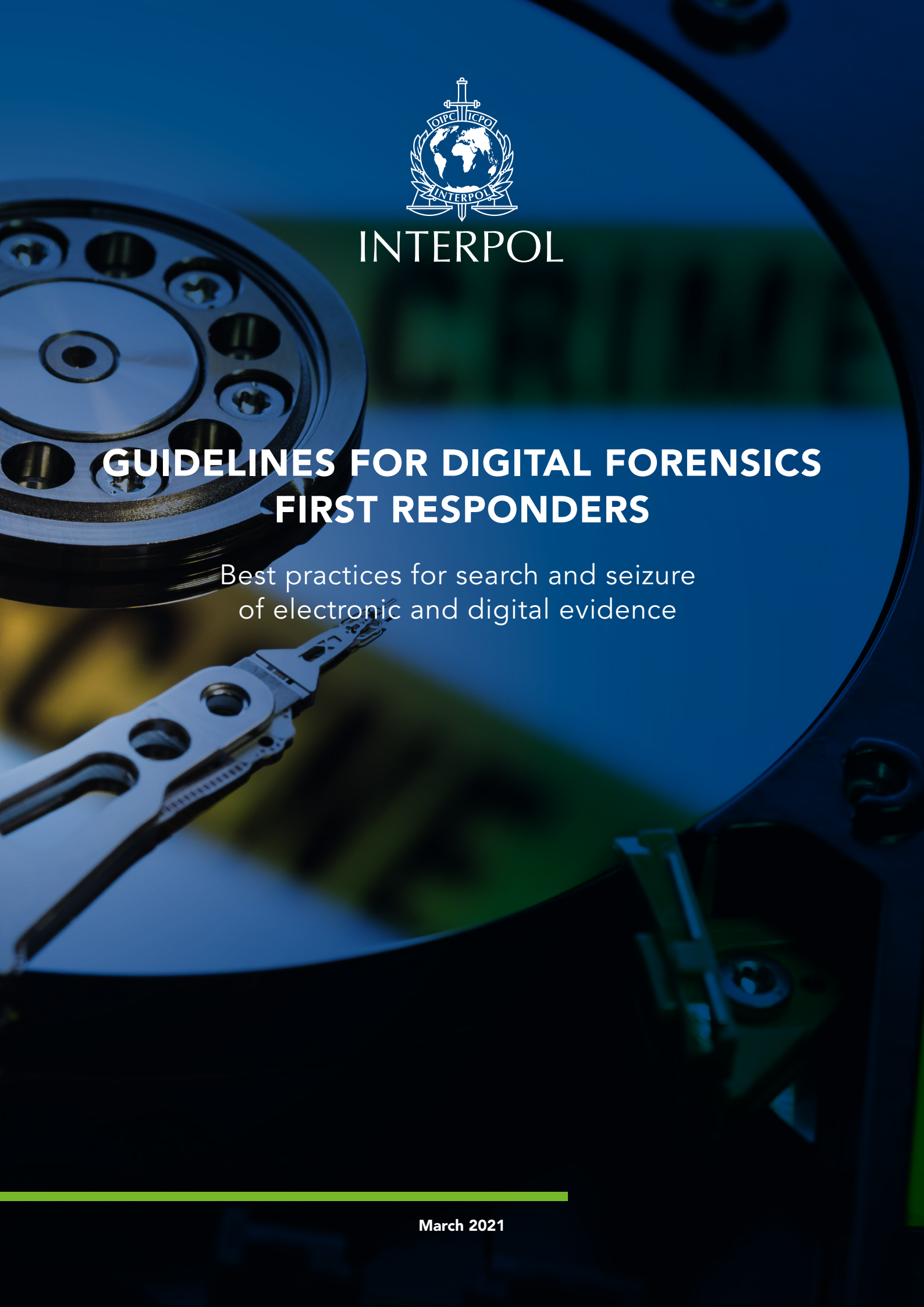

INTERPOL

GUIDELINES FOR DIGITAL FORENSICS FIRST RESPONDERS

Best practices for search and seizure of electronic and digital evidence

March 2021

Disclaimer

These “Guidelines for Digital Forensics First Responders” (the “**Guidelines**”) have been prepared as technical guidelines to provide information and advice on digital forensic approaches that may be adopted when seizing and analysing different kinds of devices. These Guidelines are solely for the use of law enforcement professionals having the necessary legal basis or authorisation to perform the actions described herein.

The legal, procedural and customary frameworks in respect of search, seizure, chain of custody, analysis, reporting, submission in criminal/prosecution/judicial process, evidentiary evaluation, admissibility and probative value, etc., differ widely by jurisdiction. These Guidelines do not provide any recommendations, advice or instructions in respect of requirements under such legal and procedural frameworks in any jurisdiction and any references seemingly suggesting as such should be read as being subject to domestic laws and procedures in this regard.

Readers are advised to ensure, when taking any actions based on these Guidelines, to verify and be satisfied that such actions are in compliance with appropriate legal and procedural requirements or standards in their jurisdictions.

These Guidelines are not mandatory in nature and have no enforceability. INTERPOL shall not be liable for any actions taken by any parties based on these Guidelines which are contrary to or inconsistent with or not in compliance with any relevant legal, regulatory, administrative, procedural, evidentiary, customary, or other requirements, exhibit extraction processes, chain of custody records to be maintained, etc.

These Guidelines also include mentions of open source, proprietary and publicly available tools and services (collectively, the “**Tools**” and each, a “**Tool**”) that offer various functionalities. They may be viewed, downloaded and/or used at the discretion of the user. In relation to these, please note the following:

- INTERPOL has not developed or verified the Tools, does not endorse them, has no association with their providers, and does not license or provide any support for the use of such Tools. INTERPOL provides no warranties (express or implied) in relation to the Tools or any of them, their utility for any purpose or effectiveness.

- Links to other websites from these Guidelines do not constitute an endorsement by INTERPOL, and are only provided as a convenience. It is the responsibility of the user to evaluate the content and usefulness of information obtained from other websites/ using these Tools.

- INTERPOL does not control, monitor or guarantee the contents of the links or the Tools provided herein, or their data collection practices; it does not endorse any views expressed or products or services offered therein.

- It may be necessary to create user accounts, pay subscription or one-time fees or upgradation fees in order to use some of these Tools. Registration or creation of user accounts, payment of fees or charges may require authorisation from your organisation and be subject to legal requirements in your jurisdiction (including for the creation of fake or assumed identities for this purpose). Please ensure that you have the requisite authorisations to use the Tools. INTERPOL does not encourage or in any manner, authorise doing so, and will not be liable in respect of any actions you take to create accounts or registrations, pay any fees or subscriptions, or if you assume any identities or create fake credentials, in order to use any Tool.

- Each of these Tools may be subject to licenses, privacy policies and to the terms contained therein. Please review carefully any such terms, conditions or privacy policies that apply to the use of any Tool you wish to use.

- Information entered into any of the Tools may be saved on the servers of the company that provides the Tool, and the legality of this within your jurisdiction must be tested and verified by you. It is also the responsibility of the user to test the data collection practices and privacy policies of the Tools as against their national legal requirements.

- Any use of the Tools (or any of them) is at your own risk, and INTERPOL shall not be liable or responsible under any circumstances for any damage or loss incurred, caused or alleged to be caused due to your use of or reliance upon any of these Tools. Any claims or actions in relation to any damage or loss incurred by a user should be directed to the providers of the Tool(s) and not INTERPOL.

- No data that is input in the use of any of these Tools will be transmitted to or be available to INTERPOL in any way. Should you choose to use any of the Tools for forensic, analytical or investigative purposes, you acknowledge that INTERPOL shall not receive any information in this regard, and at no point will be in the chain of custody of any evidence analyzed or generated using any such Tool.

Acknowledgements

The Guidelines are based on the Electronic Evidence Guide of the Council of Europe, on the Digital Evidence Collection Certificate Manual of the National Center of Excellence in Cybersecurity in Spain (INCIBE), and other best practice guides of law enforcement agencies concerning the seizure and treatment of electronic evidence. The INTERPOL Innovation Centre Digital Forensics Laboratory (IC DFL) also received feedback from digital forensic experts from different parts of the world, to meet a consensus for some of the debated or troublesome aspects encountered by digital forensic first responders. We wish to mention and thank the following colleagues below, whose valuable input has helped to improve the agencies worldwide:

- BRAZIL: National Institute of Criminalistics Brazilian Federal Police;
- SPAIN: Cybercrime Unit, General Commissary of Criminal Police (CGPJ) of Spanish National Police (CNP);
- The Scientific Working Group on Digital Evidence (SWGDE)

INTERPOL would also like to express its sincere gratitude to the Norwegian Ministry of Foreign Affairs for their support and contribution in the creation of the Guidelines.

The Guidelines will be referenced during an online training activity (Nov-Dec 2020), conducted in the framework of INTERPOL Project LEADER; a three-year capacity building initiative funded by the Norwegian Ministry of Foreign Affairs. The project focuses on enhancing digital forensics capacities of beneficiaries' in the South and Southeast Asia region. Through such endeavours, key stakeholders' of the project including digital forensic first responders and their law enforcement institutions will have the opportunity to strengthen their knowledge on the best practices articulated herein. Moreover, the guidelines will also serve the purpose as an invaluable reference tool across all INTERPOL member countries ensuring that advice on the handling, collecting and preservation of digital evidence to support investigations, are available to those law enforcement officers involved in such procedures.

NORWEGIAN MINISTRY
OF FOREIGN AFFAIRS

Foreword

In pursuit of providing guidance and support to law enforcement agencies across the globe, the INTERPOL Innovation Centre (IC) developed the *INTERPOL Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence*. I am pleased to present these Guidelines which aim to establish best practices for handling and using digital evidence during search and seizure preparatory and execution stages. Key technical considerations are also identified on the effective preservation of data to ensure that it can support law enforcement in criminal investigations and it can be admissible in court. This guide is intended to assist law enforcement officers from different crime areas who may attend to a crime scene, being responsible for collecting, securing, and transporting electronic and digital evidence. It will also be helpful for supervisors of aforementioned officers in guiding and supporting them. Moreover, it can be useful for prosecutors to get a better understanding of collection and handling of evidence.

As our society becomes increasingly integrated with digital technology encompassing every facet of our daily lives and law enforcement work, it may be difficult to remember an occasion where you had limited interaction with a digital device. For today's law enforcement community, there is a continuous trend towards investigations relying on some form of digital evidence. While we would consider that digital evidence indeed shares similar aspects when compared to traditional forms of evidence, there are also unique considerations to be taken into account.

The intangible nature of data obtained in electronic form, its volatility, and the ease at which it can be altered, all pose challenges to the integrity of digital evidence. Thus, it is vital that first responders and law enforcement practitioners are able to properly identify and handle digital evidence ensuring that the latter stages of the digital forensic process can be performed on the basis of sound judgement.

I am grateful for the contribution of the IC team, particularly its Digital Forensics Laboratory (DFL) for sharing their knowledge and subject matter expertise. I also extend my thanks to our colleagues from the INTERPOL Capacity Building and Training Directorate (CBT) who have supported this initiative and will utilize the Guidelines in the context of projects focused on enhancing digital forensic capabilities. Finally, I would like to thank the Norwegian Ministry of Foreign Affairs for its generous support.

The Guidelines are a reflection of INTERPOL's sustained efforts in fostering international police cooperation and our commitment to assist our member countries in response to the complex global security challenges in the digital domain.

Director Anita Hazenberg

INTERPOL Innovation Centre Directorate

Contents

Acronyms, abbreviations, and initialisms

CBT	INTERPOL Capacity Building and Training
CCTV	Close Circuit Television
CGPJ	General Council of the Judiciary – s the constitutional body that governs all the Judiciary of Spain
CNP	The National Police Corps / Cuerpo Nacional de Policía - national civilian police force of Spain
CNIC	Cellular Network Isolation Card
CSIM	Subscriber Identity Module
CSV	Comma-separated values file format
DFL	Digital Forensics Laboratory
DNA	Deoxyribonucleic acid
DRM	Digital Rights Management
DSC	Digital Selective Calling
ECDIS	Electronic Chart Display and Information System
ECU	Electronic Control Units
EPIRB	Emergency Positioning Indicator Radio Beacon
GB	Gigabytes
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positioning System
GSR	Gunshot residue
HD	Hard drive
HDD	Hard disk drive
IC	INTERPOL Innovation Centre
ICCID	Integrated circuit card
IMEI	International Mobile Equipment Identity
INCIBE	Instituto Nacional de Ciberseguridad / The Spanish National Cybersecurity Institute
IP	Internet Protocol
LRIT	Long Range Tracking and Identification System
NVMe	Non-Volatile Memory Express
OS	Operating System
P2P / P2MP	point-to-point & point-to-multipoint (P2MP)
PIN	Personal Identification Number
PUK	Personal unlocking keys – sometimes known as a network unlocking code (NUC) or personal unlocking code (PUC)
RAM	Random Access Memory
RAID	Redundant Array of Inexpensive Disks
RF	Radio Frequency
RPAS	Remotely Piloted Aircraft System
RUIM	Removable User Identity Module
SMS	Short Message Service
SSD	Solid-State Drive
sUAS	Small Unmanned Aerial System
TB	Terabyte
TPM	Trusted Platform Module chips
UAV	Unmanned Aerial Vehicle
UAS	Unmanned Aerial System
UPS	Uninterruptible Power Supply System

USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module – a SIM card for 3G services
VHF	Very High Frequency Radio
VMS	Vessel Monitoring System
VIN	Vehicle Identification Number
WIF	Wallet Import Format

List of figures

SEARCH AND SEIZURE OF DIGITAL EVIDENCE

1. INTRODUCTION

This guide aims to offer support and advice to Digital Forensic practitioners from law enforcement during the activities of search and seizure for identification and handling of electronic evidence through methods that guarantee their integrity.

An electronic device should not be seized without due preconditions. It is the investigation team together with the digital forensic experts that will assist in the collection and processing of electronic evidence, who will determine whether it is relevant or not to obtain and process those electronic devices.

Electronic evidence, like all other traditional evidence, must be carefully manipulated so that they can be incorporated as evidence in the judicial process. This affects both the physical integrity of the devices and the information or data contained therein. It must be taken into consideration that some electronic devices require specific procedures for collecting, packing and transporting, either because they are susceptible to damage by electromagnetic fields or because they may suffer changes in their contents during handling and preservation.

It should be taken in consideration that the possibility of obtaining traditional (non-electronic) evidence from the investigated scenario should not be excluded and that it could be relevant both for the investigation and for the subsequent treatment of electronic evidence. This is the case of any annotation related to the use of passwords, settings, email accounts, etc. These pieces of evidence must be manipulated according to the established procedures to preserve and assure their probative value.

2. SEARCH AND SEIZURE PREPARATION PHASE

2.1. Planning

Digital data is a fundamental pillar for most law enforcement investigations today. With the advent of the smartphone, social media and internet personalization with services like Google and Apple, a person leaves a digital trail and it is important that the digital trail is captured and analyzed for intelligence and evidence relating to the crime. The search and seizure phase is critical as this will safeguard the devices and the data held on them. If digital equipment is seized and not handled correctly, there will be potential for the data to be lost through deletion by the user, remote wiping or manipulation by a third party.

Suppose a team of police officers together with one or more digital forensic expert(s) have to fulfill the order of a prosecutor to enter inside the house of an alleged criminal suspected of a serious crime such as murder or robbery. There is a possibility that the suspect, within their devices, such as telephones or computers, may hold files or documents that are decisive in resolving the case. These devices must therefore be searched and, if deemed suitable for the investigation, seized.

In such cases, before starting any search and seizure activity, a series of considerations must be taken into account:

• A preparatory meeting should be held in order to exchange information between the unit in charge of the investigation and the personnel of other specialties that go on a support mission.

• The intervention on the scene of these specialized units should be prioritized and coordinated, which will depend on the specific case under investigation. For example, priority may be given to the action of Canine Units for the detection of explosives or DNA sampling collection prior to any other activity.

It is necessary that the unit carrying out the investigation provides in advance certain information needed for the coordination of the various specialists who may participate in the search and seizure. In the preparatory meeting regarding the appropriate treatment of electronic evidence, participants should assess all the basic information of the case, the details about the search warrant regarding electronic evidence or advice on the appropriate terms for the request of the warrant and, finally, specify the final destination of the seized goods.

From the point of view of the collection of digital evidence, it is essential to carefully prepare and plan all of the activities that will be carried out, taking into account a series of considerations such as:

• **Nature of crime under investigation**. The nature of the crime will determine the forecast of the necessary equipment and the preparation of the most appropriate technical procedures for each case.

For example, for crimes related to child sexual abuse, it is probably necessary to determine, in the same act of search and seizure, the possession of this material, so it will be necessary to find evidence or obtain the necessary samples (pictures, videos, chat sessions, etc.) “On-site” in an adequate and safe way.

In cases of financial crimes, it is very common to find infrastructure networks with user data stored in centralized or cloud servers, so it will be necessary to be clear about what type of electronic documentation is being sought, what is the best method to obtain it and where to store the data captured from those sources.

• **Suspect’s Technical knowledge.** Information about the suspects and their technical ability must be collected as they could have protected their equipment or data in some way that could compromise the acquisition of the evidence. Encryption systems or automatic data deletion applications make it difficult to obtain evidence.

• **Location of data storage**. It is not unusual for information to be stored in a place other than the physical computer equipment of the suspect. Given this, it is necessary to verify the actual location in order to require an additional legal authorization, especially if it is stored in a different jurisdiction, or if additional technical equipment is required to ensure the integrity of the evidence.

All data that is needed to carry out specific actions in relation to the processing of electronic evidence should be specified in the search warrant application or relevant procedural requirement prior to search and seizure.

In completing the procedural requirements, the final objectives of the action must be clear and specifically, in regard to:

- The authorization for the seizure
- Obtaining forensic images (“on-site” or not)
- Analysis of the devices “on-site”

- Use of applications to obtain access passwords
- Authorization to change the password of email accounts or social networks, etc.

Given the number of different case scenarios, we should consider the most appropriate actions to the specific case. Although, and in most cases, it is advisable to use expressions that support without any doubts the different actions to be performed. For example, *"it is requested that the seizure, copying and analysis of electronic devices capable of containing information in digital format will be done on-site."* The extent of precision and specificity that is required will depend on the jurisdiction and its legal and procedural frameworks.

2.2. The final destination of the evidence

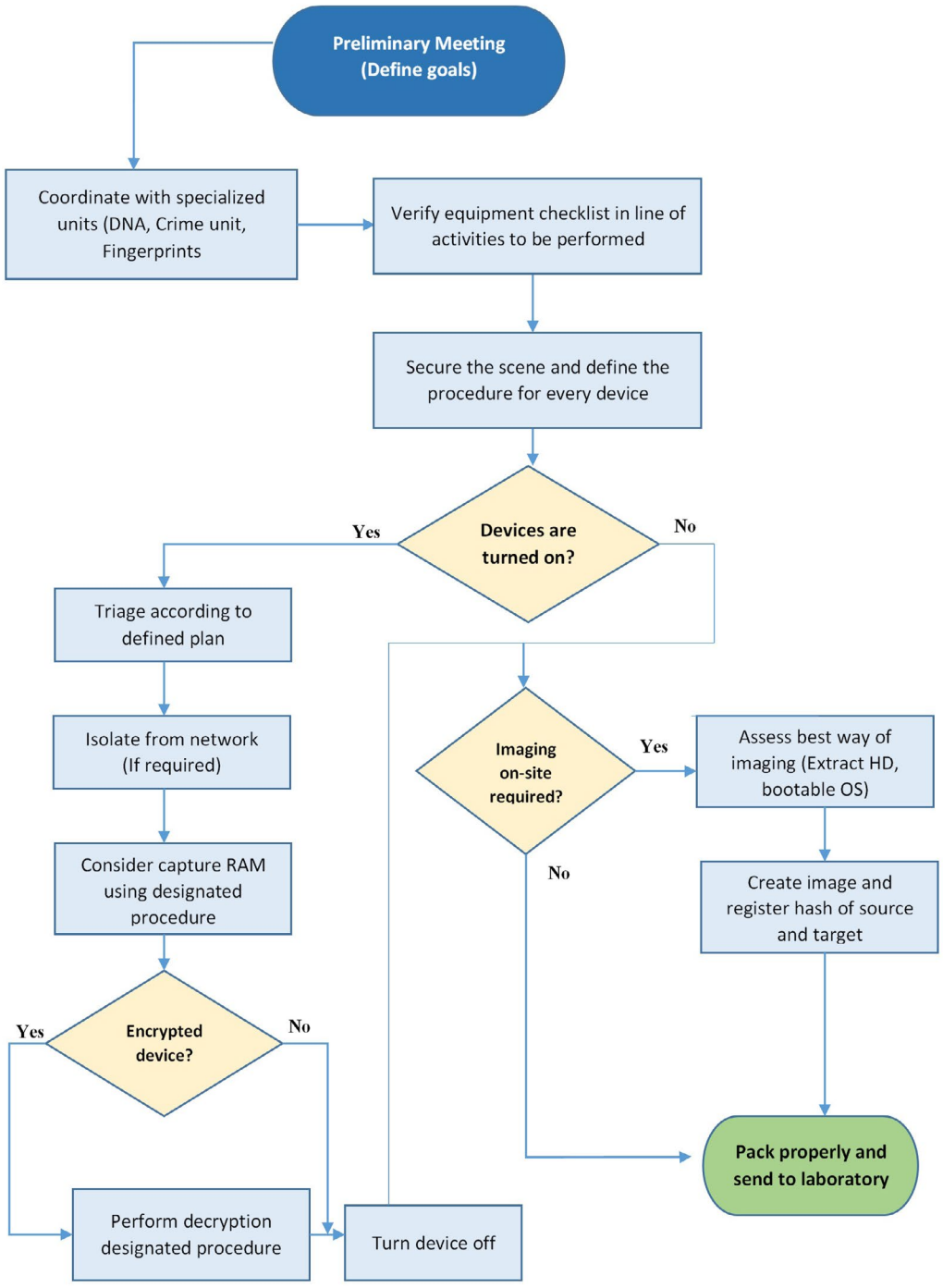

Figure 1: Flowchart showing the procedure and planning phase

The destination of the seized items must be defined before starting any activity of search and seizure.

Forensic copies, as well as devices that require specific treatment, should be sent to the corresponding department/team for processing and analysis.

For each case, adequate packaging, transport and documentation must be provided to maintain the chain of custody that begins during the seizure.

2.3. Equipment preparation

It is advisable to have a checklist with the material to be carried to the destination so that one can verify that everything needed is available and in good condition. A template is provided below (to be customized according to the procedural and legal requirements in the relevant jurisdiction).

It is crucial to have enough devices where forensic images, clones or data from remote sources will be stored. These devices should preferably be brand new or, at least, securely wiped overwriting all of the data with a known sequence of characters, usually "00" in hexadecimal, to avoid any possible data contamination.

The following is a list that the officer must take into account consisting of the minimum forensic tools needed for a successful search and seizure activity:

Forensic equipment	
◯	Laptop with the necessary standard forensic tools installed
◯	Hardware write blockers
◯	Forensic tools dongle licenses □ Dongle 1 □ Dongle 2 □ Dongle 3
◯	Enough memory storage media (external HDDs) for images and remote data destination □ Hard Disk 1 □ Hard Disk 2 □ SD card 1
◯	HD with extra forensic software or bootable devices
Tools to Disassemble	
◯	Screwdrivers (flat, star, hexagonal and other specific for certain models such as Hewlett Packard, Apple)

◯	Pliers (standard and pointed)
◯	Clamps (for cutting cables)
◯	Small tweezers
Exhibit Documentation	
◯	Photo or video camera (to take pictures of the scene and the screen content)
◯	Permanent markers (to encode and identify the investigated material)
◯	Labels (to mark and identify parts of the equipment, power supplies)
◯	Evidence tags
Resources needed for packaging and transport/Consumables	
◯	Evidence bags and seal
◯	Evidence carton boxes for media storage devices such as USB devices, DVDs, or CDs;
◯	Anti-static zip-lock evidence bags
◯	Faraday Bags to inhibit signals to mobile phones and other devices that may receive data from mobile/Wi-Fi network
Other items	
◯	Small torch with stand

◯	Gloves
◯	Large rubber bands
◯	Magnifying glasses
◯	Network cables (crossed and braided)
◯	Mask

3. SEARCH AND SEIZURE EXECUTION PHASE

Participant's safety at the search and seizure is a priority issue. For this purpose, there are specially trained units. No one should enter the perimeter without having secured the area. People who are in the scene will remain controlled at all times during the operations to avoid any alteration or data compromise.

The technical procedural steps described below are suggested, subject to applicable legal and procedural requirements in the country.

3.1. Secure the scene

In the case of electronic evidence collection, the aim is to avoid the loss, alteration or destruction of any possible evidence. For this, the following measures will be taken:

- Remove and forbid unauthorized personnel from accessing the scene. They must be kept away from computers, mobile phones or any other sensitive items, including power supplies. In addition, suspects should not be able to communicate with anyone who is not on-site to prevent remote data destruction.
- Quickly locate the most obvious elements, computers and mobile phones, especially those that are connected to the Internet and those that need special assurance measures to prevent data loss.
- Check the existence of wireless networks that allow access and modification of data from outside.
- Refuse any help offered from unauthorized personnel in the investigation.

3.2. Assessment

After first securing the scene, first responders should make a general assessment of the scenario. This includes, having a global idea in quantitative terms of the material that is possible to process, the type of processing that is going to be carried out and the costs in equipment and time that will be required. This is the best time to produce a photographic report of the scene since in this first phase it will have suffered minor contaminations.

Although the traditional method of conducting a search was to maintain a clear order starting with a thorough search of a room to continue with the next one, in the processing of electronic evidence it becomes difficult to follow that working method. This is due to the fact that obtaining or copying the evidence is a slow process that can last for many hours. Therefore, it is crucial to start processing this evidence as soon as possible while continuing conventional search and seizure.

It is worth pointing out that digital devices containing potential evidence may be easily hidden, integrated or contained within cupboards or drawers, (memory cards, mobile phones, etc.) so a careful sweep for electronic devices of a crime scene may be required depending on your points to prove.

3.3. Document the scene

All processes to collect and gather the evidence should be duly documented according to applicable procedural and legal requirements. To do this, you must keep an exhaustive record of the location and original condition of the devices.

The following are examples for proper documentation of the scene:

- Laptop computer: evidence number EVI001
- Internal hard drive: evidence number EVI001A
- USB Thumb drive: evidence number EVI001B
- DVD: evidence number EVI001C

At that moment, the possibility of seizing only devices that contain information can be assessed, documenting the effects that have been reviewed but will not be processed. In the previous example, the devices that contain data to be analyzed are internal hard disks, thumb drives and DVDs, while the laptop without the above elements lacks useful information. It should therefore be avoided to transport and store devices that we already know do not provide any data. This option must be assessed by a specialist, since the intervened effects may have some kind of technical relationship with the device they come from and without which it would not be possible to analyze them. This procedure will be discussed more in-depth in the specific procedures.

For each device, the following data must be documented:

- Type: Computer, hard drive, flash drive, DVD, etc.,
- Brand and model
- Storage capacity, indicating if it is MB, GB or TB
- Serial number
- State: Damaged, on, off, etc.,
- Location: Stay and specific place
- Security: Access password, PIN
- Comments: Used only by children, not connected to the Internet, etc.,

Finally, any annotation related to the use of passwords, settings, email accounts, etc., as well as the SIM cardholders with their ICCID, original PIN and PUK number and any other relevant information that may be searched will be searched and documented. They will be used in the subsequent analysis of the devices.

3.4. Collection and the handling of digital evidence

As a general rule the following principles will be applied, but refer to the following sections for specific devices:

a) If the equipment is on, do not turn it off.

Verify installation of anti-forensic systems: local or remote erasing programs, external access. Stop these processes even by pulling the power cable or removing the battery if necessary.

Isolate the device from the networks to which it is connected unless you are authorized to access cloud services.

Disable screensavers and screen locking in order to prevent the equipment from being hibernated or suspended.

Check if the device has any kind of encryption system running (Bitlocker, FileVault, VeraCrypt, PGP Disk, etc.).

Check if it is connected to power.

b) If the equipment is turned off, do not turn it on until it is processed with guarantees, as further explained later.

If the local legislation allows it, the suspect's password/pin must be asked and checked if it is correct.

Even if the device is not fully encrypted, it is important to have the suspect's passwords. The suspect might have encrypted a file or used the same pattern in another system.

The following actions can be performed on the devices:

- **Seizure**. The device is simply documented, described and sealed, leaving the decision for further analysis to the court or any other rightful authority. No further actions are taken on it until it is again unsealed.
- **Generate a forensic copy**. For each evidence, apply the specific procedures described in this manual.

The process performed will have to be documented:

- **The procedure used**: cloned, image or any other system used.
- **Tool**: Hardware duplicator, write blocker, software, etc.,
- **Destination location**: Destination disk, file with the data obtained from a telephone, etc.,
- **HASH:** Algorithm used and the signature obtained.
- **Observations**: Any incident arising during the copy process.

3.4.1. Live analysis of powered computers and laptops

It is necessary to carry out an exhaustive record of all the actions performed, as well as the date and time at which they were fulfilled.

The variety of possible scenarios in a capture procedure requires specific considerations for each of them. However, it is advisable to follow a predetermined methodology when it comes to capturing volatile data based on its volatility order.

If using a forensic tool at a scene, this must only be carried out by trained personnel and ensure that the reason for examining the evidence at the scene is documented and controlled.

There are some tools specially developed for law enforcement that can help in the live analysis. One of them is **FiRST**, which is a first responder tool part of the FREETOOL project, developed by the Berlin State Police (Germany). The purpose of FiRST is to inform the first responder if the machine can be powered down. FiRST checks for signs that traditional post mortem forensics may not be successful or complete. These signs include the presence of encryption or disk-wiping software, cloud/network storage locations, virtualization, etc. If these signs are detected, the first responder is warned of the dangers inherent in pulling the plug and advised to contact an expert. For more information consider visiting the official page of the project at https://freetool.ucd.ie.

If a specific tool like FiRST is not available, you could consider the list shown below based on the list created by Kuhlee and Völzow (*Computer Forensik Hacks, O'Reilly, ISBN 978-3-86899-121-5*), aimed at facilitating the choice of the most appropriate tool to capture specific fragments of volatile data.

Volatile Fragment	**Windows tools**	**Linux tools**
RAM content	Dumpit, Winen, Mdd, FTK Imager	dd, fmem
Routing table, ARP cache, Kernel statistics	Route PRINT, arp –a, netstat	netstat –r –n route arp -a
DNS cache	Ipconfig/displaydns	mdc dumpdb (if installed)
List of running processes	PsList, ListDLLs, CurrProcess, tasklist	ps –ef, lsof
Active network connections		netstat –a, ifconfig
Programs and services using the network	sc queryex, netstat -ab	netstat -tunp
Open files	Handle, PsFile, Openfiles, net file	lsof, fuser
Network shares	Net share, Dumpsec	showmount –e, showmount –a smbclient -L
Open ports	OpenPorts, ports, netstat -an	netstat –an, lsof
Connected users	Psloggedon, whoami, ntlast, netusers /l	w, who –T, last
Encrypted archives	Manage-bde (Bitlocker), efsinfo (EFS)	mount –v, ls /media

Active network shares	Fsinfo, reg (mounted Devices)	mount –v, ls /media
Remote accesses and network monitoring	Psloglist	/etc/syslog.conf Port UDP 514
System and network configuration	Systeminfo, msinfo32, ipconfig /all	ifconfig –a netstat -in
Storage devices	Reg (Mounted Devices), Net share, netstat -a	mount –v, ls /media
Date and time	Time /T, date /T, uptime	time, date, uptime
Environment variables	Cmd /c set	env, set
Clipboard	pclip	
Disk content	FTK Imager, EnCase, Tableau Imager	dc3dd, ewfacquire, Guymager

Many of these tools are available on the Microsoft Sysinternals website or in the official Linux repositories.

In the selection of tools, it is necessary to take into account a series of considerations:

- Tools that have less impact on the system should be used. To capture RAM, for example, in order to avoid overwriting data, it is preferable to use a small tool such as "dumpit" than another that uses a graphical environment such as "FTK Imager".
- It is also preferable to use tools that have their own executables and not use those of the system under investigation. Likewise, the investigator must be able to motivate in the judicial procedure the utility and functionality of the tool.
- The tools used should only capture volatile information. The data that will be available on the hard disk can be analyzed later using the procedural guarantees mentioned.
- The suspect's media device should never be used to store the captured information and data. This information must be saved on external storage devices.
- These are processes that can last for several hours. Therefore, it is necessary to verify that no energy-saving system will interrupt the capture procedure while active.

3.4.2. Inability to access information on powered devices

There are times when the equipment to intervene is turned on and yet it is not possible to access the content. It may be the case where the device has entered idle mode or the screensaver is active and when leaving this state the device requests credentials or a password to access it. The initial and technically simple option is to request that password from the user/owner. In case of refusal, there may be several techniques to avoid the loss of volatile data.

It should be noted that these techniques will be used by qualified personnel and in cases in which it is certain that the loss of volatile information implies the possibility of not being able to access the contents of the rest of the device when it can be found encrypted.

In the rest of the cases, the action will be explained in the shutdown of switched-on equipment.

a) "Cold-boot RAM" technique. It is a technique consisting of freezing the RAM with the equipment on using liquid nitrogen. Once this is done, the computer is turned off and restarted with its own operating system from a CD or pen drive, with tools that manage to dump the RAM. When this memory is frozen in the shutdown process, it keeps the data it had.

This technique is based on research carried out by the University of Princeton [1]and might not be useful in an operational environment.

b) Transport the intervened device without turning it off. Another method may be to use portable power systems that keep the equipment on until the arrival at the forensic laboratory where it will be subsequently treated.

3.5. Seizure Phase

The record of the search and seizure process usually involves the beginning of the chain of custody of the evidence involved. So, it will be necessary to specify the next destination and the person(s) responsible for the custody of transfers. This process will be informed by the legal requirements in the applicable jurisdiction.

3.5.1 Packaging and Transport

All evidence from a search and seizure must meet the following conditions:

- Ensure that all the collected material has been properly registered and labelled before proceeding to its packaging.
- When possible, the original packaging will be used to package and transport the seized devices.
- They have to be uniquely identified, through labelling.
- The label must show whether or not they have been subjected to the cloning/copying process.

Suitable material must be used for its sealing to avoid possible manipulation of the devices. The seal must prevent access to internal elements (hard drives or internal memories) both physically and through the connection ports of the equipment.

Depending on their destination, they will be packaged separately, without mixing them with other documentation or other devices. This will facilitate the diligence of the unsealing and acquisition of forensic copies or their direct submission to the laboratory. Each package containing electronic evidence will have on its exterior the identification that shows the nature and origin of the content.

The means used for transport and temporary storage must ensure the integrity of the devices sufficiently, protecting them from shocks, and from sources of electromagnetic radiation, heat or humidity that may damage them.

4. TECHNICAL CONSIDERATIONS

4.1. The forensic copy

One of the main premises in the forensic analysis process warns that, excluding exceptional cases, an examination of the evidence should not be performed using the original device. Therefore, it will be

[1] Halderman A., Schoen S. D., Heninger N., et alia, "Lest We Remember: Cold Boot Attacks on Encryption Keys", appeared in *Proc. 17th USENIX Security Symposium* (Sec '08), San Jose, CA, July 2008. Available at: halderman.pdf (usenix.org)

required to copy or clone the data contained in the original device, to avoid compromising its integrity. The forensic experts will then use the imaged/copied data to perform the analysis.

This copy must be an exact bit-by-bit replica of the original device, regardless of its content.

This process can be done in two formats:

a) Device to Device (clone): This can be performed by obtaining an exact bit-by-bit replica of an original device in another - previously wiped - device with equal or greater capacity.

b) Device to File (image): This can be performed by generating one or more files that contain, linked together, an identical copy of the original device. The most widespread is "dd" (raw) or "E01" formats.

It is possible to perform these processes through hardware duplicators or through specific software installed on forensic computers. Forensic duplicators protect the original device from any writing or alteration during the process, and when specific software is used to make forensic copies it is advisable to use hardware or software write blockers.

Advantages of creating image files:

- Allows the copy to be spread in multiple files configurable in size, facilitating its storage and subsequent analysis.
- Provides file compression without data loss, in order to save storage space on the destination device.
- Allows encryption if needed, in order to provide more security.
- May include case information, data on image creation and verification of the integrity of the evidence including the results of the HASH.
- Prevents contamination of the copy.

These formats can be read directly and more efficiently on the analysis programs.

4.2. Alternatives to the forensic copy

There are other scenarios in which it will not always be possible to obtain an exact physical copy, bit by bit, of the entire source device, such as the acquisition of files or information from servers, NAS, virtual disks or encrypted volumes.

In these cases, there are other techniques to acquire digital evidence.

a) Logical copy of volumes. This method is applied, for example, when it is needed to acquire the content of an encrypted volume that is being used on a powered computer. To preserve that information, a logical copy of the volume will be produced. By making a physical copy of the disk, a partition would be obtained that would be unreadable since the data is encrypted. However, the logical copy allows the user to acquire the content in the same way the user accesses it.

b) Logical copy of files. It is performed by generating, using suitable software, a replica of the original data after selecting what may be of interest to the investigation. For example, in a business environment, we can make a logical copy of the suspect user's folder. The drawback is that the file-slack space in our copy will be lost, and the metadata of the original file system may not always be maintained.

Making forensic logical copies does not prevent the properties of the evidence from being maintained. Whenever it is carried out, use the appropriate tool and method, protect against writing, preserve

metadata as much as possible and use a cryptographic algorithm that allows verifying the integrity of the acquired data.

4.3. HASH function

The HASH function or summary function is used to verify the integrity of a data set. In other words, it is about obtaining its “fingerprint”.

In the case of electronic evidence, this procedure is applied when making copies of the original devices, so that, once the HASH value of the origin and destination has been calculated, they must be identical. This process is known as verification.

This procedure is also used to detect known files within the evidence. There are reliable file databases (from the installation of operating systems or other applications), such as those of the NSRL (National Software Reference Library) that allow them to be discarded, and other databases with the signatures of known files, for example, of child sexual abuse material, which allow investigators to identify, track, and even share them amongst law enforcement without the need to distribute the original files.

It is important to remark that some technologies like SSD are becoming a new challenge when considering evidence verification methods. Due to how the SSDs work they can sometimes purge data all by themselves even if they are not connected to any interface with only the power on. Alternatives to traditional evidence hashing must be considered, such as hashing of logical partition or file hashing.

5. SPECIFIC PROCEDURES

In the previous sections a general procedure has been explained in order to preserve the integrity of digital evidence. However, during the search and seizure the Digital Forensic Expert will find many devices that require specific procedures due to their nature. It will be due to complexity in terms of connection processes for some of them, encryption systems present, large amount of data to be extracted or lack of standard extraction tools.

In the following sections you will find the general guidelines for some of the devices that can frequently be found in search and seizure environments.

Figure 2: Devices: Smart phones and tablets

5.1. Smartphones - Tablets

Mobile phones have become a primary source of digital forensics as they are always on and are very personal to each user. A smartphone such as an Android or Apple device can contain from 16GB to 1TB of data.

Also, a mobile handset may contain a SIM CARD and a removable media card if supported.

Each of these elements are essential to an investigation as they contain data that may enable to either identify the owner or understand their activity using the mobile phone.

With the advent of the smartphone and the introduction of application stores such as Google Play and iTunes store, the user can install applications that may allow the handset to utilize new services such as online gaming, instant messaging, and file sharing. With each mobile handset, the examiner should access the application for investigational value and its relevance to the case and the points to prove, subject to applicable procedural and legal requirements in their jurisdiction.

5.1.1. Considerations when securing mobile phone evidence

Mobile devices present a unique forensic challenge due to rapid changes in technology. There are numerous makes and models of mobile devices in use today. Many of these devices use closed source operating systems and proprietary interfaces, sometimes making it difficult to extract digital evidence. Version specific expertise may be necessary to attain access and may alter workflows listed below.

Examples encountered are as follows:

- **Incoming and Outgoing Signals** – Attempts should be made to block incoming and outgoing signals of a mobile device. A common method includes Radio Frequency (RF) blocking containers (e.g., Faraday bag or room). RF signal blocking containers may not always be successful. They may drain the battery and failure may result in data alteration.
- **Cables** – Data cables can be unique to a particular device and forensic tool.
- **Destruction of Data** – There are methods to destroy data locally and remotely on a mobile device. This is why the device must be isolated from all networks (e.g., carrier, Wi-Fi, Bluetooth) as soon as possible. Examiners should be cognizant that a mobile operating system may have automated processes which will destroy data on power-on, or after a specific duration of time, and choose an extraction method or schedule that addresses these concerns, where applicable.
- **Drivers** – Conflicts may occur due to existing operating system drivers, proprietary drivers, driver version inconsistencies, and vendor-specific drivers. Ability to find proper drivers may be difficult. Drivers may be included with a forensic tool or downloaded from a website. Drivers may compete for control for the same resource if more than one forensic product is installed on the analysis machine.
- **Dynamic Nature of the Data** – Data on active (powered-on) mobile devices is constantly changing. There are no write-blocking methods for mobile devices.
- **Encryption** – Data may be stored in an encrypted state preventing access or analysis.
- **Equipment** – Equipment used during examinations may not be the most recent version due to a variety of reasons, such as purchasing/budgeting delays or verification requirements of hardware, firmware, or software.
- **Field analysis** – Triaging mobile devices is not considered a full examination. However, if triage is performed, the device should be protected and isolated from all networks.
- **Inconsistent Industry Standards** – Manufacturers and carriers may use proprietary methods to store data (e.g., closed operating systems, proprietary data connections).
- **Loss of Power** – Many mobile devices may lose data or initiate additional security measures once powered off.
- **Passwords** – Authentication mechanisms can restrict access to a device and its data. Traditional password cracking methods can lead to permanent inaccessibility or destruction of data.
- **Removable Media Cards** – Processing media cards while still inside the device poses risks (e.g., not obtaining all data including the deleted data, altering date/time stamps).
- **Identity Module e.g., USIM, CSIM, RUIM Cards** – Lack of or removal of an identity module may prevent the examiner from accessing data stored on the internal memory of a handset. Inserting an identity module from another device may cause loss of data.
- **Training** – The individual collecting, examining, and analyzing a mobile device should be trained to preserve and maintain data integrity.

- **Unallocated Data / Deleted Data** – Mobile device forensic tools may support only a logical acquisition of data that may limit the amount of data that can be recovered.

Document the collection of devices in accordance with organizational guidelines and procedures and any applicable laws. Documentation may include a written description or photographs of the collection location, the device state (e.g., powered on/off, presence of a passcode), examiner interactions with the device, and physical characteristics of each device (e.g., damage, identifying information such as make, model, serial number, and any identifying marks, and connections).

The chain of custody documentation should be contemporaneous to the collection and include a description or unique identifier for the evidence, and the date and time of receipt and transfers. The record should fully identify each person (e.g., name, title, signature) taking possession of an item.

5.1.2. Mobile Phone Evidence Preservation Process for First Responders

The following flow charts provide a basic overview of the best practices for preserving evidence when seizing particular types of mobile devices and are not meant to be all-encompassing.[2]
Circumstances may warrant deviation from the procedures outlined herein. Subjects should not be access to the device (e.g., subject applies biometric identifiers or enters a passcode).

5.1.3 iOS Preservation Process and Flowchart

iOS is a mobile operating system created and developed by Apple exclusively for its mobile hardware, including the iPhone, iPad, and iPod Touch. The following flowchart details steps that should be taken to preserve digital evidence on an iOS device.

All iPhones utilize hardware and software encryption so if the device has a password/passcode/Face ID then the user of the handset must supply the information required to gain access to the handset otherwise the forensic lab may not be able to access the handset data.

Figure 3: An Apple iPhone.

[2] This guidance is replicated from the Scientific Working Group on Digital Evidence (SWGDE) Best Practice for Mobile Device Evidence Collection and Preservation Handling and Acquisition Scientific Working Group DE v1.9 (dated 2020-09-17). It is the readers' responsibility to ensure they have the most current version of the document. Please see swgde.org/documents/published for more information. Please also refer to the references section at the end of this report for the SWGDE disclaimer and redistribution policy.

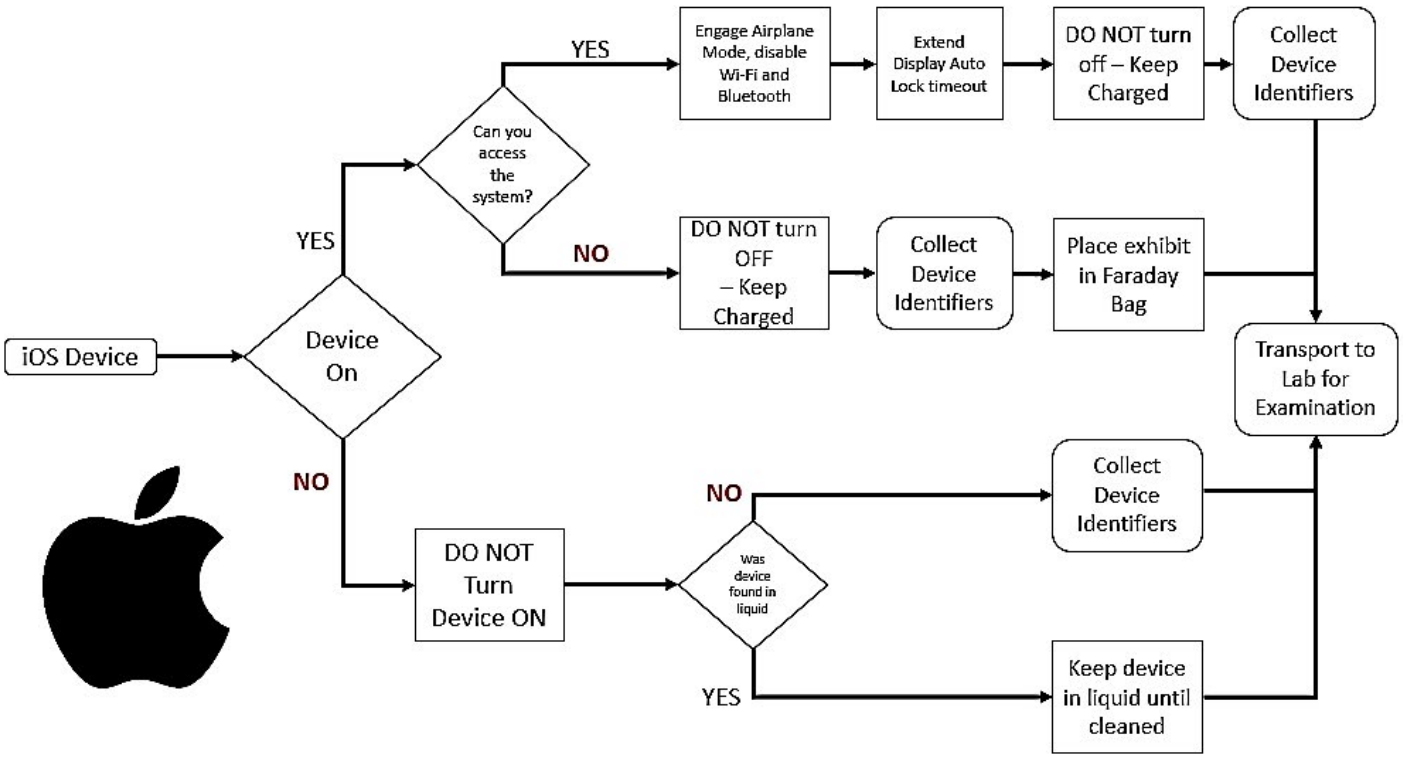

Figure 4: Flowchart for Apple iOS device evidence acquisition procedure

The flow chart above is not all-inclusive for all versions of iOS. Version specific expertise may be necessary in order to obtain access and may alter the foregoing workflow. If the device is powered on, it may contain volatile data, including encryption keys, and should not be turned off.
A power source should be connected as soon as possible to prevent the device from powering down. Be sure to seize the charging cable to keep power to the device. It may be possible to adjust the Display Auto-Lock feature to extend the length of time before Auto-Lock is enabled.

If the device is unlocked, the examiner should take steps to prevent its locking such as disabling the lock code or repeatedly interacting with the touchscreen.

Place the device in “Airplane Mode” (by swiping up from the bottom and selecting airplane mode) and verify that Wi-Fi and Bluetooth are off. If the device cannot be placed in “Airplane Mode”, put it in a Faraday bag to prevent network interaction from potentially altering data on the device. Mobile devices blocked from connecting to a network will boost power output while trying to obtain a signal. This will drain a device’s battery at an accelerated rate. If it is necessary to keep the device powered on, connect it to an external power source such as a portable battery pack. Both the mobile device and the charging source should be placed inside the Faraday bag. If the charging source is not placed in the Faraday bag, the cable can act as an antenna and the device may be able to connect to the network.

If the device is off, leave it off. Collect identifying data about the device, such as model number, carrier and unique identifiers that are visible.

5.1.4 Android Preservation Process and Flowchart

Android is a Linux-based mobile operating system developed by Google and has the largest install base of any mobile operating system. Android is available in many different versions and, unlike iOS, is offered on devices manufactured by numerous companies. The following flowchart details steps that should be taken to preserve digital evidence on an Android device.

The Android device may utilize hardware and software encryption, so if the device has either a password/ passcode/Fingerprint/Face ID, then the user of the handset must supply the information required to gain access to the handset otherwise the forensic lab may not be able to access the handset-data.

Figure 5: Android smartphones

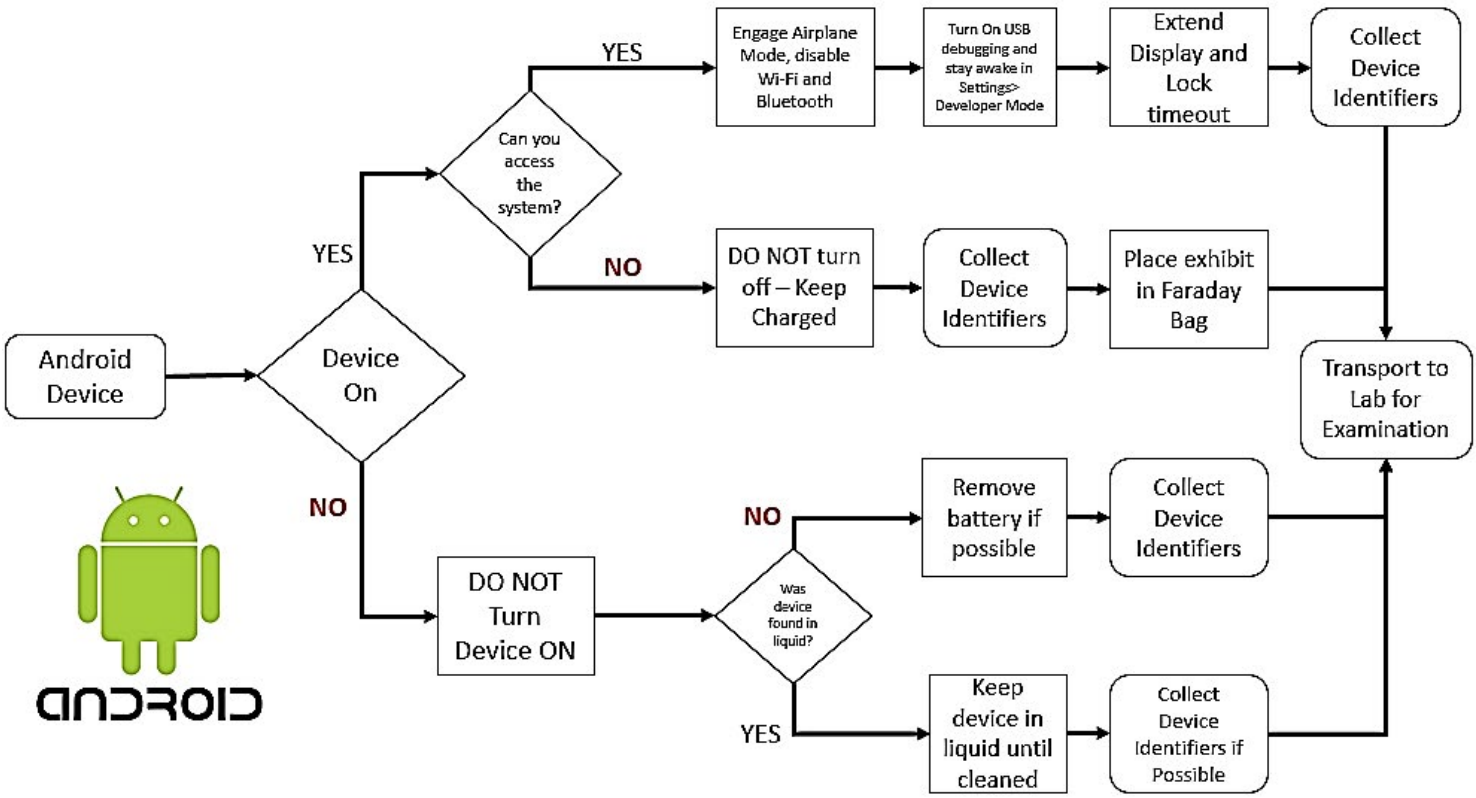

Figure 6: Flowchart for Android device evidence acquisition procedure

The flow chart above is not all-inclusive for all versions of Android. Version specific expertise may be necessary in order to attain access; and may alter the foregoing workflow.

If the device is powered on, it may contain volatile data, including encryption keys, and should not be turned off. A power source should be connected as soon as possible to avoid the device powering down. Be sure to seize the charging cable to keep power to the device. If the device is unlocked, the examiner should take steps to prevent its locking such as disabling the lock code or repeatedly interacting with the touchscreen. It may be possible to adjust the Display Screen Timeout feature to extend the length of time before Auto-Lock is enabled.

Place the device in “Airplane Mode” (by swiping down from the top and selecting airplane mode) and verify that Wi-Fi and Bluetooth are off. In order to give the best chance of accessing the evidence at a later date, enable USB debugging, if possible.

If the device cannot be placed in “Airplane Mode”, follow the same procedure as for Apple devices.

If the device is off, leave it off. Collect identifying data about the device, such as model number, carrier and unique identifiers that are visible.

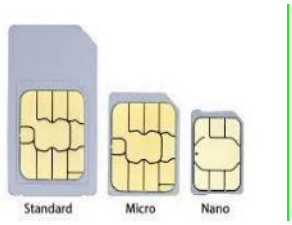

Figure 7: SIM cards.

5.1.5 SIM Card

A SIM / USIM card can contain contact lists, phone calls and SMS messages. A SIM Card may be protected by a PIN Code. If the code is attempted 3 times without success, access to the SIM Card is locked. To unlock it, you will need the PUK code, which is located on the original SIM cardholder or it can be requested from the mobile service provider. In any case, the ICCID (Integrated circuit card) will be obtained, which is its serial number.

Figure 8: SD Cards.

5.1.6 Removable Media Card

If a handset allows the use of a removable memory card, then this card is used for expansion of the phone storage capacity. Removable storage is commonplace amongst Android handsets as this allows the user to store multimedia such as photographs, movies and music files as well as application data or backups of applications or mobile phone content. Removable memory cards can potentially be used across multiple handsets over time, depending on user behaviour.

Figure 9: Components of cloud storage.

5.1.7 Cloud Data

Both Apple and Android phones require the user to have either a Google Account (Android) or an iCloud account (Apple). These cloud services enable the user to backup data to the cloud, as well as share their photos, videos and music files. They also make it possible to backup handset user data in case the device is lost or it has to be transferred to a new handset.

5.1.8 Considerations upon Seizure

Traditional Forensics

Traditional forensic processes, such as fingerprints or DNA testing, may need to be conducted in order to establish a link between a mobile device and its owner or user. If the device is not handled properly during preservation and collection, physical evidence can be contaminated and rendered useless. As such, handle all potentially evidentiary items with gloves and submit to an appropriate lab as the situation dictates. Traditional forensic processes (e.g., DNA, latent prints) on a mobile device should be completed before digital forensic processes.

Access

User-created passwords also complicate the recovery of mobile device data. Collect and document this information if possible, and subject to applicable procedural and legal requirements in your jurisdiction.

Network Isolation

Disconnect mobile devices from their networks to ensure data is not remotely modified or destroyed. Mobile devices typically have a reset capability that clears all user content, resetting device memory to the original factory condition. Because this may be performed in person or remotely, immediate precautions (e.g., separate the device from its user, network isolation) are necessary to ensure evidence is not modified or destroyed.

Generally, examiners isolated a mobile device from network connectivity by placing the device in “airplane mode”. The “airplane mode” feature in newer versions of mobile operating systems may not disable Bluetooth, Wi-Fi, and other wireless protocols or may only disconnect them temporarily. Examiners should manually confirm that network connectivity has been disabled or consider alternate means of isolation, including placing the device in an RF shielded enclosure, removing the SIM card from the device or utilizing a Cellular Network Isolation Card (CNIC) for GSM phones.

The responder should also restrict any interaction with the device unless in a controlled environment. This is to safeguard the data on the device and also ensure that the device does not automatically connect to cloud services or networks as this may change the data on the device or enable wiping of the device remotely.

Powering off the device to isolate it from the network poses the risk of engaging authentication mechanisms (e.g., passwords, PINs) or enabling enhanced security features, potentially rendering data inaccessible.

Points to Prove

The responder should also consider points to prove for the investigation when submitting the device to the digital forensics lab as smartphones contain lots of data and not all data will be pertinent to the case.

Some forensics software allow the data from the exhibits SIM card to be cloned onto a blank SIM card (Clone) with the original data copied onto the cloned SIM card with the network data omitted. The phone associates call logs, settings and other data with the SIM card. If a mobile phone is started with another card or without a card, this information cannot be accessed and maybe be lost.

How to proceed:

a) The device is on.

- Photograph the screen in the state it is in. Check the battery and if the date and time the device shows correspond to the actual date and time upon seizure.
- IMEI check: dial * # 06 # and photograph.
- Make a logical image of the device with the forensic device, including reading the SIM.
- Make a physical image of the device if it is supported.
- Turn off the device. Remove battery, SIM / USIM card and memory expansion card and photograph the assembly with the identification tag.
- Make a forensic image of the memory card, as described in its specific procedure, if it has not been performed by the forensic team.
- Do not turn on the equipment again.
- All elements are sealed together and marked as processed.

b) The device is off.

- Check if support is available for acquiring a forensic image.
- The battery is removed and the items to be checked are located: SIM card and external memory.

- A SIM / USIM card is read by checking if it is protected by a PIN. If available, it is entered only once, because if it is tried 3 times without success, it is blocked. To unlock it, you will need the PUK code, which is located on the original cardholder or that can be requested from the mobile service provider. In any case, the ICCID (Integrated Circuit Card Identifier) will be obtained, which is its serial number.
- A blank SIM card is recorded with the original SIM card data and inserted into the terminal. The phone associates call logs, settings and other data with the SIM card. If a mobile phone is started with another card or without a card, this information cannot be accessed. The card generated as a copy of the original guarantees, in addition to keeping this data that the device will not connect to the network.
- A forensic copy is made of the memory card, if any, following the procedure proposed for this type of storage media.
- The device is recomposed, turned on and a logical image is extracted following the system instructions.
- If it is supported, a physical image is also made.
- All elements are sealed together and marked as processed.
- Try to locate and create a record of original containers and SIM cardholders with visible PIN and PUK.

5.2. Servers

Server-type computer equipment provides service to other client computers. We can find them mainly in business environments performing functions of a file server, mail, web services, database, user management, etc.

Physically they can look like a normal workstation or they can be mounted on rack systems.

Before proceeding with a server some aspects have to be considered:

What does the Court order/relevant legal authorization permit? Servers can be a fundamental part of the normal development of a company's activity, which does not have to be necessarily involved in the commission of the criminal act. Is it justified to leave an organization, possibly extraneous to the crime, without service? Is the equipment seizure really needed?

Do we have the collaboration of the administrator or system management personnel? Can they be trusted? Are they involved in the criminal activity?

Is it clear what kind of information has to be acquired?

Are we familiar with server environments and their operating systems? Can we disconnect the server from the data network and even turn it off to isolate it from the outside?

The preferred process to seize information from servers is to make a selective logical copy of the suspect's folder. But you also have to consider getting the event logs, the active directory settings, mailboxes and the backups.

5.3. Personal Computers

The first step will be to determine if the computer is turned on. Many computers can be in a power-saving mode, with the monitor simply turned off, in a state of sleep, hibernation (Windows) giving the feeling that they are disconnected or powered off. We will have to check if the monitor has power and connection to the equipment and if the unit has power or has a LED that indicates activity.

To remove the computer from this state we will avoid pressing the power or reset button or the "Enter" key. It is best to move the mouse first or use the scroll or shift keys. Take note of the exact time of this action for further records.

If the equipment is turned on and shows activity, it is advisable to take the following measures:

- Take a picture of the screen as it appears and include date, time and time zone.
- Check the activity the user is performing at that moment, like active icons, process bars, and application operation indicator. If it is observed that any destructive process is being executed, such as secure deletion, deletion of logs or records, etc., it must be interrupted immediately, even and if necessary, by pulling the power cable.
- Check the existence of network, wireless or cable connections.
- Disable screensavers or power setting modes. The purpose is to avoid the device to enter savings states or shut down, losing the original state of the system.
- Check the mounted volumes and their characteristics, basically looking for the use of encryption or connection to shared folders on another computer in the network.
- Check the possible existing activities and connections to remote repositories such as Dropbox, Google Drive, OneDrive, etc. and the current activity of browsers, like webmail pages, social networks, etc.

At this time, the possibility of maintaining or disconnecting the network connections must be assessed, isolating the equipment.

a) If the device is switched on

Evaluation on-site (Triage). As a continuation of the preservation process and in cases where a specific data set is being sought or the existence of certain information must be established immediately (due to legal or procedural requirements), a direct examination of the equipment can be carried out in the presence of the interested party and the witnesses. Forensic logical copies of the data of interest can be performed. This procedure is common in cases of child sexual abuse in certain jurisdictions, however, from a technical point of view and good practices, certain nuances should be considered.

The less invasive procedure will be used. Just as we try to preserve a device as much as possible so that other types of traces can be obtained (DNA, fingerprints, etc.) in the same way it is convenient not to compromise the original data for the subsequent analysis performed by experts if needed.

If you have to use applications, they must be reliable and if possible, be specifically designed for this function and validated by the competent laboratory for the environment that is presented to us.

Procedure of "Live data forensics" or live analysis. The purpose is to obtain the maximum information from the equipment before it is turned off, with minimal necessary alteration of the original, including those volatile elements of the equipment that are of interest to the investigation to be analyzed later, such as RAM.

It is necessary in devices that contain encrypted volumes or disks, but which are mounted at the time of the intervention, as in the case of systems with BitLocker, FileVault, VeraCrypt, TrueCrypt, BestCrypt or PGP Disk or similar solutions. With this procedure, we will obtain the decrypted data without having to resort to the password, without prejudice to obtaining it through the analysis of other elements.

A similar case is hardware encryption using Trusted Platform Module chips (TPM) or through keys stored in external devices (USB devices), in which this procedure is performed to extract the decrypted data or it would be necessary to have the entire original system mounted to get that information.

In case of not being able to procure an expert's support, it is better to turn off the equipment in the manner mentioned in the following point to avoid destroying the original electronic content or contaminating it by risking its probative value.

Power off procedure. Once the live process part is completed, we will proceed to power off the computer. The best way to do this will depend on the type of device and its operating system. Conventionally shutting down the equipment may cause us to lose information, however, on other occasions, it will be necessary to perform that conventional shutdown to avoid losing that information.

Operating systems whose processing involves performing a sudden power off procedure, execute a series of steps to shut down properly. These process sequences imply the loss of crucial information for the analysis phase.

Unconventional shutdowns that involve the removal of the power supply cable must be done by removing the cable from the device, and not from the wall socket since an Uninterruptible Power Supply System (UPS) can be located between the wall connection and the device connection.

b) If the device is switched off

Forensic copies or direct seizure of the equipment will be obtained.

It makes no sense to compromise the integrity of original evidence of a computer that is shut down by turning it on. In case of urgency or in need of immediate location of information, the device is analyzed in read-only mode through a blocker so that it remains unchanged.

Once the scene and situation of the computer have been documented and it is verified that it is turned off, we will remove any power supply connected to the equipment to avoid unexpected electric shocks. Therefore, the power supply cable will be removed from the device, never from the wall.

Do not forget to take note of the connected elements using the sketch or device file.

The box will be disassembled to locate the hard drives. They will be labelled according to the agreed system and processed using the appropriate means.

It must be considered in the possibility of finding **disks** configured in RAID. In case of doubts, the equipment must be seized together with the hardware to facilitate its subsequent reconstruction, without removing the disks from the device.

You should check if there is any disc inside the CD-DVD readers. For this, it is not necessary to turn on the equipment; it is sufficient to operate with a clip in the mechanical unlocking hole.

General rules explained before will also be considered:

- After documenting the status and situation in which the equipment is found, the entire device is sealed. In this way, we ensure that they contain all the elements that can store information.
- Disassembling the equipment is not always straightforward. Do not do it on-site if you are not familiar and have the proper tools.
- The availability of the original hardware in the laboratory can be very useful. For example, if the computer has some kind of special elements, such as a RAID disk controller, TPM encryption chip or any other particular element that may be necessary for the reconstruction of the information. It can also make it possible to perform a live boot of the equipment in the laboratory, for example, to study the presence and behaviour of some type of malware infection.

- In case of simple or standardized equipment, it will not be necessary to seize the complete equipment and it will be enough to seize the data storage media, since there will not be compatibility issues.
- As a general rule, those media that do not provide research value are not seized. In principle, peripherals, monitors, mice, keyboards and their cables are not necessary, unless they do not correspond to the usual ones for connection types, to be proprietary models of a brand for example or, because they are already obsolete and difficult to find today. So, they can be useful in the analysis phases.
- Most user-level printers do not contain useful information. However, they can have limited memory that can be analyzed in the laboratory in exceptional cases.

5.4. Laptops

The same process as for desktop will be applied with some specificities.

When seizing a laptop, consider using its own bag, including charger, cables and accessories. Once closed, it will be sealed using a system that secures the entire assembly. To turn off the laptop, first remove the battery (if possible) and then remove the power cable.

Current laptops, especially "notebook" types, have batteries and hard drives integrated into the computer so it is not always easy or possible to remove them. We can find laptops with NVMe/SSD type disks integrated into the mainboard, in which it will not be possible to obtain a forensic copy by using methods explained in the previous section. Many of these computers require the use of special tools, and to avoid damaging them, responders should be familiar with the disassembly procedures.

One of the solutions is to boot the computer from a bootable media with its own forensic operating system, either from CD-DVD or USB. Once the operating system is booted using volatile memory, various utilities can be used to carry out evaluation work, triage or acquisition of evidence.

There are numerous products both commercial and from free/open source software:

- CAINE (https://www.caine-live.net/)
- DEFT Linux (http://www.deftlinux.net)
- ASR data SMART Linux (http://asrdata.com/forensic-software/smartlinux/)
- KALI Linux (https://www.kali.org/downloads/)

When one of these systems is used, the practitioner has to keep in mind that the original evidence should not be altered. Therefore, use products that you are familiar with and have been verified to protect the integrity of the original devices. The tools and systems mentioned above are not endorsed or promoted by INTERPOL; for further information in this respect, please review the disclaimer on page 1 of these guidelines.

5.5. Storage media (memory cards, flash drives, external hard drives, optical discs, etc.)

There is a huge variety of storage media based on flash memories. They are becoming smaller in physical size but nevertheless with a greater data storage capacity. We can find memories of these types camouflaged or integrated into objects of the most varied shapes, so the specialist who identifies these elements has to be familiar with the different presentations.

With the emergence of other data storage media, optical discs are currently falling into disuse. However, they are still an element to consider. We may find the discs grouped in batches or tubs of discs.

The applications are endless. We can see external memories in virtually all electronic devices, from video game consoles, phones, cameras to video cameras, etc. But they are also capable of housing fully functional, complete operating systems that facilitate the anonymity of the activity carried out with them.

On the other hand, it is also common to find storage systems on external hard drives, which through USB, Wi-Fi or Ethernet connections are capable of storing large amounts of data.

How to proceed:

a) Forensic image

Although many devices have a tab for write blocking, you should not trust that it works and does it correctly. Therefore, we will use our forensic equipment with the appropriate blocker, either hardware or software.

As for external hard drives, it is possible to extract the internal disk it contains, to perform the copying process directly on that element. This procedure requires the corresponding documentation process, both of the internal disk and of the enclosure that contains it, as previously seen.

Once the evidence is connected to the write-blocker and the latter to the forensic station, a forensic image can be made.

There are precautions to take with these devices. Sometimes it is necessary to locate evidence of the use of external devices on a computer. The use of the above mentioned blockers might not be able to record a device's serial number that is registered in the operating systems; which may be vital to help us link a device with a memory. This number is collected from the memory controller chip and is not recorded in the HD, and therefore in the forensic image we acquire.

b) Evaluation (Triage)

In order to access the contents of a memory device to assess its relevance to the case, it is essential to use blockers as noted above, either by software - provided and validated by reference laboratories - or by blockers by firmware. In case of optical discs, you can proceed with your exam using a CD / DVD reader that does not allow writing.

Through this prior examination, you determine whether or not they may be interesting to the investigation. Keep in mind that we can find a large number of these types of elements during the search warrant and it is not effective to copy all the material without previously evaluating it (unless there is any requirement to the contrary in the laws or procedures of your jurisdiction).

In case of seizure of optical discs, the same container in which they are kept can be used, ensuring that it is closed and placed in a sealed bag after being identified by the evidence number. If they appear individually, they are placed in a plastic case that physically protects them where the identification of the evidence is incorporated, sealing them in an evidence collection bag. It is not advised to use adhesives directly on the discs. It can cause reading errors when decompensated or physically damage them when removing the adhesives. Permanent markers can be used to identify them. It is not advisable to group them with rubber bands or flanges since they damage the ends of the discs and can leave them unusable.

Figure 10: Digital cameras

5.6. Other devices (Digital cameras, GPS navigation systems, Dash Cameras, etc.)

Data sources in these devices include:

a) External storage memory: to work with any other external storage device.

b) Internal memory: a large part of the devices also have an integrated memory, usually of limited capacity, but which allows data to be stored and must be checked.

The proposed procedure is as follows:

- Once the device is located, a picture in situ is taken.
- The camera is documented with its general data by assigning an evidence number. The serial number is important.
- It is checked if it has an external storage media; if so, it is extracted and documented.
- A forensic image of the card is acquired.
- The camera should be turned on (without a card) and the internal memory should be checked.

If there is content it can be extracted:

- Through the connection cable of the device to the PC, making an image. Not all devices have that possibility.
- Inserting a new card and copying the data to the latter, so that we get a logical copy.
- If the other options are not possible you can take photographs of the content trying to show the interesting data related to the investigation.
- It is checked in the camera settings: date, time and time zone.

All elements are sealed together and marked as processed.

If the device is not going to be processed and simply seized, proceed as follows:

- Document the equipment: photography, general data and situation of the finding. If possible, locate discs with software and PC connection cables.

Pack everything, if possible, using the original boxes, in an identified seal bag and with the number of evidence.

5.7. IoT devices

In addition to the traditional IT devices described above, in recent years several devices have been defined as "IoT" or the Internet of Things. These devices can be very different from each other in terms

of functionality, such as smartwatches, smart TVs, video surveillance devices, and so on. Below we will see some examples of the most popular devices that could be found in use by our suspect.

Figure 11: Smart watches

5.7.1. Smartwatches

A smartwatch contains several functionalities, allowing you to do many things you normally do with your phone. In fact, it is a peripheral; an extension of the screen of your smartphone that you have in your pocket. The smartwatch could be on the suspect and they are usually discreet: they do not emit sounds but vibrate gently and they can be connected to an iPhone or Android, so you must be careful when looking for them. There are many different Smartwatches on the market; the most common ones are Apple Watch, Xiaomi, Sony Smartwatch, Honor and Samsung Gear.

Depending on the case, they may contain useful information for investigators, but please keep in mind that these devices usually have very limited storage capacity, mostly related to contacts in the phone book, SMS, information on sports habits, etc.

Usually, they are equipped with Bluetooth connection but some of them can be equipped with a USB port, so the investigator can usually acquire the content through the usual equipment, almost the same as on any Android smartphone/tablet would be.

If you intend to seize a smartwatch, it would be preferable to follow the same indications already provided in the smartphone section.

Figure 12: A Smart TV.

5.7.2. Smart TV

It is becoming popular to find Smart TVs with the capability to connect to the internet, run apps or play games. Some are based on Android while some others are based on proprietary operating

systems. The exact functionality provided depends on the make, model, peripherals attached or apps installed.

From the perspective of a digital-first responder, extracting the information from these devices is a challenge as every extraction would be different depending on the factors listed before as well as the current version of the operating system.

Most of the Smart TVs present vulnerabilities that can be exploited. Possible extraction opportunities imply a modification of firmware, browser attacks, network attacks, use of malicious apps or chip off.

However, most of these extraction processes are not straightforward and require sophisticated equipment (especially for chip-off) or complex network structures that are incompatible with first responders' activity. Improper processes can "brick the device" and make further attempts impossible to extract information.

As a general rule the **process** will include the following steps:

- Review connections to find connected USBs, HDMI or network connections.
- Check with the manufacturer if the model has a wireless capability (if the device is not connected in any way it might be dismissed).
- Verify if the system is powered off or on standby.
- Use the user interface to explore the device configuration, create a visual record of the investigator's actions, preferable with video records.
- Try to minimize the interaction by reading the TV manual before testing.
- Secure packing including remote and power cable.

Possible evidence to be found during the search and seizure:

- Connected devices (for screen mirroring, synchronization).
- Browsing history.
- Users of the installed applications (Facebook, Skype, Twitter, Netflix, Amazon…). However, passwords will not be easy to recover at this stage and might require further processes at the Digital Forensic Lab.

Figure 13: Devices such as Amazon's Echo, Apple's HomePod are examples of Smart Speakers.

5.7.3. Home kits/Smart speakers

Home kits allow users to communicate with and control connected accessories in their home simply using an app. With the Home Kit framework, you can provide a way to configure accessories and create actions to control them.

HomePod is an audio device produced by Apple that adapts to its location and delivers high-fidelity audio wherever it is playing. Together with Apple Music and Siri, it creates a way to interact with music at home.

Possible evidence to be found during the search and seizure:

- They usually contain a very limited amount of data. It is advisable to seize them only if you have reasons to believe they contain useful data for your case. Just disconnect them from the power grid and seize them the way you found them. Document everything, take pictures of the device, label and pack it.

Figure 14: Internet Protocol Cameras send image data over an IP network

5.7.4. IP and concealed cameras

IP cameras or concealed cameras are typically used for small scale monitoring and, unlike CCTV, these devices might not have local storage capabilities. Most of the IP cameras available only need a Wi-Fi connection to work. The user can watch the camera live stream from any device connected to the Internet. It also might be possible, if the user subscribed for a cloud-stored package, to watch recorded footage (usually in a loop of the previous days).

Despite that, first responders must assure that such devices do not have a memory card (usually a micro-SD) for local storage.

First responders must also be aware that cameras can be concealed almost everywhere: from teddy bears to buttons in a jacket.

Possible evidence to be found during the search and seizure:

- For cloud-stored data, it is important to obtain the online access credentials (usually username and password or QR code). Those credentials might be stored in the camera itself or in computers/smartphones found with the suspect.
- For local-stored data, usually, only the memory card needs to be seized. However, due to the possibility of encryption, proprietary file systems or non-documented settings, it is advisable to seize the whole equipment.
- For live-only data (the camera only streams live footage - not cloud or local storage), it is advisable to seize it only if you have reasons to believe that it contains useful data for your case.
- For video forensic analysis, comparing previous footage with the camera found, the device must always be seized.

When the seizure is necessary, just disconnect it, document everything, take pictures of the device, label and pack it.

Figure 15: Nintendo, Sony's PS Series, and Microsoft's XBOX are examples of gaming consoles with smart functions.

5.8. Gaming consoles

The complexity of video game consoles is increasing in every new model. Most of them contain an internal hard drive that can be extracted and imaged following forensic procedures explained before. However, the heavy usage of encryption and use of special file types makes it extremely difficult to discern any information in a later analysis. On top of that, a good amount of the information generated would be stored in the gaming social platforms and never stored in the hard drive.

Finally, it is important to consider that users from other locations might easily alter the information contained within these devices and remove potential evidence.

Possible evidence to be found during the search and seizure:

- Define periods on which the video console was used for gaming.
- Browsing history.
- Illicit files stored on Video console media.
- Application passwords.
- User Accounts.

Figure 16: Drones, also known as UAVs (Unmanned Aerial Vehicles)

5.9. Drones

Drones - also referred as unmanned aerial vehicle (UAV), unmanned aerial system (UAS), small unmanned aerial system (sUAS) or remotely piloted aircraft system (RPAS) - can be used for a variety of operations, ranging from aerial photography and videos to transporting goods from one place to another. Therefore, the aim of carrying out digital forensics on drones and associated equipment is to identify flight paths, user data, and associated pictures and videos contained within the devices that will assist in understanding the drone and its usage.

A drone usually consists of the following two types of components:

- **Physical Components**: The physical components which make up the body and flight mechanisms can be broken down into the following categories:

  - **Drone Body**: The core fuselage of the UAV used to house all other components.
  - **Flight Controller**: Used to control flight. This device will stabilize the drone and generally accept navigation input from a radio control device. In more sophisticated systems the flight controller can both be controlled remotely in real-time and be pre-programmed for autonomous flight.
  - **Motors, Rotors/Propellers/Wings, and Speed Controllers**: These component parts combined provide the lift and propulsion for the UAV. Different designs exist, for example, specializing in increased speed or flight duration.
  - **Protective Casing**: This protection securely encases the motors and propellers (the most vulnerable component of any drone) to prevent collision and loss of control and subsequent damage to the system.
  - **GPS Receiver**: Not essential in all drones, but common in the leading solutions. This component is used to effectively manage UAV position, return to home functionally, and autonomous flight routes.
  - **Radio Receiver**: Used to receive control input signals received/gathered from the ground-based transmitter.
  - **Transmitter**: Transmits manual input from the operator on the ground to the drone.
  - **LED Lights**: Some drones come equipped with LED lights (usually green and red) which can be used to aid the pilot of the orientation of the drone, and help other airspace users to identify the drone.

- **Software**: All drones include an application or software that is used to control the system when it is operational. There is now a huge selection of open-source flight control and ground control applications available online that can be freely downloaded and easily modified to perform any number of tasks. The majority of drones come with companion mobile

applications to either pilot the drone or view the camera feed and location of the drone overlaid on a map.

Drones/controllers are usually presented with two distinct media storage types that require separate handling techniques, as in the following summary:

- **Memory Cards**: These can be examined as a computer hard disk. Both logical and physical extraction can be conducted on these cards, as long as the forensic tools support this feature. The examiner has to access the card, extract the data, and then put it back into the device before switching it on. Some devices store data in the memory card, and if it detects that the card is not available, it could cause data loss from the drone/controller. If time and resources allow, a bit-to-bit clone of the memory card should be created and that clone inserted into the handset.
- **Internal Memory**: This requires drone/mobile compatible manufacturer/forensic tools. Some devices are supported by forensic tools for physical extraction. The forensic tools will boot the device in a particular way and conduct physical extraction without making any changes or alterations to the user data on the device.

As a general rule the technical process will include the following steps:

- If on, take pictures of the controller's display then turn off the drone and its components.
- Isolate the drone from GPS satellites and other devices to ensure that GPS/Wi-Fi/Network signals are not picked up.
- Identify the make and model of the drone.
- Search the drone for any external storage media, i.e. SD Cards.
- Photograph and label the status of the drone and its components.
- Securely pack all of the components.

Possible evidence to be found during the search and seizure:

- Update history
- Diagnostic logs
- Registered email accounts
- Paired devices
- Multimedia files
- Flight/telematics logs
- Drone media thumbnail caches
- Map artefacts such as geo-coordinates, waypoints, and home locations
- Drone specific software such as manufacturers' drone management software
- Emails that show new registration of drones or update notifications from the manufacturer
- CSV files that contain telematics, diagnostics or GPS coordinates.

For a more detailed information in this area, please refer to "INTERPOL Framework for Responding to a Drone Incident – For First Responders and Digital Forensics Practitioners."

Figure 17: CCTV Cameras being used for surveillance purposes.

5.10. CCTV

Closed-circuit television (CCTV), also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted, though it may employ point-to-point (P2P), point-to-multipoint (P2MP), or mesh wired or wireless links. Though almost all video cameras fit this definition, the term is most often applied to those used for surveillance in areas that may need monitoring such as banks, stores, and other areas where security is needed.

CCTV security system consists of different components. These include:

- **CCTV Camera**: used for video surveillance and acts as the input device to the system CCTV Monitor. This device receives signals and reproduces pictures or videos captured by the CCTV camera.
- **Main Power Supply**: the primary electrical supply unit.
- **Backup Power Supply** (optional): backup power supply comes in handy in case of a power outage
- **Cables**: these are used to connect several CCTV cameras to one video recorder, video switcher for CCTV monitor, also modern CCTV systems may utilize Wi-Fi networks to transmit the pictures to a central point.
- **Video Recorder**: transforms and records signals sent by a CCTV camera in the form of a video that is generally stored on a hard drive and may be deleted automatically depending on the device settings.
- **Video Switcher**: switches the video mode between different CCTV cameras.

As a general rule the technical **process** will include the following steps:

- Check time and date set on the video recorder and report if they differ from the current ones

- Take pictures of the screen(s)
- Shut the recorder down to avoid data to be overwritten
- Disconnect cables
- Identify make and model
- Photograph and label all the components
- Securely pack everything.

Usually, CCTV system components are proprietary, therefore it is advised to seize every part of the CCTV system, in order to avoid issues during the analysis phase.

Remote monitoring may also be applied to CCTV systems and may also have alert systems in place to warn the user if the systems sense movement. This should be considered when approaching a crime scene as the suspect may be alerted/notified if police approach a scene that is being monitored by CCTV camera systems such as RING etc. Therefore, when examining the CCTV system you should also consider the registered users who have remote access to the CCTV system.

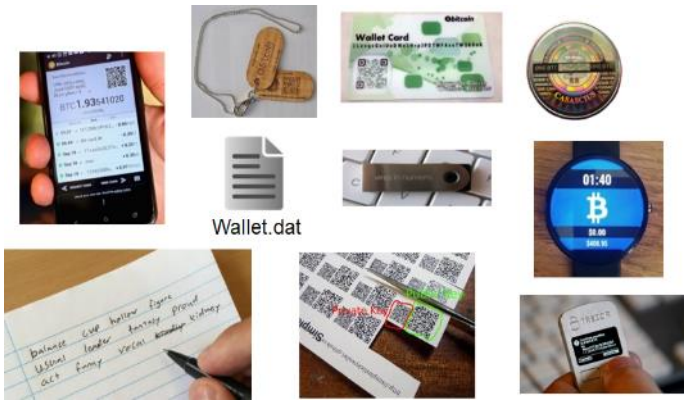

Figure 18: Virtual asset devices, used for storing information about cryptocurrencies and other virtual currencies.

5.11. Virtual assets devices

First responders need to be aware of the different ways to access, store and transfer virtual assets. To allow the proper seizure of a cryptocurrency, and if permitted by the laws of the jurisdiction and the terms of the relevant judicial or other authorization, law enforcement needs to transfer the funds from the suspect's wallet to an official and secured wallet controlled by the seizing agency.

Furthermore, first responders need to bear in mind that an accomplice might have a copy of the information needed to transfer the funds to a wallet not controlled by the law enforcement agency. Thus, as soon as the cryptocurrencies are securely transferred, the better.

Cryptocurrency wallets come in different shapes and forms: files in a computer/phone, hardware devices, QR codes or even a sequence of words written in a piece of paper or memorized by the suspect. During a police search, first responders might face:

- **Desktop wallets**: Bitcoin Core, Armory, Electrum, Wasabi, Bither, etc.
- **Mobile wallets**: Mycelium, Edge, BRD, Trust, etc.
- **Online wallets**: BitGo, BTC.com, Coin.Space, Blockchain.com, etc.
- **Hardware wallets**: BitBox, Coldcard, KeepKey, Ledger, Trezor, etc.
- **Paper wallets**: addresses generated by bitaddress.org, segwitaddress.org, etc.

- **Brain wallets**: seed (list of words which store all the information needed to restore the wallet).

Regardless of the wallet type, the crucial information that first responders need to access is the **unencrypted Private Key**, which will allow the transactions to be properly signed and the funds transferred.

In most cases, however, the Private Key is protected, or it might not be stored locally. Thus, first responders should also seek for:

- **Passwords:** used to encrypt the private key
- **PINs**: to access hardware wallets or phones
- **Credentials**: username and password for online wallets
- **QR codes:** that can store the full private key
- **Seeds:** the sequence of words (typically 24 or more) used to recreate the private key.

For the most popular cryptocurrency[3], Bitcoin, private keys are 256-bit numbers that can be represented in many different ways. Wallet Import Format (WIF) is the most common type and the keys start with '**5**', '**K**' or '**L**'. An encrypted private key starts with '**6P**'.

For example, the same Private Key can be represented as:

- *Base58 Wallet Import Format (51 characters base58, starts with a '5'):* `5JoBSup7GzCohqzfCdU3FQmuQM8KLCu3TTKiTAtbzmWywJfzTni`
- *Base58 Wallet Import Format Compressed (52 characters base58, starts with a 'K' or 'L'):* `L1Yq7N6vhZV79HFVcKxLvbwCJ3qHumWhqmBbxWemTyVLJHfaUjTc`
- *Private Key BIP38 Encrypted Format (58 characters base58, starts with '6P') - password: 'asdfg':* `6PYLTEjqt2huN6zgG8Gc2Sdifh33tcDLoJMXXqdK52YrQWXa3fD8az9Za7`

First responders must also be able to identify a **Public Key** (or simply **Address**), which is the possible destination of a transfer or payment. For example, Bitcoins Addresses can start with '**1**', '**3**' or '**bc1**':

- P2PKH Format: `1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2`
- P2SH Format: `3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy`
- Bech32 Format: `bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq`

Some examples of what first responders might find during a search warrant:

Figure 19: Paper wallets

[3] Other examples of cryptocurrencies include: Ethereum, XRP, Bitcoin Cash, Litecoin, Monero and Zcash.

Figure 20: Hardware wallets, used to store information about crypto assets.

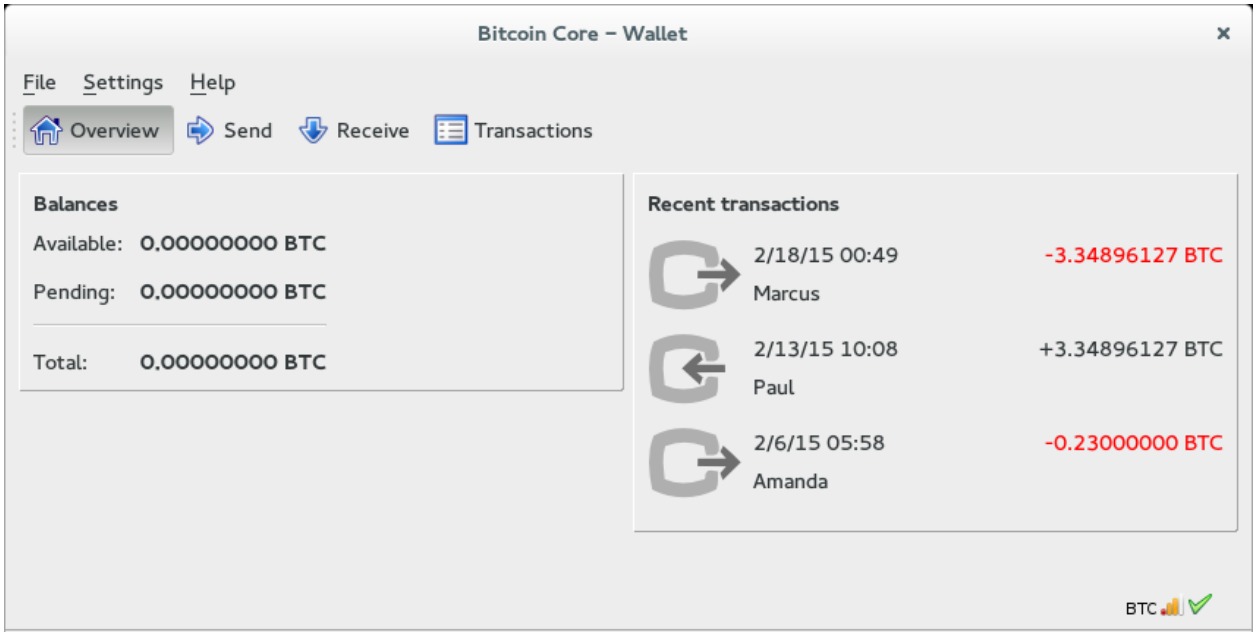

Figure 21: Example of a desktop wallet.

Desktop wallets

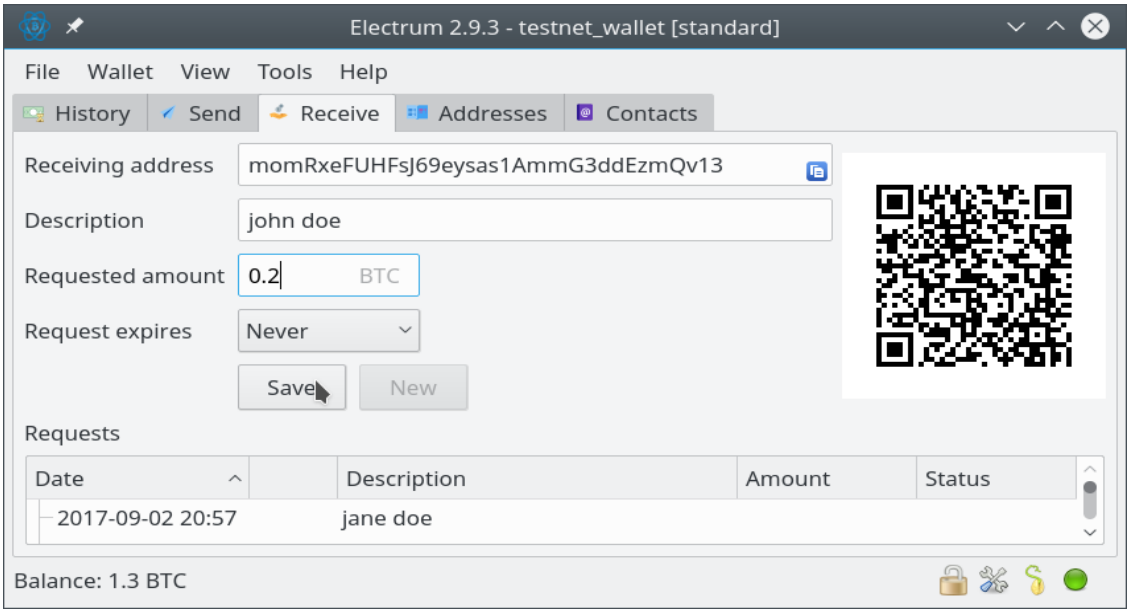

Figure 22: Electrum, a desktop wallet

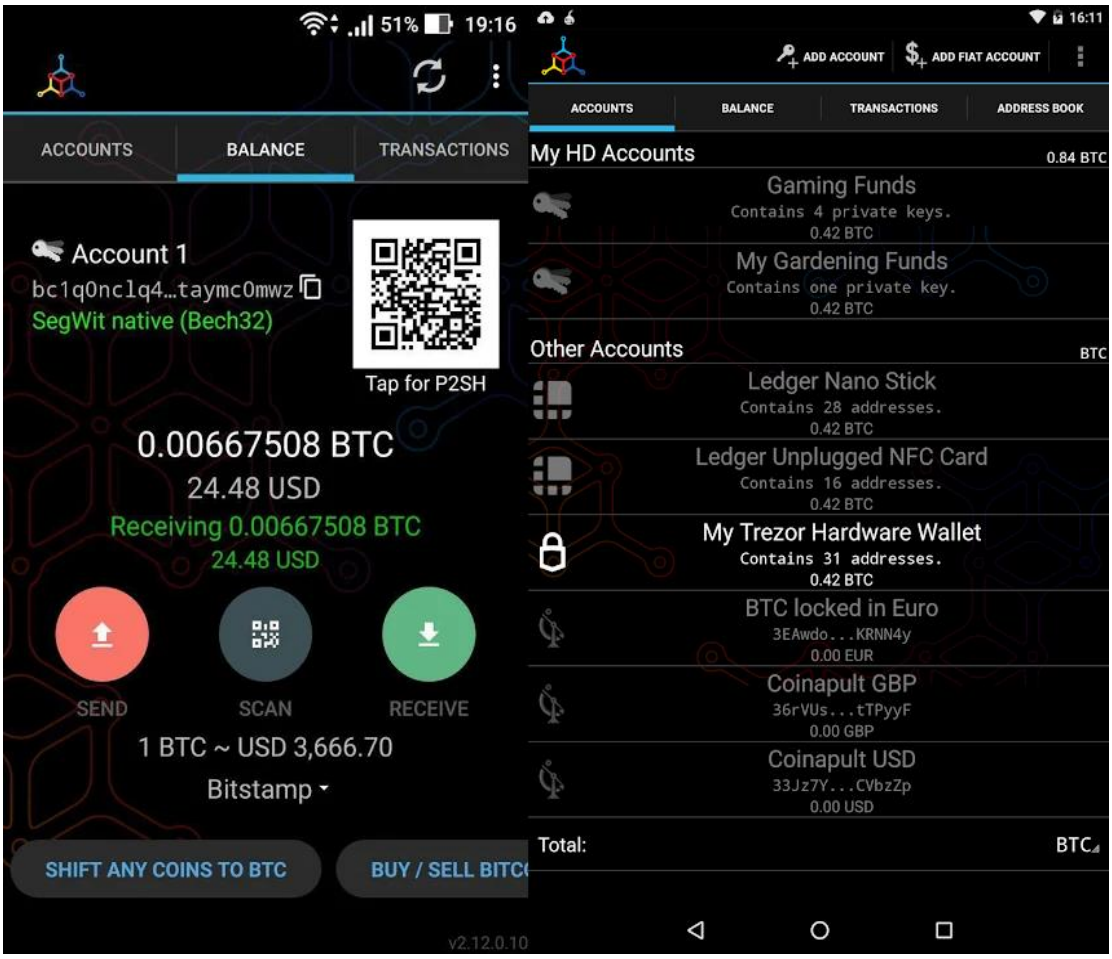

Figure 23: Example of a mobile wallet used for storing cryptocurrency information.

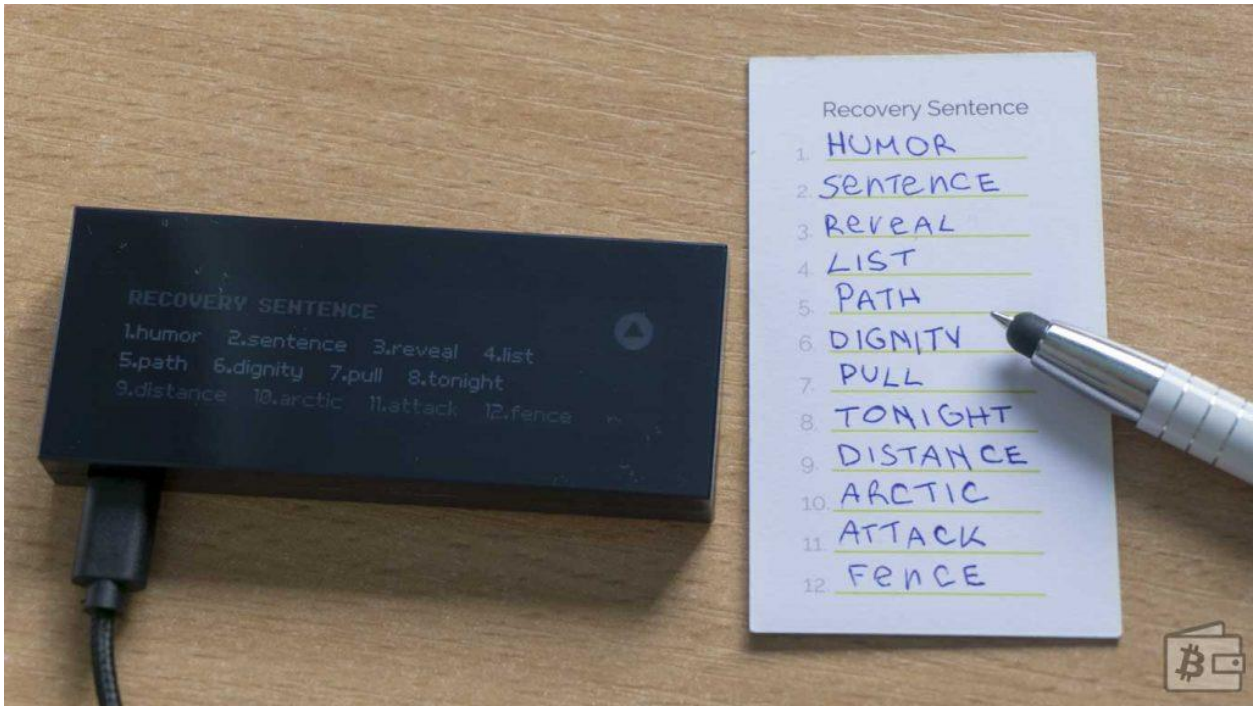

Figure 24: Brain wallets (seed)

Figure 25: Brain wallets (seed)

An important consideration that must be taken into account, depending on your legal system, is what to do with the transferred virtual asset: exchange into fiat money as soon as possible or keep it in the official wallet until there is a final sentence.

Finally, do not forget to document all the steps taken, including the transaction fees, the value of the bitcoin in local currency and exchanges eventually used. Also, it can be useful to add screenshots of the transaction (using for example www.walletexplorer.com).

For further details, please refer to your local legislation. Guidelines, like the **INTERPOL Guidelines on Darknet and Cryptocurrencies for Counter-Terrorism Practitioners** may also be useful to refer for further background on virtual assets.

5.12 Automotive Vehicles

Modern vehicles have two systems that could contain data that may be pertinent to an investigation. There are:

Telematics Network – This includes various Electronic Control Units (ECU) that monitor the vehicles state and apply user input to move the vehicle such as acceleration, braking and steering. These ECUs contain vehicle event data that may assist an investigation in locating historical routes the car has taken or in the way it is driven.

Infotainment Systems – These systems provide multimedia entertainment such as music, radio broadcasts and streamed or locally stored videos to the vehicle occupants as well as allow a connected experience to the internet or a connected phone. If a user connects a phone to the system, then data from the phone such as address book, SMS/instant messages and calls will be stored within the infotainment system. This information may be recovered when the device connected to the system and to verify any event data recorded from the connected device.

Infotainment and telematics systems present unique challenges to law enforcement due to differences in hardware designs and manufacturers, limited information on the underlying software and proprietary operating systems, encrypted media associated with Digital Rights Management (DRM), and rapid changes in technology. Acquisition options may be limited by hardware and software available to facilitate data extraction. A visual examination of an active screen/system may be required if other techniques are unsuccessful. Examiners should be aware that the vehicle's digital systems are like any other digital device/system and therefore, must be handled appropriately to prevent data destruction. A modern-day vehicle will contain multiple computers and/or networks and consequently the examiner should take reasonable measures to isolate the car from wireless networks (Wi-Fi, cellular, Bluetooth, etc.).

ECUs always draw power from a vehicle's battery, even while the ignition switch is in the off position. Many ECUs, like the infotainment and telematics systems, utilize critical components such as an unlock event or doors opening/closing as cues to enter low-power mode or start the power-up procedure. Minimizing the number and duration of power cycles helps preserve volatile data stored on ECUs. Processing a vehicle for physical evidence may cause additional power cycles resulting in the loss of relevant volatile data from the ECUs. To mitigate this risk, document the on-screen data and properly shut down the vehicle to allow the ECUs to correctly power down before processing physical evidence (latent prints, DNA, GSR, etc.)

The following are general guidelines for properly shutting down a vehicle to preserve evidence:

- Document the date and time these steps are performed. Turn off the vehicle and exit with all key fobs.
- Close all doors · Open the driver's door for 5 secs.
- Close the driver's door and wait approximately 2 minutes.
- Disconnect vehicle power (e.g. disconnect the battery or place the vehicle into transport mode).

To verify that the car was completely shut down, ensure the center stack of the vehicle, as well as the instrument cluster and interior/exterior lights, have been off for 30-45 seconds after all doors were closed. Wait 60 seconds.

Evidence Handling

Review legal authority before handling and collecting evidence, ensuring any restrictions are noted. If necessary, during the collection phase, obtain additional authorization for evidence outside the original scope. Infotainment and telematics systems may consist of separate ECUs located in different locations within a vehicle or maybe a single integrated ECU that has dual functionality. General guidelines for working with vehicles associated with an investigation include:

- Handle evidence according to agency policy and maintain a chain of custody.
- Preserve the state of the ECUs before the physical processing of a vehicle.
- If physical forensic processing of a car (DNA, latent prints, etc.) is required, discuss these requirements and the order in which they should be performed with the investigator and crime lab personnel to avoid inadvertent destruction of physical and digital forensic evidence.
- Biological contaminants and physical destruction provide unique challenges to the recovery of data. Use universal precautions to protect the health and safety of the examiner.
- Infotainment and/or telematics systems may have active external connections (e.g. cellular, Wi-Fi, or Bluetooth). Isolate the vehicle from connecting to external networks when possible; e.g., disconnect antennas or cellular modems, remove SIM cards, etc.

Data that can be obtained from a vehicle may include the following:

- **Vehicle System Information:** Serial Number, Part Number, VIN Number, Build Number.
- **Installed Application Data:** Weather, Traffic, Facebook, Twitter, and YouTube.
- **Connected Devices:** Phones, Media Players USB devices, SD Cards, Wireless access points.
- **Navigation Data:** Tracklogs and track points, saved locations, previous destinations, active and inactive routes.
- **Device Information:** Device IDs, calls, contacts, SMS, Audio, Video, Images.
- **Vehicle Events:** Doors opening and closing, lights on/off, Bluetooth/Wi-Fi/USB connections, GPS time syncs. Odometer readings and telematics information such as speed, brake and angle of steering data.

Every car is different, and the ECUs may record various events and store different data depending on the configuration of the vehicle when assembled in the factory. The examiner or first responder should verify the vehicle's configuration by obtaining a build sheet which is referenced by the Vehicle Identification Number (VIN) before starting any practical forensics on the vehicle. In addition, if the examiner can obtain an IMEI from an ECU, they may be able to carry out investigations with the mobile

service provider to locate historical locations where the vehicle has been. They should also ensure they try to capture associated evidence such as CCTV, automatic number plate recognition logs etc. from places that the car has been in to ensure that the evidence corroborated. [4]

5.13 Shipborne Equipment

All vessels are different, even between sister-ships, as vessel equipment is generally dependent on the intended activity of the vessel, and more technically, its classification by the registration flag. Further, the vessel operator or Captain might also change the capabilities of the vessel once received, in line with what they think is the best and most efficient way to operate the vessel. For a more detailed information in this area, please refer to "*INTERPOL Guidelines for First Responders - Digital Forensics on Shipborne Equipment*" developed in cooperation with the Global Fisheries Enforcement (Organized and Emerging Crime directorate).

The level and type of shipborne equipment fitted on each vessel is therefore linked to this classification and/or operator perspectives. Investigators and first responders can therefore expect very different levels of equipment from one vessel to another. In fact, the level of equipment on board a vessel can range from a basic configuration of a magnetic compass and a Very High Frequency VHF radio (VHF), to a high-tech configuration of cutting-edge technological equipment - including satellite communication technologies. In some cases, the bridges of the latter vessels share more resemblance with the cockpit of an airplane rather than to a vessel's wheelhouse.

Due to the high diversity of Shipborne Equipment, first responders should have knowledge of the vessel's onboard equipment including brands, series, models and serial numbers. This is crucial and will give them the ability to expect what kind of evidence they might find in the ship and equipped with all needed tools (cables, sockets, plugs, etc.). Moreover, learning about ship equipment will save time by giving hints about the location of each device and which one is useful for the investigation. In the following figure, examples of Shipborne Equipment that include data with their locations.

[4] This process is replicated from the Scientific Working Group on Digital Evidence (SWGDE) Best Practices for Vehicle Infotainment and Telematics System v2 (dated 2016-06-23). It is the readers' responsibility to ensure they have the most current version of the document. Please see swgde.org/documents/published for more information. Please also refer to the references section at the end of this report for the SWGDE disclaimer and redistribution policy.

Equipment	Location	Type of data
AIS Transponders	Bridge	
Echo Sounder	Bridge	
Electronic Chart Display and Information System (ECDIS)	Bridge, Captain quarters, Nav Room	
Emergency Positioning Indicator Radio Beacon (EPIRB)	Bridge, Bridge Wings, Flying bridge	
GMDSS System	Bridge	
GPS	Bridge	
Long Range Tracking and Identification System (LRIT)	Bridge	
Vessel Monitoring System (VMS)	Bridge, Fly Bridge	
RADAR	Bridge	
Digital Selective Calling (DSC)	Bridge, captain cabin, navigation room	
Sat-phone	Bridge, captain cabin, navigation room	

Figure 26: Examples of Shipborne equipment with data and their location

REFERENCES

SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition

SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition Version: 1.2 (September 17, 2020). This document includes a cover page with the SWGDE disclaimer.

Disclaimer:

As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.

2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.

3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

SWGDE Best Practices for Vehicle Infotainment and Telematics Systems

SWGDE Best Practices for Vehicle Infotainment and Telematics Systems Version: 2.0 (June 23, 2016). This document includes a cover page with the SWGDE disclaimer.

Disclaimer:

As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.

2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.

3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

INTERPOL

ABOUT INTERPOL

INTERPOL is the world's largest international police organization. Our role is to assist law enforcement agencies in our 194 member countries to combat all forms of transnational crime. We work to help police across the world meet the growing challenges of crime in the 21st century by providing a high-tech infrastructure of technical and operational support. Our services include targeted training, expert investigative support, specialized databases and secure police communications channels.

OUR VISION:

"CONNECTING POLICE FOR A SAFER WORLD"

Our vision is that of a world where each and every law enforcement professional will be able through INTERPOL to securely communicate, share and access vital police information whenever and wherever needed, ensuring the safety of the world's citizens. We constantly provide and promote innovative and cutting-edge solutions to global challenges in policing and security.