard operating procedures

### 5.5.3 Receivers

Those receiving items for forensic examination should first review all items for the integrity of their packaging.

■ *Any deficiency in the packaging should be noted and documented.*

## 6. First responder considerations

The first person at the scene of a suspected computer crime (i.e. the First Responder) has a duty to preserve as much evidence as possible for subsequent examination.

This means that whoever get to the scene first must recognize that relevant evidence may be found on all sorts of devices (computers, PDAs, mobile phones, as well as in the RAM of fax/voice/ modems), media (systems, media, smart card, etc) and even hard copy.

### 6.1 General rules for specific devices

While most of what had been described in the previous section applies to computers and digital devices in general, other devices require additional consideration<sup>iii</sup>.

- 
- *ON or OFF? Whether a device should be left on or off is a decision that should be left to law enforcement or professional computer forensics examiners*
  - *Any questions regarding electronic equipment at the scene, should be directed to a computer forensic examiner as soon as possible*
  - *In all cases, follow the law!*
- 

#### 6.1.0 Volatile memories

Computer forensics professionals who work with equipment with volatile memories should have a system in place for the systematic replacement of batteries should such need arise.

#### 6.1.1 Mobile Telephones

When dealing with a mobile telephone:

- First, do not try to access the device.
- Record any information located on the screen of the device (write or photograph).
- If the owner of the phone (i.e. the subject) is on hand, briefly ask him/her for any PIN or personal code numbers. Otherwise, look around the area for any PIN or related code numbers.
- Do not let the subject touch the device for ANY reason
- Thoroughly document what has been done

If possible the type (brand, model, etc.) of mobile phone involved.

##### 6.1.1.1 Additional consideration for computer forensics professionals

If the first responder happens to be a computer forensics professional, he/she has the added duties of:

- Properly identifying the type of mobile phone (as well as being familiar with current mobile phones, batteries and accessories)
- Properly labeling, storing, handling and transporting the device so no damage occurs.

- In addition, if the item need to be tested for fingerprints or DNA appropriate handling and evidence packaging procedures must be applied
- Taking the evidence to the appropriate lab for examination as soon as possible particularly as evidence may be lost when the battery dies.

#### 6.1.1.1.1 Special Considerations

Computer forensics professionals should look out for:

- Any SMART/SIM cards at the scene
- Batteries
- Power supplies
- Cables
- Operators manuals
- Software and
- Packaging

Finally, computer forensics professionals must be aware of potential links between computers and mobile phones *as any computer in the area may have synchronized information also contained on the device.*

### 6.1.2 Electronic Paging Devices

When dealing with a paging device (e.g. a ‘Blackberry’) the rules are the similar to those that apply to a mobile phone:

- First, do not try to access the device.
- Record any information located on the screen of the device (write or photograph).
- Do not let the subject touch the device for ANY reason
- Thoroughly document what has been done

If possible, identify the paging device (i.e. make, model) involved.

#### 6.1.2.1 Additional consideration for computer forensics professionals

If the first responder happens to be a computer forensics professional, he/she has the added duties of:

- Properly identifying the type of paging device (as well as being familiar with current pagers, batteries and accessories)
- Properly labeling, storing, handling and transporting the device so no damage occurs
  - In addition, if the item need to be tested for fingerprints or DNA appropriate handling and evidence packaging procedures must be applied
- Taking the evidence to the appropriate lab for examination as soon as possible particularly as evidence may be lost when the battery dies.

The paging company should be identified as soon as possible so that the pager records can be held.

#### 6.1.2.1.1 Special Considerations

Computer forensics professionals should look out for:

- Batteries
- Chargers
- Cables
- Operators manuals
- Software and
- Packaging

### 6.1.3 PDAs / Personal Digital Organizers / Handheld Computers

When dealing with a PDA (e.g. a Palm), Personal Digital Organizer, Handheld computer or other similar device), the rules are the similar to those that apply to a mobile phone and pager:

- First, do not try to access the device.
- Record any information located on the screen of the device (write or photograph).
- If the owner of the PDA (i.e. the subject) is around, ask the subject for any passwords, personal code numbers and type of operating system used. Otherwise, look around the area for any passwords or related code numbers.
- Do not let the subject touch the device for ANY reason
- Thoroughly document what has been done

If possible, identify the device (i.e. make, model) involved.

#### 6.1.3.1 Additional consideration for computer forensics professionals

If the first responder happens to be a computer forensics professional, he/she has the added duties of:

- Properly identifying the type of PDAs, handheld computers, personal data organizers (as well as being familiar with current such devices, batteries and accessories)
- Properly labeling, storing, handling and transporting the device so no damage occurs
  - In addition, if the item need to be tested for fingerprints or DNA appropriate handling and evidence packaging procedures must be applied
- Taking the evidence to the appropriate lab for examination as soon as possible particularly as evidence may be lost when the battery dies.

#### 6.1.3.1.1 Special Considerations

Computer forensics professionals should look out for:

- Any associated devices (extended memory or expansion cards) at the scene
- Batteries
- Docking stations
- Power supplies

- Cables
- Operators manuals
- Software and
- Packaging

Finally, computer forensics professionals must be aware of potential links between computers and such handheld devices *as any computer in the area may have synchronized information also contained on the device.*

#### 6.1.4 Smart Cards

Smart cards, like PDAs or mobile phones, have operating systems and memories and should be treated accordingly.

When dealing with smart cards, the first rules are:

- Do not try to access the device.
- If the smart card is connected to a computer, record any information located on the screen (write or photograph).
- Record any information located on the screen of the device (write or photograph).
- If the owner of the smart card (i.e. the subject) is around, ask the subject for any passwords and personal code numbers. Otherwise, look around the area for any passwords or related code numbers.
- Do not let the subject touch the device for ANY reason
- Thoroughly document what has been done

---

*If the smart card is connected to a reader/encoder or a computer contact a forensic examiner for advice.*

Any questions regarding this electronic equipment at the scene should be directed to a computer forensic examiner as soon as possible.

---

##### 6.1.4.1 Additional consideration for computer forensics professionals

If the first responder happens to be a computer forensics professional, he/she has the added duties of:

- Properly identifying the type of smart cards, accessories and readers/encoders (as well as being familiar with current smart cards, readers/encoders and accessories)
- Properly labeling, storing, handling and transporting the device so no damage occurs
  - In addition, if the item need to be tested for fingerprints or DNA appropriate handling and evidence packaging procedures must be applied
- Taking the evidence to the appropriate lab for examination as soon as possible

##### 6.1.4.1.1 Special Considerations

Computer forensics professionals should look out for:

- Any associated devices (computers, readers/encoders) or other cards at the scene
- Readers
- Encoders
- Cables
- Power supplies
- Operators manuals
- Software and
- Packaging

Finally, computer forensics professionals must be aware of potential links between computers and smart cards *as any computer in the area may have synchronized information also contained on the device.*

### 6.1.5 Digital and Audio Systems

New technologies may make it possible to determine someone's activity from the audit of history files on devices such as interactive television systems. (For a more complete list of potential sources of digital image, audio or video evidence refer to Appendix 2)

In dealing with evidence on a digital image, video or audio system, a first responder's duty is to:

- Do no harm
- Preserve the most fragile evidence – both physical and evidence
- Prevent others from tampering with the device

First responders must be aware that image processing methods can alter images or other evidence

Therefore, when dealing with such devices, the first rules are:

- Do not try to access the device.
- Determine if the devices are active (if so, see below)
- Record any information located on the screen of the device (write or photograph).
- Record any information located on the screen of the device (write or photograph).
- If the owner of the smart card (i.e. the subject) is around, ask the subject for any passwords and personal code numbers. Otherwise, look around the area for any passwords or related code numbers.
- Do not let the subject touch the device for ANY reason.
- Thoroughly document what has been done including whether a device connected to the main power source or the battery.

If possible, identify the device(s) (i.e. make, model) involved.

#### 6.1.5.1 Devices that are active

Considerations must be given to whether objects should be switched off, or maintained in their present state in order to preserve the best evidence.

As with all electronic devices and media, sources of digital audio, image and video evidence are sensitive to physical shock [dropping], water, magnetism and electrostatic discharge, and should be as

far as possible, protected from these extremes. Objects and media should be placed in containers designed where possible to exclude this damage.

Objects and media should be secured so that no accidental access or tampering can occur. Any storage medium should not allow the device to be viewed and manipulated through the container. Special handling may also be required to preserve traditional forensic evidence (e.g. fingerprints).

#### **6.1.5.2 Additional consideration for computer forensics professionals**

If the first responder happens to be a computer forensics professional, he/she must be aware that information can get lost when digitizing analog audio and video material. I.e. The number of lines might be altered, frames in the video may be skipped, etc. Furthermore the quality of the audio and video might degrade when digitizing.

The computer forensics professional has the added duties of:

- Properly identifying the type of devices (as well as being familiar with current such devices and accessories)
- Ascertaining who had access of a device
- Recording the location of the devices, drawing a layout if necessary
- Locating all potential media on which such evidence could be stored (e.g. DVDs, CD ROMs, etc)
- Checking the status and condition of the media
- Identifying the format of the audio and video evidence (e.g. Compression standard, file formats, NTSC, PAL, SECAM).
- Making a digital copy of the part for investigation and compute a hash code (if possible)
- Properly labeling, storing, handling and transporting the device so no damage occurs
  - In addition, if the item need to be tested for fingerprints or DNA appropriate handling and evidence packaging procedures must be applied
- Taking the evidence to the appropriate lab for examination as soon as possible particularly as evidence may be lost when the battery dies.

If possible, the forensics professional should obtain evidence (i.e. copy the image, video or audio data) directly at the scene of crime, making a digital copy of the part for investigation and computing a hash code (if possible) while keeping in mind that information can get lost when digitizing analog audio and video material (e.g. the number of lines might be altered, frames in a video may be skipped or the quality of the audio and video might degrade when digitizing).

He/she must also be aware of tape material that could have been installed backwards (i.e. back to front) for the purpose of deception and that distribution of certain kinds of images (child pornography) is illegal (this is something to be noted in a report).

*6.1.5.2.1 Special Considerations*

Computer forensics professionals should also:

- Remove external communication connections to prevent potential deletion from an outside location
- Note any other relevant information about the camera or/and the recorders
- Record the system time and compare this to the real time
- Note the recording parameters such as recording intervals, recording speeds, etc.



## 7. Evidence Handling

### 7.1 Receiving Digital Evidence

As noted previously, those receiving items for forensic examination should first review all items for the integrity of their packaging. Any deficiency in the packaging should be noted and documented.

#### 7.1.1 Additional considerations for Mobile Telephones, Smart Cards, PDAs, Handheld computers, Pagers, Smart Cards, Personal Data Organizers

When dealing with:

- Mobile Telephones,
- Smart Cards
- PDAs
- Handheld computers
- Pagers
- Smart Cards
- Personal Data Organizers

the computer forensics professional should not only follow normal handling procedures for forensic evidence but also check the power and battery status upon receipt of such devices (where this applies) and should also be familiar with the device he/she is working on. He/she should check with the first responder or investigator for passwords, codes, etc. where relevant.

He/she also must be cognizant of other forensic procedures (fingerprinting, DNA) and know his/her limitations.

Most importantly, the computer forensics professional must alert to the fact that some devices may affect data on other devices.

### 7.2 Reconstruction and Reporting

---

#### Classification, comparison and individualism of digital evidence:

- Classify
  - Graphical files (e.g. JPEG, TIFF, GIF, etc.)
  - E-mails (by the applications used to create them)
- Compare characteristics with others
- Content, function and characteristics
  - Check:
    - Cookies
    - Cache
    - Temp files
    - Etc.

**Digital evidence and reconstruction:**

- Reconstructing deleted, damaged hidden and encrypted evidence
  - System specialists
    - Reconstruction of the incident (relational, functional, temporal)
  - Forensics specialists
- 

Once working copies of the evidence have been made, the Computer Forensics specialist will proceed to examine the systems and data in question in order to:

1. Reconstruct deleted or damaged files,
2. Build a timeline of events, and
3. Assess relationships between data if any.

Standard operating procedures should be followed during such examination.

Any anti-contamination precautions or requirements relevant to this case (e.g. guarding against the presence of booby traps, etc.) must be considered *before* any examination proceeds, with appropriate precautions identified and implemented.

In situations where equipment has been physically seized, computers and peripherals may be reassembled in the laboratory, using photographs of the equipment in place before its removal, or labels on wires.

From here Computer Forensics specialists analyze the data collected searching across a wide range of areas inside a computer, including e-mail, temporary files, swap fields that hold data temporarily, logical file structures, slack and free space on the hard drive, software settings, script files that perform pre-set activities, Web browser data caches, bookmarks and history and session logs that record patterns of usage -- sometimes at the bit level.

Computer Forensics specialists will then attempt to reconstruct files, locate and reveal hidden files (e.g. files hidden with steganographic tools) and look for evidence in the subject system that tells them what is in the encrypted file rather than attempt to decode encrypted files.

### 7.2.1 Classification

Files should be classified according to type. Such classification is important because it provides additional, reliable details that may in turn lead to additional evidence.

Furthermore, the identification and classification of files that are already known to be safe (such as certain operating system files) can help save time during an investigation by eliminating the need for an investigator to examine these files.

#### 7.2.1.2 Trustworthy and Untrustworthy

During an examination, Computer Forensics specialists must bear in mind that as a suspect might have corrupted all of the operating system, applications and communications in a subject system or that the software itself might erase evidence while operating, *only the physical level of magnetic materials where the 1s and 0s of data are recorded is real, and everything else is untrustworthy.*

---

### Digital evidence and reconstruction

- Relational – how one object is related to another: Correlation
- Functional – how one object is used to achieve the results, process
- Temporal – events related to the timeline

### Two common pitfalls in reconstruction of an event:

- Media influence
  - Excessive dependence on digital evidence
- 

### 7.2.2 Handling of Mobile phones, pagers, PDAs, Smart Cards, etc.

When dealing with mobile phones, pagers, PDAs, handheld computers, smart cards, personal data organizers, etc., the computer forensics professional should follow all the steps involved in the examination of any other form of digital data. That is, he/she must fully describe devices and associated items, document thoroughly, and examine the device using validated forensics tools and accepted forensics procedures using methods that minimize any loss or alteration of data.

In particular, the computer forensics professional should use validated software and be able to explain, for example to a court, what kind of image and sound-processing methods have been used.

## 7.3 Reconstruction

After analyzing the evidence, Computer Forensics specialists then attempt to reconstruct the case correlating evidence to activities and sources considering, if necessary, background information and other evidence (notes, photographs, etc.) during the evaluation and interpretation of the case findings.

All data or records that were generated during the course of the examination supporting the findings must be kept.

### 7.3.1 Final Report

The final report must provide the reader with *all the relevant information* in a clear, concise, structured and unambiguous manner.

Descriptions should be made in plain language avoiding technical jargon wherever possible and the report should contain factual findings. It also may include interpretation and expert opinion with all expert opinion and interpretation *clearly identified* in the report.

If the report is to be used in litigation, the style and content of written reports must meet the requirements of the criminal justice system.

## 7.4 Case File Review

All work undertaken should be subjected to both a Technical Review and an Administrative review.

The Technical review should consider:

- The validity of all the critical examination findings and all the raw data used in preparation of the statement/report
- Whether the conclusions drawn are justified by the work done and the information available or
- If circumstances warrant additional independent testing

A written record of the technical review should be made and retained with the case records.

The Administrative review should be performed to ensure that the requesters' needs are properly addressed, that policies are properly adhered to and that the report document meets appropriate editorial standards.

## *Section 5: Considerations of Law*

## 8. Considerations of law

*NOTE: This document, this section in particular, is not intended to offer legal advice. For matters of law, the ISFS recommends that readers seek proper qualified legal counsel in the relevant jurisdiction(s).*

Why are all these careful, methodical processes necessary? Why is all this effort directed at locating and reconstructing digital evidence needed?

### 8.1 General principles

While there can be no doubt that evidence is required in order to prosecute a computer criminal, as we have seen, obtaining reliable evidence may not be easy. What's more, the evidence must also be admissible in court.

#### 8.1.1. Authenticity

For evidence to be admissible it must be authentic and this means that the:

- Records must not be altered, manipulated or damaged after they were created
- Software programs generating the records must be reliable

In general, the identity of the author(s) of the electronically stored records should be properly established (for a more thorough discussion of the legal reasons for this, refer to 'Evidence Considerations' below and Appendix 3).

Therefore to protect the integrity of the records and defend against attacks by an opposing counsel questioning the authenticity of the evidence, Computer Forensics specialists must take care to ensure that records are not damaged or changed in any way and that analysis is done carefully and methodically.

Another consideration is Best Evidence.

#### 8.1.2 Best Evidence

If information generated by a computing device is a 'document' then the best evidence rule, that traditionally required the person producing a document to produce the original of the document in order to prove its contents, or otherwise give a satisfactory explanation of why the original cannot be adduced and an accurate copy is being relied upon, applies.

But with modern computing systems that can store and produce vast amounts of physical material, this rule is impractical to implement. Furthermore, in the digital world, there may be no difference between the original document, a copy of the document and a hard copy print out in terms of accuracy.

### 8.2 Electronic Records as Admissible Evidence

Fortunately, Hong Kong law provides a solution.

Under Section 9 of Hong Kong's Electronic Transactions Ordinance, an electronic record cannot be denied admissibility as legal evidence on 'the sole ground that it is an electronic record.'<sup>3</sup>

In addition, Section 5 of the Electronic Transactions Ordinance also provides that if information must be given in writing, an electronic record can suffice as long as the information contained in the record is accessible (so as to be usable for subsequent references).

(Please refer to Appendix 3 which provides a more thorough discussion of evidence and Appendix 4 which contains the relevant sections of the Electronic Transactions Ordinance as well as additional sections of the ordinance pertaining to digital signatures and retention of records)

### **8.3. Evidence Considerations in Hong Kong**

From an evidentiary standpoint, the reliability (and thus probative value) of digital records will depend on:

- a. How the information is stored, preserved and retrieved
- b. How the information is supplied in the course of normal activities
- c. How well the device is protected from undue interference or whether it was working properly.

Therefore as the strength of the digital evidence is dependent on the procedures used to create the record as well as the safeguards used to preserve this data or the operational integrity of the device, it is imperative that Computer Forensics specialists undertake such careful processes to preserve evidence, maintain chains of custody and extract file data such as the time of creation or whether data had been deliberately tampered with.

The above applies to both criminal and civil prosecution though in the former situation, the rules of evidence are stricter. (See Appendix 3)

---

<sup>3</sup> However, the evidence may be challenged on other grounds, for example as 'hearsay' but this discussion is beyond the scope of this document

## *Appendices*



## Appendix 1: Sample Statement of Findings

### Statement of Findings

**Date:**

**Name:**

**Current Position:**

**Current Organization;**

**Current Work Experience:**

**Previous Work Experience** (related to IT and/or Computer Forensics):

**Academic or other Professional Qualifications:**

**Case Background:**

(e.g. purpose, objectives, date/time/location, and any other relevant preparatory work related to the computer forensics examination)

**Actions done at the scene:** (if any)

**Search, Seizure, and Packaging of Computer Exhibits, etc.:** (if any)

**Scope of the Examination**

**Examination Process:**

(Physical check, System Check, Cloning, Searching, Analyzing, etc., if any)

**Summary of Findings:**

**Conclusions:**

## Appendix 2: Sources of Data

The following is *not intended to be a comprehensive list of sources of information or data* but rather an extensive list of potential sources or evidence that may be overlooked in an investigation.

Examiners must also remember that documents that may not be available from the original electronic source by normal search techniques may be located from other sources in electronic form or in hard copy. Documents that have been deleted from one database or memory may be retained on other hardware or in storage media or may be recovered in whole or part.

- Access control devices
- Access records to buildings and rooms
- Acknowledgment of receipt of email
- Audit trails
- Automatic backup copies: created & saved by OS to provide backup in case of emergencies
- Backup tapes, diskettes, email storage
- Bookmarks or favorites indicate web sites frequently visited
- Browser information
- Buffer memory in fax machines, printers, digital copiers
- Buffer memory in fax, printer, voice mail
- Cable connections
- Cache
- CDs
- Cell phone records of calls and locations of callers
- Commands: particularly copy, print or purge
- Computer bulletin boards
- Contact Lists
- Cookies
- Copies of documents or drafts created by the operating system without the user's knowledge
- Copy machines
- Corporate intranets: manuals, employee suggestions
- Credit card and banking records showing transactions and locations
- Data bases
- Deleted files that can be recovered from the hard drive or other storage
- Deletions undeleted until overwritten after indefinite period
- Digital cameras
- Digital evidence on the Internet

Areas that would attract the suspect

Check:

- E-mail address
- Name
- Newsgroups
- Nickname
- Search engines
- Usenet archives

[www.dejanews.com](http://www.dejanews.com)

- Directories that may show content of information though information was erased

- Discarded, "damaged" hard drives and floppies with recoverable information
- Diskettes, floppies
- Dissemination logs to track persons who access sensitive data & reports
- Distribution lists may reveal sources of information, potential witnesses, repository or documents
- Documentation
- Dongles
- Downloads --- when, who, where
- EDI [Electronic Data Interchange] audit trails of business purchases through VAN [value added network]
- Edit history [e.g. date, time and person accessing network or document] and
- Electronic calendars etc.
- Electronic forms of documents at variance to or in lieu of hard copy
- Email header: communication trail, and information re creation, recipients, transmittal & receipt times
- E-mail sent and received
- Email text and attachment of documents otherwise unavailable
- Email threads provide context and informality; message numbers; connections, replies, activity logs,
- Embedded information created without user's knowledge; does not appear in printed documents:
- Employer software to monitor activities of employee: email, files, web sites
- Employer software to record activities of employees, audit trails and computer logs
- Evidence of destruction, back dating or variations from retention policy
- Evidence of other documents or activity from e.g. email headers
- Evidence of atypical, systematic destruction as evidence of a possible cover-up
- Fax text and related information [sender, date, time]
- File clones on hard drive, servers, home computers, email attachments etc.
- File fragments in slack space not overwritten with new data after "deletion"
- File fragments: only part of deleted file overwritten; slack space
- File header information: date creator, who worked on file and when
- File modifications, by who, when
- Files accessed: who, where, when & for how long
- Fingerprint scanners
- Firewall logs
- Flash memory cards
- GPS tracking of rental cars and trucks
- Grocery or other store discount cards
- Hidden comments [may explain changes, authenticate documents]
- Hidden Comments in inserts, headers or footers that don't appear on hard copy
- Hidden comments to co-workers
- History of time or date of sites visited
- Home computers
- Information generated by application or OS on PC or network;
- Information remnants when deletion or overwriting is incomplete
- Instant Messaging
- Internet Chat, ICQ
- Intrusion Detection Systems
- IP Addresses
- Jazz and zip drive backups
- LAN with document saved on server and PC or only one

- Laptops
- Magnetic tapes
- Metadata
- Mobile telephone handsets
- Modem
- Multiple Memory: PC, email, voice mail, multiple servers, ISP, VAN, VPN
- Name date & time of creation, review, access or modification
- Network and PC operating systems
- Network Data on the Host
- Network interface card (MAC Address)
- News servers
- Non-printing information
- Notebook computers
- Obsolete information not deleted from computers or backup tapes
- Operating System Logs
- Original document backup
- Pagers
- PDA, palmtops, electronic calendars
- Personal data assistants, laptops, personal computers
- Physical notepads
- Portable hard drives
- Postings on Internet newsgroups or bulletin boards
- Printer spool files
- Printers
- Printouts
- Prior versions, drafts etc. on backup tapes, diskettes, home computers
- Programs used
- Proliferation of copies; email to group; to entire organization + forwarded copies
- Proxy servers
- RAM
- Relationship/arrangement of files may indicate authenticity [dates w/in]
- Remote access logs
- Residual data
- Recycle Bin
- Routers
- Screen shots
- Servers that may retain copies: networks, VAN, ISP, VPN
- Slack space
- Smart cards
- Structures of tables and records
- Surveillance cameras and web cameras everywhere
- Swap files
- Telephone records
- Temp files
- Temporary files, automatic backup of drafts
- Timed document backup

- Toll booth records showing presence and speeds
- Trash bin
- Undelete or salvage commands in OS or special program
- Undo and redo features of word processing application
- Undo feature on software may reveal important revisions of documents
- Unknown copies, file remnants, versions, drafts or portions of documents
- Versions of documents from collaborative efforts
- Video cameras
- Voice mail & voice mail backup, forwarding
- Web site log files re visitors [date & time of access and Internet address; prior web sites]
- Web sites visited, date & how long

#### **Audio Devices**

- Answering machines
- Audio files stored on mp3 players
- Dictaphones
- Memory sticks
- Mobile telephones
- On videos
- Recorders
- Telephone systems
- Voice over IP – computers
- Also
  - Fax/voice/ modems -
  - PDA/personal organizer

#### **Video devices / Sources of digital image data**

- Digital still cameras
- CD-ROM/DVD
- Flash Memory
- Floppy disks
- GPS-systems
- Image files stored on mp3 players
- Media
- Memory Sticks
- Public door access
- Surveillance cameras
- Video conferencing systems –standalone or PC based
- Web cameras

#### **Applications, Users and Home Computers**


In addition, there are sources of data from applications. For instance, transaction or accounting data extracted from an organization's general ledger application can be applied in a damages claim or an accounting investigation.

Users and witness may also provide useful information of may lead to sources of information.

Perhaps the most overlooked source of electronic evidence is the home computer. Data usually ends up on these machines in one of two ways: First, it can be transferred to and from the workplace on diskettes or other portable media; second, an employee may be able to log on to the company network from home. In this latter situation, the home computer acts just like the employee's office workstation.

**Written Policies and Documents**

There are also documents that may offer valuable information including:

- Systems Operation manuals
  - Access control lists
  - Audit trails & computer logs to show who actually accessed, when, for how long etc.
  - Security policies, hacking experience, intrusion software used
  - Encryption programs & passwords: may assist access and authentication
  - Revocation of passwords and access codes
  - Policies re employee use, privacy, retention, copies of files
- 

## Appendix 3: Additional Evidence Considerations

*NOTE: This document, this section in particular, is not intended to offer legal advice. For matters of law, the ISFS recommends that readers seek proper qualified legal counsel in the relevant jurisdiction(s).*

### Appendix 3.1 Data categories

Generally speaking, digital data may be stored either on an ad hoc basis or as part of a process.

#### Appendix 3.1.1 Ad Hoc Data

For instance, a father may take a photograph of his children with his digital camera and store the image on his computer. This would be an example of the former (i.e. a digital file being stored on an ad hoc basis) and is circumstantial in nature.

In court this evidence would be admissible on the basis that it was ‘a picture was found on the man’s computer’ However, to prove the event depicted in the picture actually occurred would require testimony - for example, if the picture showed children at a park on a particular day and time the father might need to testify that his children were indeed at the park on that day and time.

#### Appendix 3.1.2 Data kept as part of a process

On the other hand, a library may use a computer as part of its lending process. For example, if a person borrows a book, the librarian may scan in the information from the bar code attached to the book into a computer, which would then make a digital record of the transactions (i.e. That John Lee took out Book ABC on a particular date).

At some future date, the information can be retrieved for other purposes, for example to check whether John Lee has any overdue books.

Notice that in the second example the record is kept as part of a regular process. In this case it would be difficult, though not impossible for the librarian to recall that he/she gave out a particular book on a particular date to a particular person.

In this second situation, unless:

- The integrity of the process can be successfully challenged (for example, the Librarian gives specific testimony about the accuracy or validity of a particular record)
- It can be shown that the computer had been tampered with, was not working properly, or was not sufficiently protected from undue interference

the computer would be presumed to be working properly, the data is presumed to be reliable therefore the record(s) is/are admissible as evidence; for example, to show that John Lee took out Book ABC on a particular date by the production of that computer record. (Whether evidence is classified as ‘real’ or ‘hearsay’ is relevant in criminal prosecution as hearsay evidence is not admissible in criminal trials).

### Appendix 3.2 Admissibility of Digital Evidence

As noted earlier, Hong Kong law permits the use of electronic records as evidence.

### Appendix 3.2.1 Criminal Proceedings

Under Section 22A of Hong Kong's Evidence Ordinance, information contained in a computer can be admitted as prima facie evidence of that information in a criminal proceeding if certain conditions are met (See Appendix 5).

The strength of the evidence is dependent on its historical significance (Sec. 22B (1) (A) of the Evidence Ordinance states: *In estimating the weight, if any, to be attached to a statement admitted in evidence by virtue of section 22 or 22A, regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the statement and, in particular.....the record containing the statement was compiled did so **contemporaneously** with the occurrence or existence of the facts dealt with in that information) and whether the person 'concerned with the supply of information to that computer, or with the operation of that computer or any equipment by means of which the document containing the statement was produced by it, had any incentive to conceal or misrepresent the facts'*

Moreover, in criminal proceedings, the Computer Forensics specialist would take extra care to ensure data is properly handled so as to avoid it later being dismissed (as hearsay evidence)

### Appendix 3.2.2 Civil Proceedings

For civil proceedings, the rules of evidence are slightly more relaxed than for criminal cases (notably in that hearsay evidence is admissible -- hearsay evidence is not admissible in criminal proceedings under Hong Kong law)).

#### Appendix 3.2.2.1 Evidence types

To better understand this distinction between real and hearsay evidence, let us consider that electronic records may be:

- Device generated records that were created by software programs, without human intervention. Examples include activity logs or automatically generated receipts.
- Information the device has been programmed to record.
- Entered by a person, whether directly or indirectly, then recorded and processed by the device.

In many cases, where electronic records contain only data that is generated by a device, without human intervention the records do not contain hearsay and records containing human statements are often considered to be hearsay. But there are instances where this is not the case, *for* example, a computer-generated invoice found at the scene of the crime to prove that business has been carried out is not hearsay. (Though to prove the contents of the invoice would be hearsay)

A further discussion of hearsay evidence is beyond the scope of this document. However, if readers are interested in the relevant sections of the Evidence Ordinance pertaining to evidence in civil proceedings, they should refer to Sections 47, 49, 53 and 54 of the Evidence Ordinance that are provided, for readers' convenience, in Appendix 5.

Readers may want to pay particular note to Section 53 of the Evidence Ordinance that allows a statement contained in a document to be admissible as evidence (in civil proceedings) if the document or a copy can be produced. (See Appendix 5)



## Appendix 4: Selections from the Hong Kong Electronic Transactions Ordinance:

### ELECTRONIC TRANSACTIONS ORDINANCE - SECT 5

#### Requirement for writing

#### PART III

#### ELECTRONIC RECORDS AND DIGITAL SIGNATURES

- (1) If a rule of law requires information to be or given in writing or provides for certain consequences if it is not, an electronic record satisfies the requirement if the information contained in the electronic record is accessible so as to be usable for subsequent reference.
- (2) If a rule of law permits information to be or given in writing, an electronic record satisfies that rule of law if the information contained in the electronic record is accessible so as to be usable for subsequent reference.

### ELECTRONIC TRANSACTIONS ORDINANCE - SECT 6

#### Digital signatures

- (1) If a rule of law requires the signature of a person or provides for certain consequences if a document is not signed by a person, a digital signature of the person satisfies the requirement but only if the digital signature is supported by a recognized certificate and is generated within the validity of that certificate.
- (2) In subsection (1), "within the validity of that certificate" means that at the time the digital signature is generated-
  - (a) the recognition of the recognized certificate is not revoked or suspended;
  - (b) if the Director has specified a period of validity for the recognition of the recognized certificate, the certificate is within that period; and
  - (c) if the recognized certification authority has specified a period of validity for the recognized certificate, the certificate is within that period "within the validity of that certificate"

### ELECTRONIC TRANSACTIONS ORDINANCE - SECT 7

#### Presentation or retention of information in its original form

- (1) Where a rule of law requires that certain information be presented or retained in its original form, the requirement is satisfied by presenting or retaining the information in the form of electronic records if-

- (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form; and
  - (b) where it is required that information be presented, the information is capable of being displayed in a legible form to the person to whom it is to be presented.
- (2) For the purposes of subsection (1)(a)-
- (a) the criterion for assessing the integrity of the information is whether the information has remained complete and unaltered, apart from the addition of any endorsement or any change which arises in the normal course of communication, storage or display; and
  - (b) the standard for reliability of the assurance is to be assessed having regard to the purpose for which the information was generated and all the other relevant circumstances.
- (3) This section applies whether the requirement in subsection (1) is in the form of an obligation or whether the rule of law merely provides consequences for the information not being presented or retained in its original form.

## ELECTRONIC TRANSACTIONS ORDINANCE - SECT 8

### **Retention of information in electronic records**

(1) Where a rule of law requires certain information to be retained, whether in writing or otherwise, the requirement is satisfied by retaining electronic records, if-

- (a) the information contained in the electronic record remains accessible so as to be usable for subsequent reference;
- (b) the relevant electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; and
- (c) the information, which enables the identification of the origin and destination of the electronic record and the date and time when it was sent or received, is retained.

(2) This section applies whether the requirement in subsection (1) is in the form of an obligation or whether the rule of law merely provides consequences for the information not being retained.

## ELECTRONIC TRANSACTIONS ORDINANCE - SECT 9

### **Admissibility of electronic records**

Without prejudice to any rules of evidence, an electronic record shall not be denied admissibility in evidence in any legal proceeding on the sole ground that it is an electronic record.

## Appendix 5: Selections from the Hong Kong Evidence Ordinance:

### EVIDENCE ORDINANCE - SECT 22A

#### **Documentary evidence in criminal proceedings from computer records**

(1) Subject to this section and section 22B, a statement contained in a document produced by a computer shall be admitted in any criminal proceedings as prima facie evidence of any fact stated therein if-

(a) direct oral evidence of that fact would be admissible in those proceedings; and

(b) it is shown that the conditions in subsection (2) are satisfied in relation to the statement and computer in question.

(2) The conditions referred to in subsection (1)(b) are-

(a) that the computer was used to store, process or retrieve information for the purposes of any activities carried on by any body or individual;

(b) that the information contained in the statement reproduces or is derived from information supplied to the computer in the course of those activities; and

(c) that while the computer was so used in the course of those activities-

(i) appropriate measures were in force for preventing unauthorized interference with the computer; and

(ii) the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents.

(3) Notwithstanding subsection (1), a statement contained in a document produced by a computer used over any period to store, process or retrieve information for the purposes of any activities ("the relevant activities") carried on over that period shall be admitted in any criminal proceedings as prima facie evidence of any fact stated therein if-

(a) direct oral evidence of that fact would be admissible in those proceedings;

(b) it is shown that no person (other than a person charged with an offence to which such statement relates) who occupied a responsible position during that period in relation to the operation of the computer or the management of the relevant activities-

(i) can be found; or

(ii) if such a person is found, is willing and able to give evidence relating to the operation of the computer during that period;

(c) the document was so produced under the direction of a person having practical knowledge of and experience in the use of computers as a means of storing, processing or retrieving information; and

(d) at the time that the document was so produced the computer was operating properly or, if not, any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents, but a statement contained in any such document which is tendered in evidence in criminal proceedings by or on behalf of any person charged with an offence to which such statement relates shall not be admissible under this subsection if that person occupied a responsible position during that period in relation to the operation of the computer or the management of the relevant activities.

(4) Where over a period the function of storing, processing or retrieving information for the purposes of any activities carried on over that period was performed by computer, whether-

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers all the computers used for that purpose whether by one or more persons or bodies during that period shall be treated for the purposes of this section as constituting a single computer.

(5) Subject to subsection (6), in any criminal proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate-

(a) identifying the document containing the statement and describing the manner in which it was produced, and explaining, so far as may be relevant in the proceedings, the nature and contents of the document;

(b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer;

(b) dealing with any of the matters to which the conditions mentioned in subsection (2) relate and purporting to be signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall, on its production without further proof, be admitted in those proceedings as prima facie evidence of any matter stated in the certificate; and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(6) Unless the court otherwise orders, a certificate shall not be admitted in evidence under subsection (5) unless 14 days' notice in writing of the intention to tender such certificate in evidence, together with a copy thereof and of the statement to which it relates, has been served-

(a) where the certificate is tendered by the prosecution, on the defendant (or, if more than one, on each defendant) or his solicitor;

(b) where the certificate is tendered by a defendant, on the Secretary for Justice, (Amended L.N. 362 of 1997) but nothing in this subsection shall affect the admissibility of a certificate in respect of which notice has not been served in accordance with the requirements of this subsection if no person entitled to be so served objects to its being so admitted.

(7) Notwithstanding subsection (5), a court may (except where subsection (3) applies) require oral evidence to be given of any of the matters mentioned in subsection (5).

(8) Any person who in a certificate tendered in evidence under subsection (5) makes a statement which he knows to be false or does not believe to be true shall be guilty of an offence and shall be liable on conviction to a fine of \$50000 and to imprisonment for 2 years.

(9) For the purposes of this section-

- (a) information shall be taken to be supplied to a computer if it is supplied to it in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
- (b) where, in the course of activities carried on by any individual or body, information is supplied with a view to its being stored, processed or retrieved for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
- (c) a document shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

(10) The Criminal Procedure Rules Committee constituted under section 9 of the Criminal Procedure Ordinance (Cap 221) may make rules with respect to the procedure to be followed under this section. (Amended 13 of 1995 s. 27)

(11) Nothing in this section affects the admissibility of a document produced by a computer where the document is tendered otherwise than for the purpose of proving a fact stated in it.

(12) Subject to subsection (4), In this section "computer" means any device for storing, processing or retrieving information, and any reference to information being derived from other information is a reference to its being derived therefrom by calculation, comparison or any other process.

(13) The Legislative Council may by resolution amend subsection (12) so as to make it cover devices performing functions of a similar character to the functions performed by the devices mentioned in that subsection. (Added 37 of 1984 s. 7)

## EVIDENCE ORDINANCE - SECT 22B

### **Provisions supplementary to sections 22 and 22A**

(1) Wherein any criminal proceedings a statement contained in a document is admissible in evidence by virtue of section 22 or 22A, it may be proved by the production of that document or (whether or not that document is still in existence) by the production of a copy of that document or of the material part thereof.

(2) Where in any criminal proceedings a statement contained in a document is admitted in evidence by virtue of section 22 or 22A, the court may draw any reasonable inference from the circumstances in which the statement was made or otherwise came into being or from any other circumstances, including the form and contents of the document in which the statement is contained.

(3) In estimating the weight, if any, to be attached to a statement admitted in evidence by virtue of section 22 or 22A, regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the statement and, in particular-

- (a) in the case of a statement falling within section 22, to the question whether or not the person who supplied the information from which the record containing the statement was compiled did so contemporaneously with the occurrence or existence of the facts dealt with in that information, and to the question whether or not that person, or any person concerned with compiling or keeping the record containing the statement, had any incentive to conceal or misrepresent the facts; and
  - (b) in the case of a statement falling within section 22A, to the question whether or not the information which the information contained in the statement reproduces or is derived from was supplied to the relevant computer, or recorded for the purpose of being supplied to it, contemporaneously with the occurrence or existence of the facts dealt with in that information, and to the question whether or not any person concerned with the supply of information to that computer, or with the operation of that computer or any equipment by means of which the document containing the statement was produced by it, had any incentive to conceal or misrepresent the facts.
- (4) In sections 22 and 22A and this section "document", "copy" and "statement" have the same meaning as in Part IV.
- (5) Nothing in section 22 or 22A shall prejudice the admissibility of any evidence that would be admissible apart from that section.

## EVIDENCE ORDINANCE - SECT 47

### **Admissibility of hearsay evidence**

- (1) In civil proceedings evidence shall not be excluded on the ground that it is hearsay unless-
- (a) a party against whom the evidence is to be adduced objects to the admission of the evidence; and
  - (b) the court is satisfied, having regard to the circumstances of the case, that the exclusion of the evidence is not prejudicial to the interests of justice.
- (2) The court may determine whether or not to exclude evidence on the ground that it is hearsay-
- (a) in the case of civil proceedings before a jury, at the beginning of the proceedings and in the absence of the jury;
  - (b) in the case of any other civil proceedings, at the conclusion of the proceedings.
- (3) Nothing in this Part shall affect the admissibility of evidence admissible apart from this section.
- (4) The provisions of sections 48 to 51 shall not apply in relation to hearsay evidence admissible apart from this section, notwithstanding that it may also be admissible by virtue of this section.

## EVIDENCE ORDINANCE - SECT 49

### **Considerations relevant to weighing of hearsay evidence**

- (1) In estimating the weight, if any, to be given to hearsay evidence in civil proceedings the court shall have regard to any circumstances from which any inference can reasonably be drawn as to the reliability or otherwise of the evidence.
- (2) For the purposes of subsection (1), regard may be had, in particular, to the following-
  - (a) whether it would have been reasonable and practicable for the party by whom the evidence was adduced to have produced the maker of the original statement as a witness
  - (b) whether the original statement was made contemporaneously with the occurrence or existence of the matters stated;
  - (c) whether the evidence involves multiple hearsay;
  - (d) whether any person involved had any motive to conceal or misrepresent matters;
  - (e) whether the original statement was an edited account, or was made in collaboration with another or for a particular purpose;
  - (f) whether the circumstances in which the evidence is adduced as hearsay are such as to suggest an attempt to prevent proper evaluation of its weight;
  - (g) whether or not the evidence adduced by the party is consistent with any evidence previously adduced by the party.

## EVIDENCE ORDINANCE - SECT 53

### **Proof of statements contained in documents**

- (1) Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved-
  - (a) by the production of that document; or
  - (b) whether or not that document is still in existence, by the production of a copy of that document or of the material part of it authenticated in such manner as the court may approve.
- (2) It is immaterial for the purpose of subsection (1) how many removes there are between a copy and the original.

## EVIDENCE ORDINANCE - SECT 54

### **Proof of records of business or public body**

- (1) A document, which is shown to form part of the records of a business or public body, may be received in evidence in civil proceedings without further proof.

(2) A document shall be taken to form part of the records of a business or public body if there is produced to the court a certificate of that effect signed by an officer of the business or body to which the records belong.

(3) For the purposes of subsection (2)-

(a) a document purporting to be a certificate signed by an officer of a business or public body shall be deemed to have been duly given by such an officer and signed by him; and

(b) a certificate shall be treated as signed by a person if it purports to bear his signature or a facsimile of his signature.

(4) In this section-

"business" includes any activity regularly carried on over a period

of time, whether for profit or not, by any body (whether corporate or not)

or by an individual;

"officer" includes any person occupying a responsible position in relation to the relevant activities of the business or public body or in relation to its records;

"public body" includes any executive, legislative, municipal, or urban council, any Government department or undertaking, any local or public authority or undertaking, any board, commission, committee or other body whether paid or unpaid appointed by the Chief Executive or the Government or which has power to act in a public capacity under or for the purposes of any enactment;

"records" (means records in whatever form, and includes computer-generated records.

(5) The court may, having regard to the circumstances of the case, direct that all or any of the provisions of this section do not apply in relation to a particular document or record, or description of documents or records.

---

<sup>i</sup> GUIDELINES FOR BEST PRACTICE IN THE FORENSIC EXAMINATION OF DIGITAL TECHNOLOGY, IOCE 2002 DIGITAL EVIDENCE STANDARDS WORKING GROUP [www.ioce.org](http://www.ioce.org).

<sup>ii</sup> ACPO Good Practice Guide for Computer based Electronic Evidence, Association of Chief Police Officers of England, Wales and N. Ireland (ACPO)

<sup>iii</sup> Ref: Good Practices for Seizing Electronic Devices IOCE 2000 Conference – 13-15 December 2000 – Rosny sous Bois, France

First responders guidelines for digital images and audio IOCE 2000 Conference – 13-15 December 2000 – Rosny sous Bois, France

Checklist for handling digital Image and Audio evidence, International Organization of Computer Evidence