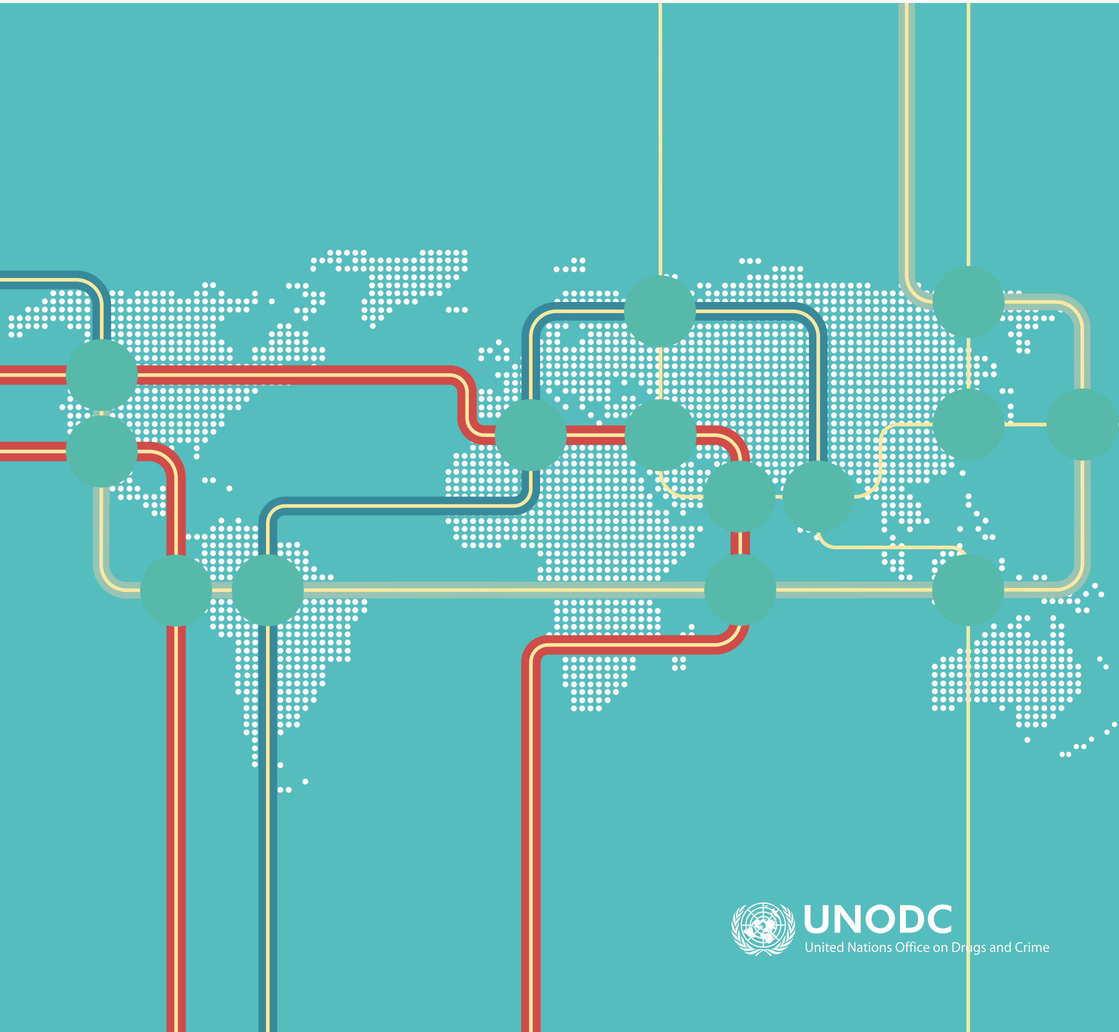
Assessing Digital Evidence:
A field guide for frontline officers



UNODC
United Nations Office on Drugs and Crime

This is not an official document of the United Nations. The designations employed and the presentation of the material in this document do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations Office on Drugs and Crime concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitations of its frontiers and boundaries.

UNODC would like to recognize the contribution of the Government of Australia, the Government of Canada and the Government of the United States of America.

To view this publication from a mobile device or to access other UNODC publications, please scan the QR code.

This content is updated regularly with new information. For the latest version of content and to access other materials and tools please visit the QR code.

Assessing Digital Evidence:
A field guide for frontline officers

This publication contributes to Sustainable Development Goal 16 that seeks to: "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels"

SUSTAINABLE DEVELOPMENT GOALS

16 PEACE, JUSTICE AND STRONG INSTITUTIONS

The Sustainable Development Goals are the blueprint to achieve a better and more sustainable future for all. They address the global challenges we face, including those related to poverty, inequality, climate, environmental degradation, prosperity, and peace and justice. The Goals interconnect and in order to leave no one behind, it ís important that we achieve each Goal and target by 2030.

INTRODUCTION

The use of digital media devices has grown exponentially as more and more people embrace technology and the convenience it provides. The ability to manage your life from a mobile device has changed the way we work, communicate and share our life experiences. As technology has developed so too has the way that criminals use this technology to facilitate their illegal activities.

The advent of web-based encrypted communication applications, email, internet banking and the increased sophistication of mobile telephones have provided criminals with greater flexibility and security. However, their use and reliance of these systems also creates an opportunity for law enforcement agencies to collect valuable intelligence and evidence.

As a frontline law enforcement officer, you may encounter suspects who are in possession of these digital media devices. This field guide will help you to understand where this information and evidence can be found and how it can be extracted, transported and stored.

You should carry this field guide with you while you are on duty. It contains quick-reference tools to address situations you are likely to experience in the course of your duty.

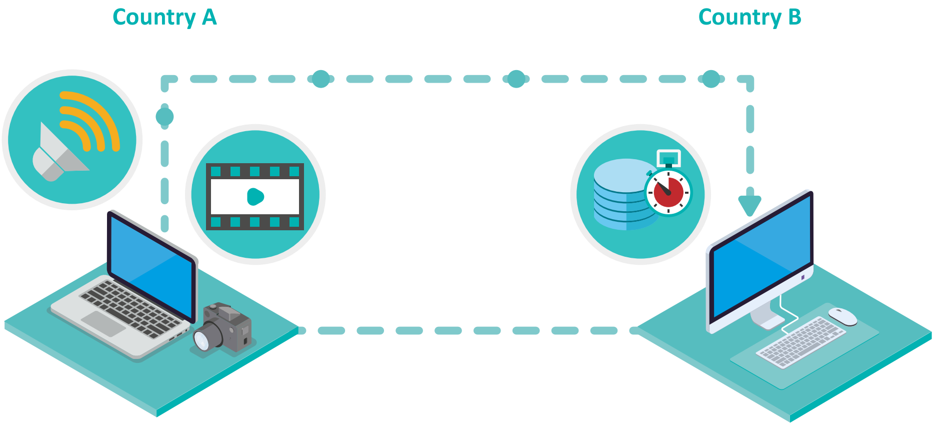
Table of Contents

Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device in binary form. The evidence is obtained when data or electronic devices are seized and secured for examination.

Digital evidence includes information on computers, audio files, video recordings and digital images.

Digital evidence:

- Is often latent in the same sense as DNA and Fingerprint Evidence
- Can cross borders with ease and speed
- Is fragile and can be easily altered, damaged or destroyed
- Is sometimes time sensitive



2. LEGAL CONSIDERATIONS FOR SEIZING DIGITAL EVIDENCE

Prior to seizing any digital evidence ensure that you have a legal basis for doing so. Seizing evidence without authority may render it inadmissible in court and may get you in trouble.

In some countries,it is a requirement of travelers at international airports, ports or immigration checkpoints to provide the login details of any electronic devices in their possession. Failure to do so may constitute an offence and/or result in a refusal for travelers to enter the country. You should research the specific laws or regulations of your country to determine what your powers are, (if any) to seize and examine digital media devices such as mobile telephone, tablets and computers at international points of entry.

Before you seize any device that may contain digital evidence ask yourself:

- Do I suspect that the owner of the device is engaged in criminal activity?
- What is the basis of my suspicion?
- Do I have a legal right to seize the device?
- Do I have a legal right to examine the device?
- Are there restrictions on the information I can examine on the device?
- Are there restrictions on how long I can keep the device?
- Do I have the authority to demand that the owner of the device provides me with access to it, including PIN numbers and passwords?
- Do I need to seek permission from a Senior Officer to seize and examine the device?

- Do I have access to facilities or equipment to undertake a forensic examination of the device?
- Do I have the facilities available to securely transport and store the device?

Remember, you may be responsible for returning a seized device to the owner should it not contain any evidence of criminal activity. Make sure that you have obtained enough details from them to enable you to return the device at a later stage.

1. Actions taken to secure and collect digital evidence should not affect the integrity of that evidence.
2. Persons conducting an examination of digital evidence should be trained for that purpose.
3. Actions taken during the seizure, examination, storage and transfer of digital evidence should be documented, preserved and available for review at a later stage

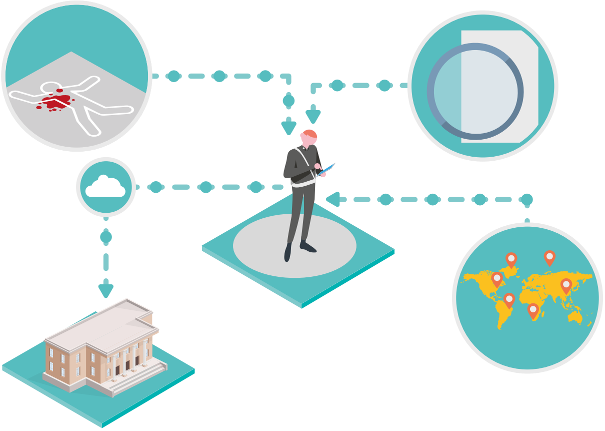
3. THE VALUE OF DIGITAL EVIDENCE

The emergence of the personal computer and the mobile telephone has had a profound impact on the law enforcement and the collection and presentation of evidence. It has also forced the introduction of new procedures and rules of evidence in relation to the presentation of this type of evidence in Courts. You should keep yourself up to date with the rules and procedures that govern your jurisdiction.

Digital evidence can link criminals to people, places and events. Telephone records, photographs, audio and video recordings, social media accounts, geotags and even search history can all be important pieces of evidence in proving a criminal case.

There are many different types of crimes where digital evidence may be relevant. These include:

- Murder
- Terrorism
- Drug Trafficking
- Precursor Trafficking
- Human Trafficking
- Migrant Smuggling
- Wildlife Crime
- Sex Crimes
- Fraud
- Chemical Waste
- Money Laundering



These are just a few examples and there are many more but remember, to extract the maximum value from digital evidence it will require that you, the front-line officer, adhere to your Departments policies and procedures in relation to the collection, analysis and storage of digital evidence to ensure its admissibility in Court.

4. THE FIVE PHASES OF DIGITAL FORENSIC EXAMINATION

There are five general phases of digital forensic examination.

1. **Preparation and Identification** – target media or suspect
2. **Collection** – collection of data from the device or the suspect
3. **Preservation** – Imaging, preserving or duplicating the data collected
4. **Examination and Analysis** – Examine and analyse the collected data
5. **Presentation** – Present the digital evidence you have obtained

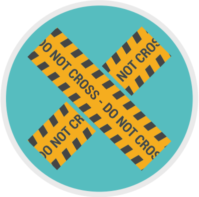
As a front-line law enforcement officer, you may only play a role in the first three phases, the remaining two phases being conducted by specialist officers or external consultants. However, you may be called upon to do all 5 phases, so you must be equipped and prepared to do this if required.

5. THE SEARCH KIT

Prior to searching a digital storage device ensure that you have the following items at hand to undertake the search (if available).

- Computer with appropriate software
- Solid surface, preferably a table top to hold devices upright
- Video and still camera with a tripod
- Storage cards (SD)
- External batteries and cables
- Evidence bags
- Ruler
- Rubber gloves
- Stationary (pens, notebook, markers)
- Aluminum foil or Faraday Bag
- Magnifying glass
- Chain of Custody Forms
- Crime Scene Tape

You will use some or all these items when searching and documenting digital evidence. It is best to be prepared and have them all readily available in a search kit.



You may find yourself in a situation where you must search a suspect to determine if they are in possession of devices capable of storing digital evidence, be it a smartphone, flash drive or SD card. You should always be vigilant when searching a suspect. This is to ensure your own safety, the safety of the suspect and any bystanders, and to prevent the disposal or destruction of any evidence.

Before the search:

- Inform the suspect of the reason for the search, of the powers you are using to conduct the search and of their legal rights.
- Ask the suspect if they are armed or in possession of anything that may harm themselves or others.
- Check the area around you for evidence or items that the suspect may have discarded or that they may use to harm themselves.
- Ask them are they in possession of a telephone, flash drive or smart card.
- Have another officer present during the search.
- Use a female officer to search female suspects (if available).
- If not accompanied by another officer, secure the suspect, especially if the suspect is prone to acts of violence.

During the search:

- If possible, conduct the search in a quiet area away from direct public view.
- Search the suspect systematically from head to foot, covering all areas including inside the suspect's mouth.
- Remove outer items of clothing, such as hats, gloves, belts, shoes, from the suspect to search these items more thoroughly.
- Gently feel clothing for objects as you search.
- Pat pockets and ask the suspect if the pockets contain harmful objects before putting your hand in the pockets.
- Put any found objects aside for later examination or seizure.
- Search bags separately after completing the search of the suspect.
- When searching, avoid standing or crouching directly in front of the suspect

Your colleague should watch your search to observe the suspect's movements or if the suspect discards evidence. If you are armed, keep your firearm away from the suspect while searching.

Watch the suspect for any signs of aggression. Watch the suspect's hands. If a more thorough search is required, such as a strip search or internal examination, then follow your agency's guidelines in relation to these more intrusive searches and gender considerations.

Safety of yourself, your colleagues, civilians and the suspect are always your number 1 priority when conducting a search.

7. SECURING THE EVIDENCE

You should only search for and seize digital media devices if you are lawfully entitled to do so.

There are many ways that evidence relating to digital evidence may come into your possession. It may be as a result of a person search, vehicle or vessel search, searching baggage, a container or searching a residential or business premises. Irrespective of how this evidence comes into your possession you must document the scene and record the actions you take when you seize the digital media device or other supporting evidence.

This evidence may consist of digital devices or other evidence that helps prove other crimes. This may include:

- Cell phones.
- Flash drives.
- Hard drives.
- Computers.
- Fax machines.
- Printers.
- Bank statements.
- Travel documentation.
- Accommodation documentation.
- Cash.
- Transporter documentation.

7. SECURING THE EVIDENCE

Prior to the search you should:

- Photograph and/or video the search area.
- Draw a map of the scene.
- If you have other officers to assist you assign each a specific role i.e. search, exhibit officer, officer in charge and photographer.

During the search you should:

- Search the area systematically.
- Video the search.
- Document the location where each item is found.
- Bag or secure items seized clearly labelling each with a unique identification number.
- Create a record of all items seized.
- Complete chain of custody documentation.

As a front-line law enforcement officer, you may need to interview suspects who you find in possession of digital media devices. It is always better if you can electronically record these interviews but if you are unable to do this then you should take comprehensive contemporaneous notes.

One potential issue when dealing with digital evidence is attributing that evidence to the suspect. Proving that they were the person who owned or used a computer or mobile telephone or showing that they had knowledge of the contents of a hard drive or that they were the ones who sent an email is very important evidence.

8. INTERVIEWING SUSPECTS

When you interview a suspect, you need to abide by the rules of interviewing as expressed by your policies, procedures and laws in your country. You should only interview a suspect when you are legally entitled to do so. Some common questions that should be asked of suspects include:

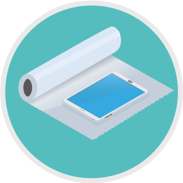
- Suspects full name, date of birth, address and identification number.
- Who owns the device?
- How long have you owned the device?
- Where did you purchase the device?
- What is the password/pin code/login details for the device?
- When was the last time you used the device?
- Where were you when you last used the device?
- What security features do you have on the device?
- Who else uses the device?
- Who else has access to the device?
- Are there any encrypted files on the device?
- What is the telephone number (if a mobile telephone)?
- Who is the service provider?
- Who is the subscriber for the account linked to the device?
- What do you use the device for?
- Clarification questions arising for material you find on the device.

Some mobile telephone and computer operating systems allow for the remote access to, or remote wiping of the contents of the device. Given that these devices may contain evidence it is crucial that you protect these devices from external manipulation.

There are several ways that you can do this. Some require the use of readily available products while others are dedicated systems developed to address these issues.

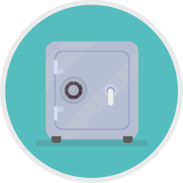
Some of the materials that you can use to prevent remote access to these systems include:

- **Aluminum foil** – Mobile phones placed in a box and then wrapped in aluminum foil will not receive a signal. The aluminum foil is an electrical conductor and creates what is called a Faraday cage preventing outside access to the device



- **Faraday bags** – these are purpose made military grade shielding bags that block all major signals including 3-4G, Bluetooth, RFID, Wi-Fi and GP

- **Stored inside a full metal safe** – A full metal safe should also be able to block any attempts to remotely access the phone

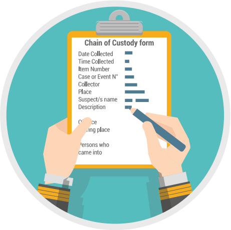


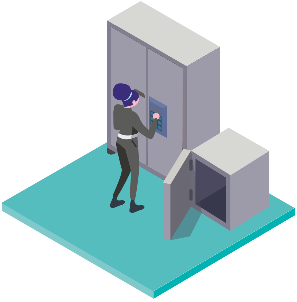
When using any of these methods it is always a good idea to try them out with your own phone first. Place your own phone inside one of the shielding devices and try to call it. If you can hear your phone ring the method is not blocking the signal.

10. CHAIN OF CUSTODY

Chain of Custody refers to the chronological documentation and/or paper trail showing the seizure, custody, control, transfer, analysis and disposition of evidence, physical or electronic. Because evidence can be used in court to convict someone of a crime, it must be handled in a careful manner to avoid allegations of tampering or misconduct which can potentially compromise a case.

As a front-line officer, you are responsible for making a record of any digital evidence that comes into your possession and what you subsequently do with that evidence. If you hand it to another officer, or to an expert, or even back to the suspect you must make a record of this movement. This is often recorded on a Chain of Custody form.





There are many examples of Chain of Custody forms available on the internet, but you should first check whether your Department has its own form before using one of these.

A chain of custody form should as a minimum include the following information about the digital evidence you have seized:

- Date Collected.
- Time Collected.
- Item Number or Barcode Number.
- Case or Event Number.
- Who collected the item.
- Where the item was collected.
- The suspects name.
- A through description of the item.
- Offence for which the item was collected.
- Where the item is stored.
- Any person who came into possession of the item, the reason for this, and the date and time that this occurred.

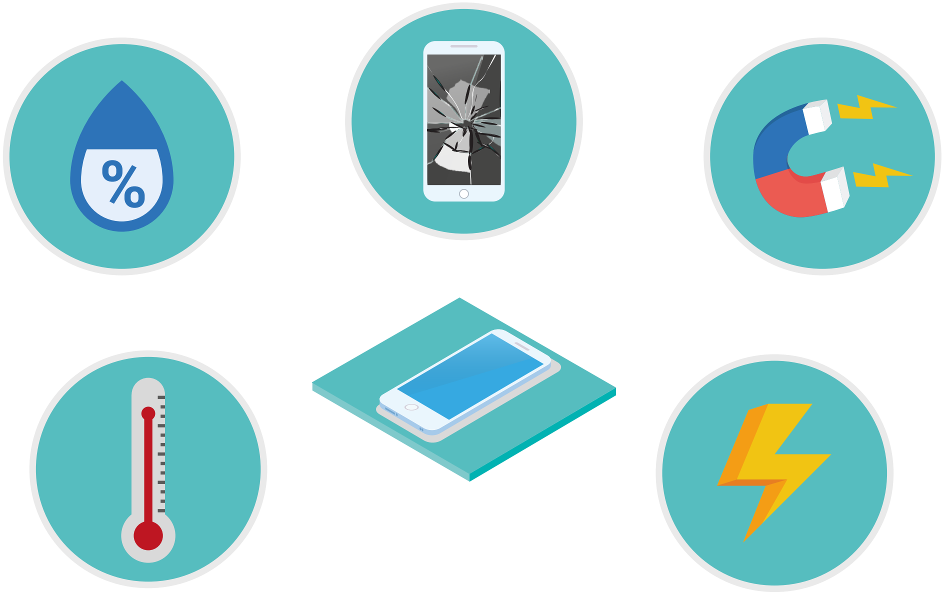
11. TRANSPORTING AND STORING DIGITAL EVIDENCE

Digital media devices are fragile and sensitive; you must treat them with care while transporting them or storing them.

You should always avoid exposing digital media devices to the following:

- Extreme temperatures.
- Moisture.
- Physical Damage.
- Magnetic Fields.
- Static Electricity.

Transporting Digital Evidence
You should ensure that all digital evidence is properly documented and labelled and that any power chords or adapters are marked with the corresponding digital device. Ensure that any chain of custody documents have been completed.



Ensure that digital evidence is not left in vehicles for protracted periods of time and never leave your vehicle unattended whilst transporting digital evidence.

When transporting digital evidence in a vehicle you should place it in the rear away from magnetic sources such as your radio and speakers.

Storing Digital Evidence

Store all digital media devices in antistatic packaging such as paper bags and envelopes, cardboard boxes and anti-static containers. Do not use plastic bags as they can produce static electricity and allow moisture to develop, which may damage or destroy the evidence contained on the device.

⚠ Ensure that the digital evidence is stored in a secure, climate-controlled environment that is not exposed to extreme temperature of humidity. Access to this room should be limited and any entry recorded.

12. HAND HELD DEVICES

Handheld devices are portable data storage devices that provide communications, digital photography, audio and video recording, navigation systems, access to the internet, data storage, and personal information.

The most commonly used hand-held device and the most likely data storage device you will encounter is the mobile telephone (cell phone). There are many different types of mobile telephones, but they will generally utilise one of several main operating systems. These systems include:

- Apple iOS.
- Android.
- Blackberry.
- Windows Mobile.
- Symbian.

The type of operating system can have a significant impact on your ability to access the data contained on the device and it is important to identify the correct operating system. Some of the security features you may encounter on the more popular operating systems include:

iOS

- 4 Digit PIN.
- 6 Digit PIN.
- Complex – Digits Only.
- Complex – Alphanumeric.
- Touch ID (Fingerprint).
- Facial Recognition.

Android

- Pattern lock.
- 6 Digit PIN.
- Knock pattern.
- Voice.
- Facial Recognition.
- Anti-theft Security Feature.

Other types of handheld devices include Global Positioning Systems (GPS), smartwatches or fitness bands, digital cameras and videos, tablets and PDA's can all contain digital evidence.

It is important to understand that data or digital evidence may be lost if power is not maintained to the device. You should always switch the device in airplane mode (if available) and keep the device charged. Make sure you also seize any power chords or adaptors for the device.[5]

There are two basic operating systems used by mobile service providers.

1. Global System for Mobile Communication (GSM).
2. Code Division Multiple Access (CDMA).

GSM is a global standard that requires a SIM card. To identify the IMEI number of the phone dial *#06#. The IMEI number is a number unique to the telephone handset and can be used to identify other SIM cards that have been used in the telephone.

CDMA does not require the use of a SIM card and the subscriber's information is stored in the handset. To identify the mobile equipment identity (MEID) dial *#06#.

There are several commercially available forensic analytical tools that you may used to extract information from digital media devices or SIM cards.

Mobile telephone and tablet analysis systems include Cellbrite and Micros Systemation's XRY and both provide the ability to analyse handheld devices and produce forensic reports, however to be accredited to use these items you will need to undergo training.

13. COMPUTER SYSTEMS

There are many different types of computers in use today, including desktops, laptops, towers systems, mainframe, touch screens and mini-computers.

Computers offer law enforcement agencies the opportunity to collect digital evidence commonly found in files that are stored on hard drives, storage devices and media. There are four general types of files found on computers that may hold examples of digital evidence. These include:

User Created Files

- Address books.
- Audio/Video files.
- Calendars.
- Database files.
- Document or text files.
- Emails.
- Search History.
- Spreadsheets.
- Social media.

User Protected Files

- Compressed files.
- Encrypted files.
- Password protected files.
- Hidden files.
- Misnamed files.

Other Data Areas

- Deleted files.
- Lost clusters.
- Bad clusters.
- Metadata.
- Hidden partitions.
- System areas.
- Unallocated space.

Computer Created Files

- Backup files.
- Configuration files.
- Cookies.
- Hidden files.
- History files.
- Log files.
- System files.
- Temporary files.
- Swap files.

There are many different software programs that can help you undertake the forensic analysis of computers to identify and extract digital evidence. You may need to be accredited to use this software if you wish to have the evidence presented in court.

You should methodically document the steps you take during your analysis and be able to report exactly what you did at a later stage.

Some computers are connected to networks and digital evidence can be stored in the servers of these networks. You may have the authority to seize these servers, but should you choose to do this make sure that you have the permission of your supervisor. Servers should be analysed by a qualified expert.

14. EXTERNAL STORAGE DEVICES

There are many different types of external storage devices that you may encounter as a frontline law enforcement officer. Some of these devices may be the size of your hand and others may be very small. Each of these devices may potentially contain digital evidence and if seized will need to be analysed.

Different types of storage devices include:

- Portable Hard Drives.
- USB Flash Drives.
- CD Discs.
- Blue-Ray Discs.
- Floppy Discs.
- Secure Digital (SD) Cards.
- Micro SD Cards.

Be aware when you are searching people, premises or vehicles that these devices can be very small and are easily concealed. Some of these devices may be encrypted, ***if you find an encrypted device it is important to ask the suspect for the password.***

Smart electronic devices are becoming more and more common including smart refrigerators, smart televisions, homes that can be managed remotely, CCTV with remote monitoring capabilities and GPS/Smart Media suites in vehicles.

All of these may provide digital evidence for investigators and the seizure and analysis of these items should be considered when you are searching a premises or vehicle.

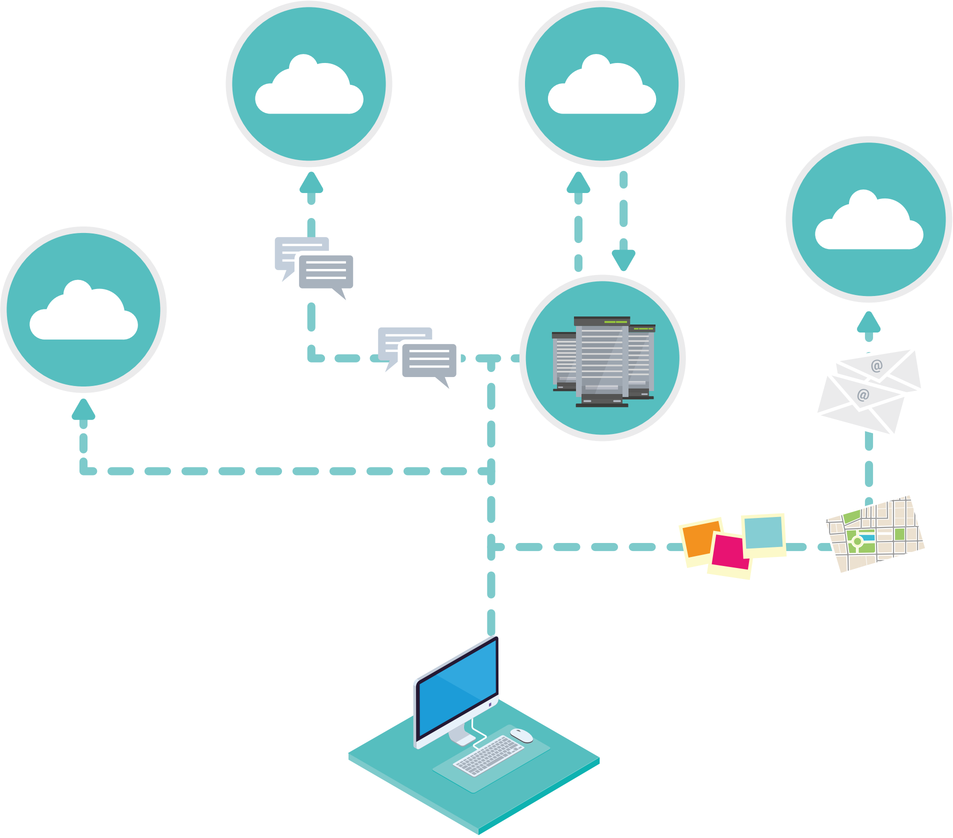
Other examples of electronic devices that may provide digital evidence include:

- Fax machines.
- Photocopiers.
- Video cameras.
- Digital tape recorders.
- Answering machines.
- Digital cameras.
- CCTV cameras.
- GPS Devices.
- Pagers.
- Scanners.
- Gaming consoles.
- Drones.
- Virtual Reality Devices.
- Pagers.

Similarly, you should consider seizing and analysing these devices.

16. THE CLOUD

The Cloud can be described as a method of delivering different types of services over the internet, including software and analytics, to secure and safe data storage and network resources. Several common cloud usages include cloud storage, cloud backup and business intelligence.



Cloud computing also has important ramifications for law enforcement. Many cloud service providers offer free cloud storage associated with mobile telephone or computer accounts. Some of these devices are automatically set to save information from the device to The Cloud. Some of the more common cloud service providers include Google, Microsoft, Dropbox and OneDrive.

Data that can be backed up to The Cloud includes calendar entries, photographs, emails, contact lists, google maps and backups of web-based communication applications such as iMessage, WhatsApp, WeChat, Line and Messenger. This information can still be maintained in Cloud accounts even when the original information is wiped from the user's phone or computer.

As frontline law enforcement officers you may be presented with investigative opportunities to search Cloud based accounts by virtue of a search warrant, telecommunications intercept warrant or permission granted by owner of the service.

There are several programs and applications that will assist you to download material from Cloud based accounts. You will need to use the same procedures to document the material you collect from the Cloud as you do with material you collect from physical storage devices.

17. CYBER CRIME AND DIGITAL EVIDENCE

The internet has revolutionised the way we live. As technology has developed so too has the ability for criminals use this technology to facilitate their illegal activities. The advent of web-based encrypted communication applications, the dark web, social media and the increased sophistication of mobile telephones have provided criminals with greater flexibility, anonymity and reach.

Crime facilitated via the internet is a major issue for law enforcement agencies. These crimes occur on both the open web and the dark web. Hacking, fraud, drug trafficking, wildlife, the promotion of extremist views, trafficking, the sale of counterfeit medicines and clothing are all common place on the internet.

While many criminals will only operate on the open web, more sophisticated networks are moving to the dark web. The use of the dark web has witnessed the trafficking of drugs, weapons, people and the facilitation of terrorist activities. Paedophile networks are able to share images of children within closed groups around the globe. Auctions of children on the dark web gives an insight into the ability for criminals to capitalize on changes in technology and the challenges faced by law enforcement to address this.

The dark web is a collection of websites operating on an encrypted network with hidden IP addresses - all of which give users strong anonymity protection. Because they are not indexed by traditional search engines, you can only access them with special anonymity browser, such as I2P, Freenet, and the most common, The Onion Router (TOR) bundle.

Several law enforcement agencies have run successful major undercover operations targeting Dark Web users. If you believe that your case involves criminal activity on the Dark Web then you should consult with the speciality unit within your department that addresses cyber crime, if one exists. These types of operations require specialist training and equipment.

One area where you will find potentially valuable evidence and intelligence is through the analysis of suspects social media accounts. Social media offers law enforcement agencies the opportunity to gather intelligence on organised crime groups and individuals. The ability to map their network of friends, images of their assets and notifications of where they are eating at restaurants, travelling on holidays, or meeting with friends may provide intelligence or investigative opportunities. Examples of social media sites include:

- Facebook.
- Snapchat.
- Instagram.
- WeChat.
- Zalo.
- Signal.

Criminals have been known to post photographs of themselves with firearms, drugs or promoting terrorist agendas. Some have even made admissions to killing their wives online.

While these platforms make it easier for criminals to commit crime, they also present opportunities for investigators. You can use them as possible entry points for undercover investigators and for collecting intelligence and potentially evidence. Never use your own account to communicate with suspects on any of these sites. You should create or utilise covert accounts for your communications.

Should you communicate with suspects on these sites with a view to collecting evidence remember to:

- Ensure that your actions are legal within your jurisdiction.
- Ensure that you have sought the permission from your supervisor.
- Always use a covert account.
- Screenshot the suspects profile – this can be changed by them at a later date.
- Screenshot any messages between you and the suspects.
- Record any videos or messages they send to you.
- Always ask for proof of possession – ask for a video with your covert name and the date.
- Do not share your photograph with a suspect.
- Do not post your photograph on your covert profile.
- Refrain from talking via video with the suspect.
- Ensure chain of custody of any evidence you collect (see chapter 10).

Another area where you may collect valuable intelligence or digital evidence are web based communication applications. These systems offer end to end encryption between users which makes interception difficult. Examples of these types of platforms include:

- WhatsApp.
- Viber.
- Line.
- WeChat.
- Telegram.
- Wire.

The easiest way to collect evidence of a suspect's criminality using these platforms (prior to arrest) is to connect and communicate directly with them in an undercover capacity. If you have the suspects phone in your possession than you can collect the digital evidence through the use of a cell phone analytical tool such as Cellbrite, or the physical recording of messages, photos, videos, call records or audio conversations.

There are dozens of terms that relate to the definition, extraction and analysis of digital evidence. As a front-line officer, you do not need to know all these terms. However, there are some terms that may assist you to in your day to day duties and increase your knowledge and effectiveness when it comes to the collection of digital evidence.

Archive Copy
A copy of data placed on media suitable for long-term storage, from which subsequent working copies can be produced.

Capture
The process of recording data, such as an image, video sequence, or audio stream.

Chain of Custody
The chronological documentation of the movement, location and possession of evidence.

Data
Information in analog or digital form that can be transmitted or processed.

Data Analysis
The assessment of the information contained within the media.

Data Extraction
A process that identifies and recovers information that may not be immediately apparent.

Digital Evidence
Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device in binary form.

Erased File Recovery
The process for recovering deleted files.

Format
The structure by which data is organised on a device.

Format Conversion
To transfer audio and/or video from one media type to another.

Image Enhancement
Any process intended to improve the visual appearance of an image or specific features within an image.

Internet Protocol (IP) Address
A 32-bit binary number that uniquely identifies a host connected to the Internet or other Internet hosts for communication through the transfer of data packets.

ISP
Internet Service Provider. A business that provides access to the internet.

JPEG
A compression technique used for saving images and photographs.

Log File
A record of actions, events and related data.

Media
Objects on which data can be stored.

Metadata
Data, frequently embedded within a file, that describes a file or directory, which can include the locations where the content is stored, dates and times, application specific information, and permissions.

Mobile Device
A portable device that has an embedded system architecture, processing capability, on board memory, and may have telephony capabilities (e.g. mobile telephone, tablets and smartphones).

Network
A configuration of independent computers, peripherals and devices capable of sharing information and resources.

Preview
A sub-process of triage where a cursory review of items is performed to assess the need for collection and/or further examination.

Source Code
The list of instructions written in programming language to construct a computer program.

Work Copy
A copy of duplicate of a recording or data that can be used for subsequent processing and/or analysis.

UNODC
United Nations Office on Drugs and Crime

Regional Office for South East Asia and the Pacific
United Nations Building, 3rd Floor B Block, Secretariat Building
Raj Damnern Avenue, Bangkok 10200, Thailand
Tel. (66 - 2) 288 100 Fax (66 - 2) 281 2129 E-mail: fo.thailand@unodc.org
Website: www.unodc.org/southeastasiaandpacific