

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

Date: 2009-11-12

**ISO/IEC WD 7934**

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: DIN

## **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.

*Editor's note: All NBs to propose a new, concise title.*

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

H:\SABS\Standards\SC 27\Workgroup 4\27037 - Digital Forensics - Guidelines for identification, collection and/or acquisition and\2\_WD\Redmond\ISO-IEC\_7570\_(E)\_27037\_20091112.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:

[Indicate the full address, telephone number, fax number, telex number, and electronic mail address, as appropriate, of the Copyright Manger of the ISO member body responsible for the secretariat of the TC or SC within the framework of which the working document has been prepared.]

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

Violators may be prosecuted.

# Contents

Page

Foreword .....	iv
Introduction.....	v
<b>1 Scope .....</b>	<b>1</b>
<b>2 Terms and definitions .....</b>	<b>1</b>
<b>3 Abbreviated terms .....</b>	<b>3</b>
<b>4 Overview.....</b>	<b>4</b>
<b>4.1 Requirements for identification, collection, acquisition and preservation of digital evidence .....</b>	<b>4</b>
4.1.1 Auditable .....	4
4.1.2 Repeatable .....	4
4.1.3 Reproducible.....	5
4.1.4 Defensible.....	5
4.2 Principle for identification, collection, acquisition and preservation of digital evidence .....	5
4.3 Digital evidence management process.....	5
4.3.1 Identification .....	6
4.3.2 Collection .....	6
4.3.3 Acquisition .....	7
4.3.4 Preservation .....	8
<b>5 Key components identification, collection, acquisition and preservation of digital evidence .....</b>	<b>8</b>
5.1 Chain of custody .....	8
5.2 Risk assessment .....	8
5.3 Roles and responsibilities.....	9
5.3.1 General .....	9
5.3.2 Competency .....	10
5.3.3 Initial actions.....	10
5.4 Briefing .....	11
5.5 Packaging of potential digital evidence .....	12
5.6 Transporting potential digital evidence .....	13
5.7 Preserving of potential digital evidence .....	13
5.8 Prioritizing collection and acquisition by order of volatility.....	13
<b>6 Use cases of identification, collection and acquisition and preservation .....</b>	<b>14</b>
6.1 Computers, peripheral devices and storage media.....	14
6.1.1 Identification .....	14
6.1.2 Collection .....	15
6.1.3 Acquisition .....	17
6.2 Networked computers and network devices .....	20
6.2.1 Identification .....	20
6.2.2 Collection and acquisition.....	21
<b>Annex A (informative) Examples of potential digital evidence that relates to specific types of investigations (in matrix form).....</b>	<b>24</b>
<b>Annex B (informative) Examples of digital devices and potential digital evidence.....</b>	<b>29</b>
<b>Bibliography.....</b>	<b>32</b>

## 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 investigation process is designed to maintain the integrity and authenticity of the digital evidence – the legally acceptable methodology in obtaining digital evidence will ensure its admissibility in meeting its purposes.

Due to the fragility of potential digital evidence, a legally acceptable methodology needs to be carried out with due care to ensure that the integrity of evidentiary value is preserved. Key components that provide credibility in the investigation are the methodology applied during the process and individuals who are qualified in performing the tasks using the methodology. This International Standard addresses this methodology for legal proceedings and for disciplinary procedures and other related actions in handling digital evidence.

This International Standard provides guidance for individuals and Digital Evidence First Responders (DEFRR) who perform required tasks in the investigation including identifying, collecting and/or acquiring and preserving of digital evidence. This International Standard ensures that responsible individuals manage digital evidence in accordance with practical ways that are acceptable worldwide, with the objective to preserve its integrity and authenticity.

This International Standard should not replace specific legal requirements of a particular jurisdiction. Instead, this International Standard may serve as a practical guideline for Digital Evidence First Responders and Digital Evidence Specialists in investigations involving potential digital evidence. This International Standard may assist in the facilitation of potential digital evidence exchange between jurisdictions. In order to make potential digital evidence valid, users of this International Standard are required to adapt and amend the procedures shown in this International Standard in accordance with the nation's legal requirements for evidence.

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

This International Standard complements ISO/IEC 27001 and ISO/IEC 27002, and in particular the control requirements concerning potential digital evidence acquisition by providing additional implementation guidance. In addition, this International 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 gives guidelines for digital evidence management. It describes the processes of identification, collection, acquisition and preservation of potential digital evidence that may be of evidentiary value. The objective is to assist organizations in their disciplinary procedures, and to facilitate the exchange of potential digital evidence between jurisdictions. This standard deals with common situations encountered throughout the digital management process.

The International Standard intends to provide guidance to those responsible for the identification, collection, acquisition and preservation of potential digital evidence. This includes Digital Evidence First Responders, Digital Evidence Specialists, incident response specialists and forensic laboratory managers. This International Standard intends to inform decision-makers who need make a determination regarding the reliability of any digital evidence presented to them.

This International Standard is applicable to organizations needing to protect, analyze and present potential digital evidence. It is relevant to policy-making bodies that create procedures relating to digital evidence and decision-making bodies need to evaluate digital evidence, often as part of a larger body of evidence. The potential digital evidence may be sourced from any type of media, and refers to data that is already in a digital format. This International Standard does not attempt to cover the conversion of analog data into digital format.

Application of this International Standard requires compliance with national laws, rules and regulations. The International Standard outlines the minimum requirements necessary for enabling transfer of digital evidence between jurisdictions. It provides a framework for the development of processes and procedures for the identification, collection, acquisition and preservation of digital evidence.

## 2 Terms and definitions

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

### 2.1

#### **acquisition**

process of creating a copy of all data within a defined set

NOTE 1 The product of an acquisition is a digital evidence copy.

NOTE 2 The digital evidence copy is retrieved and stored securely.

NOTE 3 It is preferable that the original data is left in tact, but this may not always be practical.

### 2.2

#### **collection**

process of gathering the physical items that contain potential digital

**2.3**

**digital device**

electronic equipment used to process or store digital data

**2.4**

**digital evidence**

information stored or transmitted in binary form that may be relied upon in court

**2.5**

**digital evidence copy**

copy of the digital evidence that has been produced in an evidentially reliable manner and includes both the digital evidence and a means of verifying it

**2.6**

**Digital Evidence First Responder**

**DEFR**

person(s) collecting digital evidence who is authorized, trained and/or qualified in digital evidence collection with responsibility for handling that evidence

*Editor's note: AU and SE to provide definition*

**2.7**

**Digital Evidence Specialist**

*Editor's note: AU and SE to provide definition*

**2.8**

**evidentially reliable**

*Editor's note: AU to define definition*

**2.9**

**hash-function**

function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

- it is computationally infeasible to find for a given output, an input which maps to this output
- it is computationally infeasible to find for a given input, a second input which maps to the same output

NOTE Computational feasibility depends on the specific security requirements and environment.

[ISO/IEC 10118-1:2000]

**2.10**

**hash value**

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

[ISO/IEC 10118-1: 2000]

**2.11**

**hidden protected area**

**HPA**

host protected area

*Editor's note: IT to provide definition.*

**2.12**

**imaging**

copying

process of creating a bitwise copy of a storage media, commonly adopted by digital device forensic practitioners

**2.13****peripheral**

device attached to a digital device in order to expand its functionality

**2.14****preservation**

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

**2.15****reliability**

property of consistent intended behavior and results

[ISO/IEC FDIS 27000]

**2.16****slack space**

*Editor's note: ZA to provide definition.*

**2.17****spoliation**

act of making or allowing unintentional and/or unavoidable change(s) to the potential digital evidence that diminish its evidential value

*Editor's note: US to provide note of caution so that reader understands that not all changed made to the evidence cause spoliation, even if unintended.*

**2.18****system time**

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

**2.19****tampering**

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

**2.20****timestamp**

time variant parameter which denotes a point in time with respect to a common time reference

[ISO/IEC 11770-1:1996]

**2.21****unallocated space**

*Editor's note: ZA to provide definition.*

**2.22****volatile data**

data that is especially prone to change and can be easily modified, possibly causing spoliation

**EXAMPLE** A change can be 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

**3 Abbreviated terms**

**Blob** Binary Large Object

**HPA** Host/Hidden Protected Area

**PDA** Personal Digital Assistant

- PED** Personal Electronic Device
- RAM** Random Access Memory
- RFID** Radio Frequency Identification

## 4 Overview

### 4.1 Requirements for identification, collection, acquisition and preservation of digital evidence

In most jurisdictions, there are three fundamental requirements for evidence, including digital evidence. Evidence must be relevant, reliable and sufficient. Relevance depends on the matter under consideration and in the context of this International Standard, reliability and sufficiency can be explained using a number of overarching principles. The scope of this guide is limited to addressing reliability. Requirements for ensuring reliable identification, collection, acquisition and preservation of digital evidence are auditability, repeatability, reproducibility and defensibility.

*Editor's note: AU to provide content on sufficiency.*

#### 4.1.1 Auditable

It should be possible for an independent assessor to evaluate the steps taken by the DEFR and Digital Evidence Specialist. This will be made possible by appropriately documenting all actions taken. The DEFR and Digital Evidence Specialist should also be able to justify the decision making process in selecting a given course of action. Processes performed by the DEFR and Digital Evidence Specialist should be available for independent assessment to determine if:

- The DEFR was capable of undertaking the processes and of making any conclusions; and
- An appropriate method, technique and/or procedure were followed.

**NOTE** Direct costs need to be considered in relation to evidential significance of the potential data stored on the device and the required quality level of the examination.

#### 4.1.2 Repeatable

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

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

- Using the same measurement procedure;
- Using instruments and conditions that are comparable to the original test; and
- Can be repeated at any time after the original test.

*Editor's note: Need to include new content on different storage media's data retention capabilities (e.g. limitation similar to those applied for auditing purposes and biological evidence).*

The DEFR should be aware that there might be circumstances where it would not be possible to repeat the test, e.g. when a drive has been copied and the original returned into use. In this case, the DEFR must be able to justify the reliability of the imaging process properly.

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

NOTE This subclause relates to hard disks but not volatile memory, as it is not possible to get repeatable results due to the dynamic nature of the memory.

#### 4.1.3 Reproducible

*Editor's note: US to provide content that do not overlap largely with 4.1.2.*

#### 4.1.4 Defensible

DEFRR should be able to justify his/her actions and methods used for the identification, collection, acquisition and preservation of the potential digital evidence. This justification should be achieved by demonstrating that he/she has taken training relative to the tasks performed.

DEFRR should undergo initial tests to ensure he/she is capable of performing the examination reliably. In addition, the DEFRR should be regularly reviewed to ensure ongoing competency.

*Editor's note: UK to propose content on initial test.*

*Editor's note: All NBs to comment on approaches for demonstrating and maintaining competency for both the DEFRR and Digital Evidence Specialist. This may include certifications, qualifications, etc.*

NOTE Competency tests are preferred to ensure the competency of a DEFRR that varies from one jurisdiction to another. However, it is utmost important for DEFRRs 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.

### 4.2 Principle for identification, collection, acquisition and preservation of digital evidence

DEFRRs and Digital Evidence Specialists should interface, interact and acquire the original material of the potential digital evidence in the least intrusive manner. In carrying out this process, the DEFRR should consider the available different methods of collecting and acquiring the potential digital evidence and consider the most appropriate method to use. Methods used should be clear and reproducible.

The general principle is to consider using the least intrusive method, but this needs to be balanced with circumstances, cost and time. In the event where aspects of invasiveness are used in carrying out his/her task, the DEFRR should document the reasons for using the method, and where possible, verify the extent of the effect of any intrusion.

All tools used by the DEFRR must have been validated prior to use. This validation can be carried out internally or externally, but the evidence must be available upon any challenge of the technique. Methods must be acceptable by current incident response best practices. The DEFRR should also:

- document what they did and why they did it;
- determine and apply a method for establishing the accuracy and reliability of the digital evidence copy compared to the original source; and
- recognize that the act of preservation of the potential digital evidence cannot always be non-intrusive.

The DEFRR and Digital Evidence Specialist should first consider using methods that are readily verified, such as snapshot captures of display screens for devices like mobile phones, PDAs and PEDs. However, this has to be balanced with circumstances, cost and time.

### 4.3 Digital evidence management process

The scope of this guideline is identification, collection, acquisition and preservation only.

Digital evidence is by its very nature fragile. It can be altered, tampered with or destroyed through improper handling or examination. Handlers of digital evidence must be appropriately trained to identify the risks and consequences of potential courses of action when dealing with digital evidence. Failure to handle digital devices in an appropriate manner may render the potential digital evidence contained on them unusable.

The fundamental principles of handling potential sources of digital evidence are:

- Minimize handling of the original;
- Account for any change;
- Comply with the local rules of evidence; and
- The DEFR and Digital Evidence Specialist must not exceed their knowledge.

DEFRs need to follow proper procedures and protocols to ensure the integrity and reliability of the potential digital evidence.

*Editor's note: Include information on Locard principle.*

### 4.3.1 Identification

Digital evidence is presented in physical and logical form. Physical refers to the construction and resultant appearance of the digital device. Logical may refer to the format used to arrange and store the data within the digital device, or to the actual digital data. It generally refers to an address or location where potential evidence can be located on a physical device such as a hard disk.

The identification process involves the search for, recognition and documentation of potential digital evidence at an incident scene. The identification process should identify digital storage media that may contain potential digital evidence relevant to the occurred incident.

It should also identify the volatility of data to ensure the correct order of the process of collection and acquisition to preserve the potential digital evidence. In addition, the process should identify the possibility of hidden potential digital evidence.

DEFRs should systematically carry out a thorough search of the incident scene for potential digital evidence. Different types of digital devices that may contain potential digital evidence can easily be overlooked, disguised or co-mingled amongst other irrelevant material.

Subclauses 6.1.1 and 6.2.1 indicate identification guidelines relevant to specific use cases.

*Editor's note: FIRST to provide content on off site network storage and local wireless storage identification.*

### 4.3.2 Collection

In doing either collection or acquisition, potential digital evidence can exist in two conditions: when the incident is in progress (live incident response) or when the incident already happened (dead incident response). Due to these different conditions, different approaches and tools are required.

Collection is the removal of the digital device(s) for later analysis. The collection process involves gathering and documenting potential digital evidence or devices that may contain potential digital evidence. Potential digital evidence may be tampered with or easily spoiled if proper due care is not applied.

There is a variety of reliable collection methods. The DEFR should adopt the best possible collection method based on the situation, cost and time and document this method appropriately. This International Standard recognizes the following collection method:

- Storage media collection

This collection method involves the physical removal of the storage media that may contain potential digital evidence from its original location. The DEFR collects and transports these digital devices to a forensic laboratory for digital device acquisition.

Subclauses 6.1.2 and 6.2.2 indicate collection guidelines relevant to specific use cases.

### 4.3.3 Acquisition

The acquisition process involves gathering and documenting potential digital evidence or digital devices that may contain potential digital evidence. There is a variety of acquisition methods. The DEFR should adopt the best possible acquisition method based on the situation, cost and time and document this method appropriately.

The acquisition method used should produce an image copy of the digital evidence or digital devices that may contain potential digital evidence and hash the image copy using a proven hash-function. The acquisition method employed should be able to obtain the unallocated space, slack space and HPA of the media.

This International Standard recognizes the digital evidence or digital devices that may contain potential digital evidence as follows:

- Storage media
- Partitions
- Files
- Blobs

In the event that the full media or partition is not available, the DEFR may perform a partial acquisition.

In the event that the source drive is too big to image in full, the DEFR may perform a logical acquisition. This acquisition type targets only specific file types or locations for acquisition. This generally takes places on a file and partition level.

In the event that the full media or partition is not available, the DEFR may perform a volatile data (e.g. memory, processes, active connections, etc.) acquisition.

Subclauses 6.1.3 and 6.2.2 indicate acquisition guidelines relevant to specific use cases.

NOTE ISO/IEC 10118 provides more information and examples of proven hash-functions, such as MD5, SHA1 and SHA256.

*Editor's note: IT to provide content on hash-functions.*

*Editor's note: UK to provide content on acquisition of storage media, partitions, files and blobs under the condition of a running system.*

#### 4.3.4 Preservation

Potential digital evidence should be preserved to ensure its usefulness for investigating incidents. There should be no modification to the data itself or any metadata associated with it (e.g. date and time stamps).

The preservation process involves safeguarding potential digital evidence that may contain potential digital evidence from tampering or spoliation. This safeguarding ensures the potential digital evidence's integrity and protects it throughout the digital evidence management process. The DEFR should initiate the act of preserving the potential digital evidence right after the identification process and to be maintained throughout the collection and acquisition process.

Subclause 5.7 indicates acquisition guidelines relevant to specific use cases.

*Editor's note: Extend text on identification to include chain of custody, bagging and labeling. Make use of cross reference to chain of custody.*

## 5 Key components identification, collection, acquisition and preservation of digital evidence

### 5.1 Chain of custody

Chain of custody is a record of who had the responsibility of handling collected digital device(s) and/or acquired digital data at a specific point in time. 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 evidential weighting of potential digital evidence could 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 acquisition and collection process. It should be established from the moment digital device(s) and/or potential digital evidence 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. Chain of custody is necessary to maintain evidentially reliable criteria, but the requirements may differ between jurisdictions.

NOTE Some jurisdictions may have special requirements regarding the chain of custody. The DEFR must adhere to those requirements.

### 5.2 Risk assessment

Conducting risk assessment prior to commencing the collection and acquisition processes is vital because of the safety of the personnel involved in investigating the incident is paramount. The risk assessment should focus on identifying the considerations influencing:

- The information the DEFR wants;
- The choice of collection/acquisition methods;
- The equipment that may be needed on-site; and
- What happens if data/equipment is damaged.

Things to consider during risk assessment include:

- Will the investigated individual(s) be present? If present, do they have a propensity toward violence?
- During what time of the day will the operation be conducted?
- Can the incident scene be isolated from bystanders?
- Are there weapons in the area?
- Can the incident scene be considered unsafe (contains hazardous materials, heavy machinery)?
- Does the surrounding area (office park, college campus, economically depressed) have an impact on the risk potential?
- Could data have been compromised?
- Could the digital device have been logic bombed to destroy data if switched off or accessed in an uncontrolled way?

*Editor's note: AU to provide content on the objective of risk assessment as applicable to the corporate environment.*

### 5.3 Roles and responsibilities

#### 5.3.1 General

The role of a DEFR involves the ability to identify, collect, acquire and preserve potential digital evidence at the incident scene. The role of a DEFR includes the development of a collection and acquisition report, but not necessarily the development of the analysis report. The role of DEFR is vital in ensuring the integrity and authenticity of potential digital evidence.

In ensuring that the integrity of the potential digital evidence is preserved, the DEFR should have adequate experience, skills and knowledge in handling them. Sufficient training will enable DEFRs to handle the digital devices from which they intend to create their product. This is crucial because potential digital evidence 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; and
- They should demonstrate and maintain their skills by undergoing competency test(s) in the relevant area of handling potential digital evidence which may contain potential digital evidence

**NOTE** Competence of a DEFR may vary from one jurisdiction to another. However, it is of utmost importance for a DEFR to undergo a competency test or similar to provide a measure of assurance that the DEFR is capable of performing the necessary tasks without tampering or spoiling the data, which may be of evidentiary value.

The role of a Digital Evidence Specialist involves providing technical support to the DEFR in identifying, collecting, acquiring and preserving potential digital evidence at the incident scene. The Digital Evidence Specialist provides specialist expertise to the DEFR in circumstances where the DEFR may not be adequately equipped to perform his/her duties.

*Editor's note: FIRST to provide content on what training is considered adequate.*

*Editor's note: AU to provide content on the 'product' of the DEFR.*

*Editor's note: AU to provide new content for the bullets to recognize other appropriate means of demonstrating skills.*

*Editor's note: All NBs to comment on standard level of training required for DEFRs.*

### 5.3.2 Competency

Adequate training will enable DEFRs to handle digital devices that 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 potential digital evidence using the tools used to perform the tasks.

*Editor's note: All NBs to comment on standard level of training required for DEFRs.*

### 5.3.3 Initial actions

#### 5.3.3.1 Secure and protect the incident scene

DEFRs 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:

- Secure and take control of the area containing the devices;
- Identify the person in charge of the location;
- Move people away from the devices and power supplies;
- Document anyone who has access to the location or anyone who may have a reason to be involved with the incident scene; and
- If the device is ON do not switch it OFF and if the device is OFF do not switch it ON;
- Search the areas for sticky notes, diaries, papers or notebooks with crucial details about the devices such as passwords and PIN;
- Photograph or video the incident scene, all components and cables in its original position. 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.

NOTE Some jurisdictions may have special requirements for the admission of photographs and video evidence. Even though the format is digital, the DEFR must adhere to those requirements.

#### 5.3.3.2 Employ due care

Avoid any actions that would lead to either tampering or spoliation of potential digital evidence that are stored in digital devices due to intentional or unintentional actions. For instance, exposure to magnetic fields may spoil potential digital evidence contained in magnetic storage media. Thus, the DEFR should employ good practices to avoid tampering or spoliation of potential digital evidence. The DEFR should not access digital devices, such as conducting memory dump from a live digital system, unless with the use of forensically sound tools.

There are some circumstances when it is impractical to collect digital devices. The DEFR should consider the following:

- If there is no legal entitlement to collect the digital device or there is an obligation to use other methods (e.g. to avoid interrupting a business);
- If the DEFR wants to capture the method of operation of a suspect during abuse of a system;
- If the collection or acquisition should take place covertly;
- If it is a mission-critical digital device that cannot tolerate any downtime;
- If it contains volatile data that should be acquired immediately in order to avoid any loss of data due to interruption of power supply;
- If the physical size of the digital device is too big, such as a server at the data center or RAID system;
- If it is a safety-critical digital device that would endanger life if stopped; and
- If it is a business-critical digital device that also services innocent parties.

### 5.3.3.3 Documentation

Documentation is critical when handling potential digital evidence that may contain potential digital evidence. The DEFR should adhere to the following points during documentation at the incident scene:

- Every step taken should be documented. This is to ensure that no details have been left out during the identification, collection and acquisition processes. It may also be helpful in a cross-border investigation whereby the potential digital evidence gathered from another part of the globe can be traced accordingly.
- If the digital devices are switched on, be sensitive of their time and date setting. Compare the time setting with a reliable time source, such as an atomic clock or system clock. These time settings should be documented and noted if any differences are present. Some systems require much user interaction in order to get the time and date settings. The DEFR should be cautious not to modify the system. Only properly trained personnel should retrieve these settings.
- The DEFR should document anything visible on the digital device screen: active programs and processes, as well the names of open documents.
- Any movement of the digital devices should be documented. Maintain the chain of the custody at all times.
- Document all unique identifiers of the digital devices and the associated parts such as serial numbers and unique markings.

## 5.4 Briefing

It is essential that all incident response team members be 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 the things that can occur unexpectedly. Strict warnings should be given to team members to discourage tampering or spoliation with the digital devices and data. Briefing is significant, so that members will know their roles and responsibilities; thus ensure a smooth operation.

Annex A provides content that can be used during a briefing session.

*Editor's note: AU to provide content on the risk of inherent bias.*

*Editor's note: This subclause needs to include generic guidelines on briefing.*

## 5.5 Packaging of potential digital evidence

In preserving acquired potential digital evidence and collected digital device(s) during packaging, it is important to secure these items in a manner that eliminates spoliation and controls magnetic degradation. The phenomena of magnetic degradation cause hard disks, tapes and other low volatility magnetic media to lose data 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 mandatory guidelines:

- Do not touch magnetic tape, but rather pick tapes up by their protective cases.
- To ensure correct identification, the DEFR should label all potential digital evidence. Some jurisdictions have specific requirements regarding the format of labeling evidential material. The DEFR should be familiar with, and conform to, the requirements applicable in the matter at hand. The DEFR should label all potential evidence, all collected digital device(s) and any hardware parts associated with it (them) with a utensil suitable for labeling and archiving. The label should not be placed directly on the mechanical parts of the digital device and should not cover or conceal important identifying information. All device(s) collected should be sealed with tamper-proof seals and the first responder or personnel in charge should sign on the label.
- Devices that are attached to batteries should be checked regularly to ensure that the devices always have enough power supply.
- Identify and secure digital device(s) in a container suitable for the nature of the device.
- Computers and digital devices should be packaged in such a way to prevent damage from shock and vibration during transportation.

During packaging, the DEFR should note and address the following optional guidelines, when applicable:

- Wear lint-free gloves and ensure that hands are clean and dry.
- Magnetic media should be stored in packaging that is magnetically inert, anti-static and free of particles.
- Protect the digital devices from the influence of magnetic sources (e.g. police radios, speakers, x-ray machines). The packaging environment should be free of static electricity.
- The packaging environment should be free of dust, grease and chemical pollutants that promote oxidative deterioration and moisture condensation on the magnetic layer.
- 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.

*Editor's note: SE to provide content on guidelines to prevent print-through.*

- 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.
- Potential 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. In case of prioritizing, the decision should be made by the commissioning body.

*Editor's note: ZA to provide content on packaging guidelines relevant to other media types than magnetic media.*

## 5.6 Transporting potential digital evidence

The DEFR should preserve collected digital devices and acquired potential digital evidence during transporting. The DEFR should maintain the chain of custody throughout the transporting process to prevent possible tampering or spoliation, and the maintain the integrity and authenticity of the digital devices and evidence.

During packaging and transportation the DEFR need to be aware of the possibility of electrostatic discharge.

Ensure that computers and digital 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 potential digital evidence in the transporting vehicle for prolonged periods.

## 5.7 Preserving of potential digital evidence

All collected and acquired potential digital evidence should be protected from loss, tampering or spoliation. The most important activity in the preservation process is to maintain the integrity and authenticity of the potential digital evidence and its chain of custody.

The collected digital device(s) should be wrapped or placed in appropriate packaging suitable for the nature of the device 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).

- The DEFR should consider the sensitivity of the digital device to static electricity. If this is a concern then device should be secured in an anti-static bag.
- Main system units and/or notebooks need to be secured in an appropriate container to avoid tampering or spoliation of the potential digital evidence that could reside in it.
- The packaging areas should be void of ultraviolet (UV) light (present in some types of fluorescent tubes). UV may hasten the degradation process.
- The packaging environment should have a mild temperature and humidity. A too extreme environment can lead to spoliation of potential evidence, example mold growth.

The collected digital device(s) should be stored in a secure 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.

*Editor's note: US to provide content on requirement for trusted time to be associated with evidence.*

## 5.8 Prioritizing collection and acquisition by order of volatility

Prior to collecting and acquiring digital devices that may contain potential digital evidence at an incident scene, it is important to identify them correctly. This includes all information storage equipment, for example ICT and external storage. Examples include satellite navigation systems, CCRV systems, automotive and improvised electronics (see Annex B for additional examples).

Potential digital evidence can be broken into two categories: volatile data and resident data. Volatile data can be easily destroyed or lost forever if due care to protect the data is not applied such as

removing the power supply to the device. Resident data remains on the media even if the power supply is removed.

Since potential digital evidence 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 acquisition commences. Collect and acquire the most volatile potential digital evidence first such as RAM, swap space, running processes, etc. The DEFR should possess a sound knowledge to prioritize according to volatility.

Upon identification, the DEFR should:

- Identify and prioritize potential digital evidence that would be lost forever if the power supply is removed
- Take quick actions to collect and acquire these data with forensically sound methods.

In some instances, time may be a limiting factor during an investigation. In these cases, preference should be given to potential digital evidence identified as relevant to the specific case, and not necessarily to volatile data.

NOTE 1 Some volatile data may change due to factors including but not limited to location, time and changes to the surrounding digital devices – ensure such data is preserved prior to moving the device.

NOTE 2 Devices containing potential digital evidence may be a source of physical evidence (e.g. fingerprints, DNA, particles, etc.). DEFRs need to take care not to spoil such evidence and coordinate with the relevant evidence collectors before proceeding to the next steps.

*Editor's note: UK to provide content: examples of when RAM and memory needs to be examined and recommend this is consider before attending the scene so appropriate resource can be sourced.*

*Editor's note: AU to provide content on a selecting a method for the assessment of evidential significance and providing guidance for its application and use.*

## 6 Use cases of identification, collection and acquisition and preservation

### 6.1 Computers, peripheral devices and storage media

#### 6.1.1 Identification

In the context of this subclause, computers are considered as standalone digital 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 digital 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.

A digital device that has network connectivity, but is not connected at the time of collection or acquisition, should be considered (for the purpose of this International Standard) as a standalone computer.

##### 6.1.1.1 Physical incident scene search and documentation

Before any acquisition or collection can be done, the incident scene should be recorded in a visual manner by either 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.

- The DEFR should record the type and brand of any digital devices used and identify all computer and peripheral devices that may need to be acquired or collected during this initial stage.
- The status of the computers and peripheral devices should remain as it is. If the computers or peripheral devices are powered off, do not turn them on. If the computers or peripheral devices are powered on, the DEFR should not turn them off which otherwise may spoil the potential digital evidence.
- If the computers are powered on, photograph or make a written note of 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.
- A device that has 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.
- The DEFR should also consider using a wireless signal detector to detect and identify wireless signal from wireless devices that may be hidden to locate them. If any networked devices are found, the DEFR should continue with the evidence handling process as described in Clause 6.2 of this document.

#### **6.1.1.2 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 digital devices and other relevant details. The DEFR needs to record the name and designation of this person.

The DEFR also need to collect some evidence verbally. He/she may talk to individuals who are directly or indirectly involved with the potential digital evidence or device to be collected. These individuals 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. These conversations may be recorded to ensure that the details are accurate and that the witness cannot change his/her statement.

Non-digital evidence collection should be done in all digital device investigations.

#### **6.1.2 Collection**

Two scenarios exist in which collection may need to be conducted: when the digital devices are powered on, and when the digital devices are powered off and. In many cases, the digital device systems and peripheral devices can just be collected, packaged and transported back to the forensic laboratory for acquisition (refer to subclauses 5.5 and 5.6).

##### **6.1.2.1 Powered on digital devices**

The DEFR can follow a number of guidelines for collection when the digital device is found to be powered on. All of these guidelines are ideal and appropriate in some cases, whilst other guidelines are only relevant in legacy systems. Accordingly, the guidelines can be categorized as mandatory and optional.

Following is mandatory guidelines that should be followed by DEFR in all cases involving potential digital evidence. These guidelines apply when the DEFR decided that a powered on digital system should be acquired:

- The configuration of the digital device may determine whether the DEFR need to shut the device down through normal administrative procedures, or whether the device's plug should be pulled from the power socket. The DEFR may need to consult with Digital Evidence Specialists to determine the best approach given the specific circumstances. If the decision is made to pull the plug, the DEFR need to remove the power supply cable by first removing the end attached to the digital device and not that attached to the socket. This will avoid data being written to the digital device's storage media if it is fitted with uninterruptible power supply (UPS) which will spoil the potential digital evidence.

NOTE If the power is removed from a powered on digital system, any potential evidence stored in encrypted volumes will be lost, unless the decryption key is obtained. Potentially valuable live data could be lost, leading to damage claims or loss of human lives, such as corporate data or digital devices controlling medical equipments.

- Disconnect and secure all cables from the digital device and label the ports so that the system can be reconstructed in a later stage.
- Place tape over the power switch.

Following is optional guidelines that are relevant depending on the configuration of the specific digital device.

- 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.
- Place tape over the floppy disk slot, if present.
- 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.

The DEFR must conduct non-electronic evidence collection according to procedural laws to ensure that any evidence is admissible. This is especially important if the non-electronic evidence is used to interpret electronic evidence, for example, a pass-phrase that is required to unlock encryption.

NOTE The action of depressing the power button on a digital device may be configured to kick off a script that may alter information and/or delete information from the system before shutting down.

*Editor's note: Editor to provide flow diagrams.*

#### **6.1.2.2 Powered off digital devices**

The DEFR can follow a number of guidelines for collection when the digital device is found to be powered on. All of these guidelines are ideal and appropriate in some cases, whilst other guidelines are only relevant in legacy systems. Accordingly, the guidelines can be categorized as mandatory and optional. Following is the recommended mandatory guidelines for collection when the digital device is found to be powered off:

- Remove the power supply cable by first removing the end attached to the digital device 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.
- Disconnect and secure all cables from the digital devices and label the ports so that the system can be reconstructed in a later stage.
- If field conditions allow, remove the hard disk drive(s) from the digital 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).
- Place tape over the power switch.

NOTE The hard drive should not be removed from the digital system until it is going to be acquired. Removing it from the case increases the risk of damage or mixing it up with another exhibit.

Following is optional guidelines that are relevant depending on the configuration of the specific digital device:

- Place tape over the floppy disk slot, if present.
- 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.

*Editor's note: Editor to provide flow diagrams.*

### 6.1.3 Acquisition

The DEFR needs to decide to either collect the computers, peripheral devices and storage media, or acquire the potential digital evidences from them. The choice needs to be balanced with circumstances, cost, time and available resources.

Three scenarios exist in which acquisition may need to be conducted: when the digital devices are powered on, when the digital devices are powered off and when the digital devices are powered on but cannot be powered off (such as mission-critical digital systems). In all three scenarios, the DEFR is required to make an accurate digital evidence copy of the digital devices' storage media that is suspected to contain potential digital evidence.

If an image cannot be obtained, accurate copies of specific files suspected to contain potential digital evidence may be acquired. After the acquisition process has completed, the DEFR should seal the acquired data by using hashing algorithms or digital signatures. 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 files by using any hashing function specified in ISO/IEC10118 and record the hash value. Remember that the acquired files will be used as the master digital evidence copy. Hashing generally occurs during the acquisition process and not only after the acquisition.
- Digital signatures are a secure method of binding the identity of the signer with potential digital evidence 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.

*Editor's note: AU to provide reworded paragraph, using alternative terminology to 'seal'.*

#### 6.1.3.1 Powered on digital devices

The DEFR can follow any of a number of guidelines for acquisition when the digital device is found to be powered on. All of these guidelines are ideal and appropriate in some cases, whilst other guidelines are only relevant in legacy systems. Accordingly, the guidelines can be categorized as mandatory and optional.

Following is mandatory guidelines that should be followed by DEFR in all cases involving potential digital evidence acquisition:

- First, consider acquiring the potential digital data that may otherwise be lost if the digital device is powered off. They are also known as volatile data and data stored on RAM, running processes, network connections and date/time settings. RAM also contains useful information such as decrypted applications and passwords. Other than RAM, newest digital devices (mainly notebook) may be equipped with the Turbo Memory module, which may eventually contain the same kind of information stored in the RAM.

- DEFR must never trust the programs on the systems. For this reason it is recommended that the DEFR use his own trusted tools (static binaries). The DEFR should be trained appropriately in this use, since introducing tools to the system may displace potential evidence and content of memory may be paged out when binaries are loaded. All the actions performed and the resulting changes made to the digital system must be recorded and understood.
- Consider logical acquisition when full-disk-encryption is suspected. First check if this may be the case by looking at the raw disk or some crypto-detection utility. In addition, photograph and document a reliable time source next to a DCF-clock. Record the time of each performed action.
- Execute the imaging process by using a validated imaging tool to create an image of the suspect disk. The digital evidence copy will be stored on a target disk that has been sanitized of any previous data. The sanitization process must have been validated to ensure that previous data remains. One possible solution is to follow the US Department of Defense 5220.22-M National Industrial Security Program Operating Manual (NISPOM) requirements.
- Place tape over the power switch.

Following is optional guidelines that are relevant depending on the configuration of the specific digital device:

- Place tape over the floppy disk slot, if present.
- 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.
- As an alternative to sealing the acquired data with hashing algorithms or digital signatures, the DEFR can also use biometric features. 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.

NOTE The action of depressing the power button on a digital device may be configured to kick off a script that may alter information and/or delete information from the system before shutting down.

*Editor's note: IT to provide content on how to handle the situation when the digital device is switched on but locked.*

*Editor's note: Editor to provide flow diagrams.*

*Editor's note: All NBs to provide guidelines on how to handle RAID.*

### 6.1.3.2 Powered off digital devices

It is easier to handle powered off digital system compared to powered on digital system because there is no need to acquire the volatile data. Following is mandatory guidelines for acquisition when the digital device is found to be powered off:

- Remove the power supply cable by first removing the end attached to the digital device 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.
- Disconnect and secure all cables from the digital devices and label the ports so that the system can be reconstructed in a later stage.
- Place tape over the power switch.
- If field conditions allow, remove the hard disk drive(s) from the digital 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).

- Execute the imaging process by using a validated imaging tool to create an image of the suspect disk. The digital evidence copy will be stored on a target disk that has been sanitized of any previous data. The sanitization process must have been validated to ensure that previous data remains. One possible solution is to follow the US Department of Defense 5220.22-M National Industrial Security Program Operating Manual (NISPOM) requirements.

**NOTE** The hard drive should not be removed from the digital system until it is going to be acquired. Removing it from the case increases the risk of damage or mixing it up with another exhibit.

Following are optional guidelines that are relevant depending on the configuration of the specific digital device:

- Place tape over the floppy disk slot, if present.
- 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.
- As an alternative to sealing the acquired data with hashing algorithms or digital signatures, the DEFR can also use biometric features. 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.

*Editor's note: Editor to provide flow diagrams.*

*Editor's note: All NBs to provide guidelines on how to handle RAID.*

### 6.1.3.3 Mission-critical digital devices

In some cases, the digital systems cannot be powered off due to the critical nature of the systems. These systems are such as servers at data centers that are also servicing innocent clients, surveillance systems, medical systems and many others that may have critical impact if interrupted or powered off. Special care should be taken when dealing with such systems.

After the acquisition process has completed, the DEFR should seal the acquired data by using hashing algorithms or digital signatures. 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 files by using any hashing function specified in ISO/IEC10118 and record the hash value. Remember that the acquired files will be used as the master digital evidence copy. Hashing generally occurs during the acquisition process and not only after the acquisition.
- Digital signatures are a secure method of binding the identity of the signer with potential digital evidence 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.

*Editor's note: AU to provide reworded paragraph, using alternative terminology to 'seal'.*

Following are mandatory guidelines for acquisition when the digital device cannot be powered off:

- First, consider acquiring the potential digital data that may otherwise be lost if the digital device is powered off. They are also known as volatile data and data stored on RAM, running processes, network connections and date/time settings. RAM also contains useful information such as decrypted applications and passwords. Other than RAM, newest digital devices (mainly notebook) may be equipped with the Turbo Memory module, which may eventually contain the same kind of information stored in the RAM.

- DEFR must never trust the programs on the systems. For this reason, it is recommended the DEFR to use his own trusted tools (static binaries). DEFR should be trained appropriately in this use, since introducing tools to the system may displace potential evidence and content of memory may be paged out when binaries are loaded. All the actions performed and the resulting changes made to the digital system must be recorded and understood.
- Consider logical acquisition when full-disk-encryption is suspected. First check if this may be the case by looking at the raw disk or some crypto-detection utility. In addition, photograph and document a reliable times source next to a DCF-clock. Record time of each performed action.
- Identify the part of the storage media that needs to be acquired such as a partition, a directory or a file.
- Document collection methodology and need for the partial collection.
- Execute the imaging process by using validated or otherwise well-established imaging tool to create an image of the identified partition, directory or file. The digital evidence copy will be stored on a target disk that has been sanitized of any previous data. The sanitization process must have been validated to ensure that previous data remains. One possible solution is to follow the US Department of Defense 5220.22-M National Industrial Security Program Operating Manual (NISPOM) requirements.

#### 6.1.3.4 Storage media

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 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,

- Check and record the make, model and serial number (if any) of each storage media found.
- The DEFR should decide whether to collect the identified storage media or conduct on-site acquisition. This will depend on the nature of the case and the available resources.
- If the DEFR decides to collect, the collected storage media should be wrapped or placed in appropriate packaging.
- Label all storage media and any associated parts with them. Evidence labels should not be placed directly on the mechanical parts of the digital 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
- The collected storage media should be stored in a suitable environment for data preservation.

*Editor's note: A generic discussion will be included here to offer practical guidance or reference to an appropriate standard, such as AS2838 – Computer Accommodation.*

## 6.2 Networked computers and network devices

### 6.2.1 Identification

In the context of this subclause, 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, mobile devices, PDAs, PEDs, Bluetooth devices, CCTV systems and many more. Take note that if digital devices are networked, it is difficult to ascertain where the potential digital evidence being sought is kept immediately. The data could be anywhere on the network.

Due to the general small size of mobile devices, the 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). Unauthorized people may not have access to any devices that may contain potential digital evidence. No communication devices should be able to receive or transmit data.

### 6.2.1.1 Physical incident scene search and documentation

Before any acquisition or collection can be done, the incident scene should be recorded in a visual manner by either 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.

- The DEFR should record the type, brand, model and serial number of any digital devices used. He/she should identify all digital devices that may need to be acquired or collected during this initial stage. All the mobile devices and their associated items such as memory cards, SIM cards, chargers and cradles found at the scene, their associated serial numbers and any identifying features should be recorded. Also try to find original packaging of mobile phones; these might contain notes with PIN and PUK codes.
- If the networked device is a CCTV system, the DEFR should note the number of cameras connected to the system, as well as which of these cameras are actively recording. He/she should also 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 acquisition process, it is then possible to return the system to its original state.
- The status of the digital devices should remain as is. If the digital devices are powered off, the DEFR should not turn them on. If they are powered on, the DEFR should not turn them off. This may prevent unnecessary spoliation of potential digital evidence. A device that has 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.
- The DEFR should also consider using a wireless signal detector to detect and identify wireless signal from wireless devices that may be hidden to locate them.

### 6.2.2 Collection and acquisition

The DEFR needs to decide whether to collect or acquire the potential digital evidences from the digital devices. The choice needs to be balanced with circumstances of cost, time and available resources.

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. To complicate the collection and acquisition process further, 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. Removing a storage card from a switched on mobile device might interfere with processes running in the background.

Generally, mobile devices need to be switched on in order to allow a forensic bitwise digital evidence copy. These devices cannot be powered off without data loss, whilst a powered on device continuously alters 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.

It is important that the DEFR does not introduce Wi-Fi devices into the scene that might change pairing information on potential evidential devices. This is particularly important if investigation needs to know what devices have been connected.

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

- Once the DEFR has recognized and identified the network devices, he/she should isolate the device from the network. This can be done by unplugging the connection to the telephone system, network port or wireless access point. Under some circumstances, mobile devices should be switched off upon collection to prevent data being changed from the receipt of communication and in modern phone erase commands. Switching it off will protect information from being erased or lost. If a phone is left on, documented justification must be provided (e.g. a foreign phone with an unknown PIN code that would delay time-critical examination in obtained PUK through INTERPOL).
- If collection take precedence over acquisition and it is known that the device contains volatile memory, the device should be connected to a charger continuously. Make sure that a longer power is not left unnoticed.
- For wired networks, trace the connections to the digital devices and label the ports for future reconstruction of the whole network. A device may have more than one communications method. For example, a computer may have a wired LAN, a wireless modem and a mobile phone card. The DEFR should identify all communication methods and take appropriate steps to protect against their improper use
- 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. Once the DEFR is sure that no potential evidence will be lost as a result, the connections from the digital devices can be removed.
- It is important to note that mobile phones, PDAs and PEDs may be connected to the network via Wi-Fi or Bluetooth connections. Ensure these devices are not left behind.
- For a mobile device that is found to be on, the DEFR should use a faraday box or a shielded box to prevent the device from connecting to the network. GPS (factory-built into cars) enabled devices should not be moved unshielded because new location data might be gathered during transport. Connecting to a network may result in spoliation of potential digital evidence due to the incoming calls and messages.
- 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.
- The DEFR should always acquire the mobile device before to remove the battery (to access, for example, to the SIM card), in order to prevent the loss of important information.
- Subsequently, treat each digital devices as it would be treated as a stand-alone computer (refer to subclause 6.1).

If the DEFR decided on following an acquisition process, the network devices should be kept running for further analysis to ascertain the other devices connected to the network devices. The DEFR should consider the possibility of sabotage by suspect through active network connection. Monitor for this or decide to disconnect.

DEFR must understand that the approach to extract video sequences from a PC based or embedded DVR CCTV system is different from conventional digital data extraction from a PC. Specific guidelines for the acquisition of CCTV systems:

- Before the collection and acquisition process can be started, the DEFR should determine the period required. He/she should also determine which cameras are required and whether they can be acquired separately.
- There are a few options to undertake the acquisition process:
  - 1) 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).
  - 2) Acquire the video files via USB external hard disk drive. This method is deemed the most practical at the moment.
  - 3) Acquire the video files via a network connection. This may be available if the CCTV system is a PC based system or an embedded DVR based system with a have network port.
  - 4) A quick method is by replacing the CCTV system's hard disk with a blank or cloned hard disk. However, the DEFR should assess several risks 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.

NOTE The hard disk may require the system's hardware for playback.

- Upon completing the acquisition, the acquired file should be check 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 digital device file formats) for its playability on another system.
- The media that contains the acquired file should be treated as the master digital evidence copy.
- 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.

In circumstances where not all acquisition options can 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 forensic laboratory. 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.

## Annex A (informative)

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

*Editor's note: Editors and UK to review Annex A.*

**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				

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
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				
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				

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
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								

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
Legal documents and wills				x						x	
Maps				x							
Maps to victim locations										x	
Medical records				x							
Money orders						x	x				
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				

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
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 digital devices and potential digital evidence

*Editor's note: To rework or find existing external site for further information, e.g. <http://www.unisanet.unisa.edu.au/staff/Homepage.asp?Name=Jill.Slay>*

**Table 2 – Digital devices that may contain potential digital evidence**

Devices	Potential Digital Evidence
Computer Systems	<u>User-created files</u> <ul style="list-style-type: none"> <li>— Address books</li> <li>— Audio/video files</li> <li>— Calendars</li> <li>— Database files</li> <li>— Email files</li> <li>— Image</li> </ul>
	<u>User-protected files</u> <ul style="list-style-type: none"> <li>— Compressed files</li> <li>— Encrypted files</li> <li>— Hidden files</li> <li>— Password-protected files</li> </ul>
	<u>Computer-created files</u> <ul style="list-style-type: none"> <li>— Backup files</li> <li>— Cookies</li> <li>— Configuration files</li> <li>— Log files</li> <li>— History files</li> <li>— System files</li> <li>— Temporary files</li> </ul>

	<p><u>Others</u></p> <ul style="list-style-type: none"> <li>— Computer date, time, password</li> <li>— Deleted files</li> <li>— Hidden partitions</li> <li>— Metadata</li> <li>— Software registration information</li> <li>— Unallocated space</li> </ul>
<p>Smart cards, dongles, biometric scanners</p>	<ul style="list-style-type: none"> <li>— Identification/authentication information of the card and the user, level of access, configurations, permissions, and the device itself</li> </ul>
<p>Answering machines</p>	<ul style="list-style-type: none"> <li>— Caller identification information</li> <li>— Deleted messages</li> <li>— Last number called</li> <li>— Phone numbers and names</li> </ul>
<p>Digital cameras</p>	<ul style="list-style-type: none"> <li>— Images</li> <li>— Removable cartridges</li> <li>— Sound</li> <li>— Time and data stamp</li> <li>— Video</li> </ul>
<p>Handheld devices (PDAs, PEDs, organizers)</p>	<ul style="list-style-type: none"> <li>— Address book</li> <li>— Appointment/calendar information</li> <li>— Email</li> <li>— Password</li> <li>— Phone book</li> <li>— Handwriting</li> <li>— Text messages</li> <li>— Voice messages</li> </ul>
<p>External storage media (e.g. memory card)</p>	<ul style="list-style-type: none"> <li>— (same with Computer Systems)</li> </ul>

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

## Bibliography

- [1] IOCE, *G8 proposed principles for the procedures relating to digital evidence*. Available from: <http://ioce.org/core.php?ID=5>.
- [2] ISO/IEC 24760: Information technology - Security techniques - A framework for identity management.
- [3] ISO/IEC 27031:2009 Information technology - Security techniques - Guidelines for ICT readiness for business continuity.
- [4] ISO/IEC 27035:2008 Information technology - Security techniques - Information security incident management.
- [5] *Guidelines for evidence collection and archiving*. Available from: <http://www.ietf.org/rfc/rfc3227.txt>.
- [6] Jansen, W. & Ayers, R. 2007. *Guidelines on Cell Phone Forensics*. Available from: [csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf](http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf).
- [7] Newman, Robert C., *Computer Forensics-Evidence Collection and Management*, Auerbach Publications, 2007.
- [8] *Cybercrime and Digital Forensics*, Publisher: Amorette Pedersen, ISBN 13: 978-1-59749-228-7.
- [9] Solomon, MG., Barret, D. & Broom, N. 2005. *Computer Forensics JumpStart*. Sybex: San Francisco.