



ISO/IEC JTC 1/SC 27 **N7570**

ISO/IEC JTC 1/SC 27/WG 4 **N47570**

REPLACES: N7281

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: text for working draft

TITLE: **Text for ISO/IEC 1st WD 27037 -- Guidelines for identification, collection and/or acquisition and preservation of digital evidence**

SOURCE: Co-editors (Maslina Daud, Marthie Gobler and Sivanathan Subramaniam)

DATE : 2009-07-07

PROJECT: **27037**

STATUS: In accordance with resolution 2 (contained in SC 27 N7777) of the 21st SC 27 Plenary meeting held in Beijing (China) 11th - 12th May 2009, this document is being circulated to National Bodies and liaison organizations for study and comment.

The National Bodies and liaison organizations of SC 27 are requested to send their comments / contributions on the hereby attached document directly to the SC 27 Secretariat as soon as possible but no later than **2009-09-30**.

PLEASE NOTE: For comments please use THE SC 27 TEMPLATE separately attached to this document.

ACTION: **COM**

DUE DATE: **2009-09-30**

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice Chair
E. Humphreys, K. Naemura, M. Bañón, M.-C. Kang, K. Rannenber, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 37

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

Élément introductif — Élément central — Élément complémentaire

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

D:\HOD_South_Africa\Eigene Dateien\PROJECT_admin\27037_NP_Digital
Evidence_20090420\02_01_1stWD_27037_20090708\SC27N7570_1stWD_27037_20090706\SC27N7570_1
stWD_27037_20090707.doc STD Version 2.1c2

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

Secretariat of ISO/IEC JTC 1/SC 27
DIN German Institute for Standardization
DE-10772 Berlin

Tel. + 49 30 2601 2652

Fax + 49 30 2601 1723

E-mail krystyna.passia@din.de

Web <http://www.jtc1sc27.din.de/en> (public web site)

<http://isotc.iso.org/isotcportal/index.html> (SC 27 documents)

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

Page

Foreword	v
Introduction.....	vi
1 Scope	1
1.1 Audience	2
1.2 Objective	2
2 Normative references	2
3 Terms and definitions	2
4 Abbreviated terms	4
5 Digital Evidence Management.....	4
5.1 Identification	5
5.2 Collection and/or Acquisition	5
5.3 Preservation	5
5.4 Analysis.....	6
5.5 Presentation.....	6
6 Core Principles for Identification, Collection and/or Acquisition and Preservation of Potential Digital Evidence	6
6.1 Methodical.....	6
6.2 Auditable	7
6.3 Repeatable	7
6.4 Defensible	7
7 Chain of custody	7
8 Digital Evidence First Responder	8
8.1 General	8
8.2 Competency	8
8.3 Risk assessment	8
9 Briefing	9
10 Initial Actions of A Digital Evidence First Responder	9
10.1 Secure and protect the location.....	9
10.2 Employ Due Care.....	9
10.3 Documentation	10
11 Prioritize Collection and/or Acquisition by Order of Volatility	10
12 Computers, Storage Media and Peripheral Devices	11
12.1 Identification	11
12.1.1 Physical location search and documentation	11
12.1.2 Non-digital evidence collection	12
12.2 Collection and/or Acquisition	12
12.2.1 Powered On Computer System.....	12
12.2.2 Powered Off Computer System	13
12.2.3 Mission Critical Computer System	13
12.2.4 Storage Media	14
12.3 Preservation.....	14
13 Networked Computers and Network Devices.....	15
13.1 Identification	15
13.1.1 Physical location search and documentation	15
13.1.2 Non-digital evidence collection	16

13.2	Collection and/or Acquisition.....	16
13.3	Preservation	17
14	Mobile Devices	17
14.1	Identification.....	18
14.1.1	Physical location search and documentation	18
14.2	Collection and acquisition	18
14.2.1	Switched on mobile device.....	18
14.2.2	Switched off mobile device.....	19
14.3	Preservation	19
15	Digital CCTV System	19
15.1	Identification.....	19
15.2	Collection and/or Acquisition.....	20
15.3	Preservation	21
16	Packaging and transporting of potential digital evidence	22
16.1	Packaging.....	22
16.2	Transporting.....	23
Annex A (informative)	Examples of potential digital evidence that relates to specific types of investigations (in matrix form)	24
Annex B (informative)	Examples of electronic devices and potential digital evidence	27
Annex C (informative)	List of Validated Imaging Tools for Digital Evidence Acquisition	29
Bibliography	31

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC should not be held responsible for identifying any or all such patent rights.

ISO/IEC 27037 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

Introduction

In responding to serious information security incidents, a post-event response is required to investigate the incidents. The process of the investigation emphasizes the integrity of the digital evidence and the right procedure in obtaining the digital evidence to ensure its admissability in meeting its purposes.

Due to fragility of the digital evidence, a proper procedure needs to be carried out with due care to ensure the integrity of evidentiary value is preserved. Key components that give credibility in the investigation are the methodology applied during the process and individuals who are qualified in performing the tasks using the methodology. There should be a proper procedure used to ensure the practice is credible, and that the individuals performing the tasks have met a certain certification criteria.

It becomes a great concern to many when incidents occurred involved cross-border jurisdictions. This has prompted for this International Standard to be developed to be used not only for legal proceedings, but also for disciplinary procedures and other related purposes in handling digital evidence.

This International Standard provides guidance for individuals; digital evidence first responders who perform required tasks in the investigation including identifying, collecting and/or acquiring and preserving of digital evidence. This International Standard is relevant to ensure digital evidence is managed in accordance with acceptable and practical ways that are acceptable worldwide with the objective to preserve its integrity.

This standard should not replace specific legal requirements of a particular jurisdiction. Instead, this standard may serve as a practical guideline for Digital Evidence First Responder in investigations involving digital evidence and may facilitate exchange of digital evidence between jurisdictions.

The International standard will not mandate the use of particular tools or methods. It does not also include matters pertaining to analysis of digital evidence, or admissibility, weight, relevance, and other judicially-controlled limitations on the use of digital evidence in courts of law.

This proposed standard complements ISO/IEC 27001 and ISO/IEC 27002, and in particular the control requirements concerning digital evidence acquisition by providing additional implementation guidance. In addition the standard will have applications in contexts independent of ISO/IEC 27001 and ISO/IEC 27002.

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

1 Scope

This International Standard provides guidance on the digital evidence management describing the process of recognition and identification, collection and/or acquisition and preservation of digital data which may contain information of potential evidential value.

It is applicable to organisations needing to conduct the identification, collection and/or acquisition and preservation of digital evidence in the event of computer incidents; after the incidents happened or while the incidents happen in real time.

This standard covers potential digital evidence that is collected and/or acquired regardless of the type of media involved. It should also cover potential digital evidence acquired from sources that should include but not limited to static data (e.g. data in storage media), data in transit (e.g. data traversing over networks) and volatile data (e.g. RAM).

The application of this International Standard is possible in principle, provided that special consideration is paid to identifying the competence needed by the digital evidence first responder in handling the digital evidence.

This International Standard contains 17 clauses and 3 annexes, and is organized in the following manner:

- Clause 1 (this clause) describes the scope, audience and the objective of the standard,
- Clause 2 contains the list of normative references,
- Clause 3 contains the terms and definitions,
- Clause 4 contains abbreviated terms
- Clause 5 describes the management of digital evidence,
- Clause 6 describes the core principles for identification, collection and/or acquisition and preservation of potential digital evidence
- Clause 7 describes the chain of custody,
- Clause 8 describes the Digital Evidence First Responder,
- Clause 9 describes the briefing to be done before the identification begins,
- Clause 10 describes the initial actions of a Digital Evidence First Responder,
- Clause 11 describes the prioritization of collection and/or acquisition by order of volatility,
- Clause 12 describes the process of identification, collection and preservation of computers, storage media and peripheral devices,
- Clause 13 describes the process of identification, collection and/or acquisition and preservation of networked computers and network devices,
- Clause 14 describes the process of identification, collection and/or acquisition and preservation of mobile devices,
- Clause 15 describes the process of identification, collection and preservation of digital CCTV system,
- Clause 16 describes the process of packaging and transporting of potential digital evidence,
- Annex A provides examples of potential digital evidence that relates to specific types of investigations (in matrix form),
- Annex B provides examples of electronic devices and potential evidence,
- Annex C provides examples of current validated forensic imaging tools

1.1 Audience

This standard is intended for Digital Evidence First Responders including those amongst law enforcement officers, other members in the enforcement community and personnel within organizations who are responsible in identifying, collecting and/or acquiring and preservation of potential digital evidence. This standard deals with common situations encountered throughout the whole process.

1.2 Objective

The objective of this standard is to provide guidance that describe the process of recognizing and identifying, collecting and/or acquisition and preserving potential digital evidence. Not only it will assist organisations in their disciplinary procedures, it will also facilitate the exchange of potential digital evidence between jurisdictions.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of Practice for Information security management*

ISO/IEC 10118 Series, *Information technology—Security techniques—Hash-functions*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply :

3.1

acquisition

a process of copying or imaging potential digital evidence at the incident scene and leaving the original evidence after copying or imaging is performed

3.2

collection

a process of gathering the physical items that contain potential digital evidence and taking the items away from the incident scene for investigative purposes

3.3

blob

data type specifically used to store multimedia files such as images, audio files and video clips in databases

3.4

BIOS

the program a personal computer's microprocessor uses to get the computer system started after you turn it on.

3.5**digital evidence**

any information that is stored or transmitted in a digital format and has been or is intended to be admitted as evidence

3.6**digital evidence copy**

a copy of digital data obtained in a forensically sound manner. Also called a forensic image.

3.7**Digital Evidence First Responder**

person(s) at a scene containing digital evidence who is authorized, qualified and/or trained in digital forensics with responsibility for handling that evidence

3.8**hash code**

string of bits which is the output of a hash-function

3.9**hash-function**

a function which maps strings of bits to fixed-length strings of bits, satisfying two properties

3.10**hash value**

a string of bits which is the output of a hash-function

[ISO/IEC 10118-1: 2000]

3.11**imaging**

a process of creating an exact mirror copy of a storage media

3.12**image**

An exact mirror copy of a storage media

3.13**peripherals**

any device attached to a computer in order to expand its functionality

3.14**preservation**

a process to maintain and safeguard the integrity and/or original condition of the potential digital evidence

3.15**system clock**

a clock on the motherboard of a computer system which is powered by a tiny battery

3.16**system time**

the time generated by the system clock and used by the operating system

3.17**spoilage**

the act of making or allowing accidental change(s) to the digital evidence that diminish its evidential value

3.18

tampering

the act of intentionally making or allowing change(s) to the digital evidence that diminish its evidential value

3.19

timestamp

the time of an event or events as recorded within the digital evidence

3.20

volatile data

data that is easily spoiled for example by switching off the power or passing through a magnetic field. Volatile data also includes data that changes as the system state changes. Examples include data stored in RAM and dynamic IP addresses

4 Abbreviated terms

BIOS Basic input/output system is the program a personal computer's microprocessor uses to get the computer system started after you turn it on.

Blob Binary Large Object

CMOS Complementary Metal-Oxide-Semiconductor

CPU Central processing Unit

CRC Cyclic redundancy check

DEFRR Digital Evidence First Responder

PDA Personal Digital Assistant

RAM Random Access Memory

RFID Radio Frequency Identification

5 Digital Evidence Management

Digital evidence is, by its very nature, fragile. It can be altered, damaged, or destroyed through improper handling or improper examination. The nature of digital evidence is such that it poses special challenges for its accuracy and reliability. Special precautions should be taken to identify or collect and/ or acquire, preserve and analyze this type of evidence. Failure to do so may render it unusability or may lead to an inaccurate conclusion.

Proper procedures and protocols need to be followed to ensure the integrity and the reliability of the digital evidence. Digital evidence management includes a generic model of identification, collection and/or acquisition, preservation, analysis and presentation of digital evidence

Note: The scope of this guideline is identification, collection and/or acquisition and preservation only.

5.1 Identification

Digital evidence is presented in physical and logical context. Physical refers to presentation of potential digital evidence in hardware and software components while logical refers to address or location where the potential evidence could be located eg. Hard-disk.

The identification process involves the search for, recognition of, and documentation of potential digital evidence at a location or premise. The identification process should identify potential digital evidence relevant to the incident occurred.

It should also identify the volatility of data to ensure the correct order of the process of collection and/or acquisition to preserve the potential digital evidence. This process should also identify possibilities of hidden potential digital evidence.

A thorough search of premises for potential digital evidence must be carried out systematically due to different types of digital devices which may contain potential digital evidence that is easily overlooked, disguised or co-mingled amongst other irrelevant material.

5.2 Collection and/or Acquisition

The collection and/or acquisition process involves gathering and documenting digital data or devices which may contain potential digital evidence. Remember that digital data may be tampered or easily spoiled if proper due care is not implied.

In doing acquisition, potential digital evidence can exist in two conditions; when the incident already happened or when the incident is in progress. Due to these different conditions, different approach and tools are required.

There are a variety of acquisition methods. The DEFR should adopt the best possible acquisition method based on the situation, cost and time. This standard recognizes the acquisition methods as follows:

a) Storage media acquisition

This acquisition method should produce an image copy of the entire storage media and also hash the image copy using any hash function (e.g as specified in ISO/IEC10118). This acquisition method employed must be able to obtain the unallocated space and slack space of the media.

b) Partition acquisition

This acquisition method should produce an image copy of the entire partition of a storage media and also hash the image using any hash function (e.g. as specified in ISO/IEC10118).

c) File acquisition

This acquisition method should produce an image of a file(s) in a storage media and also hash the image using any hash function (e.g. as specified in ISO/IEC10118).

d) Blob acquisition

This acquisition method should produce an image of a blob(s) in a storage media and also hash the image using any hash function (e.g. as specified in ISO/IEC10118).

5.3 Preservation

Digital evidence must be preserved to ensure its usefulness and to be deemed admissible for investigating incidents. There should be no modification to the data itself, date and time stamps associated with it.

The preservation process involves safeguarding digital data which may contain potential evidence from spoilage or tampering to ensure its integrity is well-protected throughout the whole process. The act of

preserving the potential digital evidence should be initiated right after the identification process and to be maintained throughout the collection and/ or acquisition and analysis process.

5.4 Analysis

The analysis process involves the use of scientifically proven methods to determine the characteristics of the evidence and conduct event reconstruction. Analysis does not have to be systematic rather examiners can conduct their examinations intuitively guided by their knowledge and experience. The rule of thumb is to always preserve the integrity of the digital data during this process.

5.5 Presentation

This process is where the output from the analysis will be interpreted based on findings of fact. It has to be articulated in a format appropriate for the intended audience.

6 Core Principles for Identification, Collection and/or Acquisition and Preservation of Potential Digital Evidence

Digital data or digital devices which may contain potential digital evidence must use scientifically derived and proven methods for the identification, collection and/or acquisition and preservation. There are a number of overarching principles that can be applied to guide DEFR in performing their tasks; methodical, auditable, repeatable and defensible.

6.1 Methodical

DEFR should interface, interact and acquire the original material of the potential digital evidence in the least intrusive manner. In carrying out the process, DEFR should consider the available different methods of collecting and/or acquiring the digital data and consider the most appropriate method to use. Methods used should be transparent and reproducible. DEFR should be prepared to produce the method used and have those methods tested by independent digital forensic experts.

The general principle is to consider using the least intrusive method, but this needs to be balanced with circumstances of cost and time.

In the event where aspects of invasiveness are used in carrying out his/her task, the DEFR should do the following:

- a) document the reasons for using the method; and
- b) where possible, verify the extent of the effect of any intrusion

The DEFR should also:

- a) recognize that the act of preservation of the potential digital evidence cannot always be non-intrusive;
- b) recognize that the forum for which data is intended can legitimately influence the method which is chosen;
- c) document what they did and why they did it; and
- d) determine and apply a method for establishing the accuracy and a copy has to the original source and its reliability. The DEFR should first consider the most accurate methods such as mathematical hashing to

the least accurate methods such as snapshot captures of display screens for devices like mobile phones and PDAs. However, this has to be balanced with circumstances of cost and time.

All steps used in the processes to identify and extract digital evidence should be well-documented.

6.2 Auditable

Processes performed by DEFR should be subjected to independent assessment (audit) to determine the decisions and actions taken were reasonable, valid and conducted to the highest possible standards. Processes performed by the DEFR should be available for independent assessment to determine if:

- a) The DEFR is capable of undertaking the processes and of making any conclusions;
- b) An appropriate evidential standard was followed; and
- c) Any conclusions are consistent with the digital evidence.

Note: Direct cost needs to be considered to carry out this (usually for civil matters) because in general the highest possible standards are also the most expensive.

6.3 Repeatable

A suitably skilled and experienced DEFR should without guidance or interpretation, be able to undertake all processes described in the documentation and arrive at the same results.

Repeatability is established when similar test results are produced under the following conditions:

- a) Using the same measurement procedure
- b) Performed by the same observer/operator
- c) Using the same measuring instrument, used under the same conditions
- d) Performed in the same location (lab)
- e) Repetition within a short period of time

To achieve repeatability, quality control and documentation of the process must be in place.

6.4 Defensible

DEFR should be able to defend his/her actions and methods used for the identification, collection and/or acquisition and preservation of the digital data. The defense should be achieved by demonstrating that he/she has undertaken competency tests and also trained to operate the hardware or software used to perform the tasks.

Defensible can be achieved when chain of custody is well-documented with great accuracy and in detailed documentation.

Note: Competency test is required to ensure the competency of a DEFR that varies from one jurisdiction to another. However, it is utmost important for DEFRs to undergo competency test or similar to ensure he/she is capable to deliver his/her tasks without tampering or spoiling the data with potential evidentiary value.

7 Chain of custody

Chain of custody is a record of who is responsible to handle collected digital device(s) and/or acquired digital data. The purpose of maintaining a chain of custody is to enable identification of access to the digital devices

or data at any given point in time. The evidentiary weightage of digital evidence will be substantially reduced if the chain of custody cannot be adequately established or is discredited.

Chain of custody is to be maintained throughout the entire process. It should be established from the moment digital device(s) and/or digital data are obtained and should not be broken. It should contain information such as the DEFR's name, date, time, unique identifier of the items and subsequent custodians of the item and the handover location.

8 Digital Evidence First Responder

8.1 General

The role of a DEFR involves the ability to identify, collect and/or acquire and preserve potential digital evidence at the location or premise of the incident. A DEFR may not be involved in the analysis and development of the report of the analysis. However, the role of DEFR is vital in ensuring the integrity of potential digital evidence.

In ensuring integrity of the potential digital evidence is preserved, the DEFR should have adequate experience, skills and knowledge in handling them. This is crucial because digital data can be easily spoiled. DEFRs may also require assistance from technical support personnel in related areas. Some of the pre-requisites for a DEFR and technical assistance are as follows:

- They should be properly and adequately trained to handle digital devices which may contain potential digital evidence
- They should demonstrate and maintain their skills by undergoing competency test(s) in the relevant area of handling digital data which may contain potential digital evidence

Note: Competence of a DEFR varies from from one jurisdiction to another. However, it is utmost important for a DEFR to undergo a competency test or similar to ensure he/she is capable to deliver his/her tasks without tampering or spoiling the data that has the potential evidentiary value.

8.2 Competency

DEFRs must be adequately trained to handle digital data which may contain potential digital evidence. Having the best set of tools will not guarantee the quality of the evidence if the DEFRs are not competent in performing his/her tasks.

When required, the DEFRs should be able to demonstrate that he/she is formally trained to handle digital evidence using the tools used to perform the tasks.

8.3 Risk assessment

Conducting risk assessment prior to commencing the tasks is vital because of the safety of the personnel involved in investigating the incident is paramount.

Things to consider during risk assessment include:

- a) Will the individual(s) whom are investigated be present?
- b) If present, do they have a propensity toward violence?
- c) Are there weapons in the area?
- d) Whether the location or scene is unsafe (contains hazardous materials, heavy machinery)?
- e) The surrounding area (office park, college campus, economically depressed).
- f) Can the location or scene be isolated from bystanders?

- g) The time of day the operation will be conducted.

9 Briefing

It is essential that all team members are adequately briefed before they begin performing their tasks. It cannot be assumed that having the best and competent team there is nothing to be briefed prior to responding to an incident. It is vital to have a formal briefing session to understand the incident, the things to expect and also the things that can occur unexpectedly. Strict warnings should be given to team members to discourage spoilage or tampering with the digital devices and data. Briefing is significant, so that members will know their roles and responsibilities; thus ensure a smooth operation.

10 Initial Actions of A Digital Evidence First Responder

10.1 Secure and protect the location

DEFRRs should secure and protect the location of the potential digital evidence as soon as they arrive at the incident scene. They should ensure the following:

- a) Secure and take control of the area containing the devices
- b) Identify the person in charge of the location
- c) Move people away from the devices and power supplies
- d) Document anyone who has access to the location or anyone who may have a reason to be involved with the location
- e) Photograph or video the area and all components including the leads in situ. If no camera and/or video camera available, draw a sketch plan of the system and label the ports and cables so that system may be validated and reconstructed at a later date.
- f) If the device is ON do not switch it OFF and if the device is OFF do not switch it ON
- g) Eyeball search the areas for sticky notes, diaries, papers or notebooks with crucial details about the devices such as passwords and PIN

10.2 Employ Due Care

Avoid any actions that would lead to either tampering and/or spoiling potential digital evidence that are stored in electronic devices or media due to intentional or non-intentional actions.

Digital data can be easily tampered and/or spoiled if due care is not applied. For instance, potential digital evidence that is contained in a magnetic storage media can be spoiled when exposed to magnetic fields. Thus, the DEFRR must employ good practices to avoid tampering and/or spoilage of digital data. The DEFRR should not access digital devices, such as conducting memory dump from a live computer system, unless with the usage of forensically sound tools.

In the event that digital device(s) cannot be collected, acquisition of the digital data should be performed. Such conditions include but not limited to:

- a) If it is a mission-critical computer that cannot tolerate any downtime
- b) If it contains volatile data that must be acquired immediately in order to avoid any loss of data due to interruption of power supply
- c) If the physical size of the computer is too big such as server at the data center or RAID system
- d) If it is a safety-critical computer that would endanger life if stopped

- e) If it is a business-critical computer that also services innocent parties

10.3 Documentation

Documentation is critical when handling digital data which may contain potential digital evidence. The following points should be adhered during documentation at the location of the potential digital evidence:

- a) Every step taken should be documented. This is to ensure that no details have been left out during the identification, collection and/or acquisition processes. It may also be helpful in a cross-border investigation whereby the digital data gathered from another part of the globe can be traced accordingly.
- b) If the digital devices are switched on, be sensitive of their time and date setting. Compare the time setting with the atomic clock and document them and the difference (if any). Also document anything on the screen.
- c) Any movement of the digital devices should be documented. Maintain the chain of the custody at all times.
- d) Document all unique identifiers of the digital devices and the associated parts such as serial numbers and unique markings.

11 Prioritize Collection and/or Acquisition by Order of Volatility

Prior to collecting and/or acquiring digital devices that may contain potential digital evidence at a crime scene, it is important to correctly identify them. Devices that may contain potential digital evidence should include but not limited to the following:

- a) Computer systems
- b) External storage media
- c) Smart cards, dongles, biometric scanners
- d) Answering machines
- e) Digital cameras
- f) Handheld devices (PDAs, organizers)
- g) Local Area Network (LAN) Card or Network Interface Card (NIC)
- h) Routers, Hubs, Switches
- i) Pagers
- j) Printers
- k) Scanners
- l) Telephones

The above is not a comprehensive listing of all the devices that a DEFR may encounter and the DEFR should ensure he/she has considered all devices appropriate to the circumstance.

Digital data can be broken into 2 categories; volatile data and resident data. Volatile data can be easily destroyed or lost forever if due care to protect the data is not implied such as removing the power supply to the device. Resident data on the other hand remains on the media even if the power supply is removed. Since digital data can be easily tampered and/or spoiled and thus has a very short life span, it has to be prioritized

(upon identification) by order of volatility before collection and/or acquisition. Collect and/or acquire the most volatile digital data first such as cache memory, RAM, swap space, running processes and etc. The DEFR must possess a sound knowledge to prioritize according to volatility.

Upon identification, the DEFR should:

- a) Identify and prioritize digital data that would be lost forever if the power supply is removed
- b) Take quick actions to collect and/or acquire these data with forensically sound methods

Note 1: Be aware that some volatile data may change due to location – ensure such data is preserved prior to moving the device.

Note 2: Devices containing digital evidence may also be a source of physical evidence (e.g. fingerprints, DNA, particles, etc). DEFRs need to take care not to spoil such evidence.

12 Computers, Storage Media and Peripheral Devices

12.1 Identification

In the context of this standard, computers are considered as standalone electronic devices that receive, process and store data, and produce results. These computer devices are not connected to a network, but may be connected to peripheral devices such as printers, scanners, webcams, MP3 players, GPS systems, RFID devices and so on. Usually incident scenes will contain various types of storage media. Storage media is used to store data from electronic devices and they vary in memory capacity. Storage media are such as external portable hard disks, flash drives, CD, DVD, Blu-Ray disks, floppy disks, magnetic tapes and memory cards.

12.1.1 Physical location search and documentation

- a) The first step of identification is to secure the incident scene and move people away from computers and the peripheral devices. The DEFR must ensure that no unauthorized person has access to any devices at the premise.
- b) Before any acquisition or collection can be done, the incident location should be recorded in a visual manner either by photographing, videographing or sketching the scene as it looked upon entry. The choice of recording method needs to be balanced with circumstances of cost and time. The DEFR should document all other items at the scene that may contain potential evidences such as scribbled notes, sticky notes, diary and so on.
- c) The DEFR should record the type and brand of any proprietary systems used and identify all computer and peripheral devices that may need to be acquired or collected during this initial stage.
- d) The status of the computers and peripheral devices should remain as is. If the computers or peripheral devices are powered off, do not turn them on and if they are powered on, do not turn them off which otherwise may spoil the digital data.
- e) If the computers are powered on, photograph or make a written note what is on the screens. Take note that in the event of a criminal or potential criminal investigation, it is recommended that law enforcement officers capture and collect all potential digital evidences.
- f) Take note that these computers and peripheral devices may also be a source of physical evidence, such as fingerprints, DNA and particles. The DEFR needs to take special care not to spoil these non-digital potential evidences and coordinate with the relevant evidence collectors before proceeding to the next steps.
- g) Devices that have batteries that may run down need to be power-charged to ensure information is not lost. The DEFRs need to identify potential charging media and cable during this phase.

12.1.2 Non-digital evidence collection

The DEFR needs to identify the person responsible for the facilities at the scene. This individual may be able to provide additional information and documentation such as passwords to the computer systems and other relevant details. The DEFR needs to record the name and designation of this person. Should the specific computers in question be connected to a network, the DEFR should continue with the evidence handling process as described in Clause 13 of this document.

The DEFR also need to collect some evidence verbally. He/she may talk to employees who are directly or indirectly involved with the potential digital evidence or device to be collected. These employees may include the system administrator, the owner of the device and users of the computer and peripheral devices. During this verbal evidence collection, the DEFR may request information such as the system configuration and root password. This additional information may be helpful in the analysis stage of the potential digital evidence.

12.2 Collection and/or Acquisition

DEFR needs to decide either to collect (seize) the computers and the peripheral devices or acquire the potential digital evidences from them . The choice needs to be balanced with circumstances of cost, time and available resources. Three scenarios exist in which collection and/or acquisition may need to be conducted; (a) when the computers are powered on,, (b) when the computers are powered off and (c) when the computers are powered on but cannot be powered off (such as mission critical computer systems). In all three scenarios, the DEFR is required to make an accurate image copy of the computers' storage media which is suspected to contain potential digital evidence.

In many cases, the computer systems and peripheral devices can just be collected, packaged and transported back to the lab for analysis. Please refer to the Packaging and Transporting section of this document.

12.2.1 Powered On Computer System

Following is the step-by-step guideline for acquisition when the computer is found to be powered on:

- a) First and foremost, consider acquiring the digital data that may otherwise be lost if the computer system is powered off. They are also known as volatile data and data stored on Random Access Memory (RAM) and running processes are such data. RAM also contains useful information such as decrypted applications and passwords. Ensure that all the actions performed and the resulting changes made to the computer system are recorded and understood.
- b) Remove the power supply cable by first removing the end attached to the computer and not that attached to the socket. This will avoid data being written to the computer's storage media if it is fitted with uninterruptible power supply (UPS) which will spoil the potential digital evidence.
- c) If it is a laptop computer, remove the main power source battery instead of the power button of the laptop computer. Ensure the volatile data is acquired before removing the battery.
- d) Take note that if the power is removed from a powered on computer system, any potential evidence stored in encrypted volumes will be lost, unless the decryption key is obtained. Also note that potentially valuable live data could be lost, leading to damage claims or loss of human lives, such as corporate data or computers controlling medical equipments.
- e) Disconnect and secure all cables from the computer and label the ports so that the system can be reconstructed in a later stage.
- f) Place tape over the floppy disk slot, if present.
- g) Make sure that the CD or DVD drive trays are retracted into place; note whether these drive trays are empty, contain disks, or are unchecked; and tape the drive slot closed to prevent it from opening.
- h) Place tape over the power switch.

- i) Remove the hard disk drive(s) from the computer system, taking care to ground the machine to prevent static electricity from damaging the hard disk drive(s). Label the hard disk drive(s) as suspect disk and document all the details such as make, model name, serial number and size of the disk(s).
- j) Execute the imaging process by using a validated imaging tool to create an image of the suspect disk. The image copy will be stored into a target disk which had been sanitized in accordance to the US Department of Defense 5220.22-M National Industrial Security Program Operating Manual (NISPOM) requirement. Ensure the steps taken do not spoil or tamper the digital data. Repeat this step for all the hard disk drives found in the computers.

12.2.2 Powered Off Computer System

It is easier to handle powered off computer system compared to powered on computer system because there is no need to acquire the volatile data. Following is the step-by-step guideline for acquisition when the computer is found to be powered off:

- a) Remove the power supply cable by first removing the end attached to the computer and not that attached to the socket. Be aware that some laptop computers may power on by opening the lid. Remove the main power source battery from laptop computer but before that ensure that the laptop computer is indeed powered off because some may be in standby mode.
- b) Disconnect and secure all cables from the computers and label the ports so that the system can be reconstructed in a later stage.
- c) Place tape over the floppy disk slot, if present.
- d) Make sure that the CD or DVD drive trays are retracted into place; note whether these drive trays are empty, contain disks, or are unchecked; and tape the drive slot closed to prevent it from opening.
- e) Place tape over the power switch.
- f) Remove the hard disk drive(s) from the computer system, taking care to ground the machine to prevent static electricity from damaging the hard disk drive(s). Label the hard disk drive(s) as suspect disk and document all the details such as make, model name, serial number and size of the disk(s).
- g) Execute the imaging process by using a validated imaging tool to create an image of the suspect disk. The image copy will be stored into a target disk which had been sanitized in accordance to the US Department of Defense 5220.22-M National Industrial Security Program Operating Manual (NISPOM) requirement, Ensure the steps taken do not spoil or tamper the digital data. Repeat this step for all the hard disk drives found in the computers suspected to contain potential digital evidences at the premise

12.2.3 Mission Critical Computer System

In many cases, the computer systems cannot be powered off due to the critical nature of the systems. These systems are such as servers at data centres which are also servicing innocent clients, military systems, surveillance systems, medical systems and many others which may have critical impact if interrupted or powered off. Special care must be taken when dealing with such systems. Following is the step-by-step guidelines to conduct acquisition on mission critical computer system:

- a) First and foremost, consider acquiring the digital data that may otherwise be lost if delayed. Data stored on Random Access Memory (RAM) and running processes are such data. Ensure that all the actions performed and the resulting changes made to the computer system are recorded and understood.
- b) Identify the part of the storage media that needs to be acquired such as a partition, a directory or a file.

- c) Execute the imaging process by using a validated imaging tool to create an image of the identified partition, directory or file. The image copy must be stored into a target disk which had been wiped in accordance to the US Department of Defense 5220.22-M National Industrial Security Program Operating Manual (NISPOM) requirement, Ensure the steps taken do not spoil or tamper the digital data.

12.2.4 Storage Media

- a) Various types of storage media may be found at an incident scene. Usually they are the least volatile type of data and can be at the least priority during collection and/or acquisition. This does not mean they are not important because in most cases, external storage media will contain the evidence that the analysts are looking for,
- b) Check and record the make, model and serial number (if any) of each storage media found.
- c) The DEFR should decide whether to collect the identified storage media and conduct on-site acquisition. This will depend on the nature of the case and the available resources.
- d) If the DEFR decides to collect the collected storage media should be wrapped or placed in appropriate packaging suitable for the nature of the media, such as shrink wrap plastic, to avoid contamination of the media prior to transporting to another location. Shock resistance packaging can be used to avoid physical damage to any components of the media.
- h) Label all storage media and any associated parts with them. Evidence labels should not be placed directly on the mechanical parts of the electronic devices, nor should it cover or conceal important information such as the serial number, model number and part number. All device(s) collected should be sealed with tamper evident seals, labeled and signed on the label
- i) DEFR should label evidence with ink rather than pencil. The pencil's graphite dust can interfere with the reading of the disk or tape.
- j) The collected storage media should be stored in a secure, climate controlled environment or a location that is not subject to extreme temperature or humidity. It should not be exposed to magnetic fields, dust, vibration, moisture, or any other environmental elements that may damage it.

12.3 Preservation

All collected and/or acquired digital data must be protected from potential loss, damage or spoilage. The most important activity in the preservation process is to maintain the integrity of the digital data and its chain of custody. The following are the guidelines to preserve the collected and/or acquired digital data:

- a) Seal the acquired digital data by using hashing algorithm, digital signatures or biometric features. This is necessary to confirm that the contents of the copied image have not been spoiled or tampered with since the image was created.
 - Hash the original data by using any hashing function specified in ISO/IEC10118 and record the hash value to prove that data acquired is the exact copy of the original data. Hash the acquired digital data and compare the hash value with the hash value of the original data. Both hash values must be identical. If they are not identical, repeat the above steps.
 - Digital signatures are a secure method of binding the identity of the signer with digital data integrity methods. It involves attaching a piece of code to an electronically transmitted message with the sole purpose of establishing identity. Accordingly, it is possible to use digital signatures to establish legal responsibility and the complete authenticity of the host document.
 - Biometrics uses physical and behavioral characteristics to determine the identity of an individual. By attaching a biometric feature to acquired evidence, it may ensure that the evidence cannot be tampered without compromising the biometric feature

- b) The collected digital device(s) should be wrapped or placed in appropriate packaging suitable for the nature of the device, such as shrink wrap plastic, to avoid contamination of the digital device(s) prior to transporting to other location(s). Shock resistance packaging can be used to avoid physical damage to any components of the device(s).
 - Hard disk drives need to be secured using anti-static bags.
 - Main system units and/or notebooks need to be secured in an appropriate container to avoid damage or spoilage of the potential digital evidence that could reside in it.
- c) Label all potential evidence, all collected digital device(s) and any hardware parts associated with it (them). Evidence labels should not be placed directly on the mechanical parts of the electronic devices, nor should it cover or conceal important information such as the serial number, model number and part number. All device(s) collected should be sealed with tamper-proof seals and the first responder or a personnel in charge must sign on the label.
- d) The DEFR should label the collected items with ink rather than pencil.
- e) Ensure that all digital evidence is packaged in a manner that will prevent it from being bent, scratched, or otherwise deformed.
- f) The collected digital device(s) should be stored in a secure, climate controlled environment or a location that is not subject to extreme temperature or humidity. It should not be exposed to magnetic fields, dust, vibration, moisture, or any other environmental elements that may damage it.

13 Networked Computers and Network Devices

13.1 Identification

Network devices are considered as computers or other digital devices that are connected to a network in either wired or wireless mode. These network devices may include mainframes, servers, desktop computers, access points, switches, hubs, routers, bluetooth devices and many more. Take note that if computers are networked, it is difficult to immediately ascertain where the digital data being sought are kept. The data could be anywhere on the network.

13.1.1 Physical location search and documentation

- a) The first step of identification is to secure the incident scene and move people away from computers and network devices. The DEFR must ensure that no unauthorized person has access to any devices at the premise.
- b) Before any acquisition or collection can be done, the incident location should be recorded in a visual manner either by photographing, videographing or sketching the scene as it looked upon entry. The choice of recording method needs to be balanced with circumstances of cost and time. The DEFR should document all other items at the scene that may contain potential evidences such as scribbled notes, sticky notes, diary and so on.
- c) The DEFR should record the type and brand of any proprietary systems used and identify all computers and network devices that may need to be acquired or collected during this initial stage.
- d) The status of the computers and network devices should remain as is. If the computers or network devices are powered off, do not turn them on and if they are powered on, do not turn them off which otherwise may spoil the digital data (*please refer to section 12.1 for guidelines on how to identify and handle computer systems*).

- e) If a wired network is present, there will usually be boxes called hub or switch (both look very similar). The network cables are usually connected at the rear part of the devices.
- f) Take note that a network may also be connected to a modem providing access to the Internet. They come in various flavors such as Cable modems or DSL modems. The modems are usually connected to a telephone system and directly to a computer or a switch/router. There are also modems which incorporate the router features built-in.
- g) If cost and time permit, the DEFR should also consider using a wireless signal detector to detect and identify wireless signal from wireless devices which may be hidden to locate them.
- h) Take note that these computers and network devices may also be a source of physical evidence, such as fingerprints, DNA and particles. The DEFR needs to take special care not to spoil these non-digital potential evidences and coordinate with the relevant evidence collectors before proceeding to the next steps.
- i) Devices that have batteries that may run down need to be power-charged to ensure information is not lost. The DEFR need to identify potential charging media and cable during this phase

13.1.2 Non-digital evidence collection

The DEFR needs to identify the person responsible for the facilities at the scene. This individual may be able to provide additional information and documentation such as passwords to the computer systems, network topology, IP addresses and other relevant details. The DEFR needs to record the name and designation of this person.

The DEFR also needs to collect some evidence verbally. He/she may talk to employees who are directly or indirectly involved with the potential digital evidence or devices to be collected. These employees may include the system administrator, the owner of the device and users of the computer and network devices. During this verbal evidence collection, he/she may request information such as the system configuration, root password, router password, firewall password and so on. This additional information may be helpful in the analysis stage of the potential digital evidence.

13.2 Collection and/or Acquisition

DEFR needs to decide whether to collect (seize) or acquire the potential digital evidences from the computers and the network devices. The choice needs to be balanced with circumstances of cost, time and available resources (*for guidelines to collect and/or acquire computer systems, please refer to section 12.2 of this document*).

The following are the guidelines for collecting and/or acquiring network devices:

- a) Once the DEFR has recognized and identified the network devices, he/she should isolate the network from the Internet. This can be done by unplugging the connection to the telephone system, network port or wireless access point.
- b) The network devices should be kept running for further analysis to ascertain the other devices connected to the network devices.
- c) Be aware that power removal from the network devices at this point will destroy volatile data such as running processes, network connections and data stored in memory. The DEFR should capture this information before removing the power from the devices.
- d) For wired networks, trace the connections to the computers and label the ports for future reconstruction of the whole network.

- e) Once the DEFR is sure that no potential evidence will be lost as a result, the connections from the network devices and the computers can be removed.
- f) Subsequently, treat each computer as it would be treated as a stand-alone computer (refer to section 12.2).
- g) Another important thing to note is mobile phones and PDAs may be connected to the network via WiFi or Bluetooth connections. Ensure these devices are not left behind.

13.3 Preservation

All collected and/or acquired digital data must be protected from potential loss, damage or spoilage. The most important activity in the preservation process is to maintain the integrity of the digital data and its chain of custody. If volatile data is collected and/or acquired from the network devices, this process is applicable and the following are the guidelines to preserve them:

- a) Seal the acquired digital data by using hashing algorithm, digital signatures or biometric features. This is necessary to confirm that the contents of the copied image have not been spoiled or tampered with since the image was created.
 - Hash the original data by using any hashing function specified in ISO/IEC10118 and record the hash value. Remember that this acquired volatile data will act as the master copy.
 - Digital signatures are a secure method of binding the identity of the signer with digital data integrity methods. It involves attaching a piece of code to an electronically transmitted message with the sole purpose of establishing identity. Accordingly, it is possible to use digital signatures to establish legal responsibility and the complete authenticity of the host document.
 - Biometrics uses physical and behavioral characteristics to determine the identity of an individual. By attaching a biometric feature to acquired evidence, it may ensure that the evidence cannot be tampered without compromising the biometric feature
- b) The collected network device(s) should be wrapped or placed in appropriate packaging suitable for the nature of the device, such as shrink wrap plastic, to avoid contamination of the network device(s) prior to transporting to other location(s). Shock resistance packaging can be used to avoid physical damage to any components of the device(s) (Please refer to section 12.3 for preservation methods for computer systems).
- c) Label all network devices and any hardware parts associated with them. Evidence labels should not be placed directly on the mechanical parts of the devices, nor should it cover or conceal important information such as the serial number, model number and part number. All device collected should be sealed with tamper-proof seals and the first responder or o personnel in charge must sign on the label.
- d) The DEFR should label the collected items with ink rather than pencil.
- e) Ensure that all network devices are packaged in a manner that will prevent it from being bent, scratched, or otherwise deformed.
- f) The collected network devices should be stored in a secure, climate controlled environment or a location that is not subject to extreme temperature or humidity. It should not be exposed to magnetic fields, dust, vibration, moisture, or any other environmental elements that may damage it.

14 Mobile Devices

14.1 Identification

Mobile devices are seen as pocket-sized computing devices. It works similar to computer devices, but are smaller and more portable. Mobile devices generally can connect to networks and communicate with other digital devices. It provides communications, digital photography, navigation systems, entertainment, data storage and personal information management. These devices may include Personal Digital Assistants (PDAs), mobile phones, smart phones and palmtops.

- a) Due to the general small size of mobile devices, DEFR needs to take extra care to identify all types of mobile devices that may be relevant to the case. He/she needs to secure the suspected incident scene and ensure that no individuals remove mobile devices from the scene (it is easy to remove mobile devices from the scene by placing them in a handbag or jacket pocket). No unauthorized person may have access to any devices that may contain potential digital evidence. and no communication devices should be able to receive or transmit data.

14.1.1 Physical location search and documentation

Please refer to section 12.1.1 for guidelines on how to secure an incident scene. All the mobile devices and their associated items such as memory cards, SIM cards, chargers and cradles found at the scene must be recorded.

If the handheld device is switched on, record and take photographs of any symbols or indicators on the screen such as new SMS icon, missed calls, time and date setting and the battery life indicator.

The status of the mobile devices should remain as is. If the mobile devices are powered off, do not turn it on. If the mobile devices are powered on, do not turn it off. Devices that are powered on need to be power-charged to ensure information is not lost.

14.2 Collection and acquisition

Collection and acquisition of potential digital evidence for mobile devices are complicated. Not only can these devices be powered on or off, but it can also be in a number of different states in which certain modes of interaction (such as Bluetooth, RF, touch screen, IR) can be enabled or disabled. Some mobile devices have to be switched on to access the module, whilst other acquisitions can be done directly from the SIM card. To further complicate the collection and acquisition process, the different mobile device manufacturers use different types of operating systems, requiring different methods of evidence acquisition. There is also a wide range of memory devices that are used in conjunction with mobile devices, such as MicroDrives and SD cards.

Generally, mobile devices need to be switched on in order to allow a forensic bit by bit copy. These devices cannot be powered off without data loss, whilst a powered on device continuously alter its operating environment by, for example, updating the clock timer. The associated problem is that two images of the same device will show different hash values.

Two scenarios exist in which the DEFR must decide what appropriate actions to take without spoiling or tampering with the potential digital evidences contained within the mobile devices. They are when the mobile device is switched on and when the mobile device is switched off.

14.2.1 Switched on mobile device

- a) For a mobile device which is found to be on, DEFR should also use a faraday box or a shielded box to prevent the device from connecting to the network. Take note that connecting to a network may result in spoilage of potential digital evidence due to the incoming calls and messages.
- b) If the device is continued to be left on, the battery life will be reduced due to power loss as the device tries to connect to a network. Therefore, it is highly recommended that immediate delivery of the mobile device to the lab for examination.
- c) If the device is known to contain volatile memory, consider charging the device at appropriate intervals to ensure the data is not lost.

14.2.2 Switched off mobile device

- a) If the mobile device is switched off, carefully package, seal and label the device. This is to avoid any accidental or deliberate operation of the keys or buttons is prevented. As a precaution, DEFR should also consider using the faraday or shielded boxes.
- b) Also collect all associated mobile device items such as charger, memory card, SIM card, cradle and so on.

14.3 Preservation

All potential evidence and sources of potential evidence should be protected from potential loss, damage or spoilage. The most important activity in the preservation process is to document all actions and maintain the chain of custody. The following are some guidelines regarding preservation of potential evidence:

- a) DEFR should be aware that mobile devices may have the ability to wipe data and thus any manual interaction with the device should be minimized.
- b) The chain of custody of the collected mobile device and its associated items must be maintained at all times.
- c) Before packaging, labeling and sealing of switched off mobile device, the DEFR should check and record the serial number, the type and brand of the device.
- d) The collected mobile device should be wrapped or placed in appropriate packaging, such as faraday box or shielded box. Shock resistance packaging can be used to avoid physical damage to any components of the device(s).

15 Digital CCTV System

Extraction of digital data for the purpose of digital evidence analysis from digital CCTV system is extremely challenging. The proprietary nature of most of the cctv systems in the market does not allow quick and easy access to data in a suitable form.

DEFR must understand that the approach to extract video sequences from a PC based CCTV system is different from conventional digital data extraction from a PC.

15.1 Identification

Upon arriving at the incident scene, DEFR should take the necessary steps as stipulated in section 12.1

Next, the DEFR should identify the type, brand and model of the CCTV system in order to gather more information about the system. The information will enable the DEFR to determine the options available to download the video sequences.

Below are the guidelines to identify CCTV system at an incident scene:

- a) The first step of identification is to secure the incident scene and move people away from the CCTV system and the associated items. The DEFR must ensure that no unauthorized person has access to any devices at the premise.
- b) Before any acquisition or collection can be done, the incident location should be recorded in a visual manner either by photographing, videographing or sketching the scene as it looked upon entry. The choice of recording method needs to be balanced with circumstances of cost and time. The DEFR should document all other items at the scene that may contain potential evidences such as scribbled notes, sticky notes, diary and so on.

- c) The DEFR should also record the type, brand and model of any the CCTV system used and identify all other associated items that may need to be acquired or collected during this initial stage.
- d) Note the number of cameras connected to the CCTV system.
- e) Note the basic settings of the system such as display settings and current record settings so that if changes have to be made to facilitate the collection and/or acquisition process, it is then possible to return the system to its original state.
- f) Take note the CCTV system time and compare it with real time. Record the difference (if any).

15.2 Collection and/or Acquisition

- a) Before the collection and/or acquisition process can be started, the DEFR should determine the time period required. He/she should also determine which cameras are required and whether they can be acquired separately.
- b) The storage size and the overwrite time should also be noted. This will let the DEFR know how long the video sequences will be retained on the system.
- c) Please be aware that the recording should not be stopped during the acquisition process unless the system will not allow or there is an immediate risk that important data will be overwritten, before it can be acquired.
- d) One of the most important steps is that the confirmation that the video sequences can be acquired in its original file format. Original file format is important to maintain image quality and provide best evidence.
- e) If the original data format is proprietary, the DEFR should get a copy of the player software which can play the video sequences.
- f) The practicality of acquisition must be checked. The general principle is to consider using the least intrusive method, but this needs to be balanced with circumstances of cost and time. Also long sequences of video from multiple cameras may require a very large storage size which is not very practical. The acquisition process may also take several hours to complete.
- g) There are a few options to undertake the acquisition process:
 - Acquire the video files by writing them onto CD/DVD but this may not be practical if the video file is too big (several GB in size).
 - Acquire the video files via USB external hard disk drive. This method is deemed to be the most practical at the moment.
 - Acquire the video files via a network connection. This may be available if the CCTV system is a PC based system. Please take note that some of the DVR based systems may also have network port.
 - A quick method is by replacing the CCTV system's hard disk with a blank or cloned hard disk. However, there are several risks that the DEFR should assess before using this method such as compatibility of the new hard disk with the system and the compatibility of the removed hard disk with other systems for examination.
- h) Upon completing the acquisition, the acquired file should be checked to confirm that the right file or the right portion of the file has been acquired. The file should also be checked with the player software (for proprietary file formats) for its playability.
- i) The drive which contains the acquired file should be treated as the master copy.

- j) Subsequently, DEFR should restart the CCTV system if it was powered off. This should be done in the presence of the authorized person of the premise.
- k) In circumstances where all acquisition options cannot be used or if it is not practical at all to conduct the acquisition at the scene, the whole CCTV system should be removed from the scene and the acquisition process should be undertaken back in the lab. Remember, this is the DEFR's last resort and assuming that it is physically possible to do so. However, the implications such as legal and insurance should be considered prior to the removal.

15.3 Preservation

All acquired video files must be protected from potential loss, damage or spoilage. The most important activity in the preservation process is to maintain the integrity of the video files and their chain of custody. The following are the guidelines to preserve the acquired video files:

- a) Seal the acquired data by using hashing algorithm, digital signatures or biometric features. This is necessary to confirm that the contents of the copied image have not been spoiled or tampered with since the image was created.
 - Hash the acquired video files by using any hashing function specified in ISO/IEC10118 and record the hash value. Remember that the acquired video files will be used as the master copy.
 - Digital signatures are a secure method of binding the identity of the signer with digital data integrity methods. It involves attaching a piece of code to an electronically transmitted message with the sole purpose of establishing identity. Accordingly, it is possible to use digital signatures to establish legal responsibility and the complete authenticity of the host document.
 - Biometrics uses physical and behavioral characteristics to determine the identity of an individual. By attaching a biometric feature to acquired evidence, it may ensure that the evidence cannot be tampered without compromising the biometric feature
- b) If practical, the collected CCTV system should be wrapped or placed in appropriate packaging suitable for the nature of the device, such as shrink wrap plastic, to avoid contamination of the digital device(s) prior to transporting to other location(s). Shock resistance packaging can be used to avoid physical damage to any components of the device(s).
 - Hard disk drives need to be secured using anti-static bags.
 - Main system units for PC based CCTV systems need to be secured in an appropriate container to avoid damage or spoilage of the potential digital evidence that could reside in it.
- c) Label all potential evidence, all collected digital device(s) and any hardware parts associated with it (them). Evidence labels should not be placed directly on the mechanical parts of the electronic devices, nor should it cover or conceal important information such as the serial number, model number and part number. All device(s) collected should be sealed with tamper-proof seals and the first responder or a personnel in charge must sign on the label.
- d) The DEFR should label the collected items with ink rather than pencil.
- e) It has to be ensured that all digital devices associated with the CCTV system is packaged in a manner that will prevent it from being bent, scratched, or otherwise deformed.
- f) The collected items should be stored in a secure, climate controlled environment or a location that is not subject to extreme temperature or humidity. It should not be exposed to magnetic fields, dust, vibration, moisture, or any other environmental elements that may damage it.

16 Packaging and transporting of potential digital evidence

16.1 Packaging

In preserving acquired digital data and/or collected digital device(s) during packaging, it is important to secure these items in a manner that eliminates spoilage and controls bit rot. Bit rot is the deterioration of magnetic media over time. It is therefore crucial to protect the evidence as best as possible, and use the original data as little as possible.

During packaging, the DEFR should note and address the following:

- a) Wear lint-free gloves and ensure that hands are clean and dry.
- b) The packaging areas should be void of ultraviolet (UV) light (present in some types of fluorescent tubes). UV may hasten the degradation process.
- c) Do not touch magnetic tape, but rather pick tapes up by their protective cases.
- d) Magnetic media should never be stored in paper or cardboard enclosures which tend to generate dust that interferes with the media's functioning. Investigators should store magnetic media in cases made of non-magnetic immobile material, such as polypropylene.
- e) The packaging environment should have a mild temperature and humidity. A too extreme environment can lead to spoilage of potential evidence, example mold growth.
- f) The packaging environment should be free of static electricity. Static electricity may cause electrostatic discharge (ESD). ESD is the sudden and momentary electric current that flows between two objects at difference electrical potentials caused by direct contact or an electrostatic field. During transportation, electromagnetic fields created by magnets and radio transmitters can alter or destroy data as well. Should ESD occur between two or more pieces of potential evidence, the items can suffer permanent damage and potential evidence may be permanently destroyed. Place digital device away from magnetic field sources (e.g. police radios, speakers, x-ray machines).
- g) The packaging environment should be free of dust, grease and chemical pollutants that promote oxidative deterioration and moisture condensation on the magnetic layer.
- h) The plastic covered carrier of floppies and stiffies can easily break, damaging the stored data.
- i) Print-through (the transfer of a signal from one loop of tape onto an adjacent loop) occurs when tapes are stored for long periods without active usage, resulting in poor signal quality.
- j) Disks should never be flexed, bent or picked up by the centre hole of the disk during the packaging process. DEFRs must handle potential digital evidence devices with care and prevent the media from being bumped or dropped.
- k) Cassettes and tapes should be wound to the end of one side after use. They should never be left in a partly wound state for any length of time.
- l) Investigators should label evidence with ink rather than pencil. The pencil's graphite dust can interfere with the reading of the disk or tape. The labels should stick onto a protective case, and not directly onto the magnetic tape or disk.
- m) To ensure correct identification, the investigator should tag each drive with the client name, attorney's office and evidence number. It is required that each drive link up with a chain of custody document, a job and an evidence number.
- n) Devices that are attached to batteries should be checked regularly to ensure that the devices always have enough power supply.

- o) Digital evidence may also contain latent, trace, or biological evidence and take the appropriate steps to preserve it. Digital evidence imaging should be done before latent, trace, or biological evidence processes are conducted on the evidence.
- p) Identify and secure digital device(s) in a container suitable for the nature of the device. For example, package mobile or smart phone(s) in signal-blocking material such as faraday isolation bags, radio frequency-shielding material, or aluminum foil to prevent data messages from being sent or received by the devices.
- q) Do not place label directly on the mechanical parts of a floppy disk or hard disk and avoid covering or concealing important information such as serial number, model number, and part number.
- r) Computers and digital devices should be packaged in such a way to prevent damage from shock and vibration during transportation.
- s) To ensure that nobody tampers with the evidence during transportation or storage, the last investigator to handle the evidence at the crime scene should seal the package. He/she then labels the package and signs the seal. If anybody attempts to open the package, the seal will be broken and the signature spoiled. Every time somebody needs to access the evidence, the old package should be put into a new package, and the new package be sealed and signed.

16.2 Transporting

It is important that collected digital device and/or acquired digital data are preserved during transporting to ensure that they are not tampered with and integrity is maintained. Chain of custody must be maintained at all times. If possible, the DEFR should photograph/videotape and document the handling of evidence leaving the scene to the transport vehicle.

During packaging and transportation the DEFR need to be aware of the possibility of ESD. Ensure that computers and electronic devices are packaged and secured during transportation to prevent damage from shock and vibration.

The transportation process should also allow for an average environment: moisture, high humidity and excessive heat or cold may have a negative impact on the data stored on the potential evidence media. Avoid keeping digital evidence in the transporting vehicle for prolonged periods of time.

If possible, the DEFR should photograph/videotape and document the handling of evidence leaving the transport vehicle to the examination and storage facility.

Annex A (informative)

Examples of potential digital evidence that relates to specific types of investigations (in matrix form)

Table 1 — Potential digital evidence that relates to specific types of investigations

Potential types of digital evidence	Digital evidence investigation types										
	Computer fraud	Child abuse and pornography	Network intrusion	Homicide	Narcotics	Financial fraud and counterfeiting	Identity theft	Telecommunication fraud	Domestic violence	E-mail threats, stalking, harassment	Online gambling
Account data from online auctions	x					x					
Accounting software and files	x					x					
Address books	x		x	x	x	x			x	x	x
Audio files		x		x	x				x		
Backdrops							x				
Bank logs						x					
Birth certificates							x				
Browser history		x									
Business checks						x	x				
Calendar	x				x	x					x
Cashier's checks						x	x				
Chat logs and history	x	x								x	
Check and money order images						x					
Check cashing cards						x	x				
Cloning software								x			
Configuration files			x								
Contact lists											x
Cookies		x									
Counterfeit court documents							x				
Counterfeit currency images						x					
Counterfeit gift certificates							x				
Counterfeit insurance documents							x				
Counterfeit loan documents							x				
Counterfeit sales receipts							x				
Counterfeit vehicle registrations							x				

Potential types of digital evidence	Digital evidence investigation types										
	Computer fraud	Child abuse and pornography	Network intrusion	Homicide	Narcotics	Financial fraud and counterfeiting	Identity theft	Telecommunication fraud	Domestic violence	E-mail threats, stalking, harassment	Online gambling
Currency images						x					
Customer database records								x			x
Customer information	x					x					x
Databases	x				x	x					
Deleted documents						x	x				
Diaries				x					x	x	
Digital camera software	x	x					x				
Digital photo images		x					x				
Driver's licenses							x				
Drug recipes					x						
Electronic money transfers											x
Electronic serial numbers								x			
Electronic signatures						x	x				
E-mail and newsgroup postings							x				
E-mail, notes and letters	x	x	x	x	x	x		x	x	x	x
Executable programs			x								
False identification					x	x					
Financial and asset records	x			x	x	x		x	x	x	x
Fixed and mobile identification numbers								x			
Games		x									
Graphic viewing and editing software		x									
Hardware and software tools							x				
Identification templates							x				
Images		x			x					x	
Images of signatures						x					
Internet activities and activity logs		x	x	x	x	x	x	x		x	x
Internet activity related to ID theft							x				
Internet protocol address and usernames			x								
Internet relay chat logs			x								
Legal documents and wills				x						x	
Maps				x							
Maps to victim locations										x	
Medical records				x							
Money orders						x	x				

Potential types of digital evidence	Digital evidence investigation types										
	Computer fraud	Child abuse and pornography	Network intrusion	Homicide	Narcotics	Financial fraud and counterfeiting	Identity theft	Telecommunication fraud	Domestic violence	E-mail threats, stalking, harassment	Online gambling
Movie files		x									
Negotiable instruments							x				
Network diagrams			x								
Online banking software						x					x
On-line orders						x	x				
On-line trading information						x	x				
Payment card data and numbers	x					x	x				x
Payment card reader / writer						x	x				
Personal checks						x	x				
PIN entry devices						x					
Photos of victim / suspect				x							
Prescription form images					x						
Printed email, notes and letters											x
References to online gambling sites											x
Scanner software							x				
Social security cards							x				
Source code			x								
Sports betting statistics											x
Telephone records				x					x	x	
Text files and documents with usernames / passwords			x								x
Toll free numbers (0800)								x			
Trophy photos				x							
User created directory and file names which classify images		x									
Victim background research										x	

Annex B (informative)

Examples of electronic devices and potential digital evidence

Table 2 – Electronic devices that contain potential digital evidence

Devices	Potential Digital Evidence
Computer Systems	<u>User-created files</u> <ul style="list-style-type: none"> • Address books • Audio/video files • Calendars • Database files • Email files • Image
	<u>User-protected files</u> <ul style="list-style-type: none"> • Compressed files • Encrypted files • Hidden files • Password-protected files
	<u>Computer-created files</u> <ul style="list-style-type: none"> • Backup files • Cookies • Configuration files • Log files • History files • System files • Temporary files
	<u>Others</u> <ul style="list-style-type: none"> • Computer date, time, password • Deleted files • Hidden partitions • Metadata • Software registration information • Unallocated space
Smart cards, dongles, biometric scanners	<ul style="list-style-type: none"> • Identification/authentication information of the card and the user, level of access, configurations, permissions, and the device itself
Answering machines	<ul style="list-style-type: none"> • Caller identification information • Deleted messages • Last number called • Phone numbers and names
Digital cameras	<ul style="list-style-type: none"> • Images • Removable cartridges • Sound • Time and data stamp • Video
	<ul style="list-style-type: none"> • Address book • Appointment/calendar information

Handheld devices (PDAs, organizers)	<ul style="list-style-type: none"> • Email • Password • Phone book • Handwriting • Text messages • Voice messages
External storage media (e.g. memory card)	(same with Computer Systems)
Local Area Network (LAN) Card or Network Interface Card (NIC)	<ul style="list-style-type: none"> • The device itself • MAC access address
Routers, Hubs, Switches	<ul style="list-style-type: none"> • The devices themselves. • Configuration files (for routers)
Pagers	<ul style="list-style-type: none"> • Address information • Email • Phone numbers • Text messages • Voices messages
Printers	<ul style="list-style-type: none"> • Documents • Hard drive • Network identity/information • Superimposed images on the roller • Time and date stamp • User usage log
Scanners	<ul style="list-style-type: none"> • Scanner
Telephone	<ul style="list-style-type: none"> • Appointment calendars/information • Caller identification information • Electronic serial number • Memo • Password • Phone book • Voice mail

Annex C (informative)

List of Validated Imaging Tools for Digital Evidence Acquisition

Table 3 – Acquisition tools that have been validated by the US National Institute of Standard and Technology (NIST) (as of June 2009)

Disk Imaging	Write block (Software)	Write block (Hardware)	Mobile Devices
EnCase LinEn 5.05f and 6.01	PDBLOCK Version 1.02, 2.00 and 2.10	FastBloc FE (USB Interface)	Micro Systemation .XRY 3.6
dd FreeBSD	RCMP HDL V0.4, 0.5, 0.7 and 0.8	FastBloc FE (FireWire Interface)	Guidance Software Neutrino 1.4.14
EnCase 3.20 and 4.22a	ACES Writeblocker Windows 2000 V5.02.00	Tableau T5 Forensic IDE Bridge (USB Interface)	Paraben Device Seizure 2.1
Safeback 2.18	ACES Writeblocker Windows XP V6.10.0	Tableau T5 Forensic IDE Bridge (FireWire Interface)	Susteen DataPilot Secure View 1.8.0
Safeback (Sydex) 2.0		Tableau Forensic SATA Bridge T3u (USB Interface)	
dd GNU fileutils 4.0.36, Provided with Red Hat Linux 7.1		Tableau Forensic SATA Bridge T3u (FireWire Interface)	
Iximagery (Version 2.0, Feb-01 2006)		Tableau Forensic IDE Pocket Bridge T14 (FireWire Interface)	
DCCldd (Version 2.0, June 1 2007)		Tableau T8 Forensic USB Bridge (FireWire Interface)	
FTK Imager 2.5.3.14		Tableau T8 Forensic USB Bridge (USB Interface)	
		WiebeTech Forensic SATADock (FireWire Interface)	
		WiebeTech Forensic SATADock (USB Interface)	
		FastBloc IDE (Firmware Version 16)	

		MyKey NoWrite (Firmware Version 1.05)	
		ICS ImageMasster DriveLock IDE (Firmware Version 17)	
		WiebeTech FireWire DriveDock Combo (FireWire Interface)	
		WiebeTech Forensic ComboDock (USB Interface)	
		WiebeTech Forensic ComboDock (FireWire Interface)	
		WiebeTech Bus Powered Forensic ComboDock (USB Interface)	
		WiebeTech Bus Powered Forensic ComboDock (FireWire Interface)	
		Digital Intelligence UltraBlock SATA (USB Interface)	
		Digital Intelligence UltraBlock SATA (FireWire Interface)	
		Digital Intelligence Firefly 800 IDE (FireWire Interface)	

Bibliography

- [1] ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*, 2001
- [2] ISO/IEC TR 10000-1, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework*
- [3] ISO 10241, *International terminology standards — Preparation and layout*
- [4] ISO 128-30, *Technical drawings — General principles of presentation — Part 30: Basic conventions for views*
- [5] ISO 128-34, *Technical drawings — General principles of presentation — Part 34: Views on mechanical engineering drawings*
- [6] ISO 128-40, *Technical drawings — General principles of presentation — Part 40: Basic conventions for cuts and sections*
- [7] ISO 128-44, *Technical drawings — General principles of presentation — Part 44: Sections on mechanical engineering drawings*
- [8] ISO 31 (all parts), *Quantities and units*
- [9] IEC 60027 (all parts), *Letter symbols to be used in electrical technology*
- [10] ISO 1000, *SI units and recommendations for the use of their multiples and of certain other units*
- [11] ISO 690, *Documentation — Bibliographic references — Content, form and structure*
- [12] ISO 690-2, *Information and documentation — Bibliographic references — Part 2: Electronic documents or parts thereof*
- [13] ISO/IEC 24760:Information technology -- Security techniques -- A framework for identity management
- [14] Guidelines for Evidence Collection and Archiving. Available from: <http://www.ietf.org/rfc/rfc3227.txt>.
- [15] Jansen, W. & Ayers, R. 2007. *Guidelines on Cell Phone Forensics*. Available from: csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf
- [16] Newman, Robert C., *Computer Forensics-Evidence Collection and Management*, Auerbach Publications, 2007
- [17] *Cybercrime and Digital Forensics*, Publisher: Amorette Pedersen, ISBN 13: 978-1-59749-228-7
- [18] Solomon, MG., Barret, D. & Broom, N. 2005. *Computer Forensics JumpStart*. Sybex: San Francisco.