CyberSouth
Cooperation on cybercrime
in the Southern Neighbourhood

Version 12 September 2019

Standard Operating Procedures for the collection, analysis and presentation of electronic evidence

Prepared by
Cybercrime Programme Office
of the Council of Europe (C-PROC)

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Acknowledgement

The present Standard Operating Procedures were prepared under the project CyberSouth on Cooperation on Cybercrime in the Southern Neighbourhood countries. The work on this document was coordinated by C-PROC and contributions were received from experts of the General Inspectorate of Romanian Police and the Directorate for Investigating Organised Crime and Terrorism of the General Prosecutor's Office of Romania.

Victor Volzow (Germany) and Andrea Bradley (United Kingdom) provided further inputs regarding the structure and content of this document.

Contact

Cybercrime Division
Council of Europe Directorate General Human Rights and Rule of Law
F-67075 Strasbourg Cedex (France)
Email cybercrime@coe.int

Disclaimer

CONTENTS

1 The intention of this tool

A key area of capacity building projects of the Council of Europe on cybercrime – including joint projects with the European Union – is the development of capacities in relation to electronic or digital evidence.[1]

Criminal justice authorities – police officers, prosecutors or judges – may become involved in the collection, analysis or decisions related to electronic evidence at some stage of a criminal investigation, prosecution or trial.

The Council of Europe has, therefore, developed two tools for use in capacity building activities, that is, the "Electronic Evidence Guide" and the "Basic Guide for the Management and Procedures of a Digital Forensics Laboratory"[2].

Building on the definitions, concepts and detailed explanations of these guides, the present tool on Standard Operating Procedures (SOP) is intended to provide practical technical and tactical guidance on digital evidence.

The three tools collectively provide a coherent understanding of electronic evidence and computer forensics.

These SOP were developed in response to a need expressed by practitioners and serve several purposes:

1. They may serve as a starting point for the development of such procedures for countries or authorities that do not yet have procedures for the collection, analysis and presentation of electronic evidence in place.

2. These SOP may also be applied directly by authorities dealing with electronic evidence. However, authorities will need to ensure that such use is in compliance with domestic rules and procedures.

3. They could also be used as common standard for exchanging electronic evidence in international investigations.

4. Moreover, they may be used in training activities for police officers, prosecutors and judges to enable a better understanding of technical procedures and practical issues involved in collecting and analysing digital evidence.

[1] The terms "electronic" or "digital" evidence are used here synonymously.

[2] Both documents are available on the Octopus Community: https://www.coe.int/en/web/octopus/home

2 The purpose of Standard Operating Procedures

SOP cover procedures to be followed for the onsite retrieval, securing, transport and handling of digital evidence, as well as its analysis and presentation, including situations where evidence is seized from individuals or companies, whether such evidence is made available voluntarily or following a search or another compulsory measure.

They furthermore contain procedures for the live acquisition of data onsite, while the identified computer systems are turned on/running, as accessing them later on might be prevented by passwords or encryption.

Finally, they cover procedures for the copying of data from a computer system or data storage device in cases where backup copies are required or where the physical collection of a computer system is not feasible.

A forensic analysis of a computer system or storage device requires not only the approval of a competent authority but also the observance of technical requirements and well-defined steps to ensure the integrity of the extracted data and their presentation in a way that allows prosecutors and judges to understand and admit them in prosecutions or court cases.

The basic principle[3] to be followed for all digital forensic activities is to ensure the integrity and authenticity of the data held on computer systems, digital devices or other storage devices.

Users of this guide should consult their relevant domestic rules on electronic evidence and evidence in general. These may differ from those presented here in this guide.

3 Collection of computer systems, computer data and digital devices

3.1 Preparation stage

The process of gathering digital evidence has both technical and judicial effects and should be viewed in its entirety, starting from the initial steps of collecting computer systems or storage devices made available voluntarily or obtained through searches of premises.

Gathering as much data as possible on the location to be searched in view of seizing computer systems or storage devices is key and provides relevant investigators with insights that will help them in their work. Whether seizing computer systems, computer data, digital devices and other storage devices, this activity needs to be conducted according to the national legislation in force.

It is vital that investigators or specialists are able to identify and correctly seize potential sources of digital evidence. Examples are:

- computer systems – such as Personal Computers (PCs), laptops, servers or game consoles;

[3] Electronic Evidence Guide (section 1.7)

- storage devices – Optical Discs (CD, DVD, Blu-Ray), removable data storage drives (USB thumb drives, external SSD/HDD) and memory cards;
- mobile devices - mobile (smart) phones, tablets, digital cameras, satellite navigation systems, automotive IT devices;
- network devices - NAS (Network Attached Storage), routers, wireless access points, smart sensors/actors/controls.
- Internet of things devices – e.g. sensors, actors, controller, gateways
- Automotive IT systems – embedded information systems in cars scene. Since sources of digital evidence typically need special handling, technical staff should ensure that appropriate tools and equipment are taken to the scene.[4]

Prior to arriving at a potential search scene, it is important that the investigator obtains as much information about the offence, the suspect and his/her IT skills and the scene as possible. The type of crime investigated may influence preparations prior to arrival at the scene. Since sources of digital evidence typically need special handling, technical staff should ensure that appropriate tools and equipment are taken to the scene.[5]

3.2 Necessary consent/authorisation

The first consideration in planning for any coercive activity is to ascertain the nature and level of legal permission or authorisation required. That authorisation may take a number of forms.

The simplest of these is to **obtain consent from the owner or person holding** the equipment or the data to be seized. Such consent is recommended to be obtained in writing and investigators should ensure that the person giving consent is the rightful owner and fully understands his/her rights as well as the implications and possible consequences. National legislation and guidelines must obviously be adhered to.

Other levels of authorisation will be **prescribed by law**. They will depend on the nature of the investigation. In most cases, judicial orders or warrants will be required.

Absolutely no coercive activity involving the seizure of equipment or the capture of data should be undertaken without obtaining the required level of authorisation.[6]

Whether computer systems, computer data and digital devices are willingly made available or are seized following a search of a home or the premises of a company, the technical rules on their identification, sealing, transport and subsequent analysis are the same.

[4] Electronic Evidence Guide, page 39

[5] Electronic Evidence Guide, page 39

[6] Electronic Evidence Guide, page 34

3.3 Activities at the crime scene

3.3.1 Securing the crime scene and preservation of evidence

When searching home/office premises, to eliminate the risk of discarding/destroying important evidence or of suspects leaving the scene where computer systems, computer data and digital devices are to be seized, **all location access routes need to be secured** prior to the search.

Digital data is highly volatile and thus consideration must be taken about the speed of entry to the scene. It is prudent to prevent the suspect from deleting/wiping/destroying data at the time of entry and steps should be taken to isolate the suspect from any device which may contain digital evidence.

The following activities are recommended to be carried out immediately after entering a location where computer systems, computer data and digital devices are to be seized from:

1. Identify and determine the number of computer systems available on site, their type, whether they are connected to a network and can access the Internet.

2. Forbid access to computer systems/data and digital devices or other electronic equipment as well as to power supply sources, of persons identified at the location where the activity/search is to be conducted.

3. Document the scene, all sources of digital evidence that might be target of seizure and their status and connections.

4. Use protection gloves when handling computer systems, computer data and digital devices in order to avoid damaging latent prints and ensure successful collection of fingerprint/DNA evidence, as applicable.

5. Check the operational status of each of the identified computer systems:

    - if the computer system is shut down, **do not** turn it on; If circumstances require an on-site analysis of the system, it is recommended to start the system by using either a forensic clone of the original disk or a write-protection / write-caching mechanism to maintain the integrity of the original disk.

    - if the computer system is running check if **live data acquisition** (see 3.3.4) is to be conducted or not. After that the computer system may be shut down depending on the operating system:

        - **Windows** OS (XP, Vista, 7, 8, 10) – disconnect the computer system from its source of power – always by removing the power cable from its internal power source, not by using the on/off button or unplugging it from the socket;

- **Windows Server** OS (2000 to 2019) **and Unix/Linux/macOS**, any other server-like operating system – if possible, shut down the computer system using the specific "shutdown" command;

- **Laptop computers**, disconnect the charger and remove the battery, usually placed on the bottom of the laptop. Most often, removal of battery requires resorting to specially designed buttons/latches marked accordingly on the laptop.

Practice has shown that the location searched can provide other data and information to support the subsequent analysis of computer systems, computer data and digital devices. Non-electronic, but **related evidence**, such as: written passwords and other handwritten notes, blank pads of paper with indented writing (but do not shade with graphite pencil), paper wallets for virtual currencies, hardware and software manuals, text or graphical computer printouts, photographs or information about personal interests that may be useful during the investigations.

Particular care should be given to digital devices that enable remote access of information stored on cloud servers or other IT systems, such as virtual assets beyond the reach of future asset seizure/forfeiture proceedings. Such assets can have considerable value. Thus, at the identification stage, one is advised to proceed with live acquisition or to access this information to prevent its loss, consistent with the national procedures in force. The technical rules to be followed in this case are those pertaining to imaging or live data acquisition.

3.3.2 Identification and seizure of electronic evidence

Depending on the case, the authority, the importance of a computer system for critical infrastructure, the role of the owner of the targeted computer system and the effect of the seizure on the work of individuals/companies, the computer systems can be shut down, disconnected from the power network and seized after the number of computer systems available on site has been established and information have been documented about their type, whether they are connected to the network and whether they can access the Internet. Disconnecting them from the network should be done carefully, particularly where the required computer data are stored on a different computer system and are accessible from their initial system or media.

If a large number of computer systems or storage devices are to be seized, one should use automated tools for filtering all seized electronic evidence, passing only the most relevant artefacts for further analysis by digital forensic investigators. Any tools used for this purpose should be fully tested and validated before use. The users of these tools should be appropriately trained in their use and lawfully authorised to use them. Training should incorporate an understanding of relevance of items to be seized and prioritisation to avoid the seizure of unnecessary items. The principle of record keeping should be maintained throughout the process.

All actions taken at the scene should be documented/recorded and this report should remain with the case file.

All items seized should have an exhibit label attached. An exhibit label will contain (as a minimum):

- The exhibit name (usually derived from the initials of the person seizing and a sequential number for each seizure (i.e.: AB01, AB02, etc).
- Description of the device (computer, laptop, phone, etc).
- Identifying marks of the device (make, model, serial number).
- Place of seizure (eg: under desk in kitchen of 123 Any Street, Any Town)
- Time and date of seizure
- Details of person seizing (name or identification number)
- Details of witness of seizure (name or identification number)
- Case number
- Sufficient space for a subsequent record of any other person who takes possession of the exhibit. This will ensure that continuity is maintained, and the exhibit label should remain with the exhibit for the entire period it is in the possession of Law Enforcement.

Servers, desktops and laptops

1. Disconnect all connected peripherals (mouse, keyboard, webcam, speakers, headphones, printer, scanner etc.) after photographing/video recording and/or labelling ports and cables.

2. Determine and document computer system identification elements, such as: type, make, model, serial number, colour, various inscriptions, as well as visible flaws/damage. If damage is identified a written record and photograph of the damage should be recorded, at the time of seizure. This will make it difficult for the suspect to claim, at a later date, that the damage occurred whilst in Police possession.

3. Where laptop computers are concerned, identify and seize the AC adapter together with the corresponding accessories.

4. Package the computer systems in cardboard boxes or paper bags, separately from other assets, valuable items or documentary evidence.

5. Complete an exhibit label and attach to the exhibit.

Mobile devices (mobile phones, tablet devices, modems, etc.)

1. Check the operational status of mobile communication devices:

   - If the mobile communication device is turned off, **do not** turn it on. Check for a SIM card (type, serial number), memory card (miniSD, microSD), as well as the IMEI number.

   - If the mobile communication device is turned on, proceed with identifying the IMEI number by entering the **"*#06#"** code. One should not turn it off when checking the IMEI. Turn the device into flight-mode to minimize unintended alternation of data/logs and to avoid remote locking and deletion of date. If the mobile device is

locked using an unknown code, the device should be isolated, preferable in a Faraday bag.

2. Determine the users for each mobile communication device, the allocated telephone number and the network to which it is connected, if possible.

3. Identify the lock code of the mobile communication device, where applicable.

4. Identify potential PIN/PUK codes for SIM cards. These codes can be found on the original SIM card package.

5. Identify and seize the charger and data cables for each type of mobile device.

6. Package the mobile communication devices in cardboard boxes or paper bags and **not in plastic**[7] materials, separately from other assets, valuable items or documentary evidence.

7. Complete an exhibit label and attach this to the exhibit.

Stand-alone storage devices

Individual storage devices are categorised as follows: internal and external hard disks (HDD, SSD, SSHD), CD, DVD, BluRay, SD-, miniSD-, microSD-type memory card, memory stick, etc.
Special attention should be paid when identifying these, given the small size of certain computer storage media and the fact that they can be concealed in various items of personal use (watches, plastic cards, toys, key chains etc.).

The main rules that should be followed when identifying and seizing such devices include:

1. Determine identification elements, such as: make, model, serial number, storage capacity (MB, GB, TB), colour, various inscriptions as well as visible flaws/ damage. If damage is identified a written record and photograph of the damage should be recorded at the time of seizure. This will make it difficult for the suspect to claim, at a later date, that the damage occurred whilst in Police possession.

2. Check routers (wired or wireless) with USB ports, as external hard disks could be connected to them to enable storage of network data, accessible to all computer systems on the same network. One can also check for available wireless networks, determining their name and whether they are open (access is free, does not require a password) or secured (access is password-based);

3. Identify and seize adapters or special peripheral devices required later when retrieving information from the storage media (digital video recorder – DVR, network video recorder – NVR, etc.)

[7] Plastic materials should be avoided when collecting items containing digital evidence, as plastic can cause or transmit static electricity and may lead to moisture and condensation, which could damage or destroy evidence.

4. Package storage devices, in cardboard boxes or paper bags and not in plastic materials, separately from other assets, valuable items or documentary evidence;

RAID[8] servers

RAID-type systems are data storage hardware solutions: dedicated data storage hardware equipment, with two or more disks (HDD, SSD, SSHD), usually configured in a RAID matrix (type 0, 1, 5, 6, 10, etc.) that offers increased access speed as well as protection of stored data.
The main rules applicable in such cases include:

1. Track data network cables and power supply cables, including in other rooms of the searched premises or in suspect areas. Typically, this type of data storage solutions is most often used in datacentres, however, due to the simplified connectivity and the affordable prices of the latest generation of storage media, these can also be found at private premises, whether visible or hidden, in isolated areas (attics, cellars, basements, fake walls etc.), requiring just a power supply cable and possibly also a data cable to enable network connection (unless the equipment allows for wireless communication).

2. Determine identification elements for each and every storage device, such as: make, model, serial number, various inscriptions, as well as any visible flaws/damage. If damage is identified a written record and photograph of the damage should be recorded, at the time of seizure. This will make it difficult for the suspect to claim, at a later date, that the damage occurred whilst in Police possession. These storage devices should be seized together with the hardware device they are mounted in.

3. Package data storage devices, in cardboard boxes or paper bags and NOT in plastic materials, separately from other assets, valuable items or documentary evidence.

4. Complete an exhibit label and attach it to the exhibit.

Internet of things (IoT)

Almost every physical device may contain embedded electronics that connect this device remotely or wired to either a local network, the Internet or both. There are typically three roles for IoT devices:

- sensors (thermal, movement, light, opening, moisture, location, connection, etc)
- devices (status reporting, voice/video input, data storage, actors, etc)
- gateways (connect devices, transfer data, control/filter, trigger actions).

Examples are almost indefinite and include "smart home/garden" settings, industrial robots, alarm systems, traffic sensors/management systems, supply chain management systems.

Most IoT devices will provide, at least, information about when it was used. Gathering information from available IoT sources will help considerably to document the case, adding dates and times.

[8] RAID - *Redundant Array of Independent Disks*

In some cases, timeline will help to understand the modus operandi, sometimes (in)validate an alibi or exclude people from suspect's list.

The main rules that should be followed when identifying and seizing such devices include:

1. As some IoT devices create their own unprotected WiFi access points or try to connect via Bluetooth, it is recommended that all personnel at the scene disable WiFi and Bluetooth functionality on their own devices. Otherwise their devices might connect to the unprotected networks and alter data (e.g. create new log-entries, overwrite old log-entries) or even trigger actions;

2. It is difficult to identify all IoT devices manually. A network scanner and/or spectrum analyser might help to find such devices, if legislation permits. Note should be given to the fact that different IoT standards use different frequency in different bands;

3. If possible, a specialist might analyse information on IoT while they are running, since most IoT devices lose part of their data when they are turned off. All actions taken need to be documented in detail;

4. IoT devices are most likely connected and accessible externally. They need to be isolated from their networks, e.g. by cutting the power after the live acquisition of their data.

5. Package devices, in cardboard boxes or paper bags and not in plastic materials, separately from other assets, valuable items or documentary evidence;

Automotive IT (AIT)

The amount of networked electronic components in vehicles is constantly rising and so is the amount of potentially evidential data that can be extracted from these components. Most of the components belong to the group of IoT devices, while not necessarily being linked to the Internet. The electronic systems in a vehicle typically fall in two distinct categories:

- Infotainment systems (GPS locations, Bluetooth, Messages, Phone calls, Internet history, Cameras, etc)
- Car systems (GPS, brake controller, speed, throttle controller, collision, light/indicator status, stability controller, sensor information, air bag use, occupancy, service)

All information from the sensors and control on the actuators are typically logged by the embedded systems in the car. Based on that information, some important investigation clues may be provided, including navigation data with time-stamps (speed, directions, altitude, geo-location, GPS fixes,...), doors or trunk opening / closing, use of different seats pre-configuration, presence of people on seats, calls, contacts, messages exchanged, phone book copied from connected devices, etc. The collected information may improve the investigation timeline or even provide indications about the user of the car and his/her actions.

The main rules that should be followed when identifying and seizing such devices include:

1. To avoid tampering of data on the electronic systems of a vehicle, it is recommended that all personnel at the scene disable WiFi and Bluetooth functionality on their own devices. Otherwise their device might connect to the systems and alter data (e.g. create new log-entries, overwrite old log-entries);

2. The electronic systems typically receive power from the battery in the vehicle. Depending on the power situation priority might be given to documenting visible on-screen data and setting the car systems into power saving mode to avoid loss of volatile data;

3. If possible, a specialist might analyse information on the vehicle's systems while they are running, because some data might get lost when the systems are turned off;

4. The electronic systems in a vehicle might be connected externally, e.g. to mobile networks. Some systems can be controlled remotely. Thus, the vehicle should be isolated;

5. Only qualified personnel should physically extract information systems from a vehicle. The extracted components should be considered damaged and thus never be reused in real traffic;

3.3.3 Sealing, transport and storage of electronic evidence

1. Depending on the national legislation in place, computer systems, computer data and digital devices are usually shown to the person they are being seized from as well as to those present at the scene, for recognition purposes and for marking so they cannot be changed/switched, after which they are labelled and sealed.

2. DO NOT place computer systems, computer data and digital devices next to magnetic sources or radio transmitters.

3. DO NOT store computer systems, computer data and digital devices in highly humid settings.

4. Transport computer systems, computer data and digital devices avoiding shock or excessive or lengthy vibrations.

5. Ensure that each of the seized items is properly labelled and sealed, indicating item make and model, and whether powered on or off or connected to peripherals/network, and photograph them for documentation of evidence. The computer system shall be photographed as found on site, including the image displayed on the monitor, if the computer system was powered on. The report prepared by the assigned specialist shall also include other computer systems/data and digital devices identified on site but not seized, which were photographed as potentially relevant to the case.

6. Package mobile or smart phone(s) in signal-blocking material such as Faraday isolation bags, radio frequency-shielding material, to prevent data messages from being sent or received by the devices. If incorrectly packaged or removed from shielded packaging, the device may be able to send and receive data messages. Be aware that keeping devices in signal-blocking packaging may reduce battery life significantly. In cases of low

battery power, consider putting devices into "flight-mode" instead[9]. Packing materials (materials that can produce static electricity such as Styrofoam) should also be avoided.

7. Storage: Ensure evidence is inventoried in accordance with the relevant policies.

8. Protect evidence from magnetic sources, moisture, dust and other harmful particles or contaminants.

9. IT systems in vehicles might not be removed on scene, even by qualified personnel. In those cases, the vehicle needs to be transported and stored as evidence in compliance with the general rules and processes that apply for such evidence.

Specialist support needs to be requested as soon as possible when evidence gathering raises some specific (technical) issues and the first responders in charge of evidence collection are not familiar with the issue or its implications.

Prepare a report describing the activities conducted at this stage (see 6.2).

3.3.4 Imaging and live data acquisition

In some cases, digital evidence requires extraction at the location where computer systems, computer data and digital devices are identified.

Imaging of computer data

Generally, computer systems, computer data, digital devices are seized following a search of home/company premises. One should distinguish between a search conducted at an individual's home/residence and the search that takes place on the premises of a company/business. With regard to searches conducted at a company's headquarters, the target computer systems may be part of the group considered critical, depending on the field of activity (public government, chemical and nuclear industry, power/energy, financial services, public health, ITC, public safety, etc.). In such cases, where powering off or seizing computer systems can seriously affect the company's operations, one should obtain "live" copies of the computer data, while the respective systems are turned on.

In some cases, the seizure of specific computer systems from certain companies, although those systems are not regarded as part of the critical infrastructure, may seriously disrupt the business continuity of that company. Where this is the case, those requesting the seizure of computer systems may consider making copies and leaving the original computer systems on site at the company in question.

One needs to bear in mind that a copy of the media that stores computer data from a running computer system is the equivalent of a snapshot of the data in place at the time of the copying, as computer data are continuously changing.

[9] Electronic Evidence Guide, pag 48

To conduct this type of copying activities, one may need to require prior authorisation from the relevant authority, according to the applicable national legislation in force.

In some cases, copying may take considerable time, if large amounts of data are to be copied, such information usually being stored on servers or computer data centres. In such cases, copying may need to be discontinued and resumed at a later date, which entails sealing the server or the room that hosts it. Also, to ensure data integrity and to avoid altering them, one should consider preventing remote access of that server/computer system until the copying is completed. While the integrity of individual data (e.g. files) may be easy to verify after the acquisition, this may not be possible the larger sets of data (e.g. a logical copy of the system volume), because parts of the data are likely to change during the acquisition process.

This activity requires use of specific equipment and adherence to and implementation of certain steps described in the subchapter on live data acquisition.

If it is not practical to copy the data due to its excessive size or time restraints, you may consider seizure of system 'back-ups' as this may contain sufficient information to assist your investigation.

Live data acquisition

Notice: this is only to be conducted by a person with appropriate technical knowledge, skills and training.

On many occasions, passwords and configuration files reside (in decrypted form) in the memory but can only be found on disk in encrypted form. A "live" computer can show the processes currently running (i.e. show what operations the computer is undertaking), caches (where data is temporarily stored), network connections and reveal any data stored in memory. Memory can also contain useful information such as passwords and/or encryption keys or decrypted applications (useful if a machine has encryption software installed) and sometimes even malicious code that has not been saved to disk.[10]

Other technical reasons why live data acquisition may be necessary in order to obtain important evidence which may be lost once computer systems are powered off, include: RAID servers, exotic hardware, hard disks that can't be removed, servers and network clouds.

To access computer systems (servers/computers etc.) **identified as running**, one needs the authorisation of the relevant authority, as well as the support of persons with the technical expertise required to access and apply the necessary software and equipment.

The person assigned to conduct the accessing of computer systems shall take the following steps:

1. Prior to conducting the activity, prepare a new external hard disk previously wiped and formatted with a file system that is natively compatible with the computer systems about to be analysed; recommended use of NTFS for Windows systems, EXT4 for Linux and HFS+ for macOS systems with USB 3.0/3.1 interface (and USB-C adapter) that contain

[10] Electronic Evidence Guide, page 66

the software applications required in performing the activities listed below and have a capacity large enough to enable copying of the relevant files (at least 1TB).

2. Ensure the external hard disk is connected to the target computer system.

3. All activities conducted in relation to the target computer system shall be carefully recorded in detail on a checklist, specifying the real-time date/time (using an official time source, like atomic clock) and each activity conducted. The list will form an integral part of the final report. The live forensics software suite should include tools for Windows, Linux and macOS which are tested, trusted and change as little data as possible, following Principle 1 of the principles of electronic evidence[11]. Due to their size, speed, scriptability, flexibility and availability command-line tools are to be preferred whenever possible. The following are to be conducted as a minimum:

   - Identify potential encryption software applications that provide logical container or whole disk encryption, typically PGP, Veracrypt, Truecrypt, Bitlocker, dmcrypt, FileVault, etc

   - To secure the information held in the volatile memory (RAM), the next step of the authorised access will most likely consist of imaging the target computer systems' RAM memory, using specialised software applications (the most popular are: Pmem suite consisting of Winpmem, Linpmem, OSXpmem, DumpIT for Windows, etc).
     Generally, the footprint of such applications on the RAM volatile memory should be as small as possible to limit the extent of original memory alteration.

   Important: Acquiring a computer's memory always comes with the risk of crashing the operating system (e.g. Bluescreen). In cases of active encryption being used or other critical volatile data it is advised to logically acquire those data before conducting a memory acquisition.

   Where a logical container-type encryption is identified and the container is mounted (open), copy the files held in the encrypted container using a special software app (most popular is FTK Imager on Windows and rsync on Linux/macOS) or the Copy&Paste operation. The first method is the preferred one. As for the rest of the data on the computer system, consider copying them for subsequent analysis, during the computer forensic analysis.

   In case the whole disk encryption was identified, copy all files on disk using a special software app (most popular is FTK Imager on Windows and dd on Linux/macOS) or take a logical copy of the unlocked volume.

   If no encryption applications were identified, proceed to step 4.

   Before copying computer data from live computer systems or digital devices, one can check the following:

[11] Electronic Evidence Guide, page 14

- the display screen for signs that digital evidence is being destroyed. E.g. "delete", "erase", "format", "remove", "copy", "move", "cut" or "wipe";
- which windows are opened;
- look for indications of cloud services being used;
- look for signs of active or ongoing communications with other computer systems or users such as instant messaging windows or chat rooms;
- look for signs that cameras or Web cameras (Web cams) are active.

4. The live acquisition procedure of physical disks and logical volumes differs depending on the operating system:

- When the operating system installed on the live computer system is **Windows**, the following tools have proved to be efficient and are very often used by law enforcement authorities:

  - EnCase Imager[12]
  - FTK Imager Lite – allows also for copying the RAM memory[13];
  - Belkasoft Acquisition Tool – allows also for copying the RAM memory, mobile devices and cloud accounts (limited to Email, Google Cloud, Instagram and Whatsapp)[14];
  - Winpmem – open source - only for copying the RAM memory[15]
  - DumpIt – only for copying the RAM memory[16];
  - Magnet RAM Capture – only for RAM memory[17].

- When the aim is to also copy the RAM memory, the size of the software application used for this purpose should be as small as possible to minimize the extent of RAM memory alteration and give priority to the operation. For instance, practice has shown that the DumpIt[18] application is least intrusive when copying the RAM memory.

- When the operating system installed on the live computer system is **Linux**, the following commands or tools are recommended to be used:

  - command DD if=<source> of=<destination> [options] – valid for most Linux distributions;
  - FTK Imager – command lines Debian and Ubuntu[19], Fedora and RedHat[20];

[12] https://www.guidancesoftware.com/encase-forensic-imager

[13] https://accessdata.com/product-download/ftk-imager-lite-version-3.1.1

[14] https://belkasoft.com/bat

[15] https://github.com/Velocidex/c-aff4/releases

[16] https://my.comae.io/login

[17] https://www.magnetforensics.com/free-tool-magnet-ram-capture/

[18] At the time of developing the present guide, the size of the DumpIt.exe application was 522BK

[19] https://accessdata.com/product-download/debian-and-ubuntu-x64-3.1.1

[20] https://accessdata.com/product-download/fedora-and-red-hat-version-x64-3.1.1

  - DCFLDD[21] – improved version of DD command;
  - Commands rync and TAR – for archiving of logical files.

- When the operating system installed on the live computer system is **macOS**, even a root user is not permitted to access the /dev/disk, /dev/rdisk device by default due to System Integrity Protection (SIP). If SIP is disabled the following commands or tools are recommended:

  - command DD if=<source> of=<destination> [options];
  - FTK Imager – command line[22];
  - MACQUISITION[23] – commercial solution.

Given that write blockers cannot be used when accessing computer data from running computer systems, the investigator/specialist needs to correctly and fully identify all the storage devices whose contents are to be extracted. In such cases, the mere connection of an external hard drive to the live computer system will cause certain changes to the operating system in use (whether Windows, Linux, macOS or other OS types).

For copying purposes, the investigator/specialist should use software applications that do not require installation (the portable version) on the target operating system. Even the use of portable applications causes changes (writes computer data) to the computer system intended for copying. The software used should be tested beforehand and the least invasive tool should be chosen.

Once the data is extracted it can be analysed. This should be documented in a report (see 6.2) to be prepared by the Live Data Forensics specialist and contain the following main categories of information: data about the person who conducted the activity, data about the person identified as the custodian of the computer system, data about the files that were found (size, date when created/modified).

Upon completion of the activity, the report together with the findings may need to be presented to the owner or person identified as custodian of the computer system. When and how the information is presented, as well as any potential observations are issues to be determined depending on the provisions set forth in the related national legislation.

The report should be prepared in a way that also facilitates understanding by people lacking advanced technical knowledge; it should be presented clearly and provide enough details to avoid leaving room for interpretation.

[21] http://dcfldd.sourceforge.net/

[22] https://accessdata.com/product-download/mac-os-10.5-and-10.6x-version-3.1.1

[23] https://www.blackbagtech.com/software-products/macquisition-7/macquisition.html

4 Forensic analysis of computer systems, computer data and digital devices

Notice: this is only to be conducted by a person with appropriate technical knowledge, skills and training.

The examination of computer systems or digital devices is a forensic investigation operation aimed at finding evidence on these items. This procedural activity may have different names (computer search, computer forensic examination, computer forensic analysis) and, in principle, it is conducted on the basis of an authorisation issued by the relevant authority, usually a magistrate.

Examination is conducted by specialised personnel aided by dedicated software applications and using technical means designed to ensure the integrity of the data stored on the searched device. It is usually undertaken in forensic laboratories that can provide a secure setting and the technical means required for various technical operations. (See Digital Forensics Laboratory Guide).

The computer search operations carried out are to be described in a report (see 6.4) which will include the electronic version of the evidence identified during the respective operations (documents, proof, databases, email correspondence, online discussions, pictures etc.).

4.1 Preliminary activities

1. Check the authorisation for the forensic analysis or other documentation required by law.

2. Check the integrity of the computer system or digital device as well as packaging and sealing. Photographs should be taken of the evidence bag, exhibit label and condition of the exhibit – this will verify the integrity prior to removing the exhibit from its packaging.

3. Check the identity of the people who will take part in the operation (the holder of the computer system or digital device or their representative, lawyers or other persons involved in the operation according to legal requirements).

4. Prepare the equipment intended for use during the computer search and copying operations.

Even if new storage devices are to be used, these should be wiped first (basically all device sectors are to be rewritten and checked for integrity) to avoid cross-contamination.

Also, prior to conducting the computer search, check the computer systems thoroughly for any computer storage media. Practice has shown cases when the persons who seized the computer systems failed to accurately and fully identify all the associated computer storage media or when the identification of such media failed for various technical reasons.

For mobile devices, remove the SIM card and any existing storage media. If the mobile device is on and shielded against radio signals, carry out its identification and, if necessary, its connection to USB ports, in a Faraday box which blocks external radio signals.

4.2 Physical check and accessing of electronic evidence

4.2.1 Desktops

1. Check the CD/DVD/BluRay/floppy reader/writer units and extract any disks identified, for securing and searching.

2. Check memory card reader units and extract any cards identified, for securing and searching.

3. Open the computer cases and remove all identified hard disks for securing and searching. Also look for flash drives directly connected to the mainboard (e.g. via m.2 or PCIe interfaces) and for flash storage which is soldered onto the main board and can only be remove by highly specialised personnel.

4. Provide any additional storage devices with individual exhibit references- this can be taken from the exhibit reference of the original exhibit (for example AB01/01, AB01/02). Each new exhibit will require its own exhibit label.

5. After removing all computer storage media, proceed with the following:

   - connect the desktop to a power supply source and turn it on, and try to access the BIOS/UEFI system (usually by pressing the "DEL", "F2" or "F12" keys), unless password protected;
   - if accessing the BIOS/UEFI system was successful, to determine any time differences, record the date and time displayed in the BIOS/UEFI, as well as the real date and time;
   - turn off the desktop;
   - disconnect the desktop from the power supply source.

4.2.2 Laptops

1. Disconnect the laptop power supply battery, if connected.

2. Check the CD/DVD/BluRay/floppy reader/writer units and extract any disks identified, for securing and searching.

3. Check memory card reader units and extract any cards identified, for securing and searching.

   Identify access to hard disk(s) (usually on the bottom of the laptop or on its sides, though also under the keyboard in some cases) and remove all hard disks identified for securing, imaging and searching. Also look for flash drives directly connected to the mainboard (e.g. via m.2 or PCIe interfaces).

4. Most modern laptop computers have flash storage which is soldered onto the main board and can only be remove by highly specialised personnel. In most of such cases the disk has to be acquired using a forensic boot medium (e.g. Caine[24]/Paladin[25]).

   Provide any additional storage devices with individual exhibit references- this can be taken from the exhibit reference of the original exhibit (for example AB01/01, AB01/02). Each new exhibit will require its own exhibit label.

5. Once all computer storage media removed, proceed to the following:

   - reinsert the power battery in the laptop;
   - turn the laptop on and try accessing the BIOS system (usually by pressing "DEL", "F2", "F10" or "ESC" keys), unless password protected;
   - if accessing the BIOS system was successful, to determine any time differences, record the date and time displayed in the BIOS, as well as the real date and time;
   - turn the laptop off;
   - remove battery from laptop.

4.2.3 Internal hard drives

1. Determine the communication interface: IDE, SATA, SCSI, m.2, PCIe, SAS etc.

2. Connect the hard disk to a write blocker with IDE, SATA, SCSI interface, to ensure stored data integrity (e.g. TABLEAU Forensic SATA/IDE/SCSI Bridge). Use adapters when confronted with other types of connectors.

3. Switch the jumper on "SINGLE/MASTER" or "CABLE SELECT", for IDE hard disks, if the write blocker fails to detect the hard disk.

4. Connect the write blocker to the analysis computer.

5. Be aware that once you connect a flash storage to power (even through a write blocker) the internal flash controller may start to perform write actions on the cells (e.g. garbage collection, wear-leveling, etc). This can only be avoided by desoldering all flash chips manually by specialised personnel. However, the data on the chips might be encrypted then.

4.2.4 External hard drives

1. Identify if it is possible to extract the internal hard disk from the enclosure without damaging. If that is possible, extract the disk and proceed as described in 4.2.3.

2. Determine the communication interface: USB, eSATA etc.

3. Connect the hard disk to a write blocker with USB, eSATA interface.

[24] https://www.caine-live.net

[25] https://sumuri.com/software/paladin/

4. Connect the write blocker to the analysis computer.

4.2.5 CDs, DVDs and BluRay disks

No particular steps to be followed, just to insert the disk in a proper CD, DVD, BluRay reader.

4.2.6 USB drives and memory cards (SD, miniSD, microSD, etc.)

1. If the memory card has a write protection switch, slide the switch and connect the memory card to the analysis computer via any USB or card reader.

2. If the memory card lacks a write protection switch, to access it use a card write blocker (e.g. Digital intelligence – forensic card reader).

3. Connect the write blocker to the analysis computer.

4.2.7 RAID servers

1. Access the RAID matrix configuration menu by turning on the searched computer system, identifying at least the following information: total number and port of each matrix hard disk, total capacity, matrix type and stripe size. Be carefully not to accidently start the operating system;

2. If the matrix type is RAID 1 (mirror), the standard procedure applies, using any of the RAID matrix hard disks, given that the copying/search operations are the same as for a regular hard disk.

3. If the matrix is a different RAID type (0, 5, 6, 10, 50 etc) and integrity of data on each hard disk can be ensured (by using write blocker-like devices), proceed to conducting a direct computer search. If integrity of data on each hard disk cannot be ensured, one must first make a copy (clone) of all the hard disks and recompose the RAID matrix using special computer applications, then conduct the computer search (according to the procedure indicated under item 2.4).

4. If none of the above methods enables accessing of the RAID matrix, turn on the searched computer system using a specifically designed Linux operating system, with pre-installed applications and drivers required in copying (cloning) the RAID matrix. The "AUTOMOUNT" option and udev rules on the Linux OS must be deactivated or set to read-only to ensure data integrity, while hard disks must be manually mounted using specific commands.

Use data storage write blockers to prevent alteration of stored data. There are typically two types of write-blocking methods: **hardware write blockers** and **software write blockers**.

4.3 Imaging of computer data

Depending on the existing legislation, prior to conducting the computer search, one should produce a forensic copy of the storage medium to ensure integrity of original storage device and for subsequent use of the copy.

The forensic copy can be done in two ways, either as a clone (Bit-to-bit copy of the source medium onto the target medium) or as an image (Bit-to-bit copy of the data on the source medium into an image file on a target medium; typically compressed, containing meta-data, etc).

Some 'cloning' software will only capture allocated clusters. It is important to use forensic tools to capture all data as deleted/residual data may be important to your investigation.

Subsequent investigation should be conducted on the 'image'. This is done to maintain the integrity of the original data. The process of cloning or obtaining an image will generate a unique Hash value – the hash value of any subsequent copies must be identical to the original, in order to verify integrity and show that the data on the original exhibit has not been changed.

To create such a forensic copy one can use dedicated software applications (the most popular are EnCase Forensic, X-Ways Forensic, FTK – Forensic Toolkit etc.) or free Linux applications (the most popular are Guymager[26], DD, libewf[27], FTK Imager etc.).

The imaging/cloning operation is subsequently documented in a report (see 6.3), submitted and signed by the persons involved in conducting the operation, according to the legislation in force.

4.3.1 Desktops

When removal of internal computer storage media is not necessary or not possible[28]

1. Connect the necessary peripherals to the desktop (keyboard, mouse, screen) and power it from the power grid.

2. Connect to the desktop an optical storage media (CD/DVD) or memory stick set with a forensic boot operating system (e.g. Caine[29]/Paladin[30]).

3. Disconnect any other external storage media connected to the desktop and copy them separately.

4. After powering on the computer system, access the BIOS/UEFI to rearrange the booting order and make sure that the optical storage media or memory stick containing the portable operating system to be used for copying is listed first. Record the date and time

[26] https://guymager.sourceforge.io

[27] https://github.com/libyal/libewf/

[28] Certain types of computer data storage media are glued to the motherboard, and therefore their removal could cause damage and loss of stored computer data.

[29] https://www.caine-live.net

[30] https://sumuri.com/software/paladin/

stored in the BIOS/UEFI to determine consistency with real date and time. Test at least once to ensure that the computer system loads the operating system from the media prepared by the specialist, and then reconnect the storage media using the same cables and the same order.

5. After making the above-mentioned changes and saving the settings, restart the desktop and load the operating system from the optical storage media or memory stick.

6. The portable operating system used is typically a Linux distribution which does not automatically mount the internal/external computer data storage media. The operating system creates a software protection against any alterations/changes of computer data stored on the media intended for copying.

7. The specialist needs to mount[31] in the write mode only the external storage media on which the computer data storage media are to be copied.

8. For copying purposes, one can use software applications previously installed on the portable operating system or commands by the same operating system. Copies can be made in an uncompressed RAW format, compressed E01/S01 format or other types of formats depending on the software applications used.

When removal of internal computer storage media is possible

1. Identify the hard disk(s) or any other storage media and document the ports they were removed from.

2. Depending on the hard disk interface, connect the hard disk to the write-blocker which will later on be connected to another desktop intended for the copying operation and on which specific copying-related computer applications are installed. One can also use duplicators[32] that can provide a copy of the storage media without requiring the use of another computer system. These duplicators also provide write blocker function for the source media (the media whose contents are intended for copying).

   When acquiring a forensic copy of a target disk, the examiner should always verify the integrity of the image that was created. He can do so by calculating the MD5/SHA-1/SHA-256 hash values for the original disk and the resulting copy, these values should be checked promptly as results must be identical to the values obtained initially. Note that MD5 and SHA1 hash algorithms should never be used exclusively In rare circumstances the copied computer data storage media can have faulty areas which are replacing with value "0" patterns by the forensic imaging.

3. For portable computer systems (laptop/notebook/certain types of tablet computers), the procedure is the same, although market trends show an increasing number of portable systems whereby removal of the internal computer storage drive is either not possible or it results in damaging certain components of the portable computer system.

[31] MOUNT = mounting a file system in a directory structure is attaching the file system in order to access a directory belonging to a different partition.

[32] One of the well-known duplicator producers https://www.guidancesoftware.com/tableau/hardware/td2u

4.3.2 Mobile devices (smart or regular mobile phones, tablet computers, GPS devices, smart watches, drones, etc.)

Prior to commencement of examination, the examiner should correctly determine the make, model, serial number or IMEI code and the operating system installed on the device. At the same time, it is important for the specialist to know the mobile device lock code/password. In some cases, when the mobile device is locked with an unknown code/password, and depending on the model, operating system and security patches in place, one can try to bypass the existing security measures without affecting the integrity of the data available on the device.

The most popular computer applications used to facilitate the unlocking/accessing of mobile devices include: UFED Ultimate[33], XRY Physical[34], Oxygen Forensic® Detective[35], etc. The process can be simple and fast (for old mobile device models) or it may be complex and requiring a good deal of technical expertise (for recent mobile device models).

Most software applications used when copying the mobile device internal storage drive require a 100 percent battery recharge. Occasionally, a certain battery charge level indicated by the application may help bypass the security measures in place (password, pattern or code).

Depending on the mobile device make, model and operating system, the copies made are grouped into three main categories:

1. **LOGICAL** – copying of data generated by the user: photos, audio-video recordings, unloaded documents etc.;

2. **FILE SYSTEM** – may contain all the data mentioned under the LOGICAL category as well as certain files generated by the applications installed on the operating system. For mobile devices with iOS version 4 or less, there is ADVANCED LOGICAL[36];

3. **PHYSICAL**– copying the full contents of the internal storage media. It contains both the allocated[37] and the unallocated[38] space. Even though this is the most efficient type of copy, one should make all types of copies for the same mobile device;

Prior to making the copy, each mobile device model requires changes to its settings (which differ depending on the OS in place), to enable the application used to access specific parts of the internal data storage drive. In some cases, one needs to identify the menus which are hidden to the user. Changes to the settings do not affect the data already stored on the mobile device internal drive.

---

[33] https://www.cellebrite.com/en/products/ufed-ultimate/

[34] https://www.msab.com/products/xry/xry-physical/

[35] https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective

[36] Method supported by the UFED Physical Analyzer application.

[37] Allocated space is disk space taken by current files.

[38] Unallocated space is disk space which the operating system has not written files to yet as well as space taken by previously deleted files.

Choosing which software application to use when copying the mobile device storage drive depends on the respective specialist's knowledge/training and is a very important step in obtaining a complete copy (for best results, obtaining a physical copy is preferable).

Scenarios one can encounter when copying a mobile device include:

1. Mobile device is locked and/or encrypted:

   - Handle the device in a Faraday-type box only, until all connections to mobile data are stopped. Any data connection (even a few seconds long) can cause remote deletion of the encryption key which will automatically make it impossible to recover the computer data on the device.
   - One can ask the device owner/holder for the unlocking codes.
   - One can bypass the security measures in place, depending on the device make, model and operating system. Some foreign companies[39] also provide mobile device unlocking services.

2. Device is damaged:

   - The screen does not work -> specialised personnel should either fix it or replace it.
   - The USB interface is damaged or its connectors are reversed (some mobile device models made in China). For the former, specialised personnel should either fix the interface or replace it, while for the latter, one need the original mobile device cable.

3. CHAT-type applications have an updated version and some of the applications used in the copying process require restoring a previous/older version. Here, changes should be made only to the applications (Whatsapp, Facebook Messenger, Badoo, Twitter, etc.) and not to the database that contains the message exchange.

4. No mobile device whose internal storage media requires copying can be accessed using a write-blocker. Moreover, when making the logical copy, most computer applications used for copying will send/copy a sample (file/app) to the mobile device internal storage. In this case, one should forego the write-blocker and document the reason for such action in the report. All changes made should be documented.

[39] https://www.cellebrite.com/en/cas-sales-inquiry/

4.4 Digital forensic analysis

In the preparation stage, the specialist should choose the forensic software application mainly based on the investigated case specifics, to obtain complete and accurate results.

The computer search operations should be conducted by using dedicated software applications, whether licensed (the most popular are EnCase Forensic, X-Ways Forensic, FTK - Forensic Toolkit etc), OpenSource software applications (e.g. Autopsy[40]), or developed by law enforcement agencies/international organisations, and allowed by national legislation. Most importantly, regardless of which software application is used, the results one obtains should be clear and should enable reproduction using any other software application.

There are several types of forensic software applications designed for specific types of devices or for searching certain types of information or data. The first step in a computer search is rechecking the hash values obtained when copying the computer data. If one gets the same hash values, one can continue with the next steps:

1. Check the time zone (recorded in the registries, for Windows operating systems, with the "/etc/timezone" file path, for Linux Debian distributions, etc.). Where the time zone identified on the media copy differs from the one on the computer system used in the computer search, the specialist should adjust the time zone of the computer forensic application, for accurate dates and time.

2. Depending on the type of the investigated case and on the capabilities of the software application used in the computer search, one can do the following:

    - Calculate the MD5, SHA1 and/or SHA256 hash values for all files;
    - Identify and mark the duplicate files (identical files with the same contents);
    - Index the file contents;
    - Analyse and categorise the file signatures the file signature – based on the header and occasionally on the footer;
    - Recover deleted files or file fragments;
    - Interpret and recover file metadata[41];
    - Automatically mark files with the wrong extensions;
    - Process the installed and used browser history, cache, search, passwords, bookmarks, session, etc;
    - Identify and process email files, whether email client or web-based;
    - Identify and process text message exchanges via computer applications, e.g. Skype, Yahoo Messenger, Pidgin, ICQ, Jabber, etc.
    - Identify encrypted files, containers, partitions or full storage drive. Decryption may be more or less successful depending on the quality of other data that has been obtained and on the specialist's level of expertise;

[40] https://www.sleuthkit.org/autopsy/

[41] https://en.wikipedia.org/wiki/Metadata

- Conduct a keyword search in the previously created index or directly on the image/copy; one can create search keys based on the available case data, prior to the computer search, with the aid of the case investigator;
- The computer search specialist shall mark the files containing relevant case data on the search application and also copy them in the folder prepared upon case inception, while file fragments identified on the unallocated space shall be marked and adequately outlined in the technical report.

In case a memory dump has been captured during the live data forensics process, the examiner can analyse the contents of the RAM memory copy within the same case or separately, and one may obtain the following results:

- Passwords or information on user passwords;
- Encryption keys to unlock encrypted volumes/containers;
- Applications that start running at the same time as the operating system;
- Information on the computer data storage media connected to the computer system;
- Wireless networks used;
- Internet browser history (even privacy/incognito modes;
- Unsaved documents;
- E-correspondence;
- Processes running on the operating system;
- Contents of RAM-Disks; Any other types of data and files uploaded on the RAM memory;
- Processing of data on the OS, users, installed applications, hardware, services, devices connected via USB ports, etc.

Most forensic software applications may work in a mostly automated[42] way. However, it is essential and good practice to validate their outputs (e.g. completeness, correctness) using a different tool and to know where the original data is coming.

It is important to note that while the scope of the forensic analysis might be limited by the mandate, order or other legal constraints, the role of the forensic expert is a neutral one. Thus the forensic expert should not carry out investigative tasks and should report both types of findings, the ones that might prove the guilt of a person but also the ones that might relieve that person from charges.

According to the legislation in force, the results of a computer search are recorded in a report (see 6.3) prepared by an specialist. This report should act as a contemporaneous record of all actions taken during the examination and should be written in such a way that a third party can replicate the same actions and arrive at the same results. As a minimum, this report should contain the following:

- The name of the person from whom the computer system or computer data storage media were seized, or the name of the person whose computer system is investigated;
- Assigned forensic officers and staff involved in the investigation and all laboratory staff that have had contact with the exhibits;

[42] https://www.magnetforensics.com/magnet-ief/

- The name of persons present during the search;
- Case number or crime number and type of crime;
- The points to prove or what is required from the investigation;
- Description and listing of computer systems or computer data storage media subject to the search;
- Description and listing of the activities/operations conducted;
- Computer search start and end date and time;
- Description and listing of computer data uncovered during the search;
- Signature of person who conducted the activity;
- Comments and signature of person/persons assisting in the activity;
- Comments and signature of the person/persons from whom the assets were seized.

The digital evidence included in the above-mentioned documents may be signed digitally by the specialist who conducted the operation, using an extended electronic signature based on a qualified certificate issued by an accredited provider of certification services. Where this is not available, for the digital evidence, the forensics report prepared by the assigned specialist must contain a calculation of one or more (MD5, SHA1, SHA-256, etc.) hash values.

For mobile devices, the search operation often involves use of dedicated licensed software applications (the most popular are MOBILedit Forensic, XRY Forensic, Cellebrite UFED, etc).

Persons conducting such operations shall take the following steps:

- Carefully handle the portable device, avoiding exposure to powerful electromagnetic fields, shocks, liquids etc.
- Connect the portable device to the computer undergoing the search, using a wired connection (appropriate data cable) or a wireless connection (Bluetooth, infrared).
- If the portable device has voice communication (GSM) capabilities, copy the basic information available on the telephone and SIM card, such as the contacts list, the call logs for received, dialed and missed calls, as well as the received/sent text messages.
- Depending on the portable device capabilities, also copy email messages, stored files (photos, video recordings, documents etc.) and any other case relevant accessible information.
- When the portable device is password/lock code protected, and the password or code is not known or cannot be obtained, to identify the information on the device, the unit which requested the search may ask for outside expert support.
- Upon completion of the operation, prepare a mobile device search report (see 6.3).

4.5 Resealing of electronic evidence

Upon completion of the computer system copying or search operation, the items subject to the operation shall be packaged and resealed to ensure the integrity of original data and prevent access other than by following the legal procedures in place.

These activities shall be conducted similarly to those described for packaging and sealing the devices initially seized following a home search or other operations, in compliance with relevant legal provisions.

Device storage and preservation should be safe and secure:

- If a write-blocker was used, disconnect the searched data storage media from it;
- If no write-blocker was used, shut down the desktop used for the computer search and disconnect the searched data storage media;
- If the searched item was a hard disk which was removed from a computer desktop or a laptop, reinsert it in the desktop;
- Repackage and reseal the searched data storage media, possibly together with the other items that were identified at the time of unsealing; one may also request that participants to the search provide a holographic signature, to prevent any changes, where such procedural steps are set out in the national legislation.

5 Presentation of findings

5.1 Preparation of the report

Upon completion of the computer system or digital device search operation, prepare a report (see 6.3) the form and contents of which may differ depending on the national legislation in force, but which should basically contain a description of the operations conducted, the tools used and the results obtained. An appropriate course of action would be to have this report peer reviewed to ensure all stages have been appropriately documented and the report is accurate and complete.

With regard to the results that were obtained, more specifically the identified information or data, one may include either all of them in the report or only part of them, or one may attach separate documents or even storage media (CD, memory stick, HDD) containing this information. There are times when the case-relevant information is considerable in both number and size, which is why it would be preferable to save it in electronic format, ensuring data security measures are in place (data digital signature/hash, preferably in MD5 and/or SHA1 standard). Depending on the case (e.g. child abuse material) and legislation it may be necessary to encrypt the storage media. The examiner should use software that is either accepted by the recipients or comes with a portable app to allow opening the encrypted container/volume. The password/passphrase should not be transported via the same channel as the storage media.

Usually, the software applications used in the examination of computer systems, computer data or digital devices will generate technical reports containing data on relevant files: name, category, date when created/used/last changed/deleted, full path, MD5/SHA1 HASH value etc.

These reports with technical details about case-relevant computer files and/or data are to be recorded on optical drives attached to the documents prepared according to the national legislation.

In principle, the technical report generated by the software applications contains the following data:

1. Technical identification data for the searched media, namely:
   - Make;
   - Serial number;
   - Capacity;
   - Type of installed operating system;
   - Date when the operating system was installed;
   - User accounts;
   - Network settings;
   - Directory structure.

2. Technical data individualising the files and file fragments identified during the search, namely:
   - Unique reference number – software generated;
   - File name;
   - File extension;
   - File type;
   - File category;
   - If deleted;
   - Date and time when last used;
   - Date and time when created;
   - Date and time when last modified;
   - Logical size;
   - Physical path and location (sector);
   - MD5/SHA-1/SHA-256 hashes;
   - Data contained by file fragments identified on the unallocated space.

Upon completion of the search of the computer systems, computer data or digital devices, according to the legal provisions in force, the technical report and the case-relevant files recovered during the forensic analysis shall be presented to the persons concerned (investigator, prosecutor, investigation judge, the owner or user of the computer systems, computer data or digital devices or their representative, lawyer or other persons subject of requirements/limitations from the national legislation).

5.2 Transmission of the findings and electronic evidence to the relevant authority

Upon completion of the forensic analysis of computer systems, computer data and digital devices, these together with the data that were extracted and the documents that were prepared shall be submitted to the authority which requested the execution of such operations.

The evidence, along with the computer systems, computer data and digital devices, as well as the documents that were prepared during the operations should be submitted within the specified timeline, as applicable, and where operations were not completed or could not be conducted due to certain technical issues, the requesting authority shall be informed accordingly.

The means of submission shall be agreed upon by those who requested the forensic analysis as well as by those who conducted it, ensuring security and integrity of items and documents.

The documents prepared during these operations should be as clear as possible, containing terms which are easy to understand or are explained accordingly.

At the same time, the requesting authority may ask the person who conducted the forensic analysis to provide additional explanations regarding specific results, given the technical nature of the operations conducted. Thus, clarification may be requested with regard to the software applications used in the forensic analysis, the results these generated or particular aspects identified during the operation. Certain software applications (such as those related to malware, hacking, etc.) identified on the investigated computer systems, computer data and digital devices require explaining in terms of how they work, which can be included in the document describing the forensic analysis or in a separate document.

5.3 Role of the forensic expert in court hearings

Depending on the legislation and the nature/complexity of the case it may be sufficient to provide written reports to the authorities or it may be required to hear the forensic expert orally during the court proceedings. The role of the forensic expert may be different and is often defined by the presiding judge; it typically may be similar with the role of a witness or the role of the expert witness. These roles may entail different rights and obligations in court, thus it is important for the forensic expert to understand his/her specific role and its implications.

The preparation of the forensic expert before the court hearing is essential. Since most of the legal procedures there are length in time, it is advised that the expert revisits his/her report(s) before the trial. Potential questions coming from the legal procedure or practices in front of the court might be considered for the preparation.

A standard court hearing starts with questions about expert name, age, profession and sometimes his/her qualifications, followed by a request to orally present his/her findings. The different parties in the trial might then ask questions. These questions typically refer to the qualifications, the procedures used in all steps of the forensic examination, technical details and interpretation of the findings.

When giving statements in court it is essential to present the truth, to never speculate and to be very careful and precise. In case the expert did not follow a written procedure, it is useful to explain the reason.

A common mistake to be avoided is to claim that "The suspect did…." when only some traces where found on a computer system. A better way to make a statement would be that the traces described in the report where found on the computer system that was seized at the desk of the suspect and that those traces were produced by a certain password protected user account while that same user account accessed e.g. the private mail account of the suspect.

This example shows why it is not just enough to find traces on computer system but also to look at the context and circumstances how these were created.

If there is no accompanying video material available, it is not easy to make clear statements about the natural person that was actually using a computer at a certain point of time. In situations when there are not clear evidence about the user it is recommended to say "I do not know" than starting to speculate.

Other experts might be requested for their expertise and opinion. Where results of computer system, computer data and digital devices examination operations are challenged, depending on the reasons raised, the national legislation should be observed in settling challenges.

In principle, where challenges occur, these may be clarified by providing additional information about the procedure followed or in relation to data identified or other specialists may be requested to redo the forensic analysis for the device/data in question.

Depending on the legislation and role of the expert, he/she might follow the proceeding and might even ask or suggest questions and might be requested to give his/her opinion and/or technical explanation in later stages of the hearing.

The expert needs to remain neutral, available to provide all the explanations according to his/her knowledge and always stick to the truth.

6 Appendices

6.1 Glossary[43]

BIOS: Basic Input Output System. The set of routines stored in read-only memory that enable a computer to start the operating system and to communicate with the various devices in the system such as disk drives, keyboard, monitor, printer, and communication ports.

Blu-ray Disc (BD): is an optical disc storage medium designed to supersede the DVD format. The plastic disc is 120 mm in diameter and 1.2 mm thick, the same size as DVDs and CDs. Blu-ray Discs contain 25 GB per layer, with dual layer discs (50 GB) being the norm for feature-length video discs. Triple layer discs (100 GB) and quadruple layers (128 GB) are available for *BD-XL* re-writer drives.

Compact Disk (CD): Optical disc 12cm in diameter used for storing binary information. Its formatted capacity is between 640-700 Mb and was primarily used to store audio. When used for storing generic data it is called CD-ROM.

Computer Networks: consists of connections between two or more computers that are linked by data cables or by wireless connectivity. These computers are able to share data and other resources between them. They often have other hardware components to enable the scope of activities required of the network.

Cybercrime: refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

Desktops: The term has been adopted as an adjective to distinguish office appliances (such as photocopiers and printers) which can be fitted on top of a desk, from larger equipment covering its own area on the floor. Desktop may also refer to Desktop computer, a personal computer designed to fit on a desk

Digital Forensics: Digital Forensics is a branch of forensic science related to the acquisition, processing, analysis and reporting of evidence that is stored on computer systems, digital devices and other storage media with the aim of admissibility in court.

Digital media: is a form of electronic media where data are stored in digital (as opposed to analogue) form. It can refer to the technical aspect of storage and transmission (e.g. hard disk drives or computer networking) of information or to the "end product", such as digital video, augmented reality or digital art.

Digital Versatile Disk (DVD): Digital Versatile (video) Disc. Presently the natural successor of the CD for the reproduction of quality sound and image.

[43] Sources: Electronic Evidence Guide 2.0, Council of Europe, 2014; Wikipedia.org

Electronic evidence: Electronic evidence is information generated, stored or transmitted using electronic devices that may be relied upon in court. To guarantee that the evidence is accepted in court, it is necessary to obtain the information following very well defined processes using specialised personnel and operating within an adequate legal framework.

Encryption: Method of scrambling and encoding data. Used to convert plain text into ciphertext (by using a mathematical parameter called cryptographic key) in order to prevent anyone but the intended recipient from reading that data.

External hard drives: External hard drives are a kind of external storage media. Modern external hard drives consist of a chassis, that offers connectivity via USB, Firewire, eSATA and/or Thunderbolt, and a regular 2,5" or 3,5" hard disk or SSD that is residing inside the chassis. Typically external hard drives can store a larger amount of data compared to USB thumbdrives or SD cards.

Flash cards: are devices for storing digital information. They are often used in many electronic devices such as digital cameras, mobile phones, laptop computers, music players and games consoles. They are able to retain data without power and come in a variety of capacities, meaning they can store huge amounts of data while being easy to hide from view.

Forensic copy: An exact copy (bit by bit) of the unit of storage of an IT system used in a forensic investigation.

Hard disk drives (HDD): Hard drives are the major storage device within computer systems. They consist of a circuit board, data and power connections, along with internal magnectically charged, ceramic, metal or glass platters that store the data. It is not unusual to discover hard drives that are not connected to or installed in a computer system.

Internet: Global network of data based on TCP/IP protocol that are utilised to interconnect computers and, as such, the transport of diverse services, the most popular being e-mail, web and FTP services.

Internet Service Provider (ISP): Organisation that provides connection to the internet for computers that are dedicated lines or switches. A profit-making entity that as well as providing access to the internet for individuals and / or legal entities, can offer services such as web hosting, web-design consultancy, integration of websites and intranets, etc.

IP address: Chain of 4 numbers separated by decimal points that are used to represent and identify a computer on the internet. ISP's assign IPs automatically when we connect to the internet.

Live computer system: A live computer system is a computer system that is powered on.

Live data forensics: Live data forensics is one part of computer forensics which is a branch of digital forensic science pertaining to legal evidence found in computers. Computer forensics deals with the examination of computer systems in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts that might become evidence in

a trial. Live data forensics follow this aim but is only focused on computer systems that are powered on. The main purpose is to acquire volatile data that would otherwise get lost if the computer system is turned off or would be overwritten if the computer system will stay turned on for a longer period.

Message-Digest 5 (MD5): The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database.

Memory cards: are devices for storing digital information. They are often used in many electronic devices such as digital cameras, mobile phones, laptop computers, music players and games consoles. They are able to retain data without power and come in a variety of capacities, meaning they can store huge amounts of data while being easy to hide from view.

Network Attached Storage (NAS) – A NAS is similar to an external hard-drive with the difference that it provides storage space for a whole network rather than just a single PC. NAS can often offer a lot more than just data storage. Many NAS devices house more than one hard drive and offer 'RAID' functionality.

Redundant Array of Independent Disks (RAID): is a way of arranging the storage of data (a data 'configuration') using multiple disk drives. Data is stored across the individual disks to ensure the best level of performance and/or data reliability. The operating system will access the RAID as though it were a single hard disk. The access is controlled and coordinated either by software or by a hardware RAID controller.

RAM memory: RAM stands for *Random Access Memory.* RAM memory temporarily stores data that the computer is working with. This memory loses its content as a result of a power loss.

Secure Hash Algorithm 1 (SHA-1): In cryptography, SHA-1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.

Software: Computer programs designed to perform specific tasks, such as word processing, accounting, network management, Website development, file management, or inventory management.

Solid state disk (SSD): SSDs store information in a different way than hard disks, while intending to provide access in the same way as tradtional hard disks. Whereas hard disks store data on platters, solid state disks store data using microchips that have no moving parts. As such they are less likely to be damaged by shock and they offer faster access to the data. These devices may hold valuable evidence.

Solid state hybrid drive (SSHD) In computing, a hybrid drive is a logical or physical storage device that combines a faster storage medium such as solid-state drive (SSD) with a higher-capacity hard disk drive (HDD).

Storage devices: is a device for recording (storing) information (data). Recording can be done using virtually any form of energy, spanning from manual muscle power in handwriting, to acoustic vibrations in phonographic recording, to electromagnetic energy modulating magnetic tape and optical discs.

Tablet Devices: A tablet computer is a device that is operated by touching the screen rather than using a keyboard or mouse. It is normally larger than a mobile phone.

Unified Extensible Firmware Interface (UEFI) The UEFI is a specification that defines a software interface between an operating system and platform firmware. UEFI replaces the Basic Input/Output System (BIOS) firmware interface originally present in all IBM PC-compatible personal computers, with most UEFI firmware implementations providing legacy support for BIOS services. UEFI can support remote diagnostics and repair of computers, even with no operating system installed.

Universal Serial Bus (USB): is a standard that defines the protocols for communication, connection and power supply for devices that are to be connected to computers. Since its advent in the 1990s the number of devices that are now capable of being connected using this protocol has grown and new devices in all sorts of shapes and sizes are now used to store data.

6.2 Report for collection of digital evidence[44]

1	**Date and time**	
2	**Location/address where the activity is conducted**	
3	**Reference/Case number**	
4	**Authority in charge with the case**	
5	**Reference/number of the Authorization/Court Order and Issuing Authority**	
6	**Identification of the person/persons conducting the activity**	
7	**Identification of the person/persons assisting in the activity**	*people identified/arriving at the location*
		suspect/s
		witness/witnesses
		lawyer/s
		others
8	**Description of steps followed and searching activities conducted**	
9	**Description of the site and circumstances in**	*whether these were found functional or not*

[44] **Note:** The appendices in this section are just examples showing which data are proposed to be included in the different reports. The style of report differs significantly in different countries and sometimes even within a country/state or even unit. While these reports come in the style of forms, other countries may demand a continuous text report including embedded media. Thus, the format and content of the reports may vary in accordance with the requirements from the internal regulations and national legislation.

	which the computer systems and digital devices were identified	*whether the peripherals were connected or not*

10	**Description of the evidence identified**	*types, characteristics*

11	**Description of the computer systems and digital devices to be seized**	*types, characteristics*

13	**Indication of whether judicial photos or video recordings were taken**	*identification of the video camera used for this purpose*

14	**Note on custody of the evidence**	*whether the evidence was taken over by the investigator or it remained in other persons' custody*

15	**Time when the activity started/ended**	

16	**Signature of the person/persons who conducted the activity**	

17	**Comments and signature of the person/persons from whom the evidence was seized**	

18	**Comments and signature of the person/persons who assisted at the activity**	

6.3 Report for live data acquisition/imaging

1	**Date and time**	

2	**Location/address where the activity is conducted**	

3	**Reference/Case number**	

4	**Authority in charge with the case**	

5	**Reference/number of the Authorization/Court Order and Issuing Authority**	

6	**Identifications of the person/persons conducting the activity**	

7	**Identifications of the person/persons assisting in the activity**	*people identified/arriving at the location*
		suspect/s
		witness/witnesses
		lawyer/s
		others

8	**Description of the computer systems and**	

	digital devices identified	

9	**Description of the computer systems subject of live acquisition and steps followed for the live acquisition, in chronological order**	*date and time when the functional computer system was identified*	
		details of connection to the computer system	
		date and time of logical and file system copy of the identified computer systems	
		details of hard disk used to save the computer data acquired	
		software applications used to extract volatile information	*software applications used for the extraction of volatile information from the RAM memory*
			software applications used to identify encrypted containers
			software applications used to copy internal hard disk data, ensuring computer data integrity

10	**Identification of the computer systems or digital devices for which the imaging (cloning) is required**	*if applicable*

11	**Identification of the hardware devices/software applications used to image (clone) the computer data**	*if applicable*

12	**Description of the storage media used to export the results obtained following the imaging (cloning)**	*if applicable*

13	**Date and time when the imaging (cloning) started/ended**	*if applicable*

14	**Indication of whether judicial photos or video recordings were taken**	*applications running at the time of computer system identification*
		identification of the video camera used for this purpose

15	**Signature of the person/persons who conducted the activity**	

16	**Comments and signature of the person/persons who assisted at the activity**	

6.4 Report for forensic analysis of computer systems, computer data and digital devices

1	**Date and time**	

2	**Location/address where the activity is conducted**	

3	**Reference/Case number**	

4	**Authority in charge with the case**	

5	**Reference/number of the Authorization/Court Order and Issuing Authority**	

6	**Identification of the person/persons conducting the activity**	

7	**Identification of the person/persons assisting in the activity**	*people identified/arriving at the location*
		suspect/s
		witness/s
		lawyer/s
		others

8	**Description on how the computer systems or digital devices were packaged and sealed**	

9	**Identification of the computer systems or digital devices to be forensically analysed**	

10	**Identification of the hardware devices/software used to clone (imaging) the computer data**	*if applicable*

11	**Date and time when the cloning (imaging) started/ended**	*if applicable*

12	**Description of the storage media used to export the results obtained following the cloning (imaging)**	*if applicable*

13	**Identification of the hardware devices/software applications used for the forensic analysis**	

14	**Date and time when the forensic analysis started/ended**	

15	**Description of the forensic analysis (steps followed) on chronological order**	

16	**Reference to the technical report generated by the software applications used for the forensic analysis**	*if applicable*

17	**Description of the storage media used to export the results obtained following the forensic analysis**	*DVD/Hard disk*

18	**Description of computer systems and digital devices to be packaged and sealed after the forensic analysis**	

19	**Time when the forensic analysis ended**	

20	**Signature of the person/persons who conducted the forensic analysis**	

21	**Comments and signature of the person/persons from whom the evidence was seized**	

22	**Comments and signature of person/persons who assisted at the activity**	