
**SEMESTER 2, AY2024/25 (January 2025)**

# IFS4101: Legal Aspects of Information Security

## Manual on Digital Forensics Investigation

**By: Group 2**

| NAME | STUDENT ID |
|---|---|
| V S Ashok Balaji | AXXXXXXXU |
| Hugo Chia Yong Zhi | AXXXXXXXL |
| Lim Choong Kai Joshua | AXXXXXXXH |
| Regan Choy Tian Fu | AXXXXXXXY |
| Ge Shuqing | AXXXXXXXW |


**Project Title:**
Manual on Digital Forensics Investigation: Bridging Technical and Legal Standards

**Due Date:**
Thursday, 17th April 2025

# 1. Introduction

## 1.1 Foreword

In Singapore's context, there is currently a lack of regulations, guidelines, code of conduct or code of practice governing digital forensics professionals, highlighting a gap in the industry. The aim of this manual is to provide a comprehensive guide for digital forensic investigation that bridges two international practices: *ACPO Good Practice Guide for Digital Evidence* and *Interpol Guidelines For Digital Forensics First Responders*, and align them in Singapore's legal and regulatory framework.

## 1.2 Purpose and Scope

This manual aims to offer support and advice to Digital Forensic practitioners from law enforcement and stakeholders involved in the digital forensics process who wish to better understand the legal landscape governing Singapore's digital forensics handling during the activities of search and seizure for identification and handling of electronic evidence through methods that guarantee their integrity.

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

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

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

## 1.3 Application of Guide

This guide is primarily written for the guidance of Singapore law enforcement personnel who may deal with digital evidence and stakeholders involved in the digital forensics process who wish to better understand the legal landscape governing Singapore's digital forensics handling. This may include but is not limited to:

- Persons who are involved in the securing, seizing and transporting of equipment from search scenes with a view to recovering digital evidence, as well as in the identification of the digital information needed to investigate crime;

- Investigators who plan and manage the identification, presentation and storage of digital evidence, and the use of that evidence;
- Persons who recover and reproduce seized digital evidence and are trained to carry out the function and have relevant training to give evidence in court of their actions. **Persons who have not received appropriate training and are unable to comply with the principles should not carry out this category of activity**;
- Persons who are involved in the selection and management of persons who may be required to assist in the recovery, identification and interpretation of digital evidence.
- Private sector partners and forensics experts collaborating with law enforcement, who must align with Singapore's forensic and legal requirements.

# 2. Fundamental Principles

## 2.1 Principles of Digital Evidence

**Principle 1**: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

**Principle 2**: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

**Principle 3**: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

**Principle 4**: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

## 2.2 Explanation of the Principles

All digital evidence in Singapore is subjected to the **Evidence Act (Cap. 97) ("EA")**, same rules and laws that apply to documentary evidence. All common law concepts which are inconsistent with the Evidence Act are repealed by Section 2(2) of the EA[1].

For evidence to be admissible in court, the evidence must be admitted through one of the provisions under the EA. As evidence can be categorised under Primary or Secondary evidence, each category will require different specifications and provisions to be admissible. The manual will guide users on the steps to take to ensure the evidence collected satisfies the provisions to ensure its admissibility.

The doctrine of documentary evidence may be explained thus: the onus is on the prosecution to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of law enforcement.

Automated processes (e.g. operating systems, cloud synchronization) and other programs frequently alter, add and delete the contents of electronic storage. This may happen automatically without the user necessarily being aware that the data has been changed. Investigators must mitigate risks by using write-blockers and forensic tools approved by the Cyber Security Agency of Singapore (**CSA)** or **Singapore Police Force (SPF).** Where local guidelines are insufficient or unavailable, tools compliant with internationally recognized standards, such as NIST-approved write blockers[2], should be used.

[1] https://www.daslaw.com.sg/overview-of-the-evidence-act-specific-rules-of-evidence/

[2] https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/hardware

In order to comply with the principles of digital evidence, wherever practicable, proportionate and relevant, an image should be made of the device. This will ensure that the original data is preserved, enabling an independent third party to re-examine it and achieve the same result, as noted by principle 3 and to follow the rule of best evidence under Section 66 of the Evidence Act.

This may be a physical / logical block image of the entire device, or a logical file image containing partial or selective data (which may be captured as a result of a triage process). Investigators should use their professional judgement to endeavour to capture all relevant evidence if this approach is adopted.

In cases where dealing with data which is not stored locally but is stored at a remote, possibly inaccessible location it may not be possible to obtain an image. It may become necessary for the original data to be directly accessed to recover the data. With this in mind, it is essential that a person who is competent to retrieve the data and then able to give evidence to a court of law makes any such access. Due consideration must also be given to applicable legislation if data is retrieved which resides in another jurisdiction. Refer to Section 4.5 - Handling Cross-Border Digital Evidence for considerations.

It is essential to display objectivity in a court of law, as well as the continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered, showing each process through which the evidence was obtained. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court.

It should be noted that the application of the principles does not preclude a proportionate approach to the examination of digital evidence. Those making decisions about the conduct of a digital investigation must often make judgments about the focus and scope of an investigation, taking into account available intelligence and investigative resources. This will often include a risk assessment based on technical and non-technical factors, for example the potential evidence which may be held by a particular type of device or the previous offending history of the suspect. Where this is done it should be transparent, decisions should be justifiable and the rationale recorded.

Application of the four principles will also be informed by:

- ACPO Good Practice Guide ACPO Good Practice Guide for Digital Evidence for Digital Evidence 2012
- Interpol Guidelines for digital forensics first responders - Best practices for search and seizure of electronic and digital evidence
- International standards (e.g., NIST Chain-of-Custody).

* There are currently no publicly available code of conduct, code of practice, or guideline specifically for digital forensics professionals in Singapore as of [16 April 2025].

# 3. Planning and Preparation

## 3.1 Roles and Responsibilities

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

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

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

- A preparatory meeting should be held in order to exchange information between the unit in charge of the investigation and the personnel of other specialties that go on a support mission.
- The intervention on the scene of these specialized units should be prioritized and coordinated, which will depend on the specific case under investigation. For example, priority may be given to the action of Canine Units for the detection of explosives or DNA sampling collection prior to any other activity.
- Critical Information Infrastructure (CII) Assessment:
    - Determine if the target system is a CII under Singapore's Cybersecurity Act 2018.
    - If the system is CII, notify the Cyber Security Agency of Singapore (CSA) and comply with mandatory incident reporting obligations.
    - Relevant sections from the Cybersecurity Act will apply to the investigative process

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

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

- Nature of crime under investigation. The nature of the crime will determine the forecast of the necessary equipment and the preparation of the most appropriate technical procedures for each case. For example, for crimes related to child sexual abuse, it is probably necessary to determine, in the same act of search and seizure, the possession of this material, so it will be

necessary to find evidence or obtain the necessary samples (pictures, videos, chat sessions, etc.) "On-site" in an adequate and safe way. In cases of financial crimes, it is very common to find infrastructure networks with user data stored in centralized or cloud servers, so it will be necessary to be clear about what type of electronic documentation is being sought, what is the best method to obtain it and where to store the data captured from those sources.

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

- Location of data storage. It is not unusual for information to be stored in a place other than the physical computer equipment of the suspect. Given this, it is necessary to verify the actual location in order to require an additional legal authorisation, especially if it is stored in a different jurisdiction, or if additional technical equipment is required to ensure the integrity of the evidence. All data that is needed to carry out specific actions in relation to the processing of electronic evidence should be specified in the search warrant application or relevant procedural requirement prior to search and seizure.

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

- The authorization for the seizure
- Obtaining forensic images ("on-site" or not)
- Analysis of the devices "on-site"
- Use of applications to obtain access passwords
- Authorization to change the password of email accounts or social networks, etc.

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

The destination of the seized items must be defined before starting any activity of search and seizure. Forensic copies, as well as devices that require specific treatment, should be sent to the corresponding department/team for processing and analysis. For each case, adequate packaging, transport and documentation must be provided to maintain the chain of custody that begins during the seizure.

Relevant personnel or entities that are related to the evidence should be noted down while digital evidence collection is ongoing. An attesting witness is required to ensure there is proof of execution of the document or logs, in accordance to Section 70 of the Evidence Act. While further inspection of the evidence may be required to identify attesting witnesses, it is still important to note down key entities which may aid in the finding of witnesses.

## 3.2 Search and Seizure Planning

The proliferation of digital devices and the advances in digital communications mean that digital evidence is now present or potentially present in almost every crime.

Digital evidence can be found in a number of different locations:

- Locally on an end-user device – typically a user's computer, mobile/smart phone, satellite navigation system, USB thumb drive, or digital camera;
- On a remote resource that is public – for example websites used for social networking, discussion forums, and newsgroups;
- On a remote resource that is private – an internet Service Provider's logs of users' activity, a mobile phone company's records of customers' billing, a user's webmail account, and increasingly common, a user's remote file storage;
- In transit – for example mobile phone text messages, or voice calls, emails, or internet chat.

It would be quite common for evidence of a crime to be in more than one of the locations mentioned above. However it might be much easier to obtain the evidence from one location rather than another; careful consideration should be given to the resources required to obtain the evidence.

For example, if evidence is required of contact between two mobile phone numbers, the best method would be to obtain call data from Telecommunication Providers, rather than to request a forensic examination of the mobile phones. The call data is likely to be more comprehensive than call logs from a mobile phone and the times and dates can be relied upon, which is not necessarily the case with logs from a mobile phone. Note that this is only applicable for law enforcement or authorised persons under Section 20 of the Criminal Procedure Code.[3] Digital forensic professionals should also note that call logs in Singapore are stored for at least 12 months, in accordance to the Telecommunications Act.

In addition, investigators seeking to capture 'in transit' evidence must be aware of the implications under the Criminal Procedure Code and the need to seek appropriate authorities for doing so.

As a digital forensic practitioner, it is important to understand how cybercrimes are categorised in Singapore, even if core principles like chain-of-custody remain unchanged.

- Cybercrimes are broadly classified as **cyber-dependent** or **cyber-enabled**. This distinction can shape the nature of digital evidence encountered and the investigative techniques required.

- **Cyber-dependent crimes** are offences that rely entirely on computer systems, such as hacking, malware deployment, or distributed denial-of-service (DDoS) attacks. Investigations into these crimes typically involve technical artefacts like system logs, network traffic captures, or malicious code. For instance, the investigator may be required to reverse-engineer malware, trace the origin of unauthorized access, or correlate timestamps across multiple logs to reconstruct an attacker's actions. The investigator should also look out for evidence that suggests the violation of Sections 3 to 6 of the Computer Misuse Act.

[3] Modified this from ACPO to contextualize to Singapore with regards to Telecommunications Providers and Telecommunications Act

- **Cyber-enabled crimes**, on the other hand, are traditional crimes facilitated or amplified by digital tools. A common example is cyber extortion, which might involve threats delivered through messaging apps, social media, or email. In such cases, the focus shifts to recovering and analysing communications, metadata, device traces, or cloud-stored evidence. For example, you might extract chat history from a mobile device, trace IPs or timestamps from messaging platforms, or recover deleted messages.

- Understanding the differences helps you anticipate what types of evidence to collect, which tools to use, and how to tailor your forensic approach to the nature of the offence, thus ensuring your investigation remains both efficient and legally sound within Singapore's legal framework.

With the above in mind, it is important that investigators develop appropriate strategies to identify the existence of digital evidence and to secure and interpret that evidence throughout their investigation.

Due consideration should always be given by the investigators of the benefits to the overall investigation of conducting any digital forensic work. Proportionality should be assessed when a digital forensic strategy is being considered to ensure that limited resources for digital forensic investigations are directed appropriately.

## 3.3 Cross-Border Evidence Request

With reference to Section 9.7 - Mutual Assistance in Criminal Matters Act

### 3.3.1 How to Request for Evidence from Foreign Jurisdiction with MLAT

Although MACMA provides Singapore with the option to request for evidence from abroad/foreign jurisdictions, Mutual Legal Assistance Treaties (MLATs) ensure that there are standardized procedures, clear obligations, and often faster processing of evidence requests. MLATs provide a formal, treaty-based framework that both countries are legally bound to follow. MACMA has specific provisions for "prescribed foreign countries", which are countries with whom Singapore has MLATs or equivalent arrangements. The Attorney-General's Chambers (AGC) serves as Singapore's Central Authority, overseeing the processing of formal Mutual Legal Assistance (MLA) requests in alignment with MACMA and any applicable treaties.

Through MLATs, Singapore can request a range of evidentiary assistance, including:

- Taking witness testimony
- Obtaining digital records (e.g., emails, server logs)
- Executing search and seizure of electronic devices

MLAT requests must adhere to stringent requirements and formatting. They should clearly state the applicable offences, provide detailed descriptions of the sought digital evidence, and explain its relevance. Any time sensitivity, such as upcoming court dates or risks of data deletion, should be explicitly mentioned to expedite execution. In urgent cases, Singapore permits the advance transmission of requests via secure email to the Central Authority, with official originals to follow by mail. Despite these urgent measures, obtaining evidence through MLATs can take weeks or months; thus, clear and complete requests, utilizing provided checklists and forms, tend to be processed more

efficiently. An example form can be found in Appendix 10.5. The list of all forms can be found here: https://www.agc.gov.sg/our-roles/international-law-advisor/mutual-Legal-assistance

### 3.3.2 Request for Evidence from Foreign Jurisdiction without MLAT

Prescribed foreign countries under MACMA are obligated to assist. Assistance from other countries may be rendered on a reciprocity basis, even in the absence of a formal treaty. This undertaking of reciprocity should provide that the requesting country will comply with a future request by Singapore for similar assistance in a criminal matter involving an offence that corresponds to the foreign offence for which assistance is sought.

If the other country does not have MLAT with Singapore, then the following two items should be noted down:

1) Certification standards required in foreign jurisdiction
2) Certification standards of the evidence received.

Digital forensics professionals should ensure that the certification standards of the evidence received should minimally match the certification standards of the foreign jurisdiction, in accordance to Section 88 of the Evidence Act. For example, if the other country's standard for hashing is SHA256, then the evidence received from that country should minimally be SHA256 to be admissible.

## 3.4 Evidence relating to Sensitive Documents

Digital forensics experts should be mindful of the type of documents they encounter. Documents protected under the Official Secrets Act should not be collected as evidence without prior permission as they will not be admissible under Section 126 of the Evidence Act. Permission and clarification should always be sought after from the supervising authority of the document if any doubt is present.

# 4. Digital Evidence Handling Procedure

This section details the protocols and best practices that digital forensics investigators should follow during the collection and preservation of digital evidence.

The authorised digital forensics professional should know that Section 39 of the Criminal Procedure Code and Section 18 of the Computer Misuse Act grant them the legal authority to carry out their investigations.

At all times, digital forensics professionals must make reasonable security arrangements and ensure that the digital evidence is handled in accordance with Personal Data Protection Act (PDPA) Section 24.

## 4.1 Documentation and Chain of Custody

No one should enter the perimeter without having secured the area. People who are in the scene will remain controlled at all times during the operations to avoid any alteration or data compromise. After the area has been secured, teams should document the state of the area prior to evidence collection. This is to support the admissibility and authenticity of the evidence collected in accordance with Section 116A of the Evidence Act. If necessary, photographs can be taken to support the documentation. People allowed at the scene should include those who are authorised under Section 39 of the Criminal Procedure Code and Section 18 of the Computer Misuse Act, which gives the legal authority to carry out the investigations.

All processes to collect and gather the evidence should be duly documented according to Section 37 of the Criminal Procedure Code. To do this, you must keep an exhaustive record of the location and original condition of the devices.

The following examples for proper documentation of the scene:

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

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

For each device, the following data must be documented:

- Type: Computer, hard drive, DVD
- Brand and model
- Storage capacity, indicating if it is MB, GB or TB

- Serial number
- State: Damaged, on, off etc
- Location: stay and specific place
- Security: Access password, PIN
- Comments: Used only by children, not connected to the Internet etc

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

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

- Ensure that all the collected material has been properly registered and labelled before proceeding to its packaging.
- When possible, the original packaging will be used to package and transport the seized devices.
- They have to be uniquely identified, through labelling.
- The label must show whether or not they have been subjected to the cloning/copying process. Suitable material must be used for its sealing to avoid possible manipulation of the devices. The seal must prevent access to internal elements (hard drives or internal memories) both physically and through the connection ports of the equipment.

Depending on their destination, they will be packaged separately, without mixing them with other documentation or other devices. This will facilitate the diligence of the unsealing and acquisition of forensic copies or their direct submission to the laboratory. Each package containing electronic evidence will have on its exterior the identification that shows the nature and origin of the content. The means used for transport and temporary storage must ensure the integrity of the devices sufficiently, protecting them from shocks, and from sources of electromagnetic radiation, heat or humidity that may damage them.

Digital Devices
Handle with care. If placed in a car, place upright where it will not receive serious physical shocks. Keep away from magnetic sources (loudspeakers, heated seats & windows and police radios).

Hard Disks
As for all digital devices, protect from magnetic fields. Place in anti-static bags, tough paper bags or tamper evident cardboard packaging or wrap in paper and place in aerated plastic bags.

Removable Storage
floppy disks, memory sticks, memory cards, CDs/DVDs) Protect from magnetic fields. Do not fold or bend. Do not place labels directly onto floppy disks or CDs/DVDs. Package in tamper-force approved packaging to avoid interaction with the device whilst it is sealed.

Other items
Protect from magnetic fields. Package correctly and seal in plastic bags. Do not allow items to get wet.

Other Considerations

1. If fingerprints or DNA evidence are likely to be required, always consult with the investigator;
2. Using aluminium powder on electronic devices can be dangerous and result in the loss of evidence. Before any examination using this substance, consider all options carefully.

The equipment should be stored at normal room temperature, without being subject to any extremes of humidity and free from magnetic influence such as radio receivers. Dust, smoke, sand, water and oil are also harmful to electronic equipment. Some devices are capable of storing internal data (such as the time and date set on the system) by use of batteries. If the battery is allowed to become flat, internal data will be lost. It is not possible to determine the life expectancy of any one battery. However, this is an important consideration when storing a device for long periods before forensic examination and should be addressed in local policy.

For entities with standard operating procedures (SOP) regarding digital logs generation and storage, such procedure documentation should be requested and referred to. This serves as a basis of what standard circumstance is to be expected for the evidence. If there is a mismatch between the SOP and the actual logs, then foul play is a possibility to consider. This is to further enhance the reliability of the evidence as Section 116A only allows the evidence to be admissible, but does not guarantee that the evidence is compelling.

A chain of custody must be kept and strict procedures must be adhered to in order to maintain the chain of custody and demonstrate integrity and authenticity to preserve the admissibility of the evidence, in accordance with Section 37 of the Criminal Procedure Code and Section 116A of the Evidence Act.

Refer to Appendix 10.4 for a sample Chain-of-Custody Form from NIST.

# 4.2 Identification

### 4.2.1. Crime Scenes

There are many different types of digital media and end-user devices, which may be encountered during a search of a crime scene, all of which have the potential to hold data which may be of value to the investigation. In order to preserve the data and achieve best evidence, these items must be handled and seized appropriately, and should be treated with as much care as any other item that is to be forensically examined. This section is intended to assist individuals to ensure their actions in relation to seizure are correct.

The following guidance deals with the majority of scenarios that may be encountered. The general principles, if adhered to, will ensure the best chance of evidence being recovered in an uncontaminated and, therefore, acceptable manner.

Items found during a search will normally fall into the broad categories of computer-based media items, CCTV systems and mobile devices. These are considered separately below.

### 4.2.2. Proportionality

Before seizing an item, consider whether the item is likely to hold evidence (eg, is this a family computer or a computer belonging to a suspect?) Ensure that details of where the item was found are

recorded. Consider when the offence was committed; when seizing CCTV, give consideration to narrowing down what is seized, by camera and/or time period. Check whether another system may be better placed to record the evidence. Differentiate between mobile phones found on a suspect and phones found in a drawer, as different levels of examination may be possible for these. Also consider that evidence may be stored online, or on an internet service provider's systems, and end-user devices may only be needed to obtain the details necessary to request this evidence from the service provider. If so, it is best to seize items in current usage, i.e. computers connected to the internet.

Digital devices and media should not be seized just because it is there. The person in charge of the search must have reasonable grounds to remove property and there must be justifiable reasons for doing so. The search provisions of Criminal Procedure Code (CPC) and Evidence Act (EA) equally apply to digital devices and media in Singapore. Section 5 of the Evidence Act requires evidence to be relevant to facts in issue or other relevant facts in order for evidence to be admissible. Thus, the investigator must seek to find relevant evidence.

## 4.3 Collection and Acquisition

Digital forensics professionals should be familiar with powers granted under Section 39 (S39) and Section 40 (S40) of the Criminal Procedure Code (CPC) before they visit a crime scene to conduct collection and acquisition, lest they face any obstructions. Obstructions of authorised persons under S39 and S40 are arrestable offences.

Digital forensics professionals that are appointed as an authorised person under S39 of the CPC have the powers to access computers (including making copies of data) and the necessary decryption information (S40 of the CPC) to collect evidence relating to the arrestable offence.

### 4.3.1 Collection and the Handling of Digital Evidence

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

a) If the equipment is on, do not turn it off.
   - Verify installation of anti-forensic systems: local or remote erasing programs, external access. Stop these processes even by pulling the power cable or removing the battery if necessary.
   - Isolate the device from the networks to which it is connected unless you are authorized to access cloud services.
   - Disable screensavers and screen locking in order to prevent the equipment from being hibernated or suspended.
   - Check if the device has any kind of encryption system running (Bitlocker, FileVault, VeraCrypt, PGP Disk, etc.).
   - Check if it is connected to power.

b) If the equipment is turned off, do not turn it on until it is processed with guarantees, as further explained later.
   - Section 40 of the CPC grants authorised persons the power to collect necessary decryption information, thus the suspect's password/pin should be asked and checked if it is correct.

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

The following actions can be performed on the devices:

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

The process performed will have to be documented:

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

**4.3.2 Live Analysis of Powered Computers and Laptops**

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

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

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

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

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

| Volatile Fragment | Windows tools | Linux tools |
|---|---|---|
| RAM content | Dumpit, Winen, Mdd, FTK Imager | dd, fmem |

| | | |
|---|---|---|
| Routing table, ARP cache, Kernel statistics | Route PRINT, arp –a, netstat | netstat –r –n<br>route<br>arp -a |
| DNS cache | Ipconfig/displaydns | mdc dumpdb (if installed) |
| List of running processes | PsList, ListDLLs, CurrProcess, tasklist | ps –ef, Isof |
| Active network connections | - | netstat –a, ifconfig |
| Programs and services using the network | sc queryex, netstat -ab | netstat -tunp |
| Open files | Handle, PsFile, Openfiles, net file | Isof, fuser |
| Network shares | Net share, Dumpsec | showmount –e,<br>showmount –a<br>smbclient -L |
| Open ports | OpenPorts, ports, netstat -an | netstat –an, Isof |
| Connected users | Psloggedon, whoami, ntlast, netusers /l | w, who –T, last |
| Encrypted archives | Manage-bde (Bitlocker), efsinfo (EFS) | mount –v, ls /media |
| Active network shares | Fsinfo, reg (mounted Devices) | mount –v, ls /media |
| Remote accesses and network monitoring | Psloglist | /etc/syslog.conf<br>Port UDP 514 |
| System and network configuration | Systeminfo, msinfo32, ipconfig /all | ifconfig –a<br>netstat -in |
| Storage devices | Reg (Mounted Devices), Net share, netstat -a | mount –v, ls /media |
| Date and time | Time /T, date /T, uptime | time, date, uptime |
| Environment variables | Cmd /c set | env, set |
| Clipboard | pclip | - |
| Disk content | FTK Imager, EnCase, Tableau Imager | dc3dd, ewfacquire, Guymager |

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

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

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

#### 4.3.3. Inability to Access Information on Powered Devices

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

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

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

a) "Cold-boot RAM" technique. It is a technique consisting of freezing the RAM with the equipment on using liquid nitrogen. Once this is done, the computer is turned off and restarted with its own operating system from a CD or pen drive, with tools that manage to dump the RAM. When this memory is frozen in the shutdown process, it keeps the data it had. This technique is based on research carried out by the University of Princeton and might not be useful in an operational environment.
b) Transport the intervened device without turning it off. Another method may be to use portable power systems that keep the equipment on until the arrival at the forensic laboratory where it will be subsequently treated.

## 4.4 Preservation

#### 4.4.1 The Forensic Copy

Section 66 of the Evidence Act provides the Rule of Best Evidence, where preference is given to primary evidence. Thus, it is important that the original evidence is preserved.

One of the main premises in the forensic analysis process warns that, excluding exceptional cases, an examination of the evidence should not be performed using the original device. Therefore, it will be required to copy or clone the data contained in the original device, to avoid compromising its integrity.

Digital evidence can be considered as primary evidence if it is shown to reflect the document accurately, as described in explanation 3 as given in Section 64 of the Evidence Act.

For copies to be regarded as primary evidence, hashing algorithms used to prove the integrity of the copies should meet the legal standards of Singapore. The hash value should then be noted down before analysis is conducted. This is in accordance with Section 81 of the Evidence Act for copies of digital evidence to be regarded as genuine.

The forensic experts will then use the imaged/copied data to perform the analysis.
This copy must be an exact bit-by-bit replica of the original device, regardless of its content.

This process can be done in two formats:

a) Device to Device (clone): This can be performed by obtaining an exact bit-by-bit replica of an original device in another - previously wiped - device with equal or greater capacity.
b) Device to File (image): This can be performed by generating one or more files that contain, linked together, an identical copy of the original device. The most widespread is "dd" (raw) or "E01" formats.

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

Advantages of creating image files:

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

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

**4.4.2 Alternatives to the Forensic Copy**

Digital forensics professionals should ideally first attempt to get hold of the forensic copy for it will serve as primary evidence and has higher weight in court. While there are scenarios in which it will not always be possible to obtain an exact physical or digital copy, professionals should still note down the process and attempts in obtaining the genuine copy of the digital asset as such alternatives to the forensic copy will be considered as secondary evidence. Noting down the circumstance that illustrates why the primary evidence is not available and enables the alternatives to the forensic copy to be admissible in court under Section 67 of the Evidence Act.

Alternatives to the forensic copy can be bit by bit, of the entire source device, such as the acquisition of files or information from servers, NAS, virtual disks or encrypted volumes.

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

a) Logical copy of volumes. This method is applied, for example, when it is needed to acquire the content of an encrypted volume that is being used on a powered computer. To preserve that information, a logical copy of the volume will be produced. By making a physical copy of the disk, a partition would be obtained that would be unreadable since the data is encrypted. However, the logical copy allows the user to acquire the content in the same way the user accesses it.
b) Logical copy of files. It is performed by generating, using suitable software, a replica of the original data after selecting what may be of interest to the investigation. For example, in a business environment, we can make a logical copy of the suspect user's folder. The drawback is that the file-slack space in our copy will be lost, and the metadata of the original file system may not always be maintained.

Making forensic logical copies does not prevent the properties of the evidence from being maintained. Whenever it is carried out, use the appropriate tool and method, protect against writing, preserve metadata as much as possible and use a cryptographic algorithm that allows verifying the integrity of the acquired data.

### 4.4.3 Hash function

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

In order for a copy of digital evidence to be considered primary evidence, it must be shown to reflect the original accurately. Thus, it is important for the forensic investigator to make use of hash functions to show that the integrity of the digital evidence has been preserved.

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

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

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

## 4.5 Handling Cross-Border Digital Evidence

### 4.5.1 Admissibility of Cross-Border Digital Evidence

Countries with which Singapore has an existing MLAT are gazetted as “prescribed foreign countries” under the Act. Such countries may be rendered assistance in accordance with the terms of the Act and relevant MLAT. (agc, n.d). With reference to 9.7 - MACMA and 3.3 - MLATs, evidence obtained through Mutual Legal Assistance (MLA) Requests are assumed to be admissible in Singaporean court.

If the other country does not have MLAT with Singapore, then the following two items should be noted down:

1) Certification standards required in foreign jurisdiction
2) Certification standards of the evidence received.

Digital forensics professionals should ensure that the certification standards of the evidence received should minimally match the certification standards of the foreign jurisdiction. For example, if the other country's standard for hashing is SHA256, then the evidence received from that country should minimally be SHA256 to be admissible.

### 4.5.2 Chain-Of-Custody for Cross-Border Digital Evidence

Here are the steps to follow to maintain Chain-Of-Custody:

1. Initial Collection (At the Foreign Source)
    - Adhere to Standardized Procedures:
        - Use MLAT/MLA request protocols as mandated under MACMA.
        - Employ forensic tools (e.g., write blockers, live data capture solutions) to capture volatile data (RAM, temporary files) immediately.
    - Document Collection Details:
        - Record the exact date, time, and location of evidence collection.
        - Note the methods, tools, and personnel involved.
        - Create a preliminary evidence log or fingerprint report at the time of collection.
2. Secured Packaging and Digital Preservation
    - Physical Media:
        - Use tamper-evident containers for physical storage devices (e.g., hard drives, USB devices).
        - Label containers with collection details and unique identifiers.
    - Electronic Evidence:
        - Create complete forensic images using validated tools.
        - Immediately generate cryptographic hashes (e.g., SHA-256) to serve as digital fingerprints.
        - Encrypt digital copies before transmission.
3. Controlled Transfer and Handovers
    - Secure Logistics:
        - Transfer evidence via secure channels (e.g., encrypted digital transfer or secure courier services).
        - Ensure that all electronic transmissions use end-to-end encryption.
    - Handover Documentation:
        - Complete handover records are required at each transfer point.
        - Include detailed signatures, dates, and times, establishing an unbroken chain-of-custody.
    - Central Authority Involvement:
        - The Attorney-General's Chambers (AGC) functions as the Central Authority under MACMA; evidence transmissions should be coordinated and verified by the AGC.
4. Storage and Preservation in Singapore
    - Secure Storage Facilities:

        - Store evidence in an accredited forensic laboratory with controlled access.
        - Maintain secure, access-controlled storage areas with environmental safeguards.
    - Continued Documentation:
        - Update the chain-of-custody log every time evidence is accessed or reviewed.
        - Use electronic logs where possible for automated tracking and auditing purposes.
    - Regular Audits:
        - Periodically verify that all records are intact, and the evidence remains in its original condition.
5. Final Preparation for Court Admissibility
    - Comprehensive Evidence Package:
        - Compile forensic reports that include all logs, hash values, and transfer records.
        - Ensure that all documentation meets both domestic and international evidentiary standards.
    - Readiness for Testimony:
        - Forensic analysts should be prepared to explain each step of the chain-of-custody process in court.
        - Documentation should support that no tampering occurred throughout the handling process.

# 5. Analysis

## 5.1 Analysis of Data

Devices seized as part of a search will typically be submitted to the Technology Crime Forensics Branch (TCFB) of the Singapore Police Force (SPF) or other relevant forensic units. Due to the volume and complexity of data stored on digital devices, it is not possible or desirable to extract all data held on a device for review by investigators. Instead, a forensic strategy needs to be formulated to enable the examination to be focused on the relevant data.

Section 7 of this manual provides guidelines for digital forensic examinations involving computers and mobile devices. These practices should be consulted for detailed guidance on conducting forensic examinations while ensuring adherence to the Evidence Act (EA) to maintain the integrity and admissibility of digital evidence. Other types of digital examinations should follow the same principles, briefly summarised below.

The investigator needs to properly consider the nature and purpose of the digital examination. The investigator must be clear on what priorities are placed on the examination as it may well be that key information needs to be found in order to preserve evidence that may exist elsewhere. For example, an investigator might be interested to find evidence of the violation of Sections 3 to 6 of the Computer Misuse Act.

When submitting evidence, investigators must supply specific requirements. It is not practically possible to examine every item of digital data and clear tasking is needed to ensure that the digital forensic practitioner has the best chance of finding any evidence which is relevant to the investigation.

For more complex or lengthy investigations, an initial triage/review of the digital evidence (whether or not this is done using a specific triage tool) will give investigators and practitioners a better understanding of the nature of the digital evidence held. The forensic strategy should be regularly reviewed to take account of any changes in the direction of the investigation, which may occur as a result of digital forensic examination (for example, finding emails identifying a co-conspirator) or investigations elsewhere (a witness identifying another person as being of interest to the investigation). For this reason it is vital that the investigator and the digital forensic practitioner communicate regularly regarding the progress of the investigation.

Should an evidence be considered to be used as evidence in court, digital forensics professionals should also identify potential attesting witnesses from the digital evidence. As required by Section 70 of the Evidence Act, proof of execution must be provided before evidence is admissible in court. For example, if a particular email is required as digital evidence in court, then the sender of the email will be considered as an attesting witness for he can prove that he sent the email. It is important to note that there can be multiple attesting witnesses for one evidence, hence it is advised to find as many of such witnesses or relevant parties should some be unavailable to attest in court.

If initial examination results in a large amount of data to be reviewed, consideration must be given to who is best placed to review that data. Often this will be the investigator, due to their greater knowledge of the case. Dependent on the source, this data may include:

- Internet history records;
- E-mails;
- Instant Messaging Logs;
- Media files (images and videos);
- Text documents;
- Spreadsheets;
- CCTV;
- Text Messages.

Collaboration with the SPF TCFB or digital forensic practitioners increases the likelihood that the significance of any reviewed data is not misunderstood. For example, when reviewing keyword hits which exist in deleted files, the significance of a hit's location may need explanation from a digital forensic practitioner.

For mobile phone examinations, different levels of examination may be appropriate depending on the intelligence relating to the device and the requirements of the investigation. For example, a phone which has been found in a drawer may be examined only to retrieve the necessary information to request billing details and to establish whether it is owned by the suspect (level 1). A phone which is known to be in regular use by a suspect in a high profile investigation may be subject to a much more in-depth examination involving the retrieval of deleted data and potentially the physical removal and examination of memory chips (level 4).

## 5.2 Interpretation of Digital Data

As with other forensic evidence, interpretation is often required to ensure the evidential weight of recovered digital evidence is clear. Practitioners who undertake the interpretation of digital data must be competent to do so and have had sufficient training to undertake the task assigned to them.

As an example, the presence of indecent images of children on a computer would not in itself be sufficient evidence of possession, as the possessor must be aware of the existence of the images to demonstrate intent. A digital forensic practitioner may interpret the presence of other digital evidence (such as a list of recently opened files, recent search terms, the name and location of folders/files containing the material, or whether or not the computer is password protected) to establish the likelihood of the user being aware of the existence of these images.

Establishing the provenance of digital evidence is another key task of the forensic practitioner, who must use their knowledge and skills to identify not just that the evidence exists but also how it came to be there. This is common to all forensic disciplines; for example, the presence of a defendant's fingerprint on a bottle at the crime scene may not have any bearing on whether the defendant committed the crime if the bottle may have been carried there by someone else. It is the responsibility of the practitioner to carry out analysis to identify provenance where necessary, to mitigate the risk of their findings being misinterpreted.

There is also a possibility that digital forensics professionals will encounter corrupted or illegible content. Professionals should still handle the evidence with care and adhere to the same stringent chain of custody. Whenever necessary, the use of professionals experienced in the field are

recommended and allowed to make sense of the corrupted data and add in explanations to clarify the content.

Often the role of the digital forensic practitioner will be to make investigators and prosecutors aware of the limitations of the digital evidence as well as its strengths.

It must also be borne in mind that the development of digital technology is dynamic and the practitioners may well face significant challenges to their knowledge. It is not possible to be an expert in all aspects of digital forensic examination, but a practitioner should be aware of the limits of their knowledge and where further research or additional specialist knowledge is required.

# 6. Present

Communication of the results of a digital forensic examination may be through a number of means:

- Verbally to an investigator/officer throughout a case;
- By a statement or report on conclusion of the case;
- In court if witness evidence is required.

In all cases a digital forensic practitioner must be aware of their duty of impartiality and that they must communicate both the extent and the limitations of the digital forensic evidence. This is especially important as, due to the nature of digital forensic evidence, it is not always immediately understandable by the layman.

## 6.1 Verbal Feedback

This should be given regularly throughout the progress of an examination. In this way it will enable the investigator to pursue relevant lines of enquiry as these become evident, and will ensure that the practitioner is up-to-date with any information required to better target their investigation.

It is important that this communication be recorded for potential disclosure at a later date. Good practice would be for a verbal conversation to be followed up via email, or to be recorded in contemporaneous notes.

## 6.2 Statements or Reports

The statement or report is the ultimate product of the examination. It should outline the examination process and the significant data recovered. Whilst an initial report may be relatively brief, the practitioner should be in a position to produce a full technical report should one later be required.

The report should be written to be understandable to the reader; this may include the use of a glossary, diagrams/screenshots to illustrate points, the use of examples and avoidance of technical jargon.

When particular items are reproduced in a report, care should be taken to ensure that the representation is accurate. For example, pictures should not be reproduced at a larger size without this being made clear in the report. If a report is produced digitally, items should be reproduced where possible in their original file formats, to ensure that those viewing will see the item as close as possible to its original appearance. If this is not appropriate (for example, if a file needs to be converted to a more common format for reviewing) then the fact that it has been converted must be stated in the report. Where it is not possible to reproduce the item as it would have originally been viewed, for example, when a webpage is retrieved some time after the original page was accessed, this must also be clearly stated in the report.

The report should make clear the strength of any conclusions reached and always identify where an opinion is being given, to distinguish this from fact. Where opinion evidence is provided, the practitioner must state the facts on which this is based, and how he or she came to this conclusion.

## 6.3 Witness Evidence

A practitioner may need to testify about not only the conduct of the examination, but also the validity of the procedure and their experience and qualifications to conduct the examination.

Expert witness training should be considered for digital forensic practitioners so they are familiar with the process of giving evidence and aware of their responsibilities as witnesses. A digital forensic practitioner will not always be giving expert evidence and should clearly understand the distinction between expert evidence and evidence of fact.

When giving evidence, practitioners must make clear when they are expressing facts and when they are giving opinions, as above. Practitioners, when giving expert evidence, must take care to do so only where it relates to their own area of expertise and remember that their duty when giving evidence (whether it be in report form or as a witness) is to the court, regardless of which party has instructed them.

## 6.4 Contemporaneous Notes

It is worth repeating at this point that full records should be made of all actions taken. These must be disclosed to the defence who may subsequently cause a further examination to be conducted. A significant part of such an examination will be to validate the actions and results of the original examination. Such records are also part of the unused material for the case under investigation.

# 7. Specific Evidence Collection Cases

## 7.1 Mobile Devices

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

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

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

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

### 7.1.1. Considerations when securing mobile phone evidence

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

- **Incoming and Outgoing Signals** – Attempts should be made to block incoming and outgoing signals of a mobile device. A common method includes Radio Frequency (RF) blocking containers (e.g., Faraday bag or room). RF signal blocking containers may not always be successful. They may drain the battery and failure may result in data alteration.
- **Cables** – Data cables can be unique to a particular device and forensic tool.
- **Destruction of Data** – There are methods to destroy data locally and remotely on a mobile device. This is why the device must be isolated from all networks (e.g., carrier, Wi-Fi, Bluetooth) as soon as possible. Examiners should be cognizant that a mobile operating system may have automated processes which will destroy data on power-on, or after a specific duration of time, and choose an extraction method or schedule that addresses these concerns, where applicable.
- **Drivers** – Conflicts may occur due to existing operating system drivers, proprietary drivers, driver version inconsistencies, and vendor-specific drivers. Ability to find proper drivers may be difficult. Drivers may be included with a forensic tool or downloaded from a website. Drivers may compete for control for the same resource if more than one forensic product is installed on the analysis machine.
- **Dynamic Nature of the Data** – Data on active (powered-on) mobile devices is constantly changing. There are no write-blocking methods for mobile devices.
- **Encryption** – Data may be stored in an encrypted state preventing access or analysis.
- **Equipment** – Equipment used during examinations may not be the most recent version due to a variety of reasons, such as purchasing/budgeting delays or verification requirements of hardware, firmware, or software.

- **Field analysis** – Triaging mobile devices is not considered a full examination. However, if triage is performed, the device should be protected and isolated from all networks.
- **Inconsistent Industry Standards** – Manufacturers and carriers may use proprietary methods to store data (e.g., closed operating systems, proprietary data connections).
- **Loss of Power** – Many mobile devices may lose data or initiate additional security measures once powered off.
- **Passwords** – Authentication mechanisms can restrict access to a device and its data. Traditional password cracking methods can lead to permanent inaccessibility or destruction of data.
- **Removable Media Cards** – Processing media cards while still inside the device poses risks (e.g., not obtaining all data including the deleted data, altering date/time stamps).
- **Identity Module e.g., USIM, CSIM, RUIM Cards** – Lack of or removal of an identity module may prevent the examiner from accessing data stored on the internal memory of a handset. Inserting an identity module from another device may cause loss of data.
- **Training** – The individual collecting, examining, and analyzing a mobile device should be trained to preserve and maintain data integrity.
- **Unallocated Data / Deleted Data** – Mobile device forensic tools may support only a logical acquisition of data that may limit the amount of data that can be recovered.

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

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

**7.1.2. Mobile Phone Evidence Preservation Process for First Responders**
The following flow charts provide a basic overview of the best practices for preserving evidence when seizing particular types of mobile devices and are not meant to be all-encompassing.

* This guidance is replicated from the Scientific Working Group on Digital Evidence (SWGDE) Best Practice for Mobile Device Evidence Collection and Preservation Handling and Acquisition Scientific Working Group DE v1.9 (dated 2020-09-17). It is the readers' responsibility to ensure they have the most current version of the document. Please see swgde.org/documents/published for more information.

Circumstances may warrant deviation from the procedures outlined herein. Subjects should not be access to the device (e.g., subject applies biometric identifiers or enters a passcode)

### 7.1.3. iOS Preservation Process and Flowchart

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

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

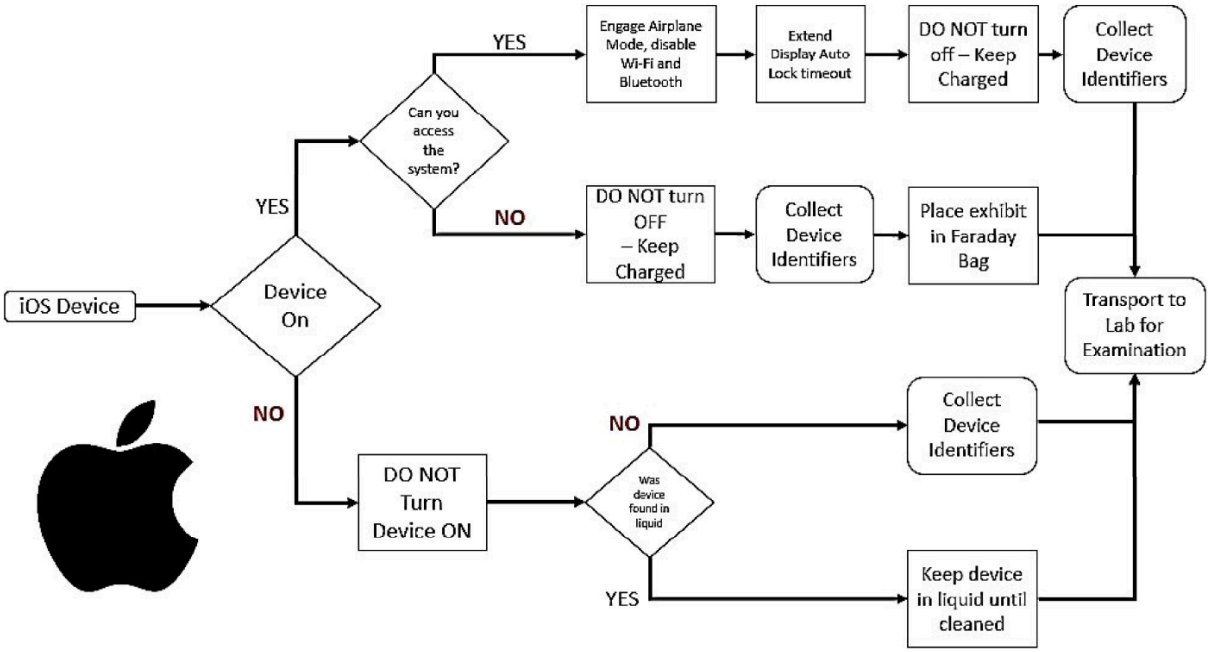


Figure 1: Flowchart for Apple iOS device evidence acquisition procedure (Interpol)

The flow chart above is not all-inclusive for all versions of iOS. Version specific expertise may be necessary in order to obtain access and may alter the foregoing workflow. If the device is powered on, it may contain volatile data, including encryption keys, and should not be turned off.

A power source should be connected as soon as possible to prevent the device from powering down. Be sure to seize the charging cable to keep power to the device. It may be possible to adjust the Display Auto-Lock feature to extend the length of time before Auto-Lock is enabled.

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

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

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

### 7.1.4. Android Preservation Process and Flowchart

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

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

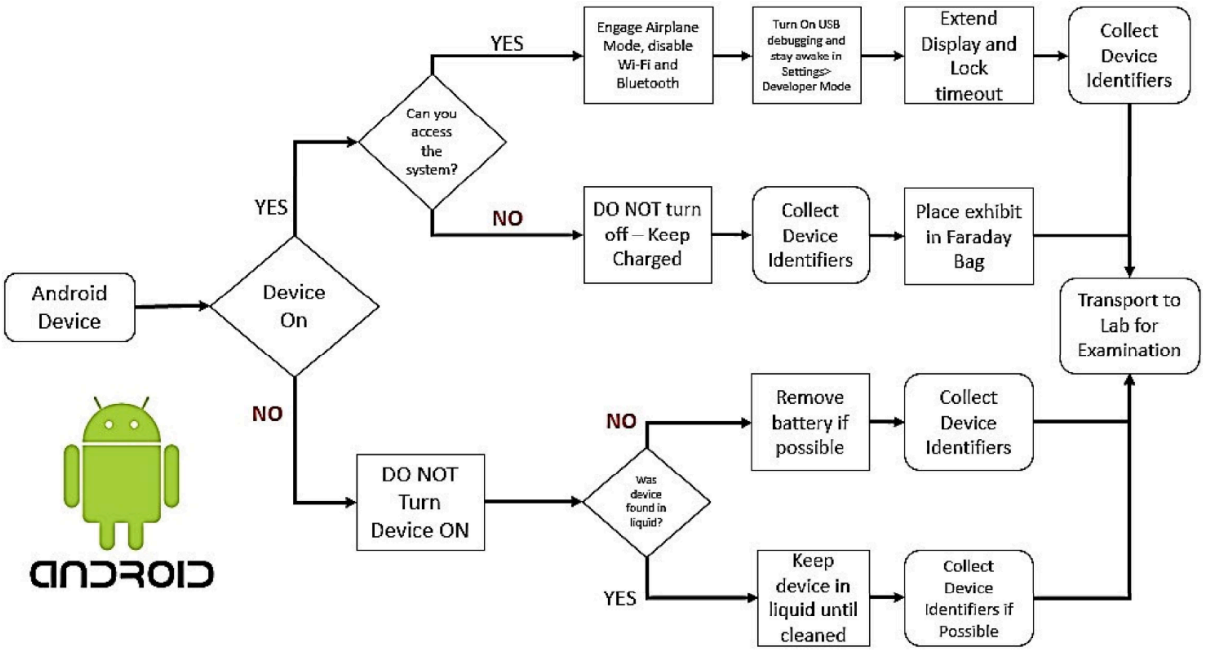


Figure 2: Flowchart for Android device evidence acquisition procedure (Interpol)

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

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

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

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

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

### 7.1.5. SIM Card

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

### 7.1.6. Removable Media Card

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

### 7.1.7. Cloud Data

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

### 7.1.8. Considerations upon Seizure

*Traditional Forensics*

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

*Access*

User-created passwords also complicate the recovery of mobile device data. Collect and document this information if possible. Section 40 of the CPC grants authorised persons the power to collect necessary decryption information.

*Network Isolation*

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

Generally, examiners isolated a mobile device from network connectivity by placing the device in “airplane mode”. The “airplane mode” feature in newer versions of mobile operating systems may not

disable Bluetooth, Wi-Fi, and other wireless protocols or may only disconnect them temporarily. Examiners should manually confirm that network connectivity has been disabled or consider alternate means of isolation, including placing the device in an RF shielded enclosure, removing the SIM card from the device or utilizing a Cellular Network Isolation Card (CNIC) for GSM phones.

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

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

*Points to Prove*
The responder should also consider points to prove for the investigation when submitting the device to the digital forensics lab as smartphones contain lots of data and not all data will be pertinent to the case, and only relevant evidence will be admissible under Section 5 of the Evidence Act.

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

How to proceed:
**a) The device is on.**

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

**b) The device is off.**

- Check if support is available for acquiring a forensic image.
- The battery is removed and the items to be checked are located: SIM card and external memory.
- A SIM / USIM card is read by checking if it is protected by a PIN. If available, it is entered only once, because if it is tried 3 times without success, it is blocked. To unlock it, you will need the PUK code, which is located on the original cardholder or that can be requested from the mobile service provider. In any case, the ICCID (Integrated Circuit Card Identifier) will be obtained, which is its serial number.

- A blank SIM card is recorded with the original SIM card data and inserted into the terminal. The phone associates call logs, settings and other data with the SIM card. If a mobile phone is started with another card or without a card, this information cannot be accessed. The card generated as a copy of the original guarantees, in addition to keeping this data that the device will not connect to the network.
- A forensic copy is made of the memory card, if any, following the procedure proposed for this type of storage media.
- The device is recomposed, turned on and a logical image is extracted following the system instructions.
- If it is supported, a physical image is also made.
- All elements are sealed together and marked as processed.
- Try to locate and create a record of original containers and SIM cardholders with visible PIN and PUK.

## 7.2 Computers

### 7.2.1. Personal Computers

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

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

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

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

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

**a) If the device is switched on**

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

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

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

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

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

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

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

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

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

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

**b) If the device is switched off**
Forensic copies or direct seizure of the equipment will be obtained.

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

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

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

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

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

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

General rules explained before will also be considered:

- After documenting the status and situation in which the equipment is found, the entire device is sealed. In this way, we ensure that they contain all the elements that can store information.
- Disassembling the equipment is not always straightforward. Do not do it on-site if you are not familiar and have the proper tools.
- The availability of the original hardware in the laboratory can be very useful. For example, if the computer has some kind of special elements, such as a RAID disk controller, TPM encryption chip or any other particular element that may be necessary for the reconstruction of the information. It can also make it possible to perform a live boot of the equipment in the laboratory, for example, to study the presence and behaviour of some type of malware infection.
- In case of simple or standardized equipment, it will not be necessary to seize the complete equipment and it will be enough to seize the data storage media, since there will not be compatibility issues.
- As a general rule, those media that do not provide research value are not seized. In principle, peripherals, monitors, mice, keyboards and their cables are not necessary, unless they do not correspond to the usual ones for connection types, to be proprietary models of a brand for example or, because they are already obsolete and difficult to find today. So, they can be useful in the analysis phases.
- Most user-level printers do not contain useful information. However, they can have limited memory that can be analyzed in the laboratory in exceptional cases.

### 7.2.2. Laptops

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

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

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

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

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

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

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

## 7.3 Storage Media

**(memory cards, flash drives, external hard drives, optical discs, etc.)**

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

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

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

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

How to proceed:

**a) Forensic image**

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

As for external hard drives, it is possible to extract the internal disk it contains, to perform the copying process directly on that element. This procedure requires the corresponding documentation process, both of the internal disk and of the enclosure that contains it, as previously seen.
Once the evidence is connected to the write-blocker and the latter to the forensic station, a forensic image can be made.

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

**b) Evaluation (Triage)**

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

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

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

## 7.4 Websites, Forums, and Blogs

Where a crime involves evidence displayed on a website the most convenient method of recovering the evidence may be by engaging the assistance of suitably trained staff to visit the website and take copies of the evidential content. In order to do this the officer taking report of the matter needs to obtain the address of the website, for example, http://www.example.com, or if it is a specific page within the site, http://www.example.com/home.

When carrying out any evidence recovery it is essential that an audit trail of all activity carried out by the investigator is recorded in a log. The recommended method for copying a website is to visit the

site and record the relevant pages using video capture software so there is a visible representation of how they look when visited at the time. If video capture software is not available then the pages can be saved as screenshots. It is also advisable to follow this by capturing the web pages themselves either by using website copying software or saving the individual pages. Copying the pages themselves, as well as obtaining a visual record, means that the code from the web pages is also secured should that become relevant later.

This work should be conducted from a computer which has been specifically set up to be non-attributable on the Internet. Failure to use an appropriate system may lead to the compromise of other police operations. Anyone visiting a website generally exposes a certain amount of information to the website, for example it is common on police systems to have a web browser which is branded with the force's name. This branding is exposed to a website being visited and so may be recorded in logs on the site along with other information amongst which, will include the pages visited.

If it appears likely that the evidence on the website might be lost by a delay in carrying out the above procedures then the person reporting may be asked to make a copy of the evidence by whatever means they are capable of (either printing, screenshot or saving pages), alternatively this could be done by the person receiving the report. Before taking these steps every effort should be made to secure the services of a competent person to carry out this work as failing to capture the information correctly could have a detrimental impact on the investigation.

Where there is difficulty in capturing the evidence by visiting the site it might be possible to make an official request to the owner of the site by legal procedures specified in Section 9, or advised by the SPF TCFB or AGC.

By making a request to the service provider hosting the site it may be possible to recover evidence of who has created the web page or posting. It is not unusual for details of the user such as name, address, phone number, banking details, email address, and alternative email address to be recorded by a host.

If there is a requirement to identify who has committed some activity on a website, for example where a fraud has been committed by purchasing goods from a website or by posting a message on a website, the likelihood is that the suspect may be traceable from logs on the site. When any user accesses the Internet they are allocated a unique address known as an IP address and their Internet Service Provider (ISP) keeps logs of the times and dates and the identity of the user allocated any IP address.

When a user visits a site and conducts some activity, for example logs on, posts a message, or makes a purchase, it is likely that the user’s IP address has been logged by the website. It is often possible to obtain copies of logs from websites if there is a requirement to see who has been active on a website by making a request via SPF Technology Crime Division (TCD) or AGC.

If the evidence is no longer available to be retrieved by any of the above means, and where the use of resources can be justified by the seriousness of the case, it may be possible to recover evidence of the site contents from an end user device that has been used to view the site by conducting a forensic examination of the device.

Where investigators wish to carry out open source intelligence research on the Internet they should be trained to do so and conduct the research from a computer which cannot be attributed to the investigator's agency.

**Covert Interaction on the Internet**

In circumstances where investigators wish to communicate covertly with an online suspect they MUST coordinate with the SPF TCD or other authorized units trained in digital undercover operations. These officers operate under strict legal protocols, including the Evidence Act and Criminal Procedure Code (Refer to Section 9), which govern lawful interception and online evidence collection. All such operations require prior authorization from the Attorney-General's Chambers (AGC) or relevant judicial bodies to ensure compliance with Singapore's laws on privacy and investigative powers. Unauthorized undercover engagement may compromise evidence and violate statutory safeguards.

**Crimes involving email communication**

There are generally two methods of sending and receiving email, one by using a web browser and accessing email online for example at the Hotmail, Windows Live, Yahoo or Google websites. In these circumstances the mail is stored on the webmail server and is read through the user's browser. The other method is to access email using a program such as Outlook or Windows Mail to download mail to the user's computer. The program is used to view and store the emails locally.

Where the evidence in a case involves an email sent from a person who the police want to trace the key evidence is usually found in what is known as the email's "Full Internet Header". Each email sent over the Internet contains this header which is normally not visible to the user. It contains details of the route taken across the Internet by the email and includes the IP address of the sender. Even where an email has been sent with a fictitious email address which has been registered with false details, it is often possible to identify the sender from the Full Internet Header.

In order to obtain the Full Internet Header the person taking the incident report needs to ascertain which of the two methods the recipient uses to access their email. Where it is web based identify the webmail host (i.e. Hotmail, Yahoo etc.) or if by a program on the computer ascertain what program and version number of the program. The version number can usually be found in the program's Help on the menu bar under an item called "About".

Each webmail provider and email program treat the Full Internet Header differently and if the officer or user does not know how to display the header the details of the webmail provider or program need to be passed to a specialist in the SPF TCFB or other relevant forensic units who will be able to provide advice.

Once the header has been exposed the relevant email should be printed together with the header, and may also be saved electronically. Depending upon the seriousness of the case and the volume of email evidence, advice may be sought from the SPF TCFB on the most appropriate method of securing and retaining the email evidence.

Once the full header has been obtained the SPF TCD will be able to use this to conduct enquiries to attempt to identify the sender from the originating IP address.

Where an email address of a suspect is known but there is no email available from which a full header can be obtained, it may be possible to identify the user of the email address and their location. Depending upon the email service provider various details of the user may be recorded together with the first registration IP address and a varying period of IP address login history. These details may be obtained by making an appropriate request for the email address. In conducting such enquiries it needs to be recognised that it is a trivial exercise to send an email with a false email address in the "From:" field of an email.

On some occasions the investigating agency might access a user's email account with written and informed consent from the user in order to secure evidence, in accordance with relevant provisions of the Evidence Act (EA) and Criminal Procedure Code (CPC), which can be found in Section 9. Where this is the case, if third party material is exposed as a consequence of viewing the user's emails, investigators should assess whether further legal authority, such as a production order, search warrant, or a request under the Telecommunications Act, should be in place in addition to the user's consent. The mere possession of login credentials (e.g., obtained during forensic imaging) does not by itself constitute lawful authority to access or search the contents of an account. Investigators must ensure they have obtained the appropriate legal authority and document such access accordingly to preserve the chain of custody and the admissibility of evidence.

## 7.5 Social Network Sites

Priority – Establish the use of Social Networking, Online Communities, Online Storage and other Cloud Services by witnesses and suspects. Whilst this may be revealed by the examination of seized devices it may be gleaned more quickly if asked during interview.

Many current investigations involve Social Networking Sites. It is imperative that early consideration is made around securing Social Networking Profiles that fall within the investigation. The best evidence is available from the service provider however they are often located outside of Singapore and may or may not secure the content on the appropriate request via the AGC (refer to Section 3.3 on evidence from foreign jurisdictions). As such the investigator should always secure a copy of what is seen by them as this may be the only opportunity to secure this evidence before it changes.

## 7.6 Servers

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

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

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

What does the Court order/relevant legal authorization permit? Servers can be a fundamental part of the normal development of a company's activity, which does not have to be necessarily involved in the

commission of the criminal act. Is it justified to leave an organization, possibly extraneous to the crime, without service? Is the equipment seizure really needed?

Under the Cybersecurity Act, CII owners are required to maintain a certain level of operations. Hence, digital forensics professionals should consider what evidence can be taken while ensuring a level of operations such as servers is still up and running. Digital forensics professionals should consult with relevant stakeholders such as CII owners to be aware of equipment that requires more special attention. As much as possible, the digital forensics collection process should not interfere with the operations of a CII.

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

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

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

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

## 7.7 Network Forensics

**Home and corporate network environments**
Networks of computers are becoming more common in the domestic environment and are well established in corporate settings. In the home, they are usually based around the broadband Internet connection, which often also offers functionality to set up a small internal (and often wireless) network within the household. In corporate environments, more advanced network setups can be found, for which no generic description can be given.

The use of wireless networks in both the corporate and home environment is also increasing at a considerable rate. To the forensic investigator, this presents a number of challenges and an increased number of potential artefacts to consider. Owing to the potential complexity of ‘technical’ crime scenes, specialist advice should be sought when planning the digital evidence aspect of the forensic strategy.

**Wireless devices**
A whole range of wired and wireless devices may be encountered:

- Network devices which connect individual systems or provide network functionality: Switches, hubs, routers, firewalls (or devices which combine all three).
- Devices to connect individual computers to the network, such as network cards (which can also be embedded within the computer)
- Devices to set up a wireless network: Wireless Access Points.
- Printers and digital cameras.
- Bluetooth (small range wireless) devices – PDAs, mobile phones, dongles.

- Hard drives which can be connected to the network.

Wireless networks cannot be controlled in the same way as a traditionally cabled solution and are potentially accessible by anyone within radio range. The implications of this should be carefully considered when planning a search or developing the wider investigative strategy. A device, such as a computer or a hard drive, may not be located on the premises where the search and seizure is conducted.

**Home networks and data**

If devices are networked, it may not be immediately obvious where the computer files and data, which are being sought, are kept. Data could be on any one of them. Networks, both wired and wireless, also enable the users of the computers to share resources; such as printers, scanners and connections to the Internet. It may well be the case that if one of the computers is connected to the Internet, some or all of the others are also.

With the widespread use of broadband type Internet subscriptions such as ADSL and cable, the Internet connection is nowadays likely to be of an 'always on' type connection. This implies that even if no-one is apparently working on a computer or using the Internet, there may be data passing to and from computers or between the network and the Internet.

If a wired network is present, there will usually be a small box (called a 'hub' or a 'switch') also present, connecting the computers together. Hubs, switches and routers look very much the same as one another. The network cables are usually connected at the rear.

The network may also be connected to another device (called a Cable Modem or a ADSL Modem) providing access to the Internet. Sometimes, the hub/switch/router mentioned before are combined with these modems in one device.

One wire from a modem will usually be connected to the telephone or television cable system and another wire will be connected either to one of the computers present or directly to the network hub, or the modem itself may be incorporated within the hub in a modem/router.

**Operation planning in networked environments**

When planning an operation involving a network, consider carefully the possibility of remote access, i.e. person(s) accessing a network with or without permissions from outside the target premises. Investigators should consider the possibility of nefarious activity being carried out through the insecure network of an innocent party. The implications of such a scenario are that search warrants could be obtained on the basis of a resolved Internet Protocol address, which actually relates to an innocent party. The implications are potentially unlawful searches, legal action taken against the relevant investigative agency and a waste of resources.

Consider also the possibility of a computer's access to remote online storage, which may physically reside in a foreign jurisdiction. This can include web-based services for email, photo or document storage or other applications offered via the Internet. There will be legal issues in relation to accessing any such material. Legal advice should be sought prior to any access or retrieval and often the provider of the particular service will have to be contacted to ensure that material is preserved while the relevant mutual legal assistance requests are being arranged.

**Network detection**

Network detecting and monitoring is a specialist area and should not be considered without expert advice. Recommendations for dealing with networks and wireless implementations involve the following steps:

- Identify and check network devices to see how much network or Internet activity is taking place. Consider using a wireless network detector to determine whether wireless is in operation and to locate wireless devices. Consideration should also be given to mobile Internet devices such as 3G or GPRS dongles or phones, which operate using the mobile phone network;
- As you do so, consider photographing the layout of the network and the location of the machines connected to it, so as to allow a possible future reconstruction;
- Once satisfied that no data will be lost as a result, you may isolate the network from the Internet. This is best done by identifying the connection to the telephone system or wireless communications point and unplugging it from the telephone point. Keep modems and routers running, as they may need to be interrogated to find out what is connected to them. Owing to their nature, it is particularly difficult to ascertain what is connected to a wireless network;
- Trace each wire from the network devices to discover the computer to which it is connected. This may not be possible in premises where cables may be buried in conduits or walls (advice in this case should be sought from the local IT administrator, if available, as to the set up of the system). Make a note of each connection. Note which computer is connected to which number 'port' on the network device (hub / switch / router or multi function device). Label each connection in such a way that the system can be rebuilt exactly as it stands, should there be any future questions as to the layout. It is highly recommended that pictures be taken of the setup;
- Consider making a connection to the access point/router in order to establish the external IP address. Most modern networks use Network Address Translation (NAT) which means that they communicate with an internal IP address and never get assigned and external IP one. In a wireless environment, remember that no cables are used between a PC and other devices. However, there will still be some physical cabling to each device (which could include a network cable to the wired network, power cables etc.), the configuration of which should be recorded. Please also note that Cable / ADSL modems can have wireless capabilities built in.
- Once satisfied that the evidential impact is acceptable, you may remove each connection in turn from the network device once it has been identified. This will isolate each computer in turn from the network. The same can be done with cabling into wireless devices;
- Seize and bag all network hardware, modems, original boxes and CDs / floppy disks etc. (provided they are easily removable);
- Subsequently treat each device as you would a stand-alone device;
- Remember that the data which is sought may be on any one of the computers on the network. Officers should make a decision based on the reasonable assumption that relevant data may be stored on a device before seizing that device;
- Bear in mind the possibility that the network may be a wireless network as well as a wired one, i.e. certain computers may be connected to the network via conventional network cabling. Others may be connected to that same network via the mains system, and others may be connected via a wireless link;
- Also, bear in mind that any mobile phones and PDAs may be wireless or Bluetooth enabled and connected to a domestic network.

Concerns with remote wireless storage often focus around the inability to locate the device. In this instance, it would be impossible to prove that an offence had been committed. Artefacts on seized computers might provide evidence that a remote storage device has been used, however the analysis of such artefacts will take time and this cannot often be done during the onsite seizure.

**Corporate network environments**

When dealing with computer systems in a corporate environment, the forensic investigator faces a number of differing challenges. If the system administrator is not part of the investigation then seek their assistance. The most significant is likely to be the inability to shut down server(s) due to company operational constraints. In such cases, it is common practice that a network enabled 'forensic software' agent is installed, which will give the ability to image data across the network 'on-the-fly', or to a network share or a locally connected removable storage medium such as a USB hard drive.

Other devices could be encountered which may assist the investigation. For example, routers and firewalls can give an insight into network configuration through Access Control Lists (ACLs) or security rule sets. This may be achieved by viewing the configuration screens as an administrator of the device. This will require the user names and passwords obtained at the time of seizure or from the suspect during interview.

By accessing the devices, data may be added, violating Principle 1 but, if the logging mechanism is researched prior to investigation, the forensic footprints added during investigation may be taken into consideration and therefore Principle 2 can be complied with.

In the case of large company networks, consider gaining the advice and assistance of the network administrator/ support team (assuming that they are not suspects).

## 7.8 Other Devices

**(Digital cameras, GPS navigation systems, Dash Cameras, etc.)**

Data sources in these devices include:

a) External storage memory: to work with any other external storage device.
b) Internal memory: a large part of the devices also have an integrated memory, usually of limited capacity, but which allows data to be stored and must be checked.

The proposed procedure is as follows:

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

If there is content it can be extracted:

- Through the connection cable of the device to the PC, making an image. Not all devices have that possibility.

- Inserting a new card and copying the data to the latter, so that we get a logical copy.
- If the other options are not possible you can take photographs of the content trying to show the interesting data related to the investigation.
- It is checked in the camera settings: date, time and time zone.

All elements are sealed together and marked as processed.

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

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

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

## 7.9 IoT Devices

In addition to the traditional IT devices described above, in recent years several devices have been defined as "IoT" or the Internet of Things. These devices can be very different from each other in terms of functionality, such as smartwatches, smart TVs, video surveillance devices, and so on. Below we will see some examples of the most popular devices that could be found in use by our suspect.

**7.9.1. Smartwatches**

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

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

Usually, they are equipped with Bluetooth connection but some of them can be equipped with a USB port, so the investigator can usually acquire the content through the usual equipment, almost the same as on any Android smartphone/tablet would be.
If you intend to seize a smartwatch, it would be preferable to follow the same indications already provided in the smartphone section.

**7.9.2. Smart TV**

It is becoming popular to find Smart TVs with the capability to connect to the internet, run apps or play games. Some are based on Android while some others are based on proprietary operating systems. The exact functionality provided depends on the make, model, peripherals attached or apps installed.

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

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

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

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

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

**Possible evidence** to be found during the search and seizure:

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

### 7.9.3. Home kits/Smart speakers

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

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

**Possible evidence** to be found during the search and seizure:

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

### 7.9.4. IP and concealed cameras

IP cameras or concealed cameras are typically used for small scale monitoring and, unlike CCTV, these devices might not have local storage capabilities. Most of the IP cameras available only need a Wi-Fi connection to work. The user can watch the camera live stream from any device connected to

the Internet. It also might be possible, if the user subscribed for a cloud-stored package, to watch recorded footage (usually in a loop of the previous days).

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

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

**Possible evidence** to be found during the search and seizure:

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

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

## 7.10 Gaming Consoles

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

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

Possible evidence to be found during the search and seizure:

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

## 7.11 Drones

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

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

- **Physical Components:** The physical components which make up the body and flight mechanisms can be broken down into the following categories:
    - **Drone Body:** The core fuselage of the UAV used to house all other components.
    - **Flight Controller:** Used to control flight. This device will stabilize the drone and generally accept navigation input from a radio control device. In more sophisticated systems the flight controller can both be controlled remotely in real-time and be pre-programmed for autonomous flight.
    - **Motors, Rotors/Propellers/Wings, and Speed Controllers:** These component parts combined provide the lift and propulsion for the UAV. Different designs exist, for example, specializing in increased speed or flight duration.
    - **Protective Casing:** This protection securely encases the motors and propellers (the most vulnerable component of any drone) to prevent collision and loss of control and subsequent damage to the system.
    - **GPS Receiver:** Not essential in all drones, but common in the leading solutions. This component is used to effectively manage UAV position, return to home functionally, and autonomous flight routes.
    - **Radio Receiver:** Used to receive control input signals received/gathered from the ground-based transmitter.
    - **Transmitter:** Transmits manual input from the operator on the ground to the drone.
    - LED Lights: Some drones come equipped with LED lights (usually green and red) which can be used to aid the pilot of the orientation of the drone, and help other airspace users to identify the drone.
- **Software:** All drones include an application or software that is used to control the system when it is operational. There is now a huge selection of open-source flight control and ground control applications available online that can be freely downloaded and easily modified to perform any number of tasks. The majority of drones come with companion mobile applications to either pilot the drone or view the camera feed and location of the drone overlaid on a map.

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

- **Memory Cards:** These can be examined as a computer hard disk. Both logical and physical extraction can be conducted on these cards, as long as the forensic tools support this feature. The examiner has to access the card, extract the data, and then put it back into the device before switching it on. Some devices store data in the memory card, and if it detects that the card is not available, it could cause data loss from the drone/controller. If time and resources allow, a bit-to-bit clone of the memory card should be created and that clone inserted into the handset.

- **Internal Memory:** This requires drone/mobile compatible manufacturer/forensic tools. Some devices are supported by forensic tools for physical extraction. The forensic tools will boot the device in a particular way and conduct physical extraction without making any changes or alterations to the user data on the device.

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

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

**Possible evidence** to be found during the search and seizure:

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

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

## 7.12 CCTVs

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

CCTV security system consists of different components. These include:

- **CCTV Camera:** used for video surveillance and acts as the input device to the system CCTV Monitor. This device receives signals and reproduces pictures or videos captured by the CCTV camera.
- **Main Power Supply:** the primary electrical supply unit.
- **Backup Power Supply (optional):** backup power supply comes in handy in case of a power outage.

- **Cables:** these are used to connect several CCTV cameras to one video recorder, video switcher for CCTV monitor, also modern CCTV systems may utilize Wi-Fi networks to transmit the pictures to a central point.
- **Video Recorder:** transforms and records signals sent by a CCTV camera in the form of a video that is generally stored on a hard drive and may be deleted automatically depending on the device settings.
- **Video Switcher:** switches the video mode between different CCTV cameras.

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

- Check time and date set on the video recorder and report if they differ from the current ones
- Take pictures of the screen(s)
- Shut the recorder down to avoid data to be overwritten
- Disconnect cables
- Identify make and model
- Photograph and label all the components
- Securely pack everything.

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

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

## 7.13 Virtual Assets Devices

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

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

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

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

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

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

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

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

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

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

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

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

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

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


Figure 3: Paper wallets (Interpol)

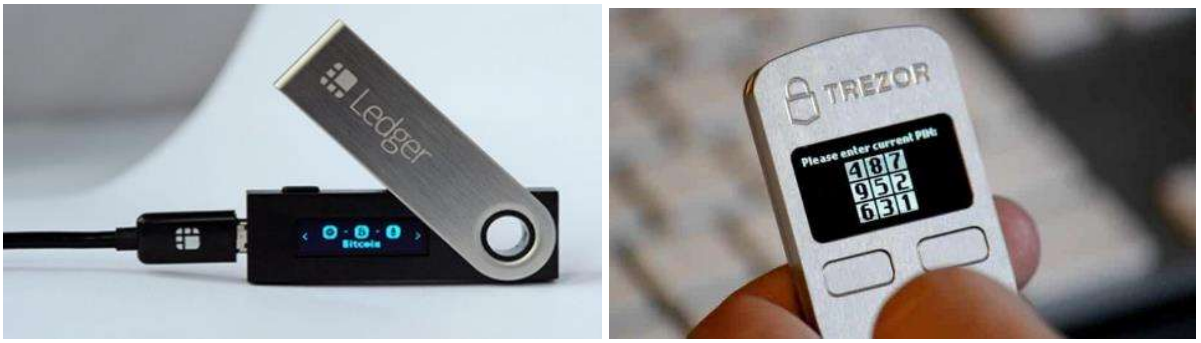


Figure 4 and 5: Hardware wallets, used to store information about crypto assets (Interpol)

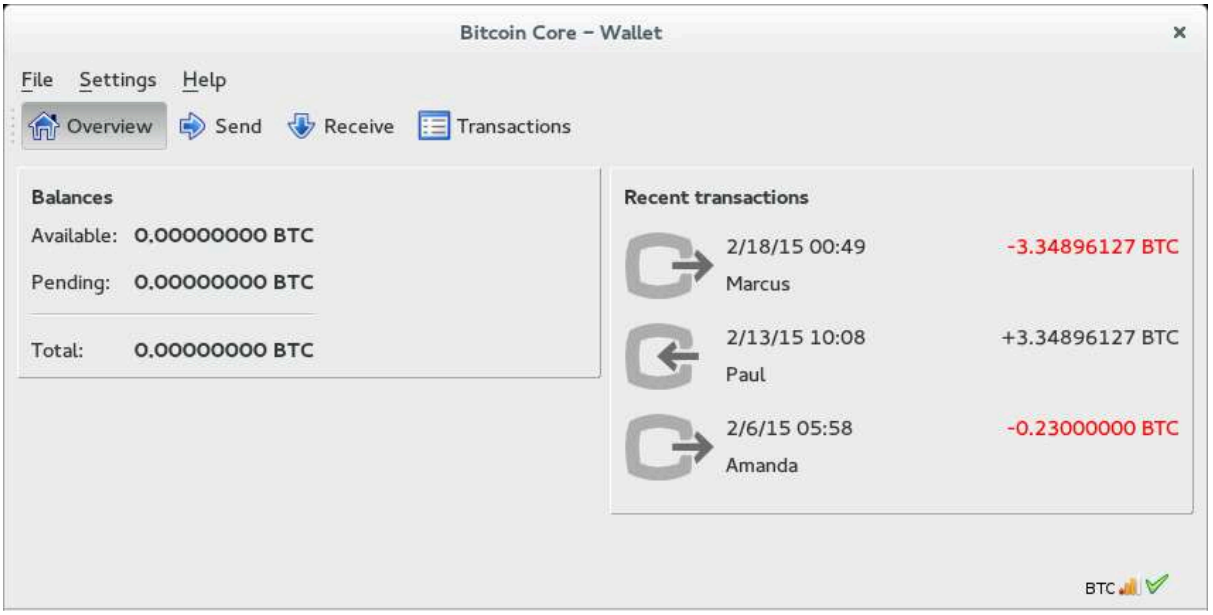


Figure 6: Example of a desktop wallet (Interpol)

Figure 7: Electrum, a desktop wallet (Interpol)

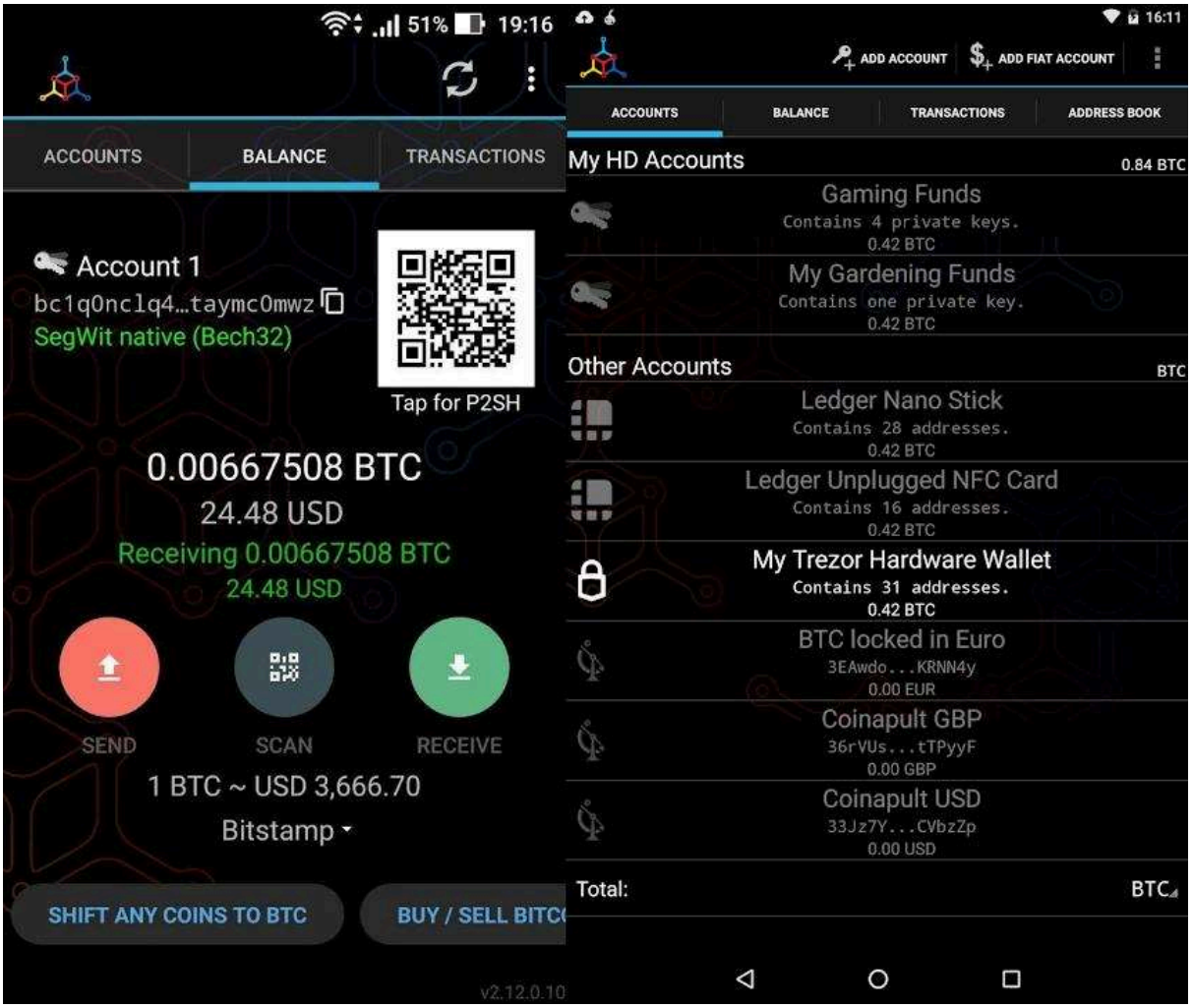

Figure 8: Example of a mobile wallet used for storing cryptocurrency information (Interpol)

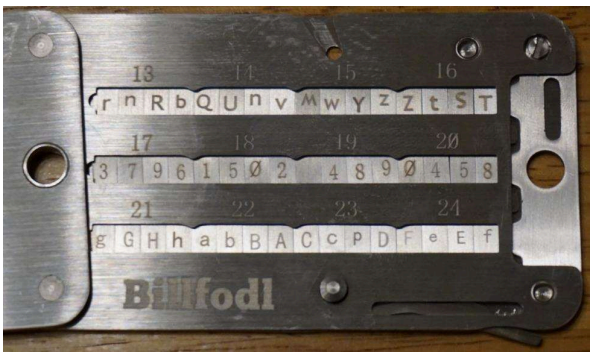

Figure 9 and 10: Brain wallets (seed) (Interpol)

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

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

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

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

## 7.14 Automotive Vehicles

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

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

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

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

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

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

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

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

**Evidence Handling**

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

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

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

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

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

ensure they try to capture associated evidence such as CCTV, automatic number plate recognition logs etc. from places that the car has been in to ensure that the evidence corroborated.
* This process is replicated from the Scientific Working Group on Digital Evidence (SWGDE) Best Practices for Vehicle Infotainment and Telematics System v2 (dated 2016-06-23). It is the readers' responsibility to ensure they have the most current version of the document. Please see swgde.org/documents/published for more information. Please also refer to the references section at the end of this report for the SWGDE disclaimer and redistribution policy.

## 7.15 Shipborne Equipment

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

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

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

| Equipment | Location | Type of data |
|---|---|---|
| AIS Transponders | Bridge |  |
| Echo Sounder | Bridge |  |
| Electronic Chart Display and Information System (ECDIS) | Bridge, Captain quarters, Nav Room |  |
| Emergency Positioning Indicator Radio Beacon (EPIRB) | Bridge, Bridge Wings, Flying bridge |  |

| | | |
|---|---|---|
| GMDSS System | Bridge |  |
| GPS | Bridge |  |
| Long Range Tracking and Identification System (LRIT) | Bridge |  |
| Vessel Monitoring System (VMS) | Bridge, Fly Bridge |  |
| RADAR | Bridge |  |
| Digital Selective Calling (DSC) | Bridge, captain cabin, navigation room |  |
| Sat-phone | Bridge, captain cabin, navigation room |  |

Examples of Shipborne equipment with data and their location

# 8. Generative AI and Digital Forensics

Generative AI is a rapidly evolving, dual-use technology that is being weaponised for cybercrime while also changing how court materials are prepared. Its growing use raises implications for investigators, both in terms of what is admissible in court and how AI-enabled attacks are carried out. This section addresses two key areas: 8.1 looks at legal and evidentiary considerations around Gen-AI use in court proceedings, while 8.2 examines its offensive applications and what investigators should take note of when assessing intent and action under the Computer Misuse Act.

As there are currently no standardised procedures for Gen-AI-related forensic work, investigators should be alert to its evolving role in both compliance and cybercrime. Forensic readiness will increasingly depend on understanding how Gen-AI can impact evidence, attribution, and legal responsibility.

## 8.1 Legal and Evidentiary Considerations of Generative AI Use in Court Proceedings

Digital forensics professionals should note Singapore's guidelines on Generative AI (Gen-AI) use for court proceedings[4] which was released in September 2024.

The key point to note is that the court **does not prohibit the use of Gen-AI tools to prepare Court documents**, but **may not be used to generate evidence that is subsequently relied upon in Court**. Failure to comply with these guidelines could jeopardise the admissibility of evidence and impact the credibility of the case. Refer to 9.4 Evidence Act and other points relating to Evidence Act throughout the document for more information.

- "General principles - (1) The Court **does not prohibit the use of Generative AI tools to prepare Court Documents**, provided that this Guide is complied with"
- "For the avoidance of doubt, **Generative AI tools should not be used to generate any evidence that you wish to rely upon in Court**."
    - "For example, you cannot use Generative AI to ask for evidence to be created, fabricated, embellished, strengthened or diluted. Asking a Generative AI tool to generate a first-cut draft of an affidavit/statement can be done (provided that this Guide is complied with), but it is not acceptable to ask a Generative AI to fabricate or tamper with evidence."

[4] https://www.judiciary.gov.sg/docs/default-source/circulars/2024/registrar's_circular_no_1_2024_supreme_court.pdf

## 8.2 Offensive Applications of Generative AI in Cyber Attacks

Gen-AI is increasingly used by attackers to enhance the scale and realism of cyberattacks. A key example is phishing and LLMs can now generate highly convincing, tailored phishing emails that mimic legitimate corporate language and branding. These messages often evade traditional detection and can be produced in volume, including across languages. This automation poses a growing threat that digital forensics professionals must be aware of.

From a legal standpoint, digital forensic professionals must assess Gen-AI's role in the context of the Computer Misuse Act (CMA) by focusing on two key legal elements: intent and action.

Intent: The CMA criminalises unauthorised access and interference. Using Gen-AI to generate malicious scripts or phishing content does not change the requirement to prove intent. Prompts or code showing deliberate tailoring for malicious purposes can reinforce premeditation. For instance, evidence of an attacker using Gen-AI to produce obfuscated PowerShell or spear-phishing templates **supports an inference of intent**.

Action: The tool used, AI or otherwise, is secondary to the act committed. Investigators should collect and preserve AI-generated artifacts (e.g., phishing emails, generated scripts, prompt logs) as part of the digital evidence trail. Gen-AI use does not mitigate liability; the focus remains on **what actions were taken**, such as unauthorised access, data theft, or service disruption.

Attribution can be harder when AI-generated content lacks clear authorship. Investigators should **prioritise collecting metadata, system logs, and signs of AI platform usage that can link activity to a suspect**. This includes prompt history, browser traces, and API call logs.

As Gen-AI capabilities grow, forensic readiness should include the ability to

A. detect AI-generated content
B. correlate it with known threat activity
C. assess it within the CMA framework

While the technology is evolving, the investigative core, proving intent and action, remains unchanged.

# 9. Legislation

A wide variety of legislation may apply in examinations of digital evidence. A non-exhaustive list of relevant legislation is detailed below with a brief explanation. A digital forensics professional should be familiar with the relevant legislation that applies to each case.

## 9.1 Cyber-dependent vs Cyber-enabled Crime

(https://www.police.gov.sg/Advisories/Crime/Cybercrime)
In Singapore, cybercrime is categorised into two clusters of crimes:

Cyber-dependent Crime: Offences under the Computer Misuse Act (CMA) in which the computer is a target. This includes offences such as ransomware, hacking and website defacements, etc.

Cyber-enabled Crime: Offences in which the computer is used to facilitate the commission of an offence. Examples of cyber-enabled crime include online scams and cyber extortion, and other Penal Code offences committed via an online medium.

## 9.2 Evidence Act

(https://sso.agc.gov.sg/Act/EA1893)
It is important to note that the Evidence Act mainly concerns relevance, admissibility, and presentation of evidence in court proceedings. It does not specify procedures or directly restrict the collection methods, including those related to digital evidence seized through searches. It does however require digital evidence presented in court to meet standards of relevance, authenticity, and integrity.

This section below aims to help readers know the relevant sections that make digital evidence relevant and admissible in court.

Amendments to the EA have clarified that computer output (e.g., logs, emails, digital documents) is admissible, subject to relevance, authenticity, and reliability requirements. More specifically, Section 116A has been introduced, and Sections 35 and 36 have been repealed. Thus, the normal rules of evidence apply to electronic evidence.[5]

Singapore thus adopts the approach of technological neutrality.[6]

**S5 Evidence may be given of facts in issue and relevant facts**

- Evidence can only be given on facts in issue and relevant facts
- No other evidence can be admitted
- This prevents irrelevant evidence

[5] https://www.mlaw.gov.sg/files/linkclick5231.pdf
[6] https://law.asia/technology-neutrality/#:~:text=What%20is%20technology%20neutrality%3F,or%20discriminate%20against%2C%20any%20technology.

**S64 Primary evidence**

- Original documents or copies of digital documents are regarded as primary evidence. However, it must reflect the original document accurately.
- Hash value of the document is needed to prove that it is an exact copy of the digital document. This is important to ensure copies share the same weight as the original.
- Electronic records and their copies are regarded as primary evidence. However, electronic records must be consistent throughout all instances.

**S65 Secondary evidence**

- Evidence that is not primary evidence will be classified as secondary.
- Refers to all evidence that is not the original document with the exception of copies of digital evidence.
- Must be able to reflect the original document reliably.

**S66 Proof of documents by primary evidence**

- Epitomises the best evidence rule, where primary evidence is favoured over secondary evidence

**S67 Cases in which secondary evidence relating to documents may be given**

- Defines the situations where secondary evidence can be used
- Usually only when primary evidence is unavailable due to the loss or destruction
- Under Section 68, if the original document is held by the opposing party, notice to produce the document must be given before secondary evidence can be used.
- For a more comprehensive list, readers should refer to the Evidence Act Section 67

**S68 Rules as to notice to produce**

- If the original document is held by the opposing party, notice to produce the document must be given before secondary evidence can be used.
- Original document as primary evidence will always take precedence over any secondary evidence unless specified otherwise.
- This enables the opposing party to be given an opportunity to produce original digital evidence which supports the integrity and authenticity of forensics findings.
- List of exceptions can be found under the Evidence Act Section 68

**S70 Proof of execution of document required by law to be attested**

- Before evidence can be admitted into court, proof of execution must be present. This means an attesting witness must be present to confirm that the digital evidence has indeed occurred.
- During the collection of digital evidence, it is crucial to note who is involved in a particular evidence trail so he can be called upon when required as an attesting witness is required.

**S81 Presumption as to genuineness of certified copies**

- Copies of digital evidence can be assumed to be genuine provided they meet legal standards.
- Hashes and relevant digital signatures that are secure are required to prove that copies are identical and accurate to the original.

**S82 Presumption as to documents produced as record of evidence**

- A document presented in court as a record or memorandum of evidence needs to be signed by a judge, magistrate or an authorized officer to certify that the document is genuine.
- This is to also certify that the evidence was properly and lawfully produced which extends a presumption of authenticity and procedural correctness when producing digital evidence.

**S88 Presumption as to certified copies of foreign judicial records**

- For digital evidence originating outside of Singapore, the evidence or its copy must achieve a level of legal standard that complies with the legal standards of the originating country.
- Digital forensics professionals are advised to compare the integrity of the evidence when receiving to the certification standards specified by the originating country.
- An authorized certification should also be produced to confirm its authenticity.

**S100 Evidence as to meaning of illegible characters, etc.**

- Introduction of evidence to explain or clarify meaning of parts in a document that may be difficult to understand, such as illegible characters, obscure abbreviations, or words used in a technical, foreign, or unusual sense is permitted.
- Potentially corrupted or encoded evidence may still be relevant in investigations and court, thus they should adhere to strict chains-of-custody to ensure integrity and admissibility.

**S116A Presumptions in relation to electronic records**

- Digital evidence is presumed to be authentic, and thus admissible in court if they have been retrieved under standard circumstances.
- While these assumptions can be challenged, it is important to document the scenario when collecting evidence so it can be compared against what standard circumstance is.
- Standard circumstance can be determined from Standard Operating Procedures (SOP) or any other documents that specify the process of handling digital evidence by the relevant entity.
- Electronic records generated, recorded, or stored in the usual course of business by a neutral party are presumed authentic.

**S126 Official communications**

- Due to the sensitive nature of certain documents, some digital evidence may be protected under the Official Secrets Act. This digital evidence may not be allowed to be collected and prior permission or guidance should be sought after before proceeding.
- Unless special permission has been granted, such evidence collected will be deemed inadmissible.
- Sensitive electronic evidence obtained from official channels may be withheld if disclosure is deemed detrimental to the public interest, potentially limiting access to certain types of digital evidence.

## 9.3 Criminal Procedure Code

(https://sso.agc.gov.sg/Act/CPC2010)

The Criminal Procedure Code (CPC) of Singapore is the key legislation governing Singapore's criminal justice process. It details the procedure for the administration of criminal law in Singapore[7] and covers arrests, investigations, trials and appeals, and sentencing matters, among others[8]. This section aims to help readers know the relevant sections that grant powers to the police with regards to digital forensics investigation, including for **investigation**, **search** and **seizure**.

**S20 Power to order production of any document or other thing**

- A police officer (sergeant rank or higher) and authorised person can issue a written order requiring an individual to produce a document or thing if it is relevant for any investigation, inquiry, trial or other proceedings under the CPC. However, if the "customer information" is kept by a "specified institution", then the police officer must be above the rank of inspector.
- S20 also explicitly covers documents in electronic form (Subsection (1)(a)(iii)) or documents contained in or available to a computer (Subsection (1)(b)).
- In the case of digital forensics, when data ("data" has the meaning given by the Computer Misuse Act 1993) is involved, the individual may be required to authenticate the data (Subsection (1)(a/b)(i)), confirming its integrity and origin, which is crucial for admissibility in court.
- In the CMA, "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer, and as such covers electronic records, such as emails, digital files, computer logs and call logs.
- This applies to both individuals and companies.

- "customer information"
    - (a) in relation to a bank or merchant bank, has the meaning given by section 40A of the Banking Act 1970; and a reference in that section to a bank is a reference to a bank or merchant bank;
    - (b) in relation to a licensed trust company, means information protected under section 49 of the Trust Companies Act 2005; and
    - (c) in relation to any other financial institution, means any information relating to, or any particulars of, an account of a customer of the financial institution or funds of a customer under management by the financial institution, but does not include any information that is not referable to any named person or group of named persons;
- "specified institution" means a financial institution that is any of the following:
    - (a) a bank or merchant bank within the meaning of section 2(1) of the Banking Act 1970;
    - (b) a licensed trust company within the meaning of section 2 of the Trust Companies Act 2005;

[7] https://nuscriminaljustice.com/the-criminal-procedure-code-learning-about-arrest-procedures-in-singapore/
[8] https://www.mha.gov.sg/mediaroom/press-releases/criminal-procedure-miscellaneous-amendments-bill-2024/

**S37 List of all things seized to be made and signed**

- Applies to police officer or any other person making the search.
- In every case, (a person acting on behalf of) the occupier or person in charge of the place search, must be given a signed copy of the list.

**S39 Power to access computer**

- S39 grants a police officer or an authorised person (a forensic specialist appointed under section 65A of the Police Force Act 2004) investigating an arrestable offence access, inspection and checking of computers (regardless if it is in Singapore or elsewhere) and to search or make a copy of any data contained in computers.
- Subsection 3: It is an arrestable offence to obstruct the lawful exercise by a police officer or an authorised person.
- Computer here has a broad meaning, given by the Computer Misuse Act 1993.
    - "computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices.

**S40 Power to access decryption information**

- S40 grants a police officer or an authorised person access to any information, code or technology which has the capability of retransforming or unscrambling encrypted data into readable and comprehensible format or text.
- The police officer or authorised person may compel access to such decryption information as may be necessary to decrypt any data required for the purposes of investigating the arrestable offence.
- Subsection 3: It is an arrestable offence to obstruct the lawful exercise by a police officer or an authorised person.
- "decryption information" means information, code or technology or part thereof that enables or facilitates the retransformation or unscrambling of encrypted data from its unreadable and incomprehensible format to its plain text version

**S364 Order for Disposal of Property by Court**

- "property" means money and all other property, movable or immovable, including things in action and other intangible or incorporeal property. This can include digital evidence, such as data.[9]
- S364 empowers the court to issue orders for the disposal of property during or at the conclusion of an inquiry or trial.
- Digital forensics investigators should handle the disposal of digital evidence in compliance with Section 24 of the PDPA to avoid causing a data breach.
- For example, equipment that holds storage media devices that contain the digital evidence should be physically destroyed, ensuring the data is unrecoverable, if directed by the court to dispose.
- Practical Considerations for Investigators [GPT-generated]:
    - Preserve Evidence Integrity: Securely store all digital devices and data until the court finalizes the disposal order, accounting for potential appeals.
    - Document Thoroughly: Maintain a detailed chain of custody for all seized items to validate their condition and handling if disposal is contested.
    - Extract and Backup Data: Before disposal, ensure all relevant data is forensically extracted and preserved in a secure format, as devices may be returned or destroyed.
    - Track Converted Property: Monitor and document any conversions of digital property (e.g., data transferred to cloud storage), as these fall under the section's scope.
    - Liaise with Legal Teams: Collaborate with prosecutors to clarify the disposal order's impact, especially if the property is needed for ongoing or future cases.

[9] https://sso.agc.gov.sg/Act/CPC2010#pr2-

## 9.4 Computer Misuse Act

(https://sso.agc.gov.sg/Act/CMA1993)

The Computer Misuse Act (CMA) criminalizes a wide range of computer-related activities[10]. This section aims to help readers know the relevant sections that apply to misuse of computers, cybersecurity incidents and police powers for investigations.

**S3 Unauthorised access to computer material**

- Criminalizes unauthorized access to computer material, such as hacking, where a person intentionally accesses data or programs without permission
- Scenario: An attacker hacks into a hospital is enough to qualify as an offence under S3 of CMA
- Digital forensic professionals should find evidence to proof unauthorised access

**S4 Access with intent to commit or facilitate commission of offence**

- Similar to S3, but a more serious crime due to intent to commit or enable further crimes, like theft or fraud
- Scenario: An attacker hacks into a hospital, exfiltrated the data, and used it to conduct spear-phishing, with the **intent to commit a further offence** such as fraud would fall under the CMA
- Digital forensic professionals should find evidence to proof unauthorised access (S3) + **intent to commit a further offence**

**S5 Unauthorised modification of computer material**

- Criminalizes unauthorized modification to computer material, and covers acts like alteration, erasure, addition, or any act occurs which impairs the normal operation of any computer

**S6 Unauthorised use or interception of computer service**

- Criminalizes the unauthorized use or interception of any computer service, including actions such as accessing, intercepting, or using a computer service without permission, whether directly or indirectly.

A digital forensics investigator should be concerned with finding evidence to show that Sections 3, 4, 5, 6 of the Computer Misuse Act have been violated.

**S13 Territorial scope of offences under this Act**

- Defines jurisdiction, applying the CMA if the offender or affected computer is in Singapore during the offense
- Covers acts from Singapore or targeting Singapore systems and ensures cross-border cybercrime accountability
- Digital forensic professionals should take note if handling cross-border evidence.

**S18 Saving for investigations by police and law enforcement officers**

- Clarifies that the CMA does not override powers granted to police or other authorised officers under other laws.

[10] https://www.daslaw.com.sg/navigating-computer-misuse-act-offences-beyond-just-hacking/

- Allows police and authorised law enforcement officers to lawfully conduct investigations, even if the actions might otherwise appear to contravene the CMA.
- Scenario: A police officer accessing a suspect's computer system without consent, under the authority of the Criminal Procedure Code, is not considered an offence under the CMA.
- Digital forensic professionals should be aware that certain actions by law enforcement are legally protected when carried out under proper authority.

**S19 Arrest by police without warrant**

- Allows police to arrest, without a warrant, anyone reasonably suspected of a CMA offense.
- Enables immediate detention in cybercrime cases.

## 9.5 Personal Data Protection Act

**S24 Protection of personal data**

- Requires organisations to make reasonable security arrangements to protect personal data in their possession or control.
- Covers protection against unauthorized access, use, disclosure, modification, loss, or other similar risks.
- Scenario: A hospital fails to encrypt patient data stored on a USB drive, which is later lost, this may be a breach of S24 if reasonable security measures were not in place.
- Digital forensic professionals should assess whether adequate safeguards were implemented and whether lapses in data protection contributed to the incident.

## 9.6 Telecommunications Act

(https://sso.agc.gov.sg/Act/TA1999)
The Telecommunications Act 1999 is an Act to provide for the provision of telecommunication systems and services in Singapore. It deals with matters that include licensing of telecoms systems and IMDA's powers to issue codes of practice, standards of performance, directions and advisory guidelines relating to telecom systems and services[11].

The Act's relevance to digital forensics lies in the fact that some data (e.g. call log or SMS data) may be better obtained from Telecommunication Providers, rather than to request a forensic examination of the mobile phones.

For digital forensics investigators who are seeking digital evidence, the key point to note is that telecommunication providers are required to maintain Call Detail Records ("CDRs") for a period of not less than twelve (12) calendar months.

IP Telephony Framework - Guidelines On Licensing And Regulatory Framework For IP Telephony Services In Singapore[12]

**Section 1.6**: In addition to the existing FBO/SBO licence general conditions, the Telecommunications Act (Cap 323), its Regulations and any Codes of Practice, **licensees would also be required to comply with the specific terms and conditions for the provision of IP Telephony services (Annex A)** if they are intending to use E.164 telephone numbers and assign them to their customers in Singapore. Where necessary, the Authority shall amend a licensee's existing FBO or SBO licence to incorporate the required Conditions.

Annex A - Specific Terms And Conditions For IP Telephony Services
8 Data Retention Requirements
8.1 The Licensee shall maintain the following data records, which shall be made available for inspection by authorised Singapore government agencies:
(a) Assigned Source IP address and Date & Time stamps; and
(b) Assigned User ID/User Name (e.g., subscriber records associated with (a)).

8.2 The Licensee shall maintain Call Detail Records ("CDRs") of all calls made and received through the Service, which are operated and/or provided in Singapore.

8.3 All data records including CDRs shall be kept by the Licensee for **a period of not less than twelve (12) calendar months**.

8.4 The Authority reserves the right to require the Licensee to retain any other details as part of data records as necessary.

[11] https://www.dlapiperintelligence.com/telecoms/index.html
[12] https://www.imda.gov.sg/regulations-and-licensing-listing/ip-telephony-framework

# 9.7 Mutual Assistance in Criminal Matters Act

(https://sso.agc.gov.sg/Act/MACMA2000)

**S8 Requests for taking of evidence, etc.**

Section 8 of Singapore's Mutual Assistance in Criminal Matters Act 2000 (MACMA) outlines the procedures for Singapore to request assistance from foreign countries in obtaining evidence and related materials for use in criminal matters within Singapore.

1. Requests for Taking Evidence

   Under Section 8(1), the Attorney-General of Singapore may request the appropriate authority of a foreign country to arrange for evidence to be taken in that country and sent back to Singapore. This is applicable when there are reasonable grounds to believe that such evidence is relevant to criminal proceedings in Singapore.

2. Requests for Obtaining Articles or Things

   Section 8(2) allows the Attorney-General to request assistance in obtaining specific items located in a foreign country, including through search and seizure if necessary. This includes the item itself or a photograph or copy of it, provided there are reasonable grounds to believe it would be relevant to a criminal matter in Singapore.

3. Admissibility of Evidence

   According to Section 8(3), any evidence or items received through such requests may be admitted in Singaporean criminal proceedings, subject to the provisions of the Criminal Procedure Code and the Evidence Act.

4. Weight of Evidence

   Section 8(4) stipulates that when evaluating the weight of a statement obtained from a foreign country, the court should consider whether the statement could be challenged by questioning its maker and whether the foreign country's laws allowed legal representation during the evidence-taking process.

# 9.8 Cybersecurity Act

(https://sso.agc.gov.sg/Acts-Supp/9-2018/)

### 9.8.1 Main Sections

**S14 Duty to report cybersecurity incident in respect of Critical Information Infrastructure, etc**

- This section mandates CII owners to report prescribed incidents. Forensic teams must understand reporting timelines and formats.
- Failure to report can result in enforcement actions under the Act.

**S19 Powers to investigate and prevent cybersecurity incidents, etc**

- This section authorizes investigation of cybersecurity threats or incidents.
- Primary focus is immediate incident response and mitigation, as it empowers the Commissioner and authorized officers to take rapid action.
- Empowers officers to:
    - Require persons to attend interviews at specified times and places
    - Compel written statements concerning cybersecurity incidents
    - Demand production of physical or electronic records and documents
    - Inspect, copy, or take extracts from relevant records without fee
    - Examine witnesses orally and reduce statements to writing
- Allows officers to seek Magistrate's order if persons fail to comply.
- Preserves legal privilege while ensuring contractual obligations don't prevent disclosure.
- Provides protection from contractual breach claims for persons complying with requirements.

**S20 Powers to investigate and prevent serious cybersecurity incidents, etc**

- Applies to incidents meeting specific severity thresholds (critical infrastructure risk, essential service disruption, national security threat).
- Primary focus is comprehensive evidence gathering and post-incident analysis.
- Includes all powers from Section 19 plus enhanced authorities to:
    - Direct remedial measures to minimize cybersecurity vulnerabilities
    - Require system owners to preserve evidence by not using systems
    - Order monitoring of systems for specified periods
    - Perform vulnerability scans on affected systems
    - Connect equipment or install programs necessary for investigation
    - Enter premises after reasonable notice
    - Access and inspect operation of affected computers
    - Copy electronic records from affected systems
    - Take possession of computers for further examination (with consent or Commissioner's authorization)
- Requires return of equipment immediately after examination.

**S38 Powers of investigation**

- Establishing general investigative powers for offenses under the Act.
- Covers broader violations like unlicensed cybersecurity service providers (Section 24).
- Ensures investigation powers exist independently of incident response.
- Prevents legal challenges that might arise if incident response powers were used for general enforcement.

**S39 Power to enter premises under warrant**

- This section establishes the process for obtaining search warrants from Magistrates.
- Warrants may be issued when:
    - Required documents haven't been furnished when demanded
    - Documents might be concealed, removed, or tampered with if requested
- Authorizes named officers to:
    - Enter and search specified premises using reasonable force if necessary
    - Take possession of or copy relevant documents
    - Require explanations about documents or their locations
    - Demand production of electronic records in portable and legible formats
- Sets warrant validity period (one month from issuance).
- Requires officers to:
    - Identify themselves to owners/occupiers
    - Show proof of identity and authorization
    - Provide copy of warrant to premises owner/occupier
    - Take reasonable steps to inform absent owners
    - Leave warrant copy in prominent place if owner absent
    - Prepare and provide itemized list of items taken
    - Leave premises secured upon departure

**9.8.2. Supporting Sections**

**S21 Production of identification card by incident response officer**

- Mandating production of identification cards when demanded.
- Ensuring proper authentication of officers collecting evidence.
- Protecting against unauthorized persons claiming investigative authority.

**S22 Appointment of cybersecurity technical experts**

- Allowing appointment of technical experts to assist investigations.
- Enabling specialized technical assistance for complex digital evidence.
- Providing framework for experts from public service, private sector, or national service.

**S43 Preservation of secrecy**

- Protects collected evidence.
- Requiring confidentiality of information obtained during investigations.
- Imposing secrecy obligations on all specified persons (officers, experts, etc.).
- Protecting business, commercial, and confidential information.
- Safeguarding identities of information providers.
- Allowing limited disclosure only when necessary for specific purposes.
- Creating a framework for handling sensitive information obtained during investigations.

# 10. Appendix

## 10.1 Glossary of Terms / Abbreviations Used

| | |
|---|---|
| **3G** | Third-generation cellular network technology |
| **ACL** | Access Control List |
| **ACPO** | Association of Chief Police Officers [now known as National Police Chiefs' Council (NPCC)] - in reference to the "Good Practice Guide for Digital Evidence" (2012) |
| **ADSL** | Asymmetric Digital Subscriber Line |
| **AGC** | Attorney-General's Chambers |
| **CCTV** | Closed Circuit Television |
| **CD** | Compact Disc |
| **CII** | Critical Information Infrastructure |
| **CMA** | Computer Misuse Act |
| **CNIC** | Cellular Network Isolation Card |
| **CPC** | Criminal Procedure Code |
| **CSA** | Cyber Security Agency of Singapore |
| **CSIM** | Subscriber Identity Module |
| **CSV** | Comma-separated values file format |
| **DDoS** | Distributed Denial-of-Service Attack |
| **DNA** | Deoxyribonucleic acid |
| **DRM** | Digital Rights Management |
| **DSC** | Digital Selective Calling |
| **DVD** | Digital Versatile Disc or Digital Video Disc |
| **EA** | Evidence Act |
| **ECDIS** | Electronic Chart Display and Information System |

| | |
|---|---|
| **ECU** | Electronic Control Units |
| **EPIRB** | Emergency Positioning Indicator Radio Beacon |
| **GB** | Gigabytes |
| **GMDSS** | Global Maritime Distress and Safety System |
| **GPRS** | General Packet Radio Service |
| **GPS** | Global Positioning System |
| **GSR** | Gunshot residue |
| **HD** | Hard drive |
| **HDD** | Hard disk drive |
| **ICCID** | Integrated circuit card |
| **IMEI** | International Mobile Equipment Identity |
| **Interpol** | The International Criminal Police Organization - in reference to the "Guidelines for Digital Forensics First Responders" (2021) |
| **IP Address** | Internet Protocol Address - numerical address assigned to device in a computer network that uses the Internet protocol for communications |
| **ISO/IEC** | International Organization for Standardization/International Electrotechnical Commission |
| **LRIT** | Long Range Tracking and Identification System |
| **MACMA** | Mutual Assistance in Criminal Matters Act |
| **MLA** | Mutual Legal Assistance |
| **MLAT** | Mutual Legal Assistance Treaties |
| **NAS** | Network Attached Storage |
| **NAT** | Network Address Translation |
| **NSRL** | National Software Reference Library |
| **NVMe** | Non-Volatile Memory Express |
| **OS** | Operating System |
| **P2P / P2MP** | point-to-point & point-to-multipoint (P2MP) |

| | |
|---|---|
| **PDA** | Personal Digital Assistant |
| **PDPA** | Personal Data Protection Act |
| **PIN** | Personal Identification Number |
| **PUK** | Personal unlocking keys – sometimes known as a network unlocking code (NUC) or personal unlocking code (PUC) |
| **RAM** | Random Access Memory |
| **RAID** | Redundant Array of Inexpensive Disks |
| **RF** | Radio Frequency |
| **RPAS** | Remotely Piloted Aircraft System |
| **RUIM** | Removable User Identity Module |
| **SHA-256** | Secure Hash Algorithm 2, 256 bits |
| **SMS** | Short Message Service |
| **SOP** | Standard Operating Procedure |
| **SPF** | Singapore Police Force |
| **SPF TCD** | Singapore Police Force Technology Crime Division |
| **SPF TCFB** | Singapore Police Force Technology Crime Forensics Branch |
| **SSD** | Solid-State Drive |
| **sUAS** | Small Unmanned Aerial System |
| **SWGDE** | Scientific Working Group on Digital Evidence |
| **TB** | Terabyte |
| **TPM** | Trusted Platform Module chips |
| **TV** | Television |
| **UAV** | Unmanned Aerial Vehicle |
| **UAS** | Unmanned Aerial System |
| **UPS** | Uninterruptible Power Supply System |

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

## 10.2 Interview of Witnesses and Suspects

The interview of witnesses/suspects is a crucial opportunity to identify key information about the nature and use of digital data relative to the investigation in hand. As such those involved must be properly briefed and competent to undertake the interview having the necessary understanding of the areas to explore.

Consideration should be given to consulting with a trained Interview Advisor with a view to the compilation of an appropriate interview strategy.

Bear in mind that the digital examination of devices seized will take time and may not necessarily reveal vital information that the witness / suspect may be aware of. Typically this may include;

- Web Mail Addresses / Username & Passwords / shared or sole use;
- Social Network Profiles / Username & Passwords / shared or sole use;
- Use of Forums & Chat Rooms / Username & Passwords;
- Use of Cloud Services / Username & Passwords / shared or sole use;
- Use of Virtual Storage / Username & Passwords / shared or sole use;
- Use of Role Play Gaming Sites / Username & Passwords / shared or sole use;
- Use of Auction sites / Username & Passwords / shared or sole use;
- Use of Online Banking;
- List of User Names;
- Use of Encryption / Encryption Keys;
- User Names of contacts;
- Use of the devices;
- Websites Visited;
- Internet Service Provider.

This list is not exhaustive

## 10.3 Open Source Research

The internet is a huge repository of information much of it of value to the investigator. Research by properly trained staff, preferably with access to a stand alone computer, will enable the investigator to get the best from the vast amount of information that is now held online. In addition to this the SPF TCD or AGC will be able to give advice on the type of data that can potentially be obtained from ISP's, web mail and web based providers.

Care should be taken when undertaking Internet research from any computer linked to the investigating agency as a digital footprint will be left and may reveal the law enforcement or investigation interest. This will not be obvious to the general internet user but will most certainly be clear to the hosts or providers of the service and those who are particularly technically aware and monitoring IP addresses.

Registration details are often asked for and whilst in some instances they will inevitably be fictitious, on many occasions they will include the following;

- IP log on;
- Name and Address;
- Landline and Mobile phone Numbers;
- Banking data;
- Emails used;
- Username and passwords;
- Linked accounts.

It is essential that the SPC TCD is engaged at the earliest opportunity to these enquiries with the objective of preserving known time critical data.

## 10.4 Chain of Custody Form (NIST)

A sample Chain-of-Custody Form from NIST is provided below:

**Property Record Number:**

_____

**Anywhere Police Department**

# EVIDENCE CHAIN OF CUSTODY TRACKING FORM[13]

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____Location of Seizure: _____

| **Description of Evidence** | | |
|---|---|---|
| **Item #** | **Quantity** | **Description of Item** (Model, Serial #, Condition, Marks, Scratches) |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| **Chain of Custody** | | | | |
|---|---|---|---|---|
| **Item #** | **Date/Time** | **Released by** (Signature & ID#) | **Received by** (Signature & ID#) | **Comments/Location** |
| | | | | |
| | | | | |
| | | | | |

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

[13] Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers*. U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

# EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM

## (Continued)

| Chain of Custody | | | | |
|---|---|---|---|---|
| **Item #** | **Date/Time** | **Released by** (Signature & ID#) | **Received by** (Signature & ID#) | **Comments/Location** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Final Disposal Authority

**Authorization for Disposal**

Item(s) #: _____ on this document pertaining to (suspect): _____
is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)

☐ Return to Owner ☐ Auction/Destroy/Divert

Name & ID# of Authorizing Officer: _____ Signature: _____Date: _____

**Witness to Destruction of Evidence**

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ID#:_____ in my presence on (date) _____.

Name & ID# of Witness to destruction: _____ Signature: _____Date: _____

**Release to Lawful Owner**

Item(s) #: _____ on this document was/were released by Evidence Custodian _____ID#:_____ to

Name _____

Address: _____ City: _____State: _____ Zip Code: _____

Telephone Number: (_____) _____

Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: _____ Date: _____

Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

**This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.**

**TO:** The Central Authority of the Republic of Singapore.

**FROM**: The Central Authority of the [*Requesting Party*]

**REQUEST FOR MUTUAL LEGAL ASSISTANCE**

**IN A CRIMINAL MATTER**

**CERTIFICATE ON BEHALF OF THE [*REQUESTING PARTY*]**

I, [*name, appointment/ position of person certifying*], on behalf of [*name of Central Authority*], who is responsible for [*state area of responsibility e.g. criminal prosecutions, investigations*] in the [*Requesting Party*] and who is also authorised to make requests for mutual legal assistance in criminal matters, certify that the Government of the [*Requesting Party*] respectfully requests the assistance of the Government of the Republic of Singapore in relation to criminal proceedings[1] involving [*describe nature of criminal proceedings, e.g. whether a trial or proceedings to determine whether a person should be tried*].

**REQUEST**

This request is made by the Government of the [*Requesting Party*] for assistance to be extended under the Mutual Assistance in Criminal Matters Act 2000 (Statutes of the Republic of Singapore).

**NATURE OF REQUEST**

This request relates to [*describe subject of criminal matter*]. The authority having the conduct of the criminal matter is [*describe authority concerned with the criminal matter*].

**CRIMINAL OFFENCES / APPLICABLE LEGISLATION / PENALTIES**

[*Set out the offences alleged to have been contravened in relation to the criminal proceedings as well as the maximum penalties for these offences and attach copies of applicable legislative provisions. State identity of suspect / accused person, if known*]

**STATEMENT OF FACTS**

[*Describe the material facts of the criminal proceedings including, in particular, those necessary to establish circumstances in the Requesting Party connected to the evidence sought and the relevance of the Singapore evidence to the criminal proceedings in the Requesting Party. Details of the witnesses from whom evidence*

*is sought to be recorded should be included as well as a statement of how the evidence that the witnesses may give will be relevant to the criminal proceedings in the Requesting Party.*]

**PURPOSE OF THE REQUEST**

By this request it is intended to [*state purpose which is intended to be achieved by the assistance sought, e.g. to secure admissible evidence to be used in the trial of* ……].

**ASSISTANCE REQUESTED**

The Government of the Republic of Singapore is requested to take such steps as are necessary to record the evidence from various witnesses and transmit the evidence so recorded to the Central Authority of [*the Requesting Party*]. The names of the said witnesses, their contact particulars[2] and the questions to be asked of them are as follows:

[*List the relevant information, including the questions to be put to each witness. In the alternative, these questions can be attached as annexes to the Request.*

**MANDATORY ASSURANCES & UNDERTAKINGS**

It is confirmed that this request:

(a) does not relate to the investigation, prosecution or punishment of a person for a criminal offence that is, or is by reason of the circumstances in which it is alleged to have been committed or was committed, an offence of a political character;

(b) is not made for the purposes of investigating, prosecuting, punishing or otherwise causing prejudice to a person on account of that person's race, religion, sex, ethnic origin, nationality or political opinions;

(c) does not relate to the investigation, prosecution or punishment of a person for an offence in a case where the person has been convicted, acquitted or pardoned by a competent court or other authority of the [*Requesting Party*] or has undergone the punishment provided by the laws of the [*Requesting Party*], in respect of that offence or of another offence constituted by the same act or omission as that offence.

The Central Authority of [*Requesting Party*] further undertakes that:

(a) any evidence obtained pursuant to this request, will only be used for the purposes of the request in connection with [*state particulars of criminal proceedings*]; and

(b) should the Honourable the Attorney-General of the Republic of Singapore require the return of any evidence obtained pursuant to this request at the conclusion of [*state particulars of criminal proceedings*] and of all consequential appeals, the evidence will be returned to the Honourable the Attorney-General of the Republic of Singapore.

**FOREIGN LAW IMMUNITY CERTIFICATE**

A certificate[3] declaring that, under the law of the [*Requesting Party*], namely [*state legal provision(s) and enclose copies*], a person can be required, in criminal proceedings instituted under the law of the [*Requesting Party*], to answer such questions as are sought to be asked through this Request, is enclosed with this Request.

**EXECUTION OF REQUEST**

**Confidentiality**

[*State confidentiality requirements of the Requesting Party, if any, and also specify whether the Requesting Party has any objections to disclosure of the Request to the Court and / or other parties to any legal proceedings that may be instituted under the Mutual Assistance in Criminal Matters Act 2000 pursuant to the Request.*]

**Procedure to be followed**

It is requested that the following procedures be observed in the execution of the request:

[*Provide details of manner and form**[4]** in which evidence is to be taken and transmitted to the Requesting Party, if relevant*]

[*State any special requirements as to certification / authentication of documents*]

[*Indicate if attendance by representative of the Requesting Party at examination of witnesses / execution of the request is required and, if so, the title of the post held by the proposed representative*]

**Period of Execution**

It is requested that the request be executed within [*state period giving reasons, e.g. specify likely trial or hearing dates or any other dates / reasons relevant to execution of request*].

**RECIPROCITY UNDERTAKING**

The Government of [*Requesting Party*] undertakes that it will comply with a future request by the Government of the Republic of Singapore for similar assistance in a criminal matter involving an offence that corresponds to the foreign offence for which assistance is sought.

**TRANSMISSION OF EVIDENCE**

Any evidence or thing obtained in response to this request should be sent to [*provide details of addressee and address to which the evidence should be sent*].

**LIAISON OFFICER**

The case officer in [*the enforcement agency or authority in the Requesting Party*] who has knowledge of this matter is [*name of officer*].

The officer in [*the Central Authority of the Requesting Party*] who is in charge of this matter is [*name of officer*], and he / she can be contacted at [*provide details of address, telephone number, email etc.*].[5]

**PRIOR CONTACT / USE OF OTHER CHANNELS**[6]

There has been previous contact between [*state the relevant authority of the Requesting Party, e.g., Interpol*] and [*state the relevant authority of the Requested Party*] on this matter.

This Request is also being sent to [*the Requested Party*] by [*state the other channel through which the Request is being sent, e.g., diplomatic channel*].

[Signature]

Name:

Office:

Date:

## **FOREIGN LAW IMMUNITY CERTIFICATE** [7]

I, [*name & designation*], on behalf of the Government of the [*Requesting Party*] certify that under the law of the [*Requesting Party*], persons generally or a specified person could, in criminal proceedings instituted under the law of the [*Requesting Party*], be required to answer such questions as are sought to be asked through this Request,.

[Signature]

Name:

Office:

Date:

---

[1] "Criminal proceedings" is defined in section 2 of Singapore's Mutual Assistance in Criminal Matters Act 2000 to include the trial of a person for a foreign offence and also any proceeding to determine whether a person should be tried for the offence. An electronic version of this Act is available at http://sso.agc.gov.sg/.

[2] Where available.

[3] A sample of the certificate is provided as an Annex.

[4] Please provide proforma or form of words as appropriate.

[5] Upon receipt of this request, an acknowledgment will be sent to this officer by the Attorney-General's Chambers of the Republic of Singapore.

[6] This paragraph may be omitted if inapplicable.

[7] This certificate may be tendered in evidence in legal proceedings that may be instituted under the Mutual Assistance in Criminal Matters Act 2000 pursuant to the Request.