MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

Guidelines on Collecting Data from Digital Evidence

August, 2025

DISCLAIMER

This document is intended to provide general guidance and recommended procedures for the collection of data from digital evidence. It has been developed based on contributions from relevant agencies, a compilation of best practices and the professional experience of practitioners in the field. The objective is to support law enforcement personnel and digital forensic practitioners in executing evidence collection activities in a consistent, standardized and methodologically sound manner.

This document is to be used as a reference guide. It is acknowledged that variations in procedures may be necessary to accommodate specific operational environments, case circumstances or jurisdictional legal requirements. For the avoidance of doubt, this document does not create, confer or imply any legal rights or obligations in relation to digital evidence whether in civil, criminal or any other legal proceedings.

References to any commercial products, manufacturers or organizations in this document are provided solely for illustrative and informational purposes. Such references do not constitute and shall not be construed as an endorsement or recommendation by CyberSecurity Malaysia.

COPYRIGHT AND CONFIDENTIALITY STATEMENT

ACKNOWLEDGEMENT

This document was developed by **CyberSecurity Malaysia (CSM)** with inputs from the **Commercial Crime Investigation Department of Polis Diraja Malaysia (PDRM),** the **Malaysian Communications and Multimedia Commission (MCMC)**, the **Securities Commission Malaysia (SC),** the **Pharmacy Enforcement Division of Ministry of Health(MoH),** the **Attorney General's Chambers (AGC)** and the **Pertubuhan Kumpulan Kerja Forensik Digital(KKFD)** to address challenges in conducting forensic investigation on digital evidence. We would like to extend our sincere appreciation to all contributing agencies for their invaluable insights, expertise, and commitment to strengthening forensic capabilities in this evolving domain.

FOREWORD CYBERSECURITY MALAYSIA

The rapid evolution of digital technology has fundamentally transformed how individuals, businesses, and governments function, unlocking new opportunities for innovation and growth. At the same time, this transformation has given rise to significant challenges, especially in the areas of cybercrime and digital investigations. As criminal activities increasingly exploit digital platform and tools, the need for robust, standardised procedures for the collection and handling of digital evidence has become more critical than ever.

In response to this need, Dr. Sarah Khadijah Taylor and her team have developed the Guidelines on Collecting Data from Digital Evidence. These guidelines are designed to equip law enforcement agencies (LEAs) and other relevant authorities with structured procedures, practical insights, and internationally aligned best practices for conducting digital forensic investigations. The document aims to promote consistent, legally sound methods for collecting, preserving, and analysing digital evidence across a wide range of criminal cases.

The successful development of these guidelines was made possible through the collaboration efforts and valuable contributions of key stakeholders. These include the **Commercial Crime Investigation Department of Polis Diraja Malaysia (PDRM),** the **Malaysian Communications and Multimedia Commission (MCMC),** the **Securities Commission Malaysia (SC),** the **Pharmacy Enforcement Division of Ministry of Health (MoH),** the **Attorney General's Chambers (AGC)** and the **Pertubuhan Kumpulan Kerja Forensik Digital (KKFD).** Their insights, expertise, and unwavering commitment were essential in ensuring the document's relevance and reliability.

This initiative embodied our collective commitment to advancing national forensic capabilities and ensuring that our enforcement agencies are fully equipped to respond and tackle the complexities of digital investigations. Through ongoing collaboration and the exchange of knowledge, we can together enhance Malaysia's capacity to protect its digital landscape effectively.

I firmly believe that the implementation of these guidelines will be a crucial catalyst in enhancing the professionalism, efficiency, and integrity of digital evidence handling. Ultimately, this will support our broader mission of upholding justice and strengthening national security in the digital age.

DATO' Ts. DR HAJI AMIRUDIN ABDUL WAHAB FASc
Chief Executive Officer(CEO)
CyberSecurity Malaysia

DOCUMENT OVERVIEW

The increasing integration of digital technologies into daily life has led to a surge in criminal cases involving digital evidence. These guidelines have been developed to address the challenges of collecting, preserving and managing such evidence in a manner that ensures its integrity and admissibility in court. Traditional investigative approaches are no longer sufficient given the volatile and often complex nature of digital data, ranging from mobile devices and cloud storage to encrypted communications. This document provides a standardized, practical framework for law enforcement officers, digital forensic analysts and relevant stakeholders to conduct digital evidence collection effectively, thereby enhancing the credibility of investigations and supporting successful legal outcomes.

DOCUMENT PURPOSE

The purpose of this document is to provide guidance to the Law Enforcement Agency (LEA) in handling digital evidence for investigation. This document is applicable to LEA operating under different operational frameworks. The statements in this document are made in general so that it can be adopted by various LEA. As each agency may have its own process, the agency may need to elaborate further on each statement.

DOCUMENT SCOPE

This document focuses on the proper handling and collection of digital evidence in investigations. It explains key methods for collecting data such as imaging, cloning and memory dumps. The document also highlights potential risks such as contamination of evidence, legal issues and data loss. It provides practical guidance to ensure digital evidence is handled correctly and securely during investigations. This document serves as a practical guide for professionals involved in digital forensics and investigations.

TABLE OF CONTENT

ABBREVIATIONS AND ACRONYM

RAM	Random Access Memory
CSI	Crime Scene Investigation
OSINT	Open Source Intelligence
CCTV	Closed-Circuit Television
VPN	Virtual Private Network
SSH	Secure Shell
VM	Virtual Machine
OS	Operating System
RDP	Remote Desktop Protocol
GPS	Global Positioning System
IMEI	International Mobile Equipment
IoT	Internet of Things
SOP	Standard Operating Procedure
CPU	Central Processing Unit
NTP	Network Time Protocol
MST	Malaysian Standard Time
SSD	Solid State Drive
CLI	Command Line Interface
MAC	Media Access Control
USB	Universal Serial Bus

LIST OF TERMINOLOGIES

Cloud	Cloud computing involves delivering a wide range of computing services over the internet, such as servers, storage, and software. It enables faster innovation, flexible resources, and cost-effectiveness by allowing users to access these services on demand from a cloud service provider, rather than maintaining their own physical infrastructure.
Hash	A hash is a function that transforms an input into a unique fixed-size string of characters, commonly used in computer security and cryptography to ensure integrity of the data.
IP address	An IP address, short for Internet Protocol address, is a numerical label given to devices on a network using the Internet Protocol for communication. It identifies the host or network interface and facilitates communication and data routing between devices on the network.
MAC address	A MAC address, or Media Access Control address, is a unique identifier assigned to network interfaces for communication within a network segment. It serves as a hardware address at the data link layer of network protocols and is provided by the manufacturer of network interface cards.
Memory/RAM	RAM, or Random Access Memory, is a type of computer memory used to store data currently in use. It allows for fast reading and writing of data and is volatile, requiring power to maintain stored information. It is utilized to store data that the CPU requires quick access to while the computer is operational.
Router	A router is a networking device that directs data packets between computer networks, connecting at least two networks and facilitating communication based on their addresses. It is widely used in homes and businesses to connect multiple devices to the Internet.
Social media	Social media encompasses online platforms where users can create, share, and engage with content, fostering social connections and communication through various media formats.

1. DIGITAL EVIDENCE OVERVIEW

Digital evidence is information or data, stored or transmitted in binary form that can be used in legal proceedings. It can be found on various devices, such as computers, mobile phones, or cameras. Digital evidence is often related to electronic crimes, such as child pornography or credit card fraud. Digital evidence can include texts, emails, social media posts, and other types of data.

Digital evidence generally is collected at the crime scene. The crime scene can take place in a house, an abandoned building, office or even in a vehicle. Nowadays, due to advancement of technology, digital evidence can also be collected remotely. For example, it can be located at the Instagram data hosted by the Meta platform. Digital evidence can also be located at online shopping platforms such as Amazon, AliBaba and SuperBuy. In order to obtain this information, the cooperation of both the platform providers and the platform users is vital.

Regardless of the place, the method of handling the digital evidence is the same. The collected digital evidence is then submitted to a digital forensic laboratory for analysis. Digital forensic is the use of scientifically derived and proven methods for the preservation, collection, authentication, analysis, interpretation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or enhancing the reconstruction of events that occurred and to be deemed criminal.

2. CHARACTERISTIC OF DIGITAL EVIDENCE

Digital evidence is unique as opposed to other criteria of evidence such as fingerprints and bloodstain. Digital evidence requires proper handling due to its unique characteristics. It is unique in the sense that digital evidence is:

a. Highly volatile

The data on the digital evidence is highly volatile, meaning it can easily be lost or altered. Changes can easily be made with human interaction or with routine activities such as software update, system reboot, cache clearing, or the automatic deletion of temporary files can permanently erase crucial data. Investigators must act swiftly and carefully when securing digital devices to prevent evidence degradation. It is essential to isolate and document devices promptly to avoid any unnecessary interaction that could change or destroy the data.

b. Can be copied without degradation

One of the defining features of digital evidence is that it can be duplicated an unlimited amount of times without any loss in quality or authenticity. Every copy can be identical to the original, making it possible for investigators to work from forensic copies rather than the source device. Investigators must ensure that proper forensic imaging tools and techniques are used to create exact copies, and cryptographic hash value should be generated to verify and maintain the integrity of the data throughout the investigation.

c. Latent

The data on the digital evidence cannot be seen unless the digital evidence is powered on. Data such as transaction records, social media user profiles and pictures can only be accessed when the digital evidence is powered on. In cases such as a server, data can only be accessed if the server is running (powered-on). If the server is shut down, the data can no longer be accessed, and therefore cannot assist the investigation. In case the digital evidence is powered-off, the digital forensic laboratory will use special tools to power-on the evidence and extract data from it.

d. Cross-border

The data can be transferred to another jurisdictional (cross-border) with ease and speed. For example, a suspect can host a financial database in a web hosting provider in Country A today, and the next day the suspect can transfer the financial database to another web hosting provider residing in Country B. Therefore investigators need to keep in mind that the data does not always reside at the identified premise; instead, the data could be hosted in a different country but is accessed using the suspect's laptop.

e. Time sensitive

Digital evidence is fragile and easily damaged over time. For example, mobile phones that have been kept for several years and have not been powered on nor charged may not function properly when powered on. This could potentially hinder investigation of a case. Therefore it is recommended that any digital evidence found at a crime scene be sent as quickly as possible to the digital forensics laboratory so that the laboratory can employ specialized equipment to create an exact copy of the evidence.

3. PRINCIPLES IN HANDLING DIGITAL EVIDENCE

When handling digital evidence, several principles need to be adhered to in order to ensure the evidence is admissible into the court. The following explains, among others, several principles in handling digital evidence:

a. Comply to legal & policies

All actions undertaken in the process of collecting digital evidence must strictly adhere to relevant legal requirements to ensure the integrity and admissibility of the evidence. Additionally, Investigators are obligated to follow the internal policies and procedures established by their agency, and must avoid taking any actions that may contradict or undermine the agency's official directions or operational protocols.

b. Officer is trained

Investigators involved in handling digital evidence must be competent to perform their duties effectively. This includes ensuring that Investigators are properly trained in the collection of digital evidence and, whenever possible, that their knowledge and skills are regularly tested to maintain high standards. Investigators should attend relevant training programs and engage in continuous professional development to stay updated with emerging tools, techniques, and legal requirements. Additionally, junior Investigators must be adequately supervised to ensure that their actions align with best practices and organizational policies.

c. Create audit trail

An audit trail is a comprehensive record that documents the sequence of activities conducted by Investigators on digital evidence. This is essential to enable third parties such as the next officer assigned to the case, auditors, or experts from the defence counsel to evaluate the Investigators actions and to accurately recall the steps taken throughout the handling process. To support this, a buddy-system should be implemented at the scene to verify that all actions are performed correctly. Investigators must document every action in a clear, accurate, and complete manner, ensuring that the records are properly organized and easy to understand. Additionally, all documentation must be stored in accordance with the agency's retention policy to preserve its integrity, maintain transparency, and support future review or legal scrutiny.

d. Maintain evidence integrity

Evidence integrity refers to the assurance that evidence remains unaltered and reliable throughout its entire lifecycle, from the point of collection to its presentation in court. This applies to both the physical condition of the evidence and the integrity of the data it contains. Data acquired from a suspect's devices must be accurate and reliable. Digital forensic techniques like hashing can demonstrate data integrity is unchanged. Investigators must establish a clear chain of custody and use cryptographic hash values to detect manipulation to the preserved data.

As highlighted in standards like ISO 27037, the UNODC Digital Evidence Best Practice Guide, and the European Committee for Standardization (CEN) Guidelines for a Complete End-to-End Mobile Forensic Investigation Chain; "any forensic activity must be balanced so as to minimize the risk of digital evidence modification while maximizing the evidentiary value of potential digital evidence collection"

e. Get specialist support as needed

A specialist is an individual with specific skill sets who may be either an internal officer or an external party, assigned to assist the Investigators in the collection of data during an investigation. These specialists provide technical expertise that may be beyond the Investigators' skills, and can include professionals such as CCTV system vendors, database administrators, fire control officers, gambling experts, or even senior investigators.

When investigators encounter new technologies or unfamiliar devices at a scene, they are encouraged to request specialist support onsite. Depending on the situation, the specialist may be a system administrator, the product's manufacturer, or any other qualified individual who can provide the necessary technical guidance to ensure accurate and lawful evidence handling.

4. DIGITAL EVIDENCE METHODOLOGY

Forensic investigation methodology of digital evidence involves six (6) main processes, which are Readiness, Preparation, Identification, Collection, Analysis and Presentation. The processes are illustrated in Figure 4.1.

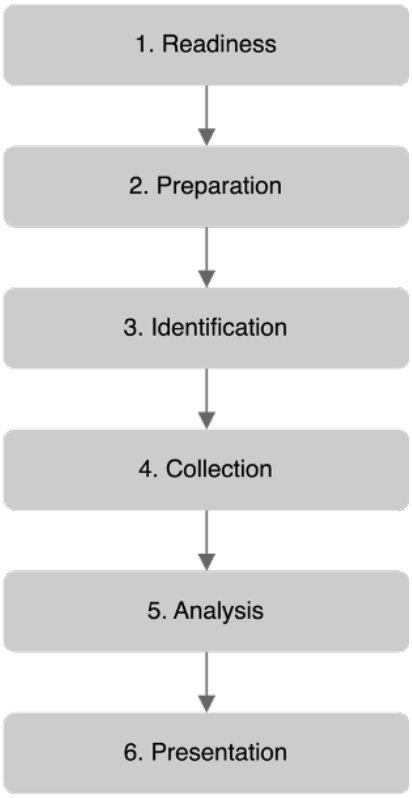


Figure 4.1. Process involved in handling with digital evidence

The next sections shall describe the steps in collecting data. It is important to understand that **while these guidelines outline step-by-step procedures for collecting digital evidence, they are not rigid mandates to be followed in every situation.** At a crime scene, investigators must assess the environment and adapt accordingly. In high-risk or volatile scenarios—such as when there is a threat to officer safety, potential evidence destruction, or hostile presence—it may be more appropriate to prioritize rapid seizure of digital devices over in-depth on-site processing. In such cases, securing the evidence quickly and exiting the scene ensures both investigator safety and the preservation of critical data, with detailed analysis to be conducted later in a controlled environment.

4.1 READINESS

Agencies must be equipped with the capabilities to collect, preserve, and analyse digital evidence following a security incident. The integrity of such efforts hinges on ensuring that all actions taken are legally admissible, technically sound, and operationally efficient. These principles not only guide the quality of the investigation but also ensure that the evidence can stand up in legal or organizational proceedings.

Before engaging in any digital forensic activities, it is essential that policies, procedures, Standard Operating Procedures (SOPs), forms and tools are made readily available. Solid documentations can provide a structured framework that guides investigators through the digital evidence lifecycle—from identification and acquisition to preservation and analysis.

Additionally, only authorized personnel should be permitted to carry out the tasks of collecting digital evidence. Authorization can be in the form of a formal document issued by the agency, such as Badge ID or letter of authorization. This ensures that the evidence is handled correctly from the outset, reducing the risk of contamination or procedural errors that could render the evidence inadmissible in court.

An effective digital investigation often starts with internal organizational policies and procedures. These documents form the foundation for assessing compliance, identifying breaches, and ensuring proper handling during investigations or civil litigation. Having clear policies in place not only streamlines the response process but also helps establish accountability and traceability.

4.2 PREPARATION

The preparation process begins with gathering factual information related to the case, which forms the foundation for developing a comprehensive CSI strategy (Crime Scene Investigation). Based on these facts, investigators can then prepare the necessary resources required to carry out the operation effectively.

The strategy and resource allocations are directly influenced by the nature and details of the information collected. These facts guide critical decisions such as the entry and exit approach, the method of data acquisition, the potential risks and mitigation measures, and the expected conditions at the scene.

Resources typically include a combination of personnel, technical tools, and legal documentation, all of which are essential to ensure the investigation is conducted lawfully, safely, and efficiently.

The steps to prepare for a CSI involves the following steps and explain in following subsection:

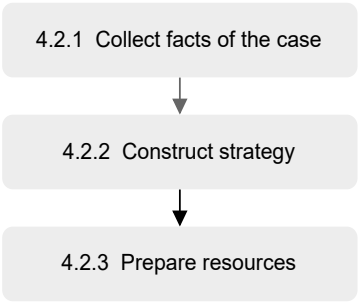


Figure 4.2 Process involve in Preparation phase

4.2.1 Collect facts of the case

Gather facts of the case to support strategic planning and resource preparation, such as the locations where relevant data may be stored and physical security features of the premises. Methods such as Open Source Intelligence (OSINT) and traditional intelligence can be used to gather these facts.

4.2.2 Construct strategy

Assess the physical security of the target location to determine the entry and exit strategies, risk mitigation, and evidence handling procedures. The nature and security posture of the premises can vary widely depending on the type of environment. A residential home and a data center may employ different types of physical security.

4.2.3 Prepare resources

Resources such as documentations, people and tools need to be well-prepared prior to engaging the CSI activity. Investigators need to have solid legal authority and documentation to perform the CSI. Personnel such as the Team Lead, the investigators, the specialist and the contact person at the scene need to be established prior to the CSI activity. Adequate forensic tools must also be prepared and brought to the scene.

4.3 IDENTIFICATION

The identification process involves **identifying potential sources of digital evidence present at the crime scene.** This critical task is conducted on-site during the initial phase of the investigation.

While performing this assessment, it is imperative to prioritize the safety of all personnel. Appropriate precautions must be taken to ensure that no team member is exposed to hazardous conditions or placed in harm's way during the operation.

The steps to conduct identify potential digital evidence at crime scene are illustrated in the following flow chart and explain in following subsection:

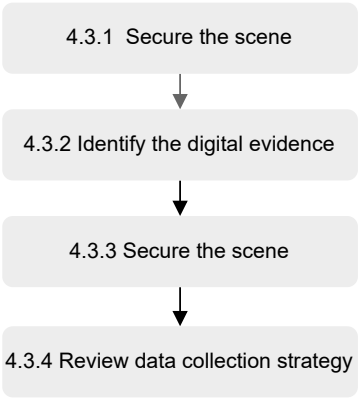


Figure 4.3 Process involve in Identification phase

4.3.1 Secure the Scene

Securing the crime scene is a critical step in any investigation, whether it's a physical crime scene or a digital one. Properly securing the crime scene helps preserve evidence, maintain the integrity of the investigation, and ensures the safety of investigators.

Upon entering the scene, introduce yourself to the premise occupier and explain the purpose of the investigation. Identify everyone else in the premise and move everyone away from the digital evidence and source of electricity. Examine every room on the premises and locate potential digital evidence.

Limit access to the digital crime scene to authorized personnel only. Restrict user permissions to prevent unintentional or intentional alterations to digital evidence. In terms of a digital scene, steps must be taken to identify and isolate the scene. Then, restrict access to the system immediately.

4.3.2 Identify Digital Evidence

Upon entering the premise, all digital evidence must be located. Once it is located, information such as (i)the purpose of the devices, (ii) the users of the device and (iii) whether the device is connected to offsite storage need to be collected. This information can be sought through a combination of manual observation and interview techniques designed to elicit relevant details.

4.3.3 Document the Scene

Create a sketch or layout of the premises, clearly marking the locations of all identified digital evidence. This visual representation helps in understanding the environment and can aid in establishing ownership or association with specific individuals. Ensure that the documented scene contains accurate placement of each digital device within the premises. The following sample of pictures provide understanding on documenting the scene.

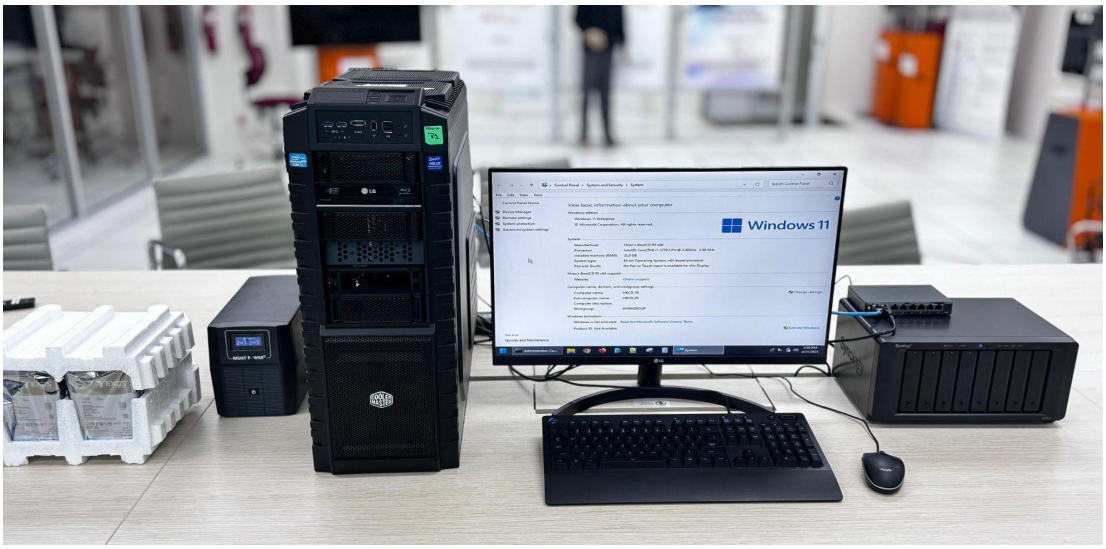


Figure 4.4 Overall frontal view of digital evidence

Figure 4.5 Overall back view of digital evidence

Figure 4.6 Detailed pictures of digital evidence

4.3.4 Review Data Collection Strategy

At this stage, assess whether the planned data collection strategy is practical and effective, or if alternative methods may yield better results. This evaluation should be based on several key considerations:

- **Scope of Collection:** Is it necessary to collect all digital evidence, or should effort focus only on items most relevant to the case?
- **Data Collection Method:** Which data collection technique will obtain the most relevant and complete data from the evidence?
- **Storage Capacity:** Does the agency's storage media have sufficient capacity to securely hold all collected data?
- **Collection Environment:** Would it be more effective and secure to conduct data extraction at a different, more controlled location?

All decisions made during this assessment must be justifiable, clearly documented, and in full compliance with legal authorizations governing the investigation.

4.4 COLLECTION

Collection refers to the **process of acquiring the digital evidence and its data using suitable forensic techniques**. All collection activities should be conducted in a manner that minimize the risk of digital evidence modification while maximizing the evidentiary value of potential digital evidence collection.

Collection involves several steps, as explained in Chapter 5 of this document.

4.5 ANALYSIS

After digital evidence is collected at the crime scene, the evidence needs to be submitted to the digital forensic laboratory for analysis purposes. The purpose of sending the digital evidence to the forensic laboratory is for data recovery, data reconstruction and data correlation.

The purposes of conducting analysis are to:

- Extract deleted, hidden, or obfuscated data.
- Reconstruct fragmented information into coherent evidence.
- Establish data correlations that support the case hypothesis.

The following **items need to be supplied to the laboratory** when requesting for digital evidence analysis:

- **The digital evidence / copy of digital evidence** - in order to conduct forensic analysis, the data to be analyzed must be available
- **Case objective** - clear scoping to focus the analysis on specific questions
- **Any available triage information** - data and information that has been documented during data collection at the scene

All activities during this phase are guided by the case objectives, ensuring that the analysis remains relevant, focused, and legally sound.

When submitting the digital evidence to the forensic lab, the investigator must ensure that the forensic analyst fills in the chain of custody form.

At the end of the analysis process, the laboratory will produce a forensic report. This report is then submitted to the prosecutor for case review and subimtted to court to support the case investigation.

4.6 PRESENTATION

Once the analysis phase is completed, the findings must be effectively communicated through the Presentation phase. This **involves compiling a structured and comprehensive report that accurately reflects the forensic process and the evidence uncovered.**

The presentation of findings should be clear, concise, and tailored to the intended audience, which may include investigators, legal professionals, or the judiciary. It is crucial to translate complex technical information into understandable language, avoiding unnecessary jargon while preserving technical accuracy.

Presentation of findings can be in the form of a forensic report. For complex cases, visual aids such as animations, simulations, flow charts, the use of figures and tables can be used to enhance clarity and reinforce the narrative and may aid understanding of layman stakeholders.

Each finding must be supported by references to specific artifacts or data sources, and all conclusions should be drawn directly from the evidence, free from speculation or bias. The report should also include a summary of the tools and methodologies used, the scope of the analysis, and any limitations encountered. Ultimately, the goal of the presentation phase is to provide a transparent, credible, and legally sound account of the digital investigation that can withstand scrutiny in both investigative and judicial environments.

5. METHOD FOR DATA COLLECTION

The process of data collection involves collecting the digital evidence and its associated data using appropriate methods. This includes proper labelling, packaging, transportation, and storage of the digital evidence in a secure and designated location. The collection process must ensure the integrity and authenticity of the evidence throughout its handling. The steps involved in the collection of digital evidence is illustrated in the following figure and are described in the following subsections.

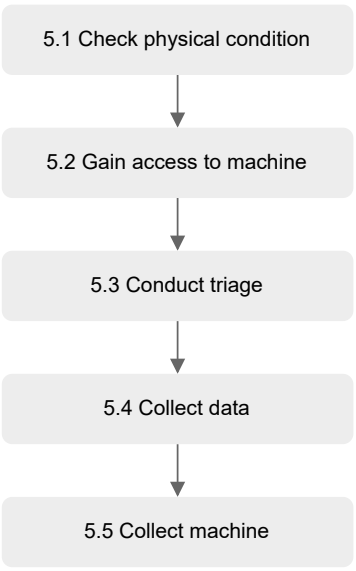


Figure 5.1 General steps for collecting data from digital evidence

5.1 CHECK PHYSICAL CONDITION

Once digital evidence is located, a thorough visual inspection of the machine or device must be conducted to assess its physical condition. The purpose of this inspection is **to determine whether the machine is in its normal operational state while ensuring the integrity of the evidence.**

The following steps can be used to assess the physical condition of the digital evidence:

- **Determine power status**
  Record whether the machine was found powered on or off at the time of inspection.
- **Observe for physical damage**
  Inspect the machine for any signs of damage, including missing components, cracks, or dents, whether caused intentionally or unintentionally.
- **Examine peripheral connections**
  Take note of all peripheral components, such as keyboards, monitors, USB devices, network cables and any suspicious devices connected to the machine.
- **Check for tampering indicators**
  Indicators of tampering, such as broken or missing security seals, hardware modifications, or attached suspicious devices, must be identified and documented.

All observations must be meticulously documented through the use of close-up and wide-angle photographs, video recordings, and detailed sketches. This documentation will help maintain the chain of custody and ensure the evidence remains intact for further analysis.

5.2 GAIN ACCESS TO THE MACHINE

After the machine or device are physically examined, next, attempt to gain access to it. This is conducted in order to triage the machine and determine whether it is valuable for the case. The process is analogous to meticulously sifting through a vast archive of office documents to identify and extract only those directly relevant to the case at hand.

Obtain the cooperation of the suspect or system operator to access the machines or devices. Then locate and access applications, services, files, or folders that are relevant to the investigation. Be mindful that a computer or a smartphone may have more than one(1) desktops or that the data is not located in the device, rather it is stored on cloud.

5.3 CONDUCT TRIAGE

When access to the machine or device is successful, conduct triage to understand its purpose and the data related to the case. **The objective of conducting triage is to assess the value of the digital evidence, whether or not it is relevant to the case.** As mentioned in the previous section, this process is analogous to meticulously sifting through a vast archive of office documents to identify and extract only those directly relevant to the case at hand.

Triage is mainly conducted to overcome the challenge of:

- inability to access the data after device is seized due to passwords
- fast moving of data from data storage to another

Triage can be conducted by using forensic software or direct access. When conducting triage, consider NOT TO TURN OFF THE INTERNET due to the following issues:

- cutting off Internet will render online account inaccessible
- cutting off Internet will prevent device from receiving multi factor authentication code, which is needed to access online account

Be cautious not to alter data when triaging evidence. This process must balance the need to preserve evidence while maximising its evidentiary value

5.4 COLLECT DATA

Data collection involves the identification, acquisition, and preservation of volatile and persistent data from digital evidence at the scene of an incident. The steps to collect data is described in following figure:

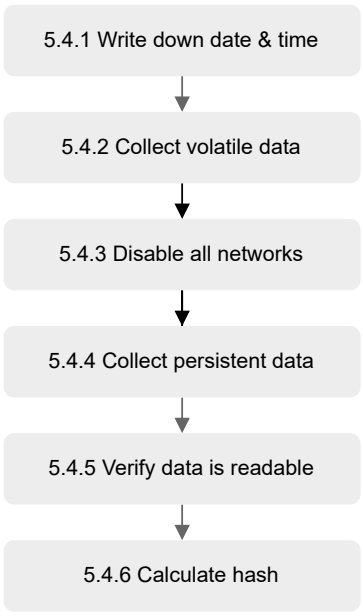


Figure 5.2 Detail steps on process of collecting data

5.4.1 Write down date & time

Before beginning any digital evidence collection, document the current date and time using a verified time source (e.g., NTP, MST clock). Next compare the device system date and time with the verified time source to identify and document any time offset. This step is essential in establishing the starting point of the evidence handling process, ensuring traceability, and supporting the integrity and admissibility of the evidence in legal proceedings.

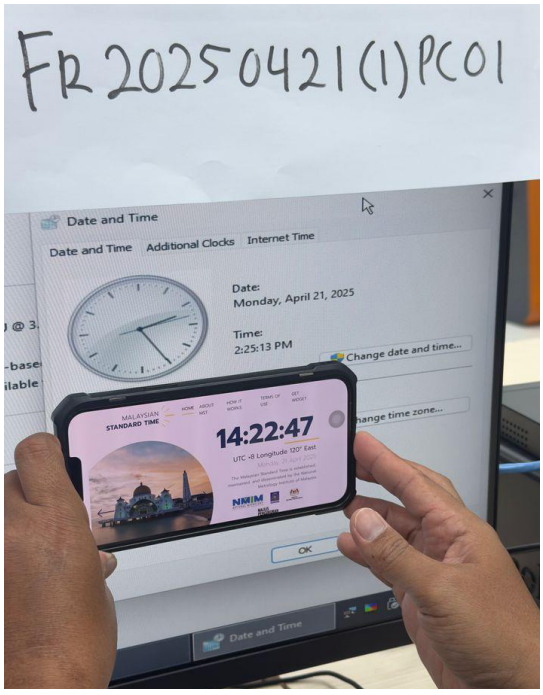


Figure 5.3 Example of documenting the time offset of digital evidence

Time Source	Malaysia Standard Time(MST) https://mst.sirim.my/	Device Time
Date	2025-04-21	2025-04-21
Time	14:22:47 (UTC+8)	14:25:13 (UTC+8)
Device Time Offset	+ 00:02:66	

Table 5.1 Example of timestamp comparison

5.4.2 Collect volatile data

Volatile data refers to the transient data held in a computer's live memory and system state - such as memory contents, CPU registers, active network connections and running processes - that exists only while the system is powered on. Because it is unavailable when a machine is shut down or rebooted, volatile data must be captured first during an investigation to preserve crucial evidence.

Collecting volatile data is crucial in a digital forensic investigation because it provides a live "snapshot" of a system's activity. Some of the artifacts present in the memory are:

- **Encryption keys and credentials**
  Many encryption keys, session tokens (e.g., VPN or SSH), and user credentials reside in the memory. These can be recovered and be used to access encrypted partitions or identify hidden partitions in the host.
- **Live malware and in-memory artifacts**
  Sophisticated malware often unpacks or operates entirely in memory to avoid leaving traces on disk. A memory dump can reveal unpacked binaries, injected code, or malicious hooks that disk analysis would miss.
- **Active network connections**
  Memory images also contain a complete capture of the network state of the host at the time of acquisition. This information is critical to identify open ports and services which in return allow for identification of malicious command and control (C2) servers.
- **Running processes and system state**
  Memory stores running processes during acquisition, allowing tracking process creation activity to discover harmful behaviour like Living off the land binaries, scripts, and libraries. Additionally, memory processes can be split for malware research.

There are several methods to collect volatile data, such as followings:

- **Memory dump**
- **Screen mirroring**
- **Screenshot / video record**
- **Writing**

The methods are described in detail in Section 6 of this document.

5.4.3 Disable all networks

Once volatile data has been captured, next disable all networks from the machine/device. Active network connections—such as Wi-Fi, Ethernet, Bluetooth or cellular data—pose risks of including remote tampering, data deletion, malware activation, or unauthorized access. By isolating the device from all networks, investigators prevent external interference and ensure that volatile or sensitive data is not altered, overwritten, or lost during the collection. This is especially important in cases involving live systems, encrypted communications, or cloud-synced data.

Network can be disabled by turning on the airplane mode option on devices such as mobile phones and tablets. Faraday bags can also be an alternative to block signals entirely. For machines like computers, turn off the Wi-Fi connection or if the computers are using internet cable lines, then plug off the cables from the computers.

5.4.4 Collect persistent data

Persistent data refers to any data that is retained on a storage media even after the system is powered off. This type of data does not get erased or lost when a computer shuts down or restarts, making it crucial during forensic investigations. Examples of such data are documents, pictures, videos and internet history.

Persistent data can be collected using the following methods:

- **Imaging**
- **Cloning**
- **Download / copy data**
- **Screen mirroring**
- **Screenshot / video record**
- **Writing**

The methods are described in detail in Section 5 of this document.

5.4.5 Verify data is readable

Once the data has been collected, ensure that it is readable and viewable. In some cases, data may become corrupted during the collection process, making it unusable for forensic analysis. This can increase the time required by the Investigators at the scene. However, it is better to be safe than sorry. Verifying that digital evidence is readable is a fundamental step in digital forensics that safeguards the quality and integrity of the collected evidence.

5.4.6 Calculate hash

A hash is a fixed-length string of characters generated by applying a mathematical algorithm to data. To calculate a hash, forensic investigations use cryptographic algorithms such as SHA-1, SHA-256 and SHA-512. Specialized forensic software or command-line tools can be used to run these algorithms on a file or disk image. This process creates unique digital fingerprints for a file, disk image , or entire dataset.

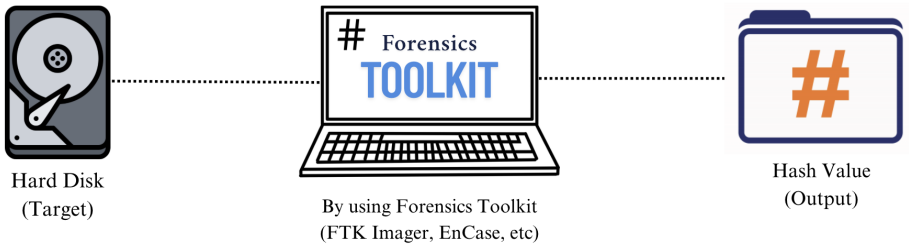


Figure 5.4 Illustration of how hash value is calculated from a target hard disk

Hash is used in digital evidence data collection to demonstrate the integrity of the collected data. If the hash value changed, that means the collected data has been altered during the transportation or analysis. Hash values build trust in the investigative process and protect the evidence from claims of tampering.

5.5 COLLECT MACHINE

Collecting a machine involves seizing digital evidence at the scene. Depending on the authority being given, machines or devices belonging to suspects may need to be collected for the purpose of conducting further forensic analysis as well as to present the evidence into the court.

Once secured, the machine should be properly labeled, documented, and packed to maintain its integrity during transportation to the forensic laboratory. The following subsections described the next steps to be taken for collecting machines.

5.5.1 Shut down

Should the CSI strategy choose to seize machines, it is necessary that the machines be appropriately shut down in order to preserve the current data state and to ensure that forensic integrity is maintained.

The process of shutting down a machine or device is as follows:

- **Force shut down by pressing the power off key for more than 5 seconds. Then pull off any attached power supply**
  This allows active data to be preserved for forensic purposes later. It immediately halts the operating system, preventing further changes from background processes or the activation of encryption mechanisms that may occur during a standard shutdown.

- **For servers, stop all running processes. Then press the shutdown function from the menu**
  This avoids the data from being corrupted. Servers typically run critical services, databases, or networked applications that can be adversely affected by improper shutdowns.

- **For mobile phones and tablets, consider not to shut down**
  Shutting down a device may trigger security features like encryption, lockouts, or remote wipe commands upon reboot. if situation permits and feasible to do so, charge the device in order to prolong the battery state.

5.5.2 Label

Labeling seized machines/devices ensures clear identification, prevents confusion, and maintains the integrity of the chain of custody. It allows for accurate tracking of evidence, helps avoid mix-ups, and supports the legal process by ensuring evidence can be reliably traced back to its source. Proper labeling is essential for preserving the evidence's credibility in court and during forensic analysis.

The recommended best practices is as follows:

- Label the machine using a unique convention - evidence must be labeled with a unique, standard format to ensure clear identification and easy tracking.
- The label must stay throughout the lifetime of the evidence in custody - Use durable materials like tamper-proof stickers or permanent markers.
- If a machine has a sub item, it must be labeled too - Sub items like SD cards must be labeled individually and linked to their parent device.
- Label at proper place - Place labels on a clean, visible part of the device, avoiding serial numbers, warranty tags, screens, or working parts.
- If you decide to seize the cables, ensure that the cables are properly labelled for future reconstruction - Cables are essential for reconstructing the digital evidence in the digital forensics laboratory during the analysis phase.

5.5.3 Register

Registering the digital evidence ensures accurate tracking, maintains the chain of custody, and preserves evidence integrity for legal use. It helps prevent confusion and supports transparency throughout the investigation. Ensure that the evidence unique identifier such as serial number is documented. Investigators may use a designated form or a computerized system to register the evidence.

5.5.4 Package and Seal

Digital evidence must be packaged immediately after collection to prevent physical damage, contamination, or tampering. The evidence should be placed in a suitable container, such as an anti-static bag, durable plastic packaging, or a rigid box, to provide adequate physical and electromagnetic protection.

Once packaged, the item must be sealed using an official agency seal. This seal must display the initials or signature of the collecting officer, a unique evidence label, and the date and time of sealing. The seal must be applied in a manner that will clearly indicate any attempt to access the contents.

Sealing the evidence formally begins the chain of custody. From this point, the collecting officer assumes responsibility for the evidence until it is officially transferred. Proper packaging and sealing preserve the integrity of the evidence and ensure its admissibility in court.

5.5.5 Transport

Digital evidence must be transported with care to maintain its condition and security. After sealing, the evidence should be promptly transported to the forensic laboratory or secure storage facility. It must remain under the direct supervision of authorized personnel at all times and must not be left unattended.

During transit, the evidence should be kept in a locked compartment or secured container within the transport vehicle. If the journey includes any stops, overnight stays, or a change in personnel, these events must be fully documented, including the time, location, and reason.

The goal of transporting digital evidence is to maintain its integrity while ensuring a complete and traceable record of its movement. This supports the continuity of the chain of custody and the credibility of the investigation.

5.5.6 Chain of Custody

A critical aspect of evidence handling is maintaining the chain of custody. This refers to the detailed documentation of every person who has handled the evidence, creating a comprehensive record that tracks its movement and ensures accountability. The chain of custody establishes the integrity of the evidence by documenting its possession from the moment of collection until its presentation in court or other resolution.

Whenever evidence is transferred, specific information must be documented. This includes the receiver's name, the purpose of the transfer, the date and time of the transfer, the location of the transfer, and the names of any witnesses present during the transfer. This information is recorded on a Chain of Custody form, establishing a clear, accurate, and unbroken record of the evidence's handling. Any alteration, modification, or deviation from standard procedures must also be documented on the Chain of Custody form.

6. DETAILED STEPS ON DATA COLLECTION

Each type of digital evidence requires specific data collection methods, which may vary depending on the nature of the evidence and the circumstances under which it is encountered. In cases where certain data sets are protected, credentials of the owner or administrator is required. Therefore, it is strongly recommended for Investigators to get the owner or administrator full cooperation during the on-site investigation. Such cooperation significantly enhances the likelihood of successfully acquiring and preserving critical digital evidence. The followings are list of methods for data collection:

6.1 IMAGING

Imaging is a widely used method in digital forensics. It creates a bit-by-bit copy of a storage device using forensic tools. This copy includes files, deleted data, hidden areas and system information. It helps protect the original data so nothing gets changed. By using a copy, digital forensics analysts can look at everything safely. This is really important in legal cases because the copy must be exactly the same as the original to be trusted in court. Once imaging is completed, the activity logs generated by the imaging tool are advised to be extracted and stored in a case file.

This method is useful to recover hidden and deleted data; to conduct keyword search; and to recover corrupted partitions and formatted hard disks.

Output of the imaging procedure is an image file in format such as file.raw, file.dd or file.e01. A forensic software is needed to read the image file.

The following subsections shall explain the imaging process from four(4) source of evidence:

- Physical computer
- Cloud disk
- Virtual machine
- Inaccessible drive

6.1.1 Physical Computer

Physical computer imaging is a method that creates a bit-by-bit copy of a computer storage drive using forensic tools. Examples of storage drives are hard disk and SSD.

The steps to conduct imaging on physical computers are as follows:

1. Shut down the computer
2. Remove the hard disk from the computer
3. Connect the target harddisk to a write blocker or imaging hardware
4. Launch the image procedure using the hardware or software
5. Once imaging is complete, the hash value will be displayed
6. Document the hash value, date and time of imaging process
7. Disconnect the hard disk from the write blocker / imaging hardware

6.1.2 Cloud Disk

Criminals nowadays move to cloud environments for scalability and mobility. Criminals leverage cloud platforms to store and distribute illegal content, manage stolen data from scams, facilitate illicit operations and host illegal shopping platforms. This makes cloud storage a critical focus in modern digital investigations.

Cloud disk can be imaged for the purpose of preserving a complete and accurate copy of a live cloud environment for analysis purposes. Some charges may be imposed by the cloud provider when mounting additional disks or downloading the collected data.

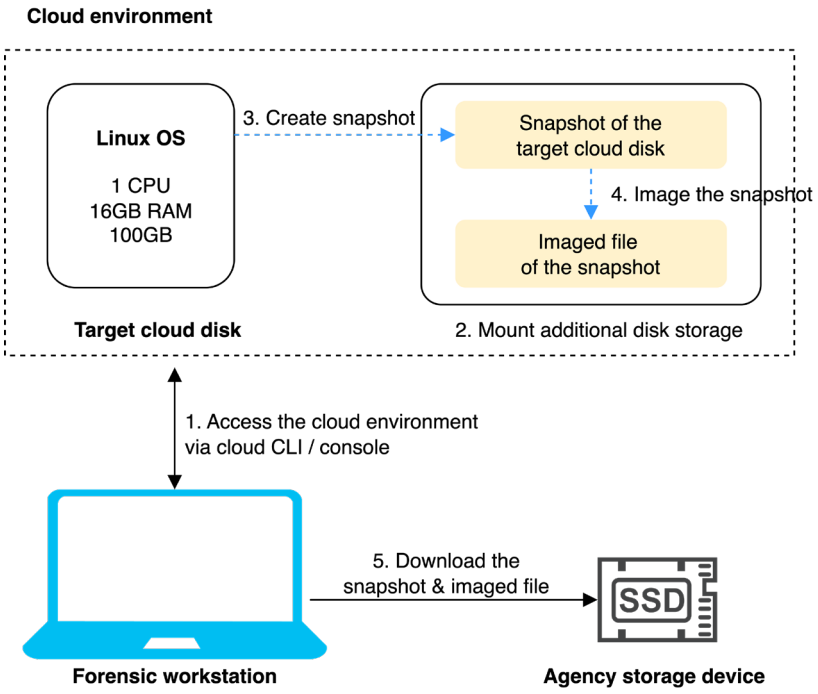


Figure 6.1 Illustration of cloud disk imaging

The steps to collect data from cloud storage are as follows:

1. Obtain access rights to the cloud provider's Command Line Interface(CLI) or console
2. Identify the disks associated with the case; including relevant data such as operating system disk, database disk, and other storage volumes (the target cloud disk)
3. Download configuration file containing timestamp, regional settings, instance type, disk sizes, network settings, assigned IP addresses, etc.
4. Mount additional disk on the cloud environment (charge may be imposed)
5. Create a snapshot of the target cloud disk and store it in the additional disk
6. Image the snapshot of the disk (This imaged file will be stored in the additional disk)
7. Download the imaged file and the snapshot into agency storage device
8. Document the hash value
9. Verify the files are running well

6.1.3 Virtual Machine

A virtual machine (VM) is a software-based replica of a real computer that enables several operating systems to run independently on the same physical machine. It is managed by a hypervisor that usually has an export function.

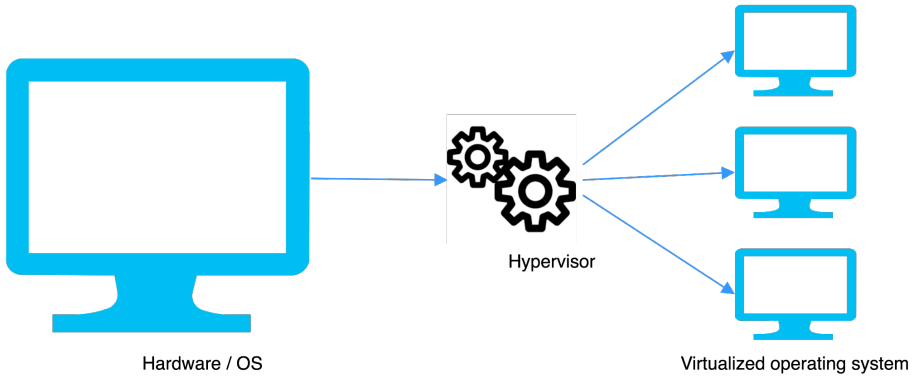


Figure 6.2 How hypervisor works

Most often, the VM file and its configuration file can be exported out. Some open-source hypervisors do not have a dedicated export function, hence, imaging methods are useful to collect the VM data.

Types of hypervisor:

a. Bare metal hypervisor - a virtualisation layer that is installed directly onto the physical hardware of a computer or server without requiring a host operating system.

b. Hosted hypervisor - a virtualization software that runs on top of an existing operating system (OS) such as Windows, MacOS, or Linux.

Methods to connect to the hypervisor:

a. Direct - connect the agency storage device directly into the hypervisor. This is done if the host machine has physical USB slots.

b. Remote - this is done if the host machine does not have a physical USB slot. Connect the forensic workstation to the hypervisor machine via network and attach the agency storage device to the forensic workstation.

Steps to collect data from the Virtual Machine:

Scenario 1 - Hypervisor has export function:

1. Power off the virtual machine.
2. Use export/backup function to export the VM disk and VM configuration file into the agency storage device.
3. Calculate hash value
4. Verify the files are running well

Scenario 2 - Hypervisor does not have Export function:

1. Confirm the VM disk file path
2. Connect forensic machine to the VM host machine using SSH
3. Image the VM using Linux-based dd or dcfldd command from the host machine
4. Store the image file into an agency storage device
5. Copy the configuration files into the agency storage device
6. Document the hash value
7. Verify the files are running well

6.1.4 Inaccessible Drive

There are cases where a drive cannot be accessed physically due to hardware constraints, remote location, or embedded design. Hence the process of conducting imaging is slightly different from the subsection above. In this case, the target hard disk can be imaged using a USB bootable disk, which contains the Linux operating system.

The steps to conduct imaging of inaccessible drive are as follows:

1. Confirm the drive is running
2. Identify the drive or partition to be imaged (e.g: /dev/sda, /dev/nvme0n1)
3. Set up a secure location for storing the image file and ensure it has enough space
4. Create an image file with Linux-based dd or dcfldd command
5. Document the hash value
6. Verify the files are running well

6.2 CLONING

Cloning is a method that creates an exact, bit-by-bit copy of a storage device onto another storage device. Examples of storage devices include hard drives and solid-state drives (SSD). **Cloning is useful for preparing identical systems for simulation, as it directly transfers the data to another physical disk.**

The steps to create a cloned hard disk are as follows:

1. Shut down the computer
2. Remove the hard disk from the computer
3. Connect the hard disk to a write blocker or cloning hardware
4. Connect agency storage device to the cloning setup
5. Launch the cloning procedure using the hardware or software
6. Once cloning is complete, verify the hash values of both drives
7. Document the hash value, date and time of imaging process
8. Verify the cloned hard disk is running well

The result of the cloning procedure is a fully usable copy of the original disk on the agency storage device, including hidden, deleted, and system files. The cloned disk can then be analyzed or used as a bootable copy.

6.3 MEMORY DUMP

A memory dump is a snapshot of a computer's memory at a specific moment. Memory contains the current state of the system, including running processes, loaded drivers, and other relevant information. This method is used to gather valuable insights into ongoing processes, user activities, network activities and potential security breaches.

The general steps of conducting memory dump are divided into two(2) categories and explained as follows:

Steps for computer or server:

1. Attach agency storage device to the machine, containing the dump tool
2. Initiate the dump tool from the agency storage device
3. Save the imaged file into the agency storage device
4. Calculate and document the hash value, date and time
5. Disconnect the agency storage device from the machine
6. Verify the image file is running well

Steps for cloud:

1. Attach agency storage device to the machine, containing the dump tool
2. Initiate remote connection to the host using methods such as SSH or RDP command
3. Mount additional cloud storage
4. Initiate the dump tool from the agency storage device
5. Save the imaged file of the cloud disk memory into the mounted cloud storage
6. Copy the image file from the mounted cloud storage into the agency storage device
7. Calculate and document the hash value, date and time
8. Disconnect the agency storage device from the machine
9. Verify the image file is running well

Steps for virtual machines:

1. Attach agency storage device to the machine
2. Locate memory file of the VM (example: file.vmem; file.vmsn; file.vsv)
3. Export the memory file into agency storage device
4. Calculate and document the hash value, date and time
5. Disconnect the agency storage device from the machine
6. Verify the file is running well

6.4 DOWNLOAD / COPY DATA

This method involves downloading or copying data into an agency storage device. The data may come from sources such as servers, computers, software, or cloud services, and can include documents, media files, software, databases, logs, social media content (both current and archived), and online transaction records.

Downloading or copying data is commonly applied in the following situations:

- When the success rate for system reconstruction is not guaranteed, even if the machine is seized - Reconstruction may be hindered by factors such as encryption, hardware damage, or proprietary system configurations.
- When data is stored remotely, where access is not guaranteed even if the machine is seized - Data located in cloud services or external servers may remain inaccessible without valid authentication or live network access.
- When only specific data is important for the investigation, such as a Facebook posting - Selective acquisition is preferred to efficiently obtain relevant evidence, eliminating the need for full live imaging in such cases.

The general steps are as follows:

1. Determine relevant data to be collected
2. Attach agency storage device to the device / machine that host the data
3. Download or copy data into the agency storage device
4. Calculate and document the data hash value, date and time
5. Disconnect the agency storage device from the machine
6. Verify the downloaded/copied data is running well
7. Alternatively, the data can also be exported into an agency email account. Once data is completely exported, an email notification will be sent to the agency email account.
8. If social media or instant messaging is involved, ensure that other relevant data such as user profile, date of posting, sender and receiver profiles are documented (via method such as download, screenshots, screen mirror, or photograph)

6.5 SCREEN MIRRORING

Screen mirroring involves duplicating the display of a device onto an external screen. It allows investigators to view and document the content and graphical user interface in real time without directly interacting with or altering the original device. It is particularly suitable for smartphones and tablets, and it offers a non-invasive means of preserving digital evidence in its original state.

Screen mirroring method is commonly applied in the following situations:

- When data resides remotely and download method could not be found
- When downloading the data takes too long (more than a day)
- When there is a need to demonstrate the data in its exact display to ease understanding (Graphical User Interface GUI)

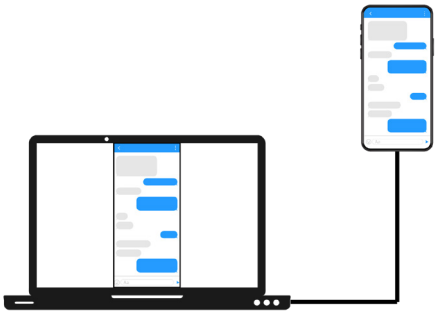


Figure 6.3 Illustration of screen mirroring of a mobile phone

The steps to screen mirror a device are as follows:

1. Establish a connection between the forensic workstation and the device (using cable or Bluetooth)
2. Initiate screen mirroring software from forensic workstation
3. Screenshot/video record relevant data to the case, using screenshots or screen recordings function; eg: Snipping tool(WinOS) or Command+Shift+5 (MacOS)
4. Store captured files on agency storage media
5. Calculate and document the hash value, date and time
6. Close the software, and disconnect the agency storage device from the machine
7. Verify the video files or screenshots are running well

6.6 SCREENSHOTS / VIDEO RECORDING

Screenshots or video recording involve the use of the suspect's device internal function to capture the data displayed on the device's screen. This method is useful when Investigators need to preserve critical, time-sensitive data such as volatile transaction records; or when investigators need to rush out of the premises due to various reasons; or when a forensic workstation is not available at the scene.

This method creates new data on the suspect's device. The data are the pictures and video files that have just been screenshot or video recorded . Nevertheless, this method does not modify or tamper any existing data on the device, rather it creates new data that can be explained by the Investigator. This process also cut down a lot of analysis hours in the digital forensics laboratory, since the right data has been captured at the scene.

In court, Investigator needs to be able to identify and explain the data that is generated by him/her during the data collection process. Therefore, activities must be properly documented by the Investigator, including the date and time.

The steps to screenshots / video recording content of a device are as follows:

1. Determine relevant data to be collected from suspect device
2. To screenshot, these are the options:
    - Windows - use Snipping Tool, Snip & Sketch or press key Windows + PrtScn
    - MacOS - press key Command + Shift + 5
    - Linux - press Shift + PrtScn; or key Alt + PrtScn; or use GNOME screenshot
    - Mobile device - press Power + Volume Down for Android, for Apple side button + Volume Up
3. To video record, these are the options:
    - Windows - use Snipping Tool or use Snip & Sketch
    - MacOS - press key Command + Shift + 5
    - Linux - press Shift + PrtScn; or key Alt + PrtScn; or use GNOME screenshot
    - Mobile device - for Android, go to Settings and look for Screen Recording. For Apple, go to Control Center to enable Screen Recording and manually start it.
4. Store captured files on agency storage media
5. Calculate and document the hash value, date and time
6. Verify the video files or screenshots are running well

6.7 WRITING

Writing is particularly useful when dealing with devices or systems that do not support automated data extraction or where forensic tools are incompatible. Writing in this sense is using pen and paper to document important information, or take photographs.

This method is commonly applied to devices such as mobile phones, GPS units, routers, vehicle infotainment systems, smart TVs, and other IoT devices where information like IP addresses, MAC addresses, IMEI numbers, GPS coordinates, and user activity logs may only be visible on-screen and cannot be exported electronically. Writing also plays a critical role in documenting ephemeral data, such as one-time pop-up messages or temporary status indicators that disappear before a screenshot or extraction can occur.

During on-site operations, it is often necessary to manually draw diagrams, floor plans, or network maps to capture the physical or digital layout of a scene. Additionally, writing is used to log any handwritten notes, labels, or markings attached to physical items that are relevant to the investigation. It is equally important in recording interview notes, such as when a device owner describes how or when a phone was used. ensure that the writings or photographs are properly kept in the Case File for future reference.

7. RISKS AND MITIGATION

It is crucial to recognize and address the risk with appropriate mitigation strategies in order to preserve the digital evidence's integrity, reliability and admissibility. The following list are the potential risks and possible mitigation to minimize the risks:

7.1 EVIDENCE CONTAMINATION

One of the primary concerns is evidence contamination, which can occur through improper handling, exposure to external interference, or unauthorized system access.

Mitigation steps:

- Use write blockers to prevent any changes to the original data
- Practice a rigid conformity to the chain of custody
- Disable network connections immediately if remote access or suspicious activity is detected on the target machines.

7.2 VOLATILE DATA LOSS

Another significant risk is volatile data loss, especially when working with live systems where memory content and running processes can lost upon shutdown.

Mitigation steps:

- Prioritize capturing volatile data (memory, running processes, network connections) before shutting down the system.
- Document the system state before and during acquisition to capture important details such as running processes, network connections, and logged-in users, to understand what was happening during the time of the incident.
- Use live forensics tools (e.g., FTK Imager, Belkasoft RAM Capture) to capture volatile data.

7.3 USE OF OPEN SOURCE TOOL

Using open-source tools can be helpful for handling digital evidence. They are free and sometimes offer better features than paid tools. However, there are risks, such as outdated algorithms, inaccurate results, and tools that might secretly collect case information.

Mitigation steps:

- Use trusted and well-known tools; such as Autopsy, Volatility and Sleuth Kit
- Always download tools from official or trusted sources - and verify the downloaded file integrity using checksum
- Test the tools prior to use - ensure that it is able to produce accurate result

7.4 LEGAL ISSUES

Legal issues may arise if evidence is obtained without appropriate authority or in violation of jurisdictional boundaries.

Mitigation steps:

- Ensure proper search warrant or legal authorizations are in place
- Limit collection to scope authorized by legal documentation.
- Work closely with legal counsel to verify compliance.

7.5 FAILURE OF THE TOOL

Failure of the tool can jeopardise the integrity of the evidence.

Mitigation steps:

- Use reliable, tested, and certified forensic tools to ensure the accuracy of data
- Carry backup tools and spare drives for imaging
- Validate image integrity using hash algorithms for data consistency and authenticity.

7.6 INADEQUATE DOCUMENTATION

A common yet serious flaw is poor documentation that can undermine the credibility and admissibility of evidence.

Mitigation steps:

- maintain detailed logs of each actions by write down in forensics diary or note
- use photographs, timestamps, and descriptive notes during collection
- record who, what, when, where, and how for all activities

7.7 UNAUTHORISED ACCESS

Unauthorized access to the crime scene or digital evidence introduces both physical and digital threats.

Mitigation steps:

- restricted the scene access to authorized personnel only
- secure the perimeter to establish a controlled environment
- Assign a scene manager to oversee security and coordination.

7.8 NETWORK DEPENDENCIES

Disconnecting systems from the network could impact other systems or trigger security responses (e.g., data wiping).

Mitigation steps:

- Coordinate with IT personnel to understand interdependencies.
- Consider capturing network traffic before isolation
- Use non-intrusive acquisition methods when feasible.

7.9 HIDDEN OR ENCRYPTED

Obtaining evidence is more difficult if the data is hidden or encrypted.

Mitigation steps:

- using advanced analysis tools capable of deep analysis and decryption attempt
- identify and document signs of encryption early
- conducting full disk imaging to preserve all data including slack and unallocated space.

7.10 HUMAN ERROR

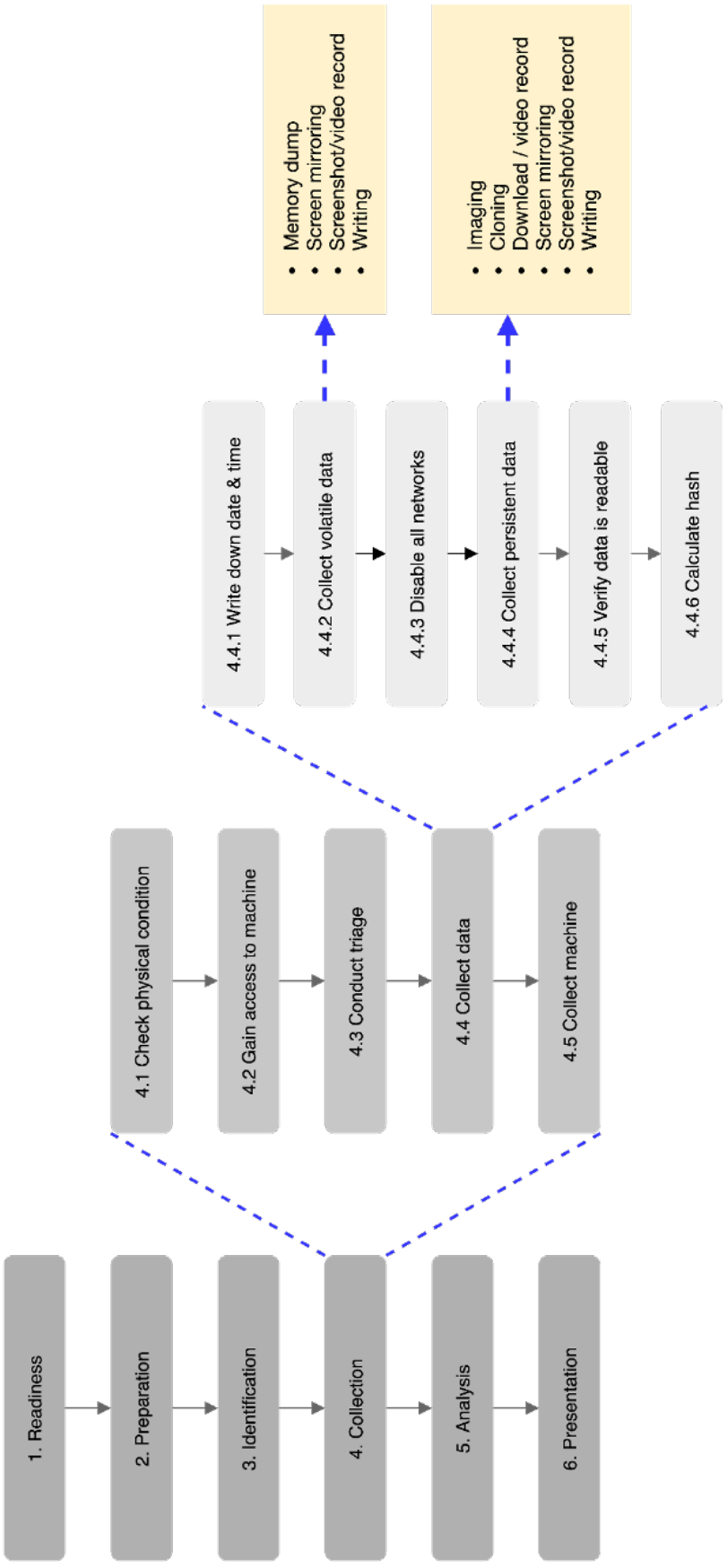
Risks related to human error, misconduct, or bias must be carefully managed.

Mitigation steps:

- use of a 'buddy system' or second officer to verify actions
- For complex systems, involving specialists such as IT support staff, system administrators, or vendors for complex system
- Use clear step-by-step SOPs and checklists

In summary, by systematically identifying and mitigating these risks, Investigators can uphold the integrity of digital evidence and contribute effectively to the overall investigation process.

APPENDIX A. OVERALL SUMMARY OF DATA COLLECTION METHODS



REFERENCE

1. Digital Evidence Guides. UNODC. 2023
2. Eoghan Casey. Digital Evidence and Computer Crime. 3rd Ed. 2011
3. Electronic Evidence Guide, A Basic Guide for Police Officers, Prosecutors and Judges. Council of Europe. Version 2.1. March 2020. https://www.coe.int/en/web/octopus/training
4. Guidelines for Digital Forensics First Responders, Best practices for search and seizure of electronic and digital evidence. INTERPOL. March 2021
5. Global Guidelines for Digital Forensics Laboratories. INTERPOL. May 2019. https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf. Viewed on 20 Dec 2021
6. SWGDE Best Practice for Mobile Device Evidence Collection & Preservation, Handling and Acquisition. Version 1.2. September 2020. https://drive.google.com/file/d/1sVko_Uo7o6iootWwn9IoLJ3mr MVXqTDg/view. Viewed on 10 Jan 2022
7. SWGDE Best Practices for Mobile Device Forensic Analysis. Version 1.0. September 2020. https://drive.google.com/file/d/1lkj3lRnIZAu8PSIp0rFUL8KCViLA5IwO/view. Viewed on 10 Jan 2022.

CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis
Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan
Malaysia

Tel: +603 8800 7999
Fax: +603 8008 7000
Email: enquiry@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
www.cybersecurity.my

@cybersecuritymy
CyberSecurityMalaysia
cybersecurity_malaysia
CyberSecurityMy

MINISTRY OF DIGITAL