INTERNATIONAL STANDARD

ISO/IEC 27037

First edition
2012-10-15

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

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

Reference number
ISO/IEC 27037:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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 shall 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, *IT Security techniques*.

Introduction

This International Standard provides guidelines for specific activities in handling potential digital evidence; these processes are: identification, collection, acquisition and preservation of potential digital evidence. These processes are required in an investigation that is designed to maintain the integrity of the digital evidence – an acceptable methodology in obtaining digital evidence that will contribute to its admissibility in legal and disciplinary actions as well as other required instances. This International Standard also provides general guidelines for the collection of non-digital evidence that may be helpful in the analysis stage of the potential digital evidence.

This International Standard intends to provide guidance to those individuals responsible for the identification, collection, acquisition and preservation of potential digital evidence. These individuals include Digital Evidence First Responders (DEFRs), Digital Evidence Specialists (DESs), incident response specialists and forensic laboratory managers. This International Standard ensures that responsible individuals manage potential digital evidence in practical ways that are acceptable worldwide, with the objective to facilitate investigation involving digital devices and digital evidence in a systematic and impartial manner while preserving its integrity and authenticity.

This International Standard also intends to inform decision-makers who need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyze and present potential digital evidence. It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

The potential digital evidence referred to in this International Standard may be sourced from different types of digital devices, networks, databases, etc. It 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.

Due to the fragility of digital evidence, it is necessary to carry out an acceptable methodology to ensure the integrity and authenticity of the potential digital evidence. This International Standard does not mandate the use of particular tools or methods. Key components that provide credibility in the investigation are the methodology applied during the process, and individuals qualified in performing the tasks specified in the methodology. This International Standard does not address the methodology for legal proceedings, disciplinary procedures and other related actions in handling potential digital evidence that are outside the scope of identification, collection, acquisition and preservation.

Application of this International Standard requires compliance with national laws, rules and regulations. It should not replace specific legal requirements of any jurisdiction. Instead, it may serve as a practical guideline for any DEFR or DES in investigations involving potential digital evidence. It does not extend to the analysis of digital evidence and it does not replace jurisdiction-specific requirements that pertain to matters such as admissibility, evidential weighting, relevance and other judicially controlled limitations on the use of potential digital evidence in courts of law. This International Standard may assist in the facilitation of potential digital evidence exchange between jurisdictions. In order to maintain the integrity of the digital evidence, users of this International Standard are required to adapt and amend the procedures described in this International Standard in accordance with the specific jurisdiction's legal requirements for evidence.

Although this International Standard does not include forensic readiness, adequate forensic readiness can largely support the identification, collection, acquisition, and preservation process of digital evidence. Forensic readiness is the achievement of an appropriate level of capability by an organization in order for it to be able to identify, collect, acquire, preserve, protect and analyze digital evidence. Whereas the processes and activities described in this International Standard are essentially reactive measures used to investigate an incident after it occurred, forensic readiness is a proactive process of attempting to plan for such events.

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. This International Standard should be read in conjunction with other standards related to digital evidence and the investigation of information security incidents.

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

1 Scope

This International Standard provides guidelines for specific activities in handling digital evidence, which are identification, collection, acquisition and preservation of digital evidence that may be of evidential value. This International Standard provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.

This International Standard gives guidance for the following devices and/or functions that are used in various circumstances:

— Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto optical disks, data devices with similar functions,

— Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards,

— Mobile navigation systems,

— Digital still and video cameras (including CCTV),

— Standard computer with network connections,

— Networks based on TCP/IP and other digital protocols, and

— Devices with similar functions as above.

NOTE 1 The above list of devices is an indicative list and not exhaustive.

NOTE 2 Circumstances include the above devices that exist in various forms. For example, an automotive system may include mobile navigation system, data storage and sensory system.

2 Normative reference

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/TR 15801, *Document management — Information stored electronically — Recommendations for trustworthiness and reliability*

ISO/IEC 17020, *Conformity assessment — Requirements for the operation of various types of bodies performing inspection*

ISO/IEC 17025:2005, *General requirements for the competence of testing and calibration laboratories*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions in ISO/IEC 27000, ISO/IEC 17020, ISO/IEC 17025 and ISO/TR 15801, as well as the following apply.

3.1
acquisition
process of creating a copy of data within a defined set

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

3.2
allocated space
area on digital media, including primary memory, which is in use for the storage of data, including metadata

3.3
collection
process of gathering the physical items that contain potential digital evidence

3.4
digital device
electronic equipment used to process or store digital data

3.5
digital evidence
information or data, stored or transmitted in binary form that may be relied on as evidence

3.6
digital evidence copy
copy of the digital evidence that has been produced to maintain the reliability of the evidence by including both the digital evidence and verification means where the method of verifying it can be either embedded in or independent from the tools used in doing the verification

3.7
Digital Evidence First Responder
DEFR
individual who is authorized, trained and qualified to act first at an incident scene in performing digital evidence collection and acquisition with the responsibility for handling that evidence

NOTE Authority, training and qualification are the expected requirements necessary to produce reliable digital evidence, but individual circumstances may result in an individual not adhering to all three requirements. In this case, the local law, organizational policy and individual circumstances should be considered.

3.8
Digital Evidence Specialist
DES
individual who can carry out the tasks of a DEFR and has specialized knowledge, skills and abilities to handle a wide range of technical issues

NOTE A DES may have additional niche skills, for example, network acquisition, RAM acquisition, operating system software or Mainframe knowledge.

3.9
digital storage medium
device on which digital data may be recorded

[Adapted from ISO/IEC 10027:1990]

3.10
evidence preservation facility
secure environment or a location where collected or acquired evidence is stored

NOTE An evidence preservation facility should not be exposed to magnetic fields, dust, vibration, moisture or any other environmental elements (such as extreme temperature or humidity) that may damage the potential digital evidence within the facility.

3.11
hash value
string of bits which is the output of a hash-function

[ISO/IEC 10118-1:2000]

3.12
identification
process involving the search for, recognition and documentation of potential digital evidence

3.13
imaging
process of creating a bitwise copy of digital storage media

NOTE The bitwise copy is also called a physical copy.

EXAMPLE When imaging a hard drive, the DEFR would also copy data that has been deleted.

3.14
peripheral
device attached to a digital device in order to expand its functionality

3.15
preservation
process to maintain and safeguard the integrity and/or original condition of the potential digital evidence

3.16
reliability
property of consistent intended behaviour and results

[ISO/IEC 27000:2009]

3.17
repeatability
property of a process conducted to get the same test results on the same testing environment (same computer, hard drive, mode of operation, etc.)

3.18
reproducibility
property of a process to get the same test results on a different testing environment (different computer, hard drive, operator, etc.)

3.19
spoliation
act of making or allowing change(s) to the potential digital evidence that diminishes its evidential value

3.20
system time
time generated by the system clock and used by the operating system, not the time computed by the operating system

3.21
tampering
act of deliberately making or allowing change(s) to digital evidence (i.e. intended or purposeful spoliation)

3.22
timestamp
time variant parameter which denotes a point in time with respect to a common time reference

[ISO/IEC 11770-1:1996]

3.23
unallocated space
area on digital media, including primary memory, which has not been allocated by the operating system, and which is available for the storage of data, including metadata

3.24
validation
confirmation, through the provision of objective proof, that the requirements for a specific intended use or application have been fulfilled

[ISO/IEC 27004:2009]

3.25
verification function
function which is used to verify that two sets of data are identical

NOTE 1 No two non-identical data sets should produce an identical match from a verification function.

NOTE 2 Verification functions are commonly implemented using hash functions such as MD5, SHA1, etc., but other methods may be used.

3.26
volatile data
data that is especially prone to change and can be easily modified

NOTE 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.

4 Abbreviated terms

AVI Audio Video Interleave

CCTV Closed Circuit Television

CD Compact Disk

DNA Deoxyribonucleic Acid

DEFR Digital Evidence First Responder

DES Digital Evidence Specialist

DVD Digital Video/Versatile Disk

ESN	Electronic Serial Number
GPS	Global Positioning System
GSM	Global System for Mobile Communication
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
ISIRT	Information Security Incident Response Team
LAN	Local Area Network
MD5	Message-Digest Algorithm 5
MP3	MPEG Audio Layer 3
MPEG	Moving Picture Experts Group
NAS	Network Attached Storage
PDA	Personal Digital Assistant
PED	Personal Electronic Device
PIN	Personal Identification Number
PUK	PIN Unlock Key
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RFID	Radio Frequency Identification
SAN	Storage Area Network
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
USB	Universal Serial Bus
UPS	Uninterruptible Power Supply
USIM	Universal Subscriber Identity Module
UV	Ultraviolet
Wi-Fi	Wireless Fidelity

5 Overview

5.1 Context for collecting digital evidence

Digital evidence can be required for use in a number of distinct scenarios, each of which has a different balance between the drivers of evidential quality, timeliness of analysis, restoration of service and cost of digital evidence collection. Organizations will therefore be required to have a prioritization process that identifies the needs and balances evidential quality, timeliness and service restoration before tasking DEFR resources. A prioritization process involves carrying out an evaluation of the material available to determine the possible evidential value and the order in which potential digital evidence should be collected, acquired or preserved. Prioritization is carried out to minimize the risk of potential digital evidence being spoiled and maximize evidentiary value of the potential digital evidence collected.

5.2 Principles of digital evidence

In most jurisdictions and organizations, digital evidence is governed by three fundamental principles: relevance, reliability and sufficiency. These three principles are important to all investigations, not just those for digital evidence to be admissible in court. Digital evidence is relevant when it goes towards proving or disproving an element of the specific case being investigated. Although the detailed definition of "reliable" varies among jurisdictions, the general meaning of the principle, "to ensure digital evidence is what it purports to be" is widely held. It is not always necessary for the DEFR to collect all data or to make a complete copy of the original digital evidence. In many jurisdictions, the concept of sufficiency means the DEFR needs to collect enough potential digital evidence to allow the elements of the matter to be adequately examined or investigated. Understanding this concept is important for the DEFR to prioritize the effort properly when time or cost is a concern.

NOTE The DEFR should ensure that the collection of potential digital evidence is in accordance with the local jurisdictional laws and regulations, as required by the specific circumstances.

All processes to be used by the DEFR and DES should have been validated prior to use. If the validation is carried out externally, the DEFR or DES should verify that the validation is appropriate for their specific use of the processes and the environment and circumstances in which the processes are about to be used. The DEFR or DES should also:

a) document all actions;

b) determine and apply a method for establishing the accuracy and reliability of the potential digital evidence copy compared to the original source; and

c) recognize that the act of preservation of the potential digital evidence cannot always be non-intrusive.

5.3 Requirements for digital evidence handling

5.3.1 General

The principles laid down in clause 5.2 above can be satisfied as follows:

— Relevance: It should be possible to demonstrate that material acquired is relevant to the investigation - i.e. that it contains information of value in assisting the investigation of the particular incident and that there is a good reason for it to have been acquired. Through auditing and justification, the DEFR should be able to describe the procedures followed and explain how the decision to acquire each item was made.

— Reliability: All processes used in handling potential digital evidence should be auditable and repeatable. The results of applying such processes should be reproducible.

— Sufficiency: The DEFR should have taken into consideration that enough material has been gathered to allow a proper investigation to be carried out. The DEFR should be able, through audit and justification, to

give an indication of how much material, in total, was considered and the procedures used to decide how much and which material to acquire.

NOTE The materials may be gathered via acquisition and/or collection activities.

There are four key aspects in digital evidence handling: auditability, justifiability and either repeatability or reproducibility depending on particular circumstances.

5.3.2 Auditability

It should be possible for an independent assessor or other authorized interested parties to evaluate the activities performed by a DEFR and DES. This will be made possible by appropriately documenting all actions taken. The DEFR and DES should be able to justify the decision-making process in selecting a given course of action. Processes performed by a DEFR and DES should be available for independent assessment to determine if an appropriate scientific method, technique or procedure was followed.

5.3.3 Repeatability

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

- Using the same measurement procedure and method;
- Using the same instruments and under the same conditions; and
- Can be repeated at any time after the original test.

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. The DEFR should be aware that there might be circumstances where it would not be possible to repeat the test, e.g. when an original hard drive has been copied and returned into use, or when an item involves volatile memory. In this case, the DEFR should assure the acquisition process is reliable. To achieve repeatability, quality control and documentation of the process should be in place.

5.3.4 Reproducibility

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

- Using the same measurement method;
- Using different instruments and under different conditions; and
- Can be reproduced at any time after the original test.

The needs to reproduce results vary according to jurisdictions and circumstances, so the DEFR, or the individual doing the reproduction will need to be informed about the applicable conditions.

5.3.5 Justifiability

The DEFR should be able to justify all actions and methods used in handling the potential digital evidence. The justification can be achieved by demonstrating that the decision was the best choice to get all the potential digital evidence. Another DEFR or DES could also demonstrate this by successfully reproducing or validating the actions and methods used.

It is in the best interest of the individual organization to employ a DEFR or DES who possesses core skills and competency as described in Annex A of this International Standard. This will ensure that the correct processes and procedures are followed when handling potential digital evidence to ensure the eventual preservation of digital evidence that may have evidentiary value. This will also ensure that organizations are able to use the

potential digital evidence, for example, in their disciplinary procedures or in facilitating the exchange of potential digital evidence between jurisdictions.

NOTE The competency described in the Annex A is limited to DEFR function which is aligned with the role of DES as defined in Clause 3.8.

5.4 Digital evidence handling processes

5.4.1 Overview

Although the complete digital evidence handling process includes other activities (i.e. presentation, disposal, etc.), the scope of this International Standard relates only to the initial handling process which consists of identification, collection, acquisition, and preservation of potential digital evidence.

Digital evidence can be fragile in nature. It may be altered, tampered with or destroyed through improper handling or examination. Handlers of digital evidence should be competent to identify and manage 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 those digital devices to be unusable.

The DEFR and DES should follow documented procedures to ensure that the integrity and reliability of potential digital evidence are maintained. The procedures should include handling guidelines for sources of potential digital evidence and should include the following fundamental principles:

— Minimize handling of the original digital device or potential digital evidence;

— Account for any changes and document actions taken (to the extent that an expert is able to form an opinion on reliability);

— Comply with the local rules of evidence; and

— The DEFR and DES should not take actions beyond their competence.

By complying with the fundamental principles and requirements of handling potential digital evidence, the evidence should be preserved. Specifically, in the case where unavoidable changes were to be made, all actions and rationale need to be documented. Each process of the digital evidence handling, i.e. identification, collection, acquisition and preservation, is discussed in more detail in the clauses to follow.

5.4.2 Identification

Digital evidence is represented in physical and logical form. The physical form includes the representation of data within a tangible device. The logical form of the potential digital evidence refers to the virtual representation of data within a device.

The identification process involves the search for, recognition and documentation of potential digital evidence. The identification process should identify digital storage media and processing devices that may contain potential digital evidence relevant to the incident. This process also includes an activity to prioritize the evidence collection based on their volatility. The volatility of the data should be identified to ensure the correct order of the collection and acquisition processes to minimize the damage to the potential digital evidence and to obtain the best evidence. In addition, the process should identify the possibility of hidden potential digital evidence. The DEFR and DES should be aware that not all types of digital storage media can be easily identified and located, for example cloud computing, NAS and SAN - all add a virtual component to the identification process.

The DEFR should systematically carry out a thorough search for items that may contain potential digital evidence. Different types of digital devices that may contain potential digital evidence can easily be overlooked (e.g. due to small size), disguised or co-mingled amongst other irrelevant material.

Clauses 6.1 and 6.6 provide more information on the chain of custody, packaging and labelling aspects of digital evidence identification. Clause 7 specifies guidelines relevant to specific instances of identification, collection, acquisition and preservation of digital evidence.

5.4.3 Collection

Once the digital devices that may contain potential digital evidence are identified, the DEFR and DES should decide whether to collect or acquire during the next process. There are a number of decision factors for this, which is discussed in more detail in Clause 7. The decision should be based on the circumstances.

Collection is a process in the digital evidence handling process where devices that may contain potential digital evidence are removed from their original location to a laboratory or another controlled environment for later acquisition and analysis. Devices containing potential digital evidence may be in one of two states: when the system is powered on or when the system is powered off. Different approaches and tools are required, depending on the state of the device. Local procedures may apply to the approaches and tools used for the collection process.

This process includes documenting the whole approach, as well as the packaging of these devices prior to transportation. It is important for the DEFR and DES to collect any material that might relate to the potential digital information (e.g. paper with passwords noted down, cradles and power connectors for embedded system devices). Potential digital evidence may be lost or damaged if reasonable care is not applied. The DEFR and DES should adopt the best possible collection method based on the situation, cost and time, and document the decision for using a particular method.

NOTE 1 Removal of digital storage media is not always recommended and the DEFR should be sure they are competent to remove storage media, and recognize when it is appropriate and permitted to do so.

NOTE 2 Details on digital devices not collected should be documented with justification for their exclusion, in accordance with requirements of applicable jurisdiction.

5.4.4 Acquisition

The acquisition process involves producing a digital evidence copy (e.g. complete hard disk, partition, selected files) and documenting the methods used and activities performed. The DEFR should adopt a suitable acquisition method based on the situation, cost and time, and document the decision for using a particular method or tool appropriately.

The methods used to acquire potential digital evidence should be clearly documented in detail and, as far as practically possible, be reproducible or verifiable by a competent DEFR. A DEFR or DES should acquire the potential digital evidence in the least intrusive manner in order to avoid introducing changes where possible. In carrying out this process, the DEFR should consider the most appropriate method to use. If the process results to unavoidable alteration to the digital data, the activities performed should be documented to account for the changes to the data.

The acquisition method used should produce a digital evidence copy of the potential digital evidence or digital devices that may contain potential digital evidence. Both the original source and the digital evidence copy should be verified with a proven verification function (proven accurate at that point in time) that is acceptable to the individual who will use the evidence. The original source and each digital evidence copy should produce the same verification function output.

In circumstances where the verification process cannot be performed, for example when acquiring a running system, the original copy contains error sectors, or the acquisition time period is limited. In such instances, the DEFR should use the best possible method available and be able to justify and defend the selection of the method. If the imaging cannot be verified, then this needs to be documented and justified. If necessary, the acquisition method used should be able to obtain the allocated and unallocated space.

NOTE 1 When the verification process cannot be performed on the full source due to errors on the source, then verification using those parts of the source that can be reliably read, may be used.

There may be instances in which it is not feasible or permissible to create a digital evidence copy of an evidence source, such as when the source is too large. In these instances, a DEFR may perform a logical acquisition, which targets only specific data types, directories or locations. This generally takes place on a file and partition level. During logical acquisition, active files and non-file-based allocated space on the digital storage media may be copied; deleted files and unallocated space may not be copied, depending on the method used. Other instances where this method can be useful are when mission-critical systems are involved that cannot be shutdown.

NOTE 2 Some jurisdictions may require special treatment for data; for example, seal it in the presence of the owner of the data. The sealing should be done in accordance with local requirements (legislative and procedural).

5.4.5 Preservation

Potential digital evidence should be preserved to ensure its usefulness in the investigation. It is important to protect the integrity of the evidence. The preservation process involves the safeguarding of potential digital evidence and digital devices that may contain potential digital evidence from tampering or spoliation. The preservation process should be initiated and maintained throughout the digital evidence handling processes, starting from the identification of the digital devices that contain potential digital evidence.

In the best-case scenario, there should be no spoliation to the data itself or any metadata associated with it (e.g. date and time-stamps). The DEFR should be able to demonstrate that the evidence has not been modified since it was collected or acquired, or provide the rationale and documented actions if unavoidable changes were made.

NOTE In some cases, the confidentiality of potential digital evidence is a requirement, either a business requirement or a legal requirement (e.g. privacy). The potential digital evidence should be preserved in a manner that ensures the confidentiality of the data.

6 Key components of identification, collection, acquisition and preservation of digital evidence

6.1 Chain of custody

In any investigation, the DEFR should be able to account for all the acquired data and devices at the time it is within the custody of the DEFR. The chain of custody record is a document identifying the chronology of the movement and handling of the potential digital evidence. It should be instituted from the collection or acquisition process. This will typically be accomplished by tracing the history of the item from the time it was identified, collected or acquired by the investigating team up to the present status and location.

The chain of custody record is a document or series of related documents that details the chain of custody and records who was responsible for handling potential digital evidence, either in the form of digital data or other formats (such as paper notes). The purpose of maintaining a chain of custody record is to enable the identification of access and movement of potential digital evidence at any given point in time. The chain of custody record itself may comprise more than one document, e.g. for potential digital evidence there should be a contemporaneous document recording the acquisition of digital data to a particular device, the movement of that device and documentation recording subsequent extracts or copies of potential digital evidence for analysis or other purposes. The chain of custody record should contain the following information as a minimum:

— Unique evidence identifier;

— Who accessed the evidence and the time and location it took place;

— Who checked the evidence in and out from the evidence preservation facility and when it happened;

— Why the evidence was checked out (which case and the purpose) and the relevant authority, if applicable; and

— Any unavoidable changes to the potential digital evidence, as well as the name of the individual responsible therefore and the justification for the introduction of the change.

The chain of custody should be maintained throughout the lifetime of the evidence and preserved for a certain period of time after the end of the lifetime of the evidence - this period of time can be set according to local jurisdictions of the collection and application of evidence. It should be established from the moment digital device(s) and/or potential digital evidence are acquired and should not be compromised.

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

6.2 Precautions at the site of incident

6.2.1 General

The DEFR should perform activities to secure and protect the location of the potential digital evidence as soon as they arrive on site. The activities should support the following, subject to local law:

— Secure and take control of the area containing the devices;

— Determine who is the individual in charge of the location;

— Ensure that individuals are moved away from the devices and power supplies;

— Document anyone who has access to the location and anyone who may have a reason to be involved with the incident scene;

— If the device is ON do not switch it OFF and if the device is OFF do not switch it ON;

— If possible, document (e.g. sketch, photograph or video) the scene, all components and cables in their original position. If no camera and/or video camera is 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; and

— If permitted, search the areas for items such as sticky notes, diaries, papers, notebook computers, or hardware and software manuals with crucial details about the devices such as passwords and PINs.

NOTE 1 Some jurisdictions may have special requirements for the admission of photographs and video evidence. The DEFR should adhere to those requirements.

NOTE 2 DEFRs need to be aware that potential digital evidence might not always be in obvious locations, such as distributed or virtualized storage.

The DEFR should first know all the risks involved in performing all processes during the investigation. Consideration should be given to protect personnel and potential digital evidence at the scene of the incident.

6.2.2 Personnel

Conducting risk assessment regarding personnel safety prior to commencing the process is important since the safety of the personnel involved in the process is vital. Issues to be considered in assessing risks to personnel include, but are not limited to the following:

— 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?

— Are there any physical hazards to individual(s) present?

— Could anything in the vicinity, including the device, have been configured to cause physical harm if handled in an inappropriate manner, e.g. concealed trap?

— Does the material to be collected have any likelihood to cause psychological damage or offence?

— Can the incident scene be considered unsafe?

— Does the surrounding area have an impact on the risk potential?

6.2.3 Potential digital evidence

The DEFR should be careful when using a specific tool to collect or acquire potential digital evidence. Not calculating risks before acting may lead to the loss of some or all of the potential digital evidence due to the technology applied during collection or acquisition. Risks should be assessed to reduce exposure to claims for damages.

The risk assessment involves the systematic evaluation of risks and the potential impact they may have on the digital evidence investigation. Aspects to consider during risk assessment for potential digital evidence include, but are not limited to the following:

— What type of collection/acquisition methods to be applied?

— What is the equipment that may be needed on-site?

— What is the level of volatility of data and information related to the potential digital evidence?

— Is remote access to any digital device possible and does it pose a threat to evidential integrity?

— What happens if data/equipment is damaged?

— Could data have been compromised?

— Could the digital device have been configured to destroy (e.g. using a logic-bomb), spoil or obfuscate data if switched off or accessed in an uncontrolled way?

6.3 Roles and responsibilities

The role of the DEFR involves the identification, collection, acquisition and preservation of potential digital evidence at the incident scene. It includes the development of a collection and acquisition report, but not necessarily the analysis report. The role of the DEFR also involves ensuring the integrity and authenticity of potential digital evidence. In fulfilling their role, the DEFR should have adequate experience, skills and knowledge in handling potential digital evidence. This is crucial because potential digital evidence can be easily spoiled.

The DEFR might also require assistance from technical support personnel in related areas. The role of a DES involves providing technical support to the DEFR in identifying, collecting, acquiring and preserving potential digital evidence at the incident scene. The DES provides specialized expertise to the DEFR. The competency matrix for the DEFR (see Annex A) serves as a guide to identify their relevant competency levels.

NOTE In the context of incident handling where an ISIRT exists, the roles of a DEFR and/or DES as a member of ISIRT team are discussed in ISO/IEC 27035:2011.

6.4 Competency

The DEFR and/or DES should have the relevant technical and legal competencies (e.g. those in Annex A) and should be able to demonstrate that they are properly trained and have sufficient technical and legal understanding to handle potential digital evidence appropriately. This includes an understanding of processes and methods appropriate for the handling of potential sources of digital evidence. Adequate training will enable DEFRs to handle digital devices that contain potential digital evidence. Having the best set of tools will not guarantee the quality of the digital evidence if the DEFR is not competent in performing the tasks.

Some jurisdictions have prescribed how DEFRs should establish their qualifications. It is the DEFRs' responsibility to ensure that they are properly informed on how to do this in the relevant jurisdictions. When required, the DEFR and/or DES should be able to demonstrate that they are competent to handle potential digital evidence using the tools and methods selected to perform the tasks. It is also required that the DEFRs are able to provide evidence of their ongoing competency.

Some of the pre-requisites for the DEFR are as follows:

— They should be properly and adequately trained to handle digital devices in the context of investigative activities;

— They should demonstrate and maintain their skills and competency to appropriate authorities in the relevant area of handling potential digital evidence; and

— It is the responsibility of individual(s) and the employer to ensure that they are adequately trained and the skills and competency maintained.

NOTE Competence of a DEFR may vary from one jurisdiction to another.

6.5 Use reasonable care

Avoid any actions that could lead to 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. The DEFR should not access digital devices, such as conducting a memory dump from a live digital device, unless they have the required competency and with the use of reliable and validated processes.

There are some circumstances when it is impractical to collect or acquire potential digital evidence. The DEFR should consider the following circumstances, but is not limited to only these:

— If there is no legal entitlement or authorization to collect the digital device;

— If 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 considered legal by the jurisdiction;

— If it is a mission-critical digital device that cannot tolerate any downtime;

— If the physical size of the digital device is too large, such as a server at a data centre or RAID system;

— If it is a safety-critical digital device that would endanger life if stopped; and

— If it is a digital device that also services innocent parties.

6.6 Documentation

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

— Every activity taken should be documented. This is to ensure that no details have been left out during the identification, collection, acquisition and preservation 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.

— The DEFR should be sensitive of the time and date setting if the digital devices are powered on. Compare the time setting with a reliable time source, such as a time that is synchronized with reliable and traceable time source. 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. This documentation should include a description of what is visible as some malicious programs may masquerade as well-known software.

— Any movement of the digital devices should be documented in accordance with local requirement.

— Document all unique identifiers of the digital devices and the associated parts such as serial numbers and unique markings.

Examples of a minimum set of documentation for cross-jurisdictional exchange of potential digital evidence are shown in Annex B.

NOTE Refer to the document management clause and record management clause of ISO/IEC 17025:2005 for more information on documentation.

6.7 Briefing

6.7.1 General

It is essential that the DEFR and DES are adequately briefed by the relevant authority prior to performing their tasks, whilst respecting any confidentiality laws and constraints (i.e. need to know basis). It is important to have a formal briefing session to understand the incident, what to expect and not to expect during the investigation, and a reminder against evidence tampering or spoliation. The briefing should be sufficient enough for members to be well-prepared in discharging their roles and responsibilities; thus ensuring the extraction of all relevant potential digital evidence.

6.7.2 Digital evidence specific

A briefing session focusing explicitly on digital evidence specific guidance is needed to inform DEFRs on details pertaining to the investigation. During the briefing session, the DEFR and DES should be provided with the relevant information and detailed instructions related to potential digital evidence to be collected or acquired. This may include:

— Type of incident (if known);

— Date and time of incident (if known);

— Investigation plan (collection and/or acquisition, known network activity, known volatile data requirement, etc.);

— Consider where and how the potential digital evidence is stored/transported after collection or acquisition;

— Specific tools needed to acquire the potential digital evidence;

— Potential digital evidence that relates to specific types of investigation;

— Equipment and manuals related to digital devices;

— Reminding team members to switch off any Bluetooth or Wi-Fi capability on their phones/computers so they do not inadvertently interact with the digital devices, except for phones/computers used to detect the connections.

— Significance of documentation throughout the investigation; and

— Applicable legal or other factors that may prohibit collecting any devices and potential digital evidence they contain.

This specific briefing session may form part of the general briefing session as described in clause 6.7.1.

6.7.3 Personnel specific

A briefing session focusing explicitly on personnel specific guidance is needed to inform DEFRs on aspects pertaining to the parties involved in the investigation. During the briefing session, the investigating team will be provided with personnel related instructions. This may include:

— Assignments, roles and responsibilities of investigation team members at the incident scene;

— Whether other authorities (medical personnel, biological forensic investigators, etc.) are expected to be involved in the investigation;

— Requiring team members not to accept technical assistance from any unauthorized individuals; and

— Requiring team members to follow the procedure strictly in minimizing the risk of spoiling potential digital evidence, such as avoiding use of any tools or materials that may produce or emit static electricity or a magnetic field as these may damage or destroy the potential digital evidence.

This specific briefing session may form part of the general briefing session as described in clause 6.7.1.

6.7.4 Real-time incidents

It is highly desirable that the investigation of an incident should be planned in advance but there are circumstances (e.g. when an incident is developing and being responded to in real-time) where full planning may not have been possible. In these situations, the team should be briefed on initial strategies and tactics for the investigation and allowed to develop new strategies and tactics in response to prevailing conditions. Information about the incident, as it develops, should be shared amongst the team as quickly as possible in order to ensure that decisions on actions to take can be made efficiently and with due regard to the need for justification.

6.7.5 Other briefing information

Apart from digital evidence and personnel, other important information to be briefed to investigating teams include:

— Designation of the area under investigation, including the name of the organization, address and a location map (if available);

— Investigation mandate;

— Details of search warrants and other authorities applicable to the investigation, including the limits of the search and seizure;

— Legal aspects and implications;

— Investigation timeframe;

— Equipment needed to be brought to the incident scene for the investigation;

— Logistical information; and

— Potential conflict of interest.

The DEFR should avoid situations where accusations of inherent bias can be made. An example of inherent bias is when a DEFR copies one computer and not another (that later turns out to contain exculpatory evidence) based on a perception formed by the briefing.

6.8 Prioritizing collection and acquisition

In prioritizing collection or acquisition of potential digital evidence, it is imperative for the DEFR to understand the reason the potential digital evidence is being collected or acquired. As a general principle, the DEFR should attempt to maximize the amount of data preserved by collection and acquisition actions. However, it may be necessary to prioritise items by volatility and/or relevance/potential evidential value. Items of high relevance/potential evidential value are those that are most likely to contain data relating directly to the incident under investigation.

Prioritization by volatility is only applicable if the specific circumstances of the case being investigated require this. Potential digital evidence can be broken into two categories: volatile and non-volatile. Volatile data can be easily destroyed or lost forever if due care to protect the data is not applied. For example, removing the power supply from a digital device may result in loss of volatile data. Non-volatile data remains on the media even if the power supply is removed. Since some types of digital evidence may have a short life span, potential digital evidence can be easily tampered with or be spoiled. Where it is not clear if digital devices contain potential digital evidence, or which items are of more relevance than others, it may be necessary to examine them prior to collection using a process to determine priority. Digital devices to be considered for collection include, but are not limited to; IT equipment and digital storage media, CCTV systems, PEDs, automotive systems, control systems and improvised electronics. 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:

— Prioritize potential digital evidence that would be lost forever if the power supply is removed; and

— Take quick actions to collect and acquire this data with validated methods.

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

NOTE 3 When encryption or malware is suspected, it is desirable to examine the volatile data.

In these circumstances, 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 incident.

6.9 Preservation of potential digital evidence

6.9.1 Overview

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 or tampering. Spoliation can result from magnetic degradation, electrical degradation, heat, high or low humidity exposure, as well as shock and vibration. Tampering can result from an act of intentionally making or allowing changes to the potential digital evidence. It is therefore crucial to protect the potential digital evidence as best as possible, and use the original data as little as possible. It is important that the DEFR is familiar with the packaging requirements specific to the relevant jurisdiction.

6.9.2 Preserving potential digital evidence

All collected digital device(s) and acquired potential digital evidence should be protected as far as possible 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) and acquired potential digital evidence should be stored in an evidence preservation facility that applies physical security controls such as access control systems, surveillance systems or intrusion detection systems or another controlled environment for digital evidence preservation. The main objectives of the physical security are to protect and prevent loss, damage and tampering, as well as enable auditability.

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 resistant 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, the device should be secured in an anti-static bag.

— Main system units and notebook computers need to be secured in an appropriate container to avoid tampering or spoliation of the potential digital evidence that may reside in it.

NOTE The use of a Faraday bag, or other Radio Frequency shielded packaging, can increase mobile phone battery drainage. This may require provision of auxiliary power to the device while inside the bag, if resources permit.

6.9.3 Packaging digital devices and potential digital evidence

6.9.3.1 Baseline activities: packaging of potential digital evidence

Baseline activities should be conducted unless there is a good reason not to. This can also be referred as the minimum actions to be taken. During packaging, the DEFR should note and address the following baseline activities:

— Do not touch magnetic tape, but rather pick tapes up by their protective cases or areas that are known not to contain data (e.g. edges of optical disks). This should only be done if the DEFR wears lint-free gloves.

NOTE The specific areas of storage media that are known not to contain data depend on the media type. It is the DEFR's responsibility to know current technology and be familiar with storage media handling.

— To ensure correct identification, the DEFR should label all potential digital evidence. Some jurisdictions have specific requirements regarding the format of labelling 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 digital evidence, collected digital device(s) and any hardware parts associated with the devices with tamper-evident labelling. 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 potential

digital evidence in collected device(s) should be acquired and stored in a manner to ensure the integrity of the evidence.

— When possible, digital devices with openings and movable components should be sealed with tamper-evident labels that are appropriate for the devices, and the DEFR should sign on the seal.

— Devices that are attached to batteries with data that is volatile 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 against the potential threats.

— Computers and digital devices should be packaged in such a way as to prevent damage from shock, vibration, high altitude, heat, and exposure to radio frequency during transportation.

— Magnetic storage media should be stored in packaging that is magnetically inert, anti-static and free of particles.

— Digital devices may also contain latent, trace or biological evidence. As such, appropriate activities need to be performed to preserve the potential digital evidence. Digital evidence imaging should be done after latent, trace, or biological evidence collection processes are conducted on the devices. However, the decision to prioritize the collection of evidence should be evaluated thoroughly to preserve the evidence.

6.9.3.2 Additional activities: packaging of potential digital evidence

Additional activities refer to activities that are strongly recommended to be carried out. During packaging, the DEFR should note and address the following additional activities, where applicable:

— Wear lint-free gloves and ensure that hands are clean and dry.

— Protect the digital devices from the influence of electromagnetic 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.

— Minimize the possibility of print-through (the transfer of a signal from one loop of tape onto an adjacent loop), which may occur when tapes are stored for long periods without active usage, resulting in poor signal quality.

— Where necessary, the packaging areas should be free from UV light. UV may cause degradation of DNA or damage some types of media. The DEFR should consider whether UV poses a risk to potential digital evidence before selecting a packaging area.

— Digital devices should be strongly protected from thermal shock.

6.9.4 Transporting potential digital evidence

The DEFR should preserve collected digital devices and acquired potential digital evidence during transporting. Potential digital evidence should not be left unattended during the transportation process. The DEFR should maintain the chain of custody throughout the transporting process to prevent possible tampering or spoliation, and maintain the integrity and authenticity of the digital devices and potential digital evidence. If the potential digital evidence is not transported by the DEFR or the DES, it is recommended that encryption is used.

NOTE The DEFR should ensure that the collection of sensitive or personal information is in accordance with the local jurisdictional laws and regulations on data protection.

During packaging and transporting, the DEFR needs to be aware of the possible presence of electrostatic discharge that may damage the evidentiary value of potential digital evidence. The DEFR should ensure that computers and digital devices are packaged securely during transportation to prevent damage from shock and vibration.

The transportation process should allow for a conducive and controlled environment. The level of moisture, humidity and temperature should be suitable for the digital devices. Avoid keeping potential digital evidence and digital devices in the transporting vehicle for prolonged periods and avoid them being in the presence of UV.

In some jurisdictions when circumstances do not allow, the DEFR is unable to accompany the evidence. In such cases, utilization of appropriate and authorised shipping mechanisms can be utilized in order to assure proper security of the evidence during transport. Documents of the transportation and verification of the package integrity should become part of the chain of custody.

7 Instances of identification, collection, acquisition and preservation

7.1 Computers, peripheral devices and digital storage media

7.1.1 Identification

7.1.1.1 Physical incident scene search and documentation

In the context of this clause, 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. A digital device that has a network interface, 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. Where a computer with a network interface, but no obvious connection is found, activities should be performed to identify devices to which it may have been connected in the recent past.

Usually incident scenes will contain various types of digital storage media. Digital storage media is used to store data from digital devices and they vary in memory capacity. Examples of digital storage media include but are not limited to external portable hard drives, flash drives, CDs, DVDs, Blu-ray disks, floppy disks, magnetic tapes and memory cards.

Before any acquisition or collection can be done, safety aspects of potential digital evidence need to be considered. These aspects are described in clauses 6.2.1 and 6.2.2. The DEFR should take care, however, to assure themselves that an apparently standalone device has not been recently connected to a network. Where it is suspected that an apparently standalone device has been recently disconnected, consideration should be given to treating it as a networked device to ensure that other parts of the network are handled correctly. The DEFR should note and address at least the following:

— The DEFR should document 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. Serial numbers, licence numbers and other identifying marks (including physical damage) should be documented wherever possible.

— At the identification 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, the DEFR should photograph or make a written document of what is displayed on the screens. Any written document should include a description of what is actually visible (e.g. approximate window positions, titles and contents).

— A device that has batteries that may run down needs to be power-charged to ensure information is not lost. The DEFR needs to identify and collect potential battery chargers and cables during this phase.

— The DEFR should also consider using a wireless signal detector to detect and identify wireless signals from wireless devices that may be hidden. There may be instances where a wireless signal detector is not used due to cost and time constraints and the DEFR should document this. If any networked devices are found, the DEFR should continue with the evidence handling process as described in clause 7.2.2.2 of this document. Where active scanning (i.e. broadcasting and/or probing) for network devices is to be used, the scanning devices should be switched off until an assessment on the possibilities of the device to interact with other devices at the scene has been determined. Team members should remember that certain devices at the scene can detect the presence of active scanning devices and the use of active scanning may trigger actions that may spoil potential digital evidence, and can, in extreme circumstances, result in the activation of concealed traps.

NOTE 1 In some jurisdictions, it is permissible to switch on digital devices at a scene to determine its relevance to the investigation if there are many digital devices present. This is done in consideration of processing time and cost that may be incurred if non-relevant digital devices are acquired. If a device is switched on for evaluation at the scene, the DEFR should ensure that thorough notes of the actions taken are maintained during the process.

NOTE 2 In preserving the power state of the digital device, the results of the volatility and relevant prioritization process should be considered. If the decision is made that the most critical information is the non-volatile information on disk, then that running system may have its console screen photographed and the power plug pulled. If the volatile information in memory is relevant, then it is critical to leave the system powered on to allow its acquisition.

7.1.1.2 Non-digital evidence collection

The DEFR should consider the collection of non-digital evidence. To enable this, the team leader should identify the individuals 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 document the name and designation of this individual.

The DEFR may also need to collect some evidence by speaking to individuals who may have useful or relevant information about the potential digital evidence or digital devices to be collected. Any responses should be accurately documented. 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 administrator/root password. This additional information may be helpful in the analysis stage of the potential digital evidence. These conversations should be documented to ensure that the details are accurate and the documented statement cannot be changed. The DEFR needs to be familiar with relevant jurisdictional requirements relevant to non-digital evidence collection.

7.1.1.3 Decision-making process for collection or acquisition

In deciding to collect a digital device or acquire potential digital evidence, several factors should be considered which include but are not limited to the following:

— volatility of the potential digital evidence which was discussed in clauses 5.4.2 and 6.8,

— existence of full disk encryption or encrypted volumes where passphrase or keys may reside as volatile data in RAM, on external tokens, smart cards, other devices or media,

— criticality of the system which was discussed in clauses 5.4.4, 7.2.1.2 and 7.1.3.4,

— legal requirements of a jurisdiction, and

— resources such as size of storage required, availability of personnel, time constraints.

Figure 1 illustrates the overview of decision-making process to do collection or acquisition.

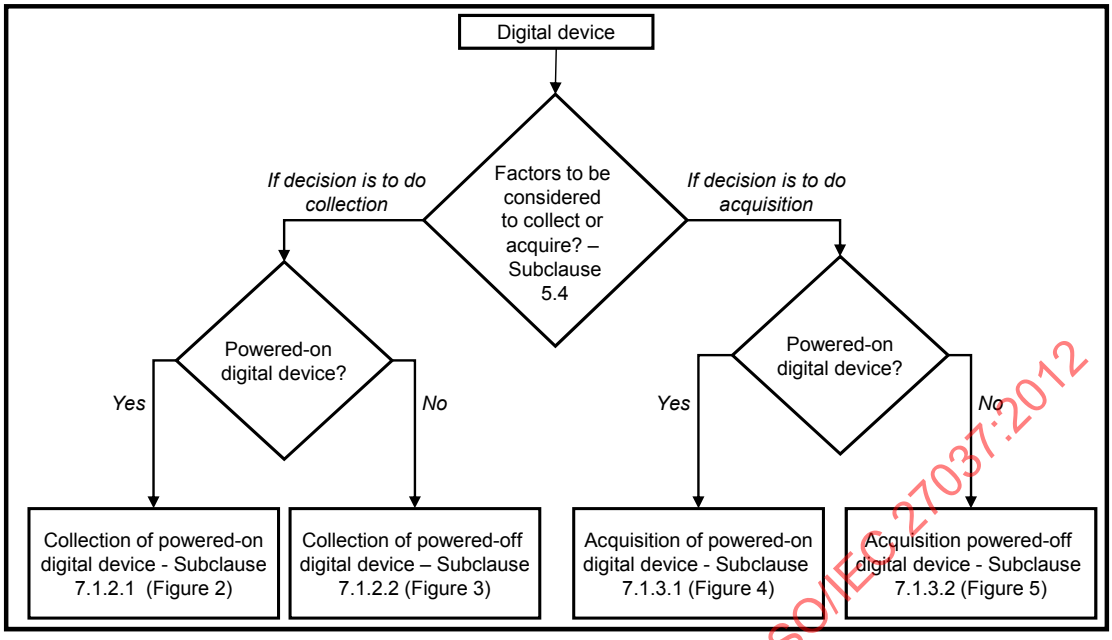

Figure 1 — Guidelines for decision-making of collection or acquisition of potential digital evidence

7.1.2 Collection

7.1.2.1 Powered on digital devices

7.1.2.1.1 Overview

The DEFR can follow a number of guidelines for collection when the digital device is powered on. Not all guidelines are ideal and appropriate for any cases; some guidelines are only relevant to specific cases. Accordingly, the guidelines can be categorized as baseline or additional. Baseline activities should be applied in all circumstances, whilst additional activities should be applied when relevant and applicable, depending on the unique device or circumstances. Figure 2 illustrates the baseline and additional activities applicable to powered on digital device collection.

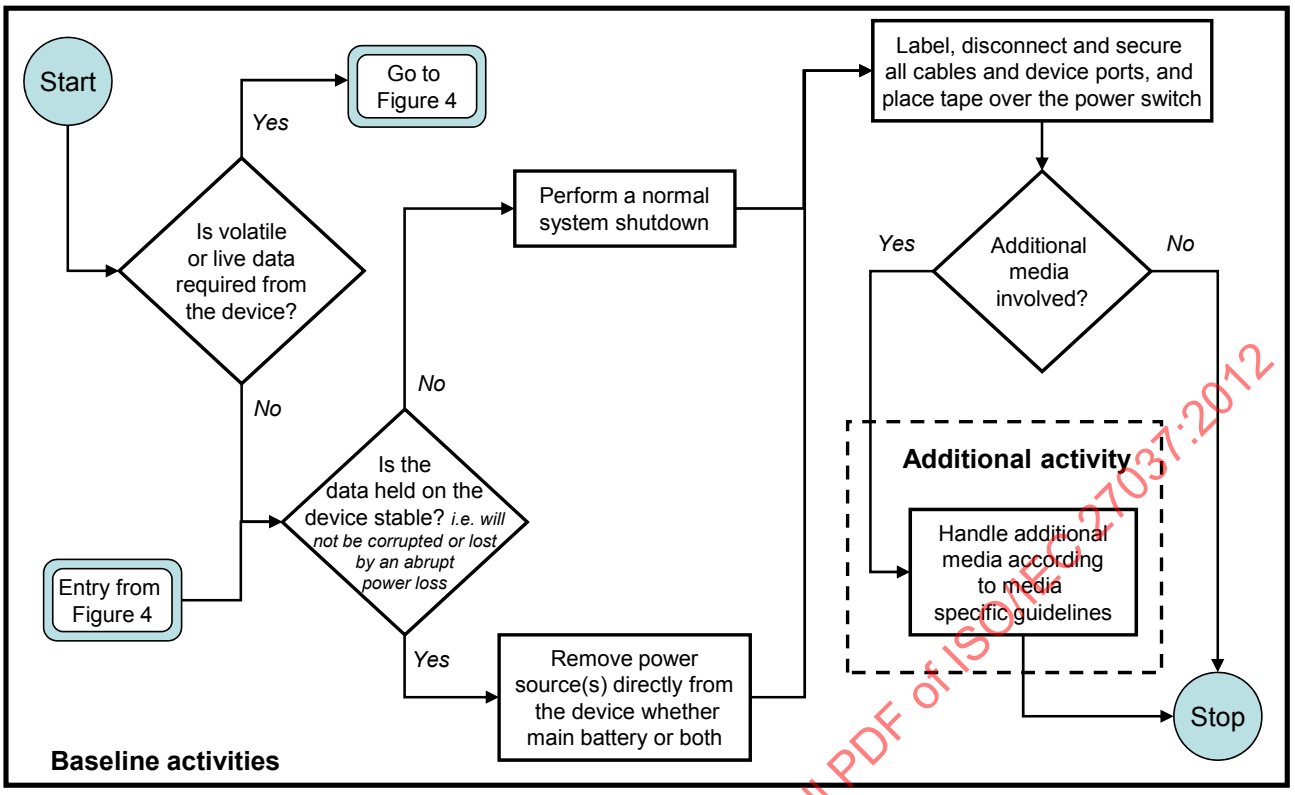

Figure 2 — Guidelines for collection of powered on digital device

NOTE All these activities should be in accordance with the local jurisdictional laws and regulations.

It is the DEFR's responsibility to know current technology and be familiar with storage media handling guidelines.

7.1.2.1.2 Baseline activities: powered on digital device collection

The following baseline activities should be followed by the DEFR in all cases involving potential digital evidence. These guidelines apply when the DEFR has decided that a powered on digital device should be collected:

— Consider an acquisition of the digital device's volatile data and current state prior to powering the system off. Encryption keys and other crucial data may reside in active memory, or in inactive memory that has not yet been cleared. Consider logical acquisition when encryption is suspected. Where this is the case, bear in mind that the live host operating system may be untrustworthy, so consider the use of appropriate trusted and validated tools.

— The configuration of the digital device may determine whether the DEFR needs to shut down the device through normal administrative procedures, or whether the device's plug should be pulled from the power socket. The DEFR may need to consult with a DES to determine the best approach given the specific circumstances. If the decision is made to pull the plug, the DEFR needs to remove the power supply cable by first removing the end attached to the digital device and not the end that attached to the socket. Be aware that a device connected to a UPS may have data altered if the power cord is removed from the wall and not the device.

NOTE 1 If the power is removed from a powered on digital device, any potential digital evidence stored in encrypted volumes will be inaccessible, unless the decryption key is obtained. Potentially valuable live data could also be lost, leading to damage claims or loss of human lives, such as corporate data or digital devices controlling medical equipment. As such, the DEFR should ensure that volatile data is collected prior to removing the power supply.

NOTE 2 There are hardware devices that allow the powered on device to be disconnected from utility power and be transferred to portable UPS without interrupting power to the device. There are also mouse-jigglers that can be used to prevent the screen-saver from activating. Both of these devices provide useful tools when dealing with a powered on device where encryption may be active. When a powered on device is collected such that the power is maintained, the packaging and transportation of a running system have to address issues associated with the provision of cooling, protection from mechanical shock, etc.

— Label, disconnect and secure all cables from the digital device and label the ports so that the system can be reconstructed at a later stage.

— Place tape over the power switch if necessary to prevent the switch changing state. Consider whether the state of the switch has been properly documented prior to taping or moving.

7.1.2.1.3 Additional activities: powered on digital device collection

Following are additional activities that are relevant depending on the configuration of the specific digital device.

— If it is a notebook computer, ensure the volatile data is acquired before removing the battery. The DEFR should remove the main power source battery first, instead of depressing the power button of the notebook computer to shut it down. The DEFR should also take note if a power adapter is present and if it is, remove the power adapter after the battery is removed.

NOTE 1 The action of depressing the power button on a digital device may be configured to initiate a script that may alter information or delete information from the system before shutting down or to alert connected systems that an unexpected event has occurred so that they may erase data of evidential value before they are identified. It may also be configured to trigger a device intended to cause physical harm to the DEFR and other individuals present.

— 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.

NOTE 2 If any bootable media is left in then when the machine is next powered up, it could boot from that media rather than hard-drive (or forensic tools flash drive) depending on the computers BIOS settings.

The DEFR should conduct non-digital evidence collection according to procedural laws to ensure that any evidence is admissible.

7.1.2.2 Powered off digital devices

7.1.2.2.1 Overview

The DEFR can follow a number of guidelines for collection when the digital device is powered off. Not all activities contained in these guidelines are relevant in all circumstances. Thus a distinction is to be made between those activities that apply in all cases (baseline activities) and those that may only apply in some cases (additional activities). Figure 3 illustrates the baseline and additional activities applicable to powered off digital device collection.

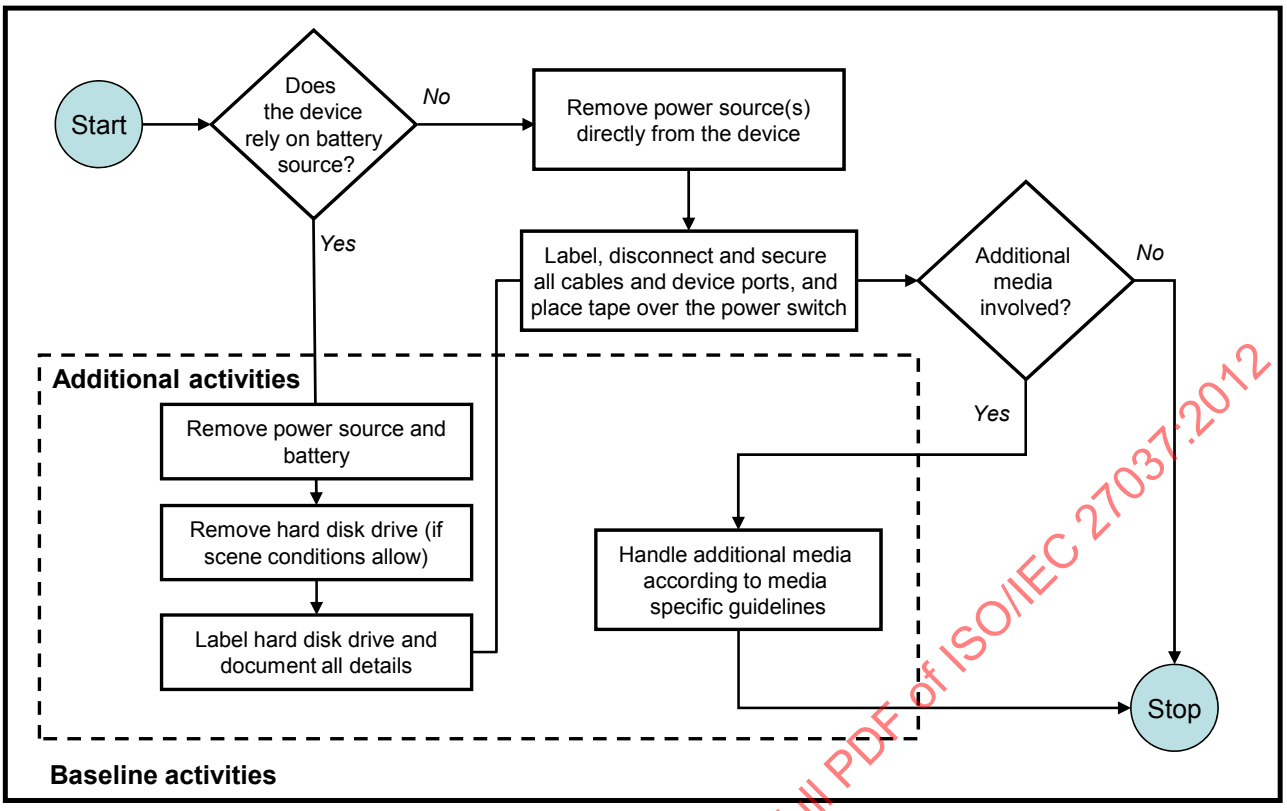

Figure 3 — Guidelines for collection of powered off digital device

It is the DEFR's responsibility to know current technology and be familiar with storage media handling guidelines.

7.1.2.2.2 Baseline activities: powered off digital device collection

Following are the recommended baseline activities for collection when the digital device is powered off:

— Remove the power supply cable by first removing the end attached to the digital device and not the end that attached to the socket.

— Disconnect and secure all cables from the digital devices and label the ports so that the system can be reconstructed at a later stage.

— Place tape over the power switch if necessary to prevent the switch changing state. Consider whether the state of the switch has been properly documented prior to taping or moving.

NOTE In most cases, the storage media should not be removed from the digital device until it is going to be acquired as removing it increases the risk of damaging or confusing it with another storage media. Local procedures regarding the need to remove storage media from degital devices should be developed and followed.

7.1.2.2.3 Additional activities: powered off digital device collection

Following are additional activities that are relevant to powered off digital device collection, depending on the configuration of the specific digital device:

— First, ensure that the notebook computer is indeed powered off since some may be in standby mode. Be aware that some notebook computers can be powered on by opening the lid. Then proceed to remove the main power source battery from the notebook computer.

— If field conditions require the hard drive to be removed, the DEFR should take care to ground the digital device to prevent static electricity from damaging the hard drive. Otherwise, the hard drive should not be removed in the field. Label the hard drive as suspect disk and document all the details such as make, model name, serial number and size of the hard drive.

— 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.

NOTE If any bootable media is left in then when the machine is next powered up, it could boot from that media rather than hard-drive (or forensic tools flash drive) depending on the computers BIOS settings.

7.1.3 Acquisition

7.1.3.1 Powered on digital devices

7.1.3.1.1 Overview

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 devices). In all these scenarios, the DEFR is required to make an accurate digital evidence copy of the digital devices' storage media that are suspected of containing potential digital evidence.

If an image cannot be obtained, accurate copies of specific files suspected to contain potential digital evidence might be acquired. Ideally, both a verified master copy and working copies should be produced. The master copy should not be used again unless it is required to verify the contents of the working copy or produce a replacement working copy following damage to the first working copy.

The DEFR can follow a number of guidelines for acquisition when the digital device is found to be powered on. Not all guidelines are ideal and appropriate for all cases; some guidelines are only relevant to specific cases. Accordingly, the guidelines can be categorized as baseline or additional. Consideration should be given to the possibility that a powered on system may enter into screensaver mode or auto-lock and that there are implications to any effort taken to prevent them. For example, the use of a mouse-jiggler will require a USB key entry into the registry and modifications will most likely take place for whatever actions taken. Using reliable methods should minimize the implications of such actions. Figure 4 illustrates the baseline and additional activities applicable to powered on digital device acquisition.

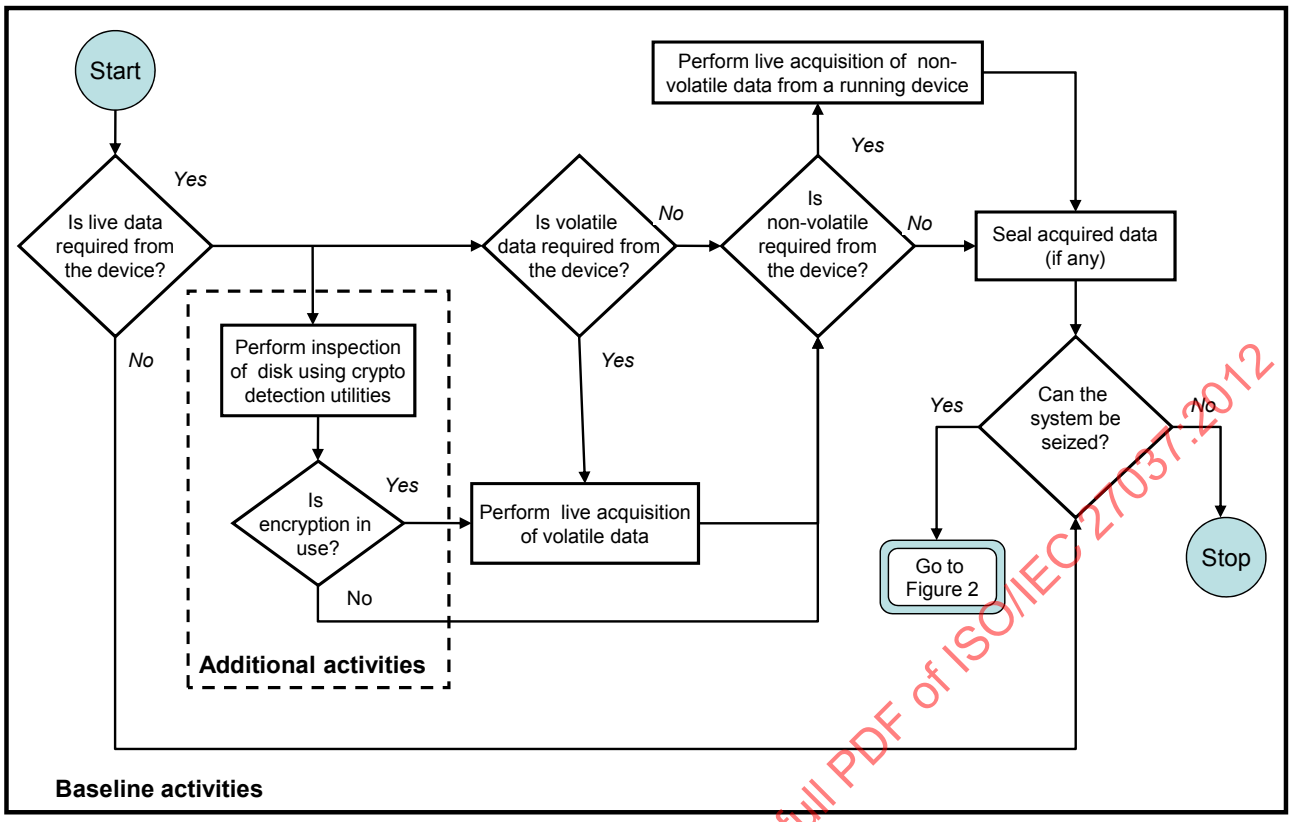

Figure 4 — Guidelines for acquisition of powered on digital device

7.1.3.1.2 Baseline activities: powered on digital device acquisition

Following are the baseline activities that should be followed by the DEFR in all cases involving potential digital evidence acquisition on powered on digital devices:

— First, consider acquiring the potential digital evidence that may otherwise be lost if the digital device is powered off. This is also known as volatile data such as data stored on RAM, running processes, network connections and date/time settings. In circumstances when it is necessary to acquire non-volatile data from devices that are still running, performing an acquisition on a powered on system should be considered.

— Performing live acquisition is necessary to acquire live data from devices that are still running. Live acquisition of volatile data in RAM may enable recovery of valuable information such as network status, decrypted application and passwords. Live acquisition can be conducted on the console or remotely via the network. The processes are different, and require the use to different set of tools.

— The DEFR should never trust the programs on the systems. For this reason, trusted tools obtained by the DEFR (static binaries) are recommended whenever possible. The DEFR should be competent to use validated tools and be competent to account for the effects such tools may have on the system (e.g. displacement of potential digital evidence, content of memory being paged out when software is loaded etc.). All the actions performed and the resulting changes made to the potential digital evidence should be documented and understood. If it is not possible to determine the likely effect of introducing tools to the system or the resulting changes cannot be determined with certainty, this should also be documented.

— When acquiring volatile data the DEFR should adopt the use of a logical file container where possible and document its hash value once it contains the volatile data file(s). Where this is not possible, a container such as a ZIP file should be used and then this file should be hashed and the value documented. The

resulting file containers should be stored on a digital storage medium that has been prepared for this purpose, i.e. formatted.

— Execute the imaging process on the live non-volatile storage using a validated imaging tool. The resulting digital evidence copy should be stored on a digital storage medium that has been prepared for this purpose. Whilst it is preferable to use a new digital storage medium, the use of digital evidence copies from validated processes ensures the integrity of the data when reconstructed. Therefore, a digital storage medium that has been sanitized will suffice. If the image has to be stored in a logical file container, the DEFR should ensure that the image cannot be corrupted or damaged.

NOTE In situations where the device is locked down, physical access may be conducted via other means that has direct memory access enabled, e.g. Firewire interface.

7.1.3.1.3 Additional activities: powered on digital device acquisition

Following are additional activities that are relevant to powered on digital device acquisition, depending on the configuration of the specific digital device:

— Consider acquisition of volatile data in RAM when usage of encryption is suspected. First check if this may be the case by inspecting the raw disk or using some crypto-detection utility. Where this is the case, bear in mind that the live host operating system may be untrustworthy and consider the use of appropriate trusted and validated tools.

— Use a reliable time source and document the time of each performed action.

— It may be appropriate to associate the DEFR with the acquired potential digital evidence, using digital signatures, biometrics and photography.

NOTE The action of depressing the power button on a digital device may be configured to initiate a script that may alter information and/or delete information from the system before shutting down or to alert connected systems that an unexpected event has occurred so that they may erase data of evidential value before they are identified. It may also be configured to trigger a device intended to cause physical harm to the DEFR and other individuals present.

7.1.3.2 Powered off digital devices

7.1.3.2.1 Overview

It is easier to handle a powered off digital device compared to a powered on digital device because there is no need to acquire the volatile data. Figure 5 illustrates activities that are applicable to powered off digital device acquisition.

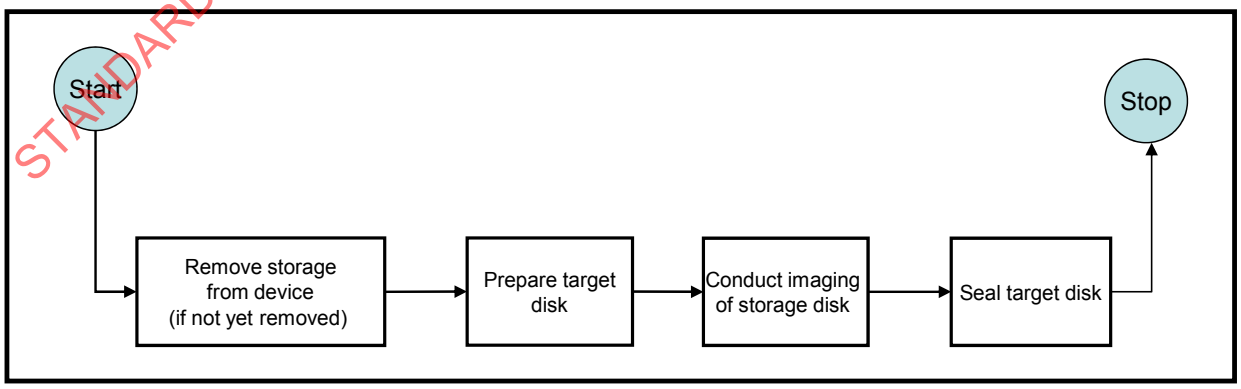

Figure 5 — Guidelines for acquisition of powered off digital device

7.1.3.2.2 Acquisition of powered off digital device

Following are the activities for acquisition when the digital device is found to be powered off:

— Ensure that the device is indeed powered off.

— If appropriate, remove the storage from the powered off digital device if it is not yet removed. Label the storage as suspect storage and document all the details such as make, model name, serial number and size of the storage.

— Execute the imaging process by using a validated imaging tool to create a digital evidence copy of the suspect disk.

NOTE In most cases, the storage media should not be removed from the digital device until it is going to be acquired as removing it increases the risk of damage or of confusing it with another storage media. Local procedures regarding the need to remove hard disks should be developed and followed.

7.1.3.3 Mission-critical digital devices

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

When the digital device cannot be powered off, conduct live and/or partial acquisition, as discussed in clauses 7.1.3.1.2 and 7.1.3.4.

7.1.3.4 Partial acquisition

Partial acquisition may be performed due to several reasons, such as:

— the system storage is too large to be acquired (e.g. database server);

— a system is too critical to be powered down;

— when only selected data to be acquired contains other irrelevant data within the same system; or

— when constrained by legal authority such as a search warrant that limits the scope of the acquisition.

When a decision has been made to do partial acquisition, the activities for acquisition should include but are not limited to the following:

— Identify folder(s), file(s) or any relevant proprietary system options available to acquire the desired data,

— Conduct logical acquisition on those identified data.

7.1.3.5 Digital storage media

Various types of digital storage media may be found at an incident scene. Usually these are the least volatile type of data and can be the lowest priority during collection and acquisition. This does not mean they are not important because in many cases, external digital storage media contain the evidence that the analysts are looking for. The DEFR needs to ensure the following:

— Check and document the location (e.g. drive bay, cable and connector, USB slot, etc.), make, model and serial number (if any) of each digital storage media found.

— Decide whether to collect the identified digital storage media or conduct on-site acquisition, the decision should be based on the nature of the incident and available resources. In order to conduct on-site acquisition of the digital storage media (primarily hard disk), refer to Figure 4.

— If the DEFR decides to and is permitted to collect digital storage media, the collected media should be wrapped or placed in appropriate packaging.

— Label all digital storage media and any associated parts with them. Evidence labels should not be placed directly on the mechanical parts of the digital media, nor should it cover or conceal important information such as the serial number, model number and part number. All media collected should be acquired and stored in a manner to ensure the integrity of the collected media. When possible evidence should be sealed with tamper-evident seals and the DEFR or personnel in charge should sign on the label.

— The collected digital storage media should be stored in an environment suitable for data preservation.

— Different digital storage media have different data retention capabilities. The DEFR should be aware of the acceptable maximum time period specified by the relevant jurisdiction, with regard to the digital storage media's data retention capabilities.

7.1.4 Preservation

After the acquisition process is completed, the DEFR should seal the acquired data using verification functions or digital signatures to determine that the digital evidence copies are equivalent to the originals. In addition, the security aspects require controls that apply the principles of preserving the confidentiality, integrity and availability of the potential digital evidence. In order to protect against spoliation, the environmental aspects should be addressed with appropriate measures. The DEFR needs to ensure the following:

— Use an appropriate verification function to provide evidence that the copied files are equivalent to the originals.

— It may be appropriate to associate the DEFR with the acquired potential digital evidence, using digital signatures, biometrics and photography.

All the digital devices that were collected need to be appropriately preserved. Different types of digital devices may require different methods of preservation. The potential digital evidence needs to be preserved throughout its lifetime, which may vary across jurisdictions and organizational policy.

NOTE As an alternative to sealing the acquired data with verification functions or digital signatures, the DEFR can also use biometric features. Biometrics uses physical and behavioural 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.

7.2 Networked devices

7.2.1 Identification

7.2.1.1 Overview

In the context of this clause, network devices are considered as computers or other digital devices that are connected to a network in either wired or wireless mode. These networked devices may include mainframes, servers, desktop computers, access points, switches, hubs, routers, mobile devices, PDAs, PEDs, Bluetooth devices, CCTV systems and many more. Note that if digital devices are networked, it is difficult to ascertain where the potential digital evidence being sought is stored. The data could be located anywhere on the network.

The identification of a digital device includes components such as manufacturer logos, serial numbers, cradles and power adapters. The DEFR can consider the following aspects as a means of identification:

— Device characteristics: The make and manufacturer of a digital device can sometimes be identified by its observable characteristics, particularly if unique design elements exist.

— Device interface: The power connector is often specific to a manufacturer and a reliable aid to identification.

— Device label: For powered off mobile devices, information obtained from within the battery cavity can be revealing, particularly when coupled with an appropriate database. For example, the IMEI is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices; the ESN is a unique 32-bit identifier documented on a secure chip in a mobile phone by the manufacturer - the first 8-14 bits identify the manufacturer and the remaining bits identify the assigned serial number.

— Reverse lookup: In the case of mobile phones, if the telephone number of the phone is known, a reverse lookup can be used to identify the network operator.

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. The DEFR needs to secure the suspected incident scene and ensure that no individuals remove mobile or any other digital devices from the scene. Digital devices that may contain digital evidence should be protected from unauthorized access.

NOTE In some cases, the communication should not be interrupted. Inform the authorized individuals about possible problems (e.g. not to warn unknown individuals about the shutdown device).

7.2.1.2 Physical incident scene search and documentation

Before any acquisition or collection can be done, the incident scene should be documented in a visual manner by either photographing, videographing or sketching the scene as it appeared upon entry. The choice of documenting method needs to be balanced with circumstances, cost, time, available resources and priorities. The DEFR should document all other items at the scene that may contain potentially relevant materials such as scribbled notes, sticky notes, diaries, etc.

— The DEFR should document the type, brand, model and serial numbers of any digital devices used and 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 documented and collected, if required. Also try to find original packaging of mobile phones; these might contain notes with PIN and PUK codes.

— If the device is networked, the DEFR should identify services rendered by the devices to understand dependencies and to ascertain the criticality of the devices within the network before deciding on disconnecting the device from the network. This is important if the devices are serving mission-critical functions which cannot tolerate any downtime or to avoid destruction of potential digital evidence. However, if there appears to be ongoing network-based threats to the devices the DEFR may need to decide on disconnecting the device from the network to protect the potential digital evidence.

— 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 operating. The DEFR should also note the make, model and basic settings of the system such as display settings, current record settings and the storage location 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.

— As far as possible, the status of the digital devices should remain as it is. Generally, if the digital devices are powered off, the DEFR should not turn them on and 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 needs to be power-charged to ensure information is not lost. The DEFR needs to identify potential charging media and cable during this phase. If a device is to be transported and examined at some indeterminate future date, it may be appropriate to switch it off in order to minimize the potential for damage to the data contained in the device.

— The DEFR should also consider using a wireless signal detector to detect and identify a wireless signal from wireless devices that may be hidden. There may be instances where wireless signal detector is not used due to cost and time constraints and the DEFR should document this.