

Digital Forensics Investigation in Singapore

IFS4101 Group Project



Ashok Balaji, Hugo Chia, Joshua Lim, Regan Choy, Ge Shuqing

Overview of our Manual



1. Introduction.....	4
1.1. Foreword.....	4
1.2. Purpose and Scope.....	4
1.3. Application of guide.....	5
2. Legislation.....	6
2.1. Computer Misuse Act.....	6
2.2. Cybersecurity Act.....	7
2.3. Evidence Act.....	9
2.4. Criminal Procedure Code.....	18
2.5. Telecommunications Act.....	20
2.6. Mutual Assistance in Criminal Matters Act.....	21
3. Fundamental Principles.....	24
3.1. Principles of Digital Evidence.....	24
3.2. Explanation of the Principles.....	24
4. Planning and Preparation.....	26
4.1. Roles and Responsibilities.....	26
4.2. Search and Seizure Planning.....	27
5. Digital Evidence Handling Procedure.....	28
5.1. Documentation and Chain of Custody.....	28
5.2. Identification.....	31
5.3. Collection and Acquisition.....	32
5.4. Preservation.....	35
6. Analysis.....	37
6.1. Analysis of Data.....	37
6.2. Interpretation of Digital Data.....	38

7. Present.....	39
7.1. Verbal Feedback.....	39
7.2. Statements or Reports.....	39
7.3. Witness Evidence.....	40
7.4. Contemporaneous Notes.....	40
8. Specific Evidence Collection Cases.....	41
8.1. Mobile Devices.....	41
8.2. Computers.....	47
8.3. Storage Media.....	50
8.4. Websites, Forums, and Blogs.....	52
8.5. Social Network Sites.....	54
8.6. Servers.....	55
8.7. Network Forensics.....	55
8.8. Other Devices.....	58
8.9. IoT Devices.....	59
8.10. Gaming Consoles.....	61
8.11. Drones.....	62
8.12. CCTVs.....	63
8.13. Virtual Assets Devices.....	64
8.14. Automotive Vehicles.....	69
8.15. Shipborne Equipment.....	71
9. Appendix.....	73
9.1. Interview of Witnesses and Suspects.....	73
9.2. Open Source Research.....	73
9.3. Definition of Key Terms.....	74

TABLE OF CONTENTS

01

Introduction

02

**Analysis of ACPO &
Interpol Guides**

03

**Analysis of Singapore
Requirements**

04

**Key Recommendations
and Trends**



01

Introduction

Digital Forensics Landscape in Singapore

Current Regulation

The Cyber Security Agency of Singapore (CSA) has released a licensing framework for two types of cybersecurity service providers:

- Penetration testing
- Managed security operations centre monitoring services

The regulations are part of the Cybersecurity (Cybersecurity Service Providers) Regulations 2022 granted by powers under Section 48 of the Cybersecurity Act 2018

Lack of Guidelines and Regulations for Digital Forensics

There is currently a lack of

- regulations
- guidelines
- code of conduct
- or code of practice

governing digital forensics, a significant gap in the industry

The aim of this manual is to adapt best practices from

- ACPO Good Practice Guide for Digital Evidence
- and Interpol Guidelines For Digital Forensics First Responders

and apply them in Singapore's context.



02

Analysis of ACPO & Interpol Guides

Overview of Guides

ACPO

Best practices for handling digital evidence during criminal investigations

Who

Created for UK law enforcement by Association of Chief Police Officers (ACPO), now known as National Police Chiefs' Council (NPCC)

When

Version 5.0 released in March 2012

Interpol

Technical and procedural advice for first responders

Designed for global law enforcement agencies by the International Criminal Police Organization (Interpol)

Version 7.0 released in March 2021

ACPO Good Practice Guide for Digital Evidence



ACPO Strengths

Universal and Foundational Principles for Digital Evidence Handling

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

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

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

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

ACPO Strengths

Clear Flow Regarding General Digital Evidence Collection Process

Section	Page
Introduction to the Guide	4
Foreword	5
1 Application of Guide	6
2 The Principles of Digital Evidence	6
3 Plan	7
4 Capture	8
5 Analyse	10
6 Present	11
7 General	13
Appendix A	Network Forensic and Volatile Data Collection
Appendix B	Crimes involving Websites, Forums and Blogs

ACPO Strengths

Strongly Aligned with UK Legal Requirements and Directly References UK Court Expectations

Proportionality

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

Digital devices and media should not be seized just because it is there. The person in charge of the search must have reasonable grounds to remove property and there must be justifiable reasons for doing so. The search provisions of PACE Legislation Codes of Practice equally apply to digital devices and media in England, Wales and Northern Ireland. In Scotland, officers should ensure they are acting within the terms of the search warrant.

Due regard should also be taken concerning any possible contravention of the European Convention of Human Rights.

ACPO Strengths

Strongly Aligned with UK Legal Requirements and Directly References UK Court Expectations

7.5 LEGISLATION

7.5.1 Also refers to:

- Legislation.gov.uk;
- ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations.

7.5.2 A wide variety of legislation may apply in examinations of digital evidence. Some of the most relevant is detailed below.

- Computer Misuse Act 1990 (UK Wide)**
(<http://www.legislation.gov.uk/ukpga/1990/18/introduction>)

S1 Unauthorised Access To Computer Material

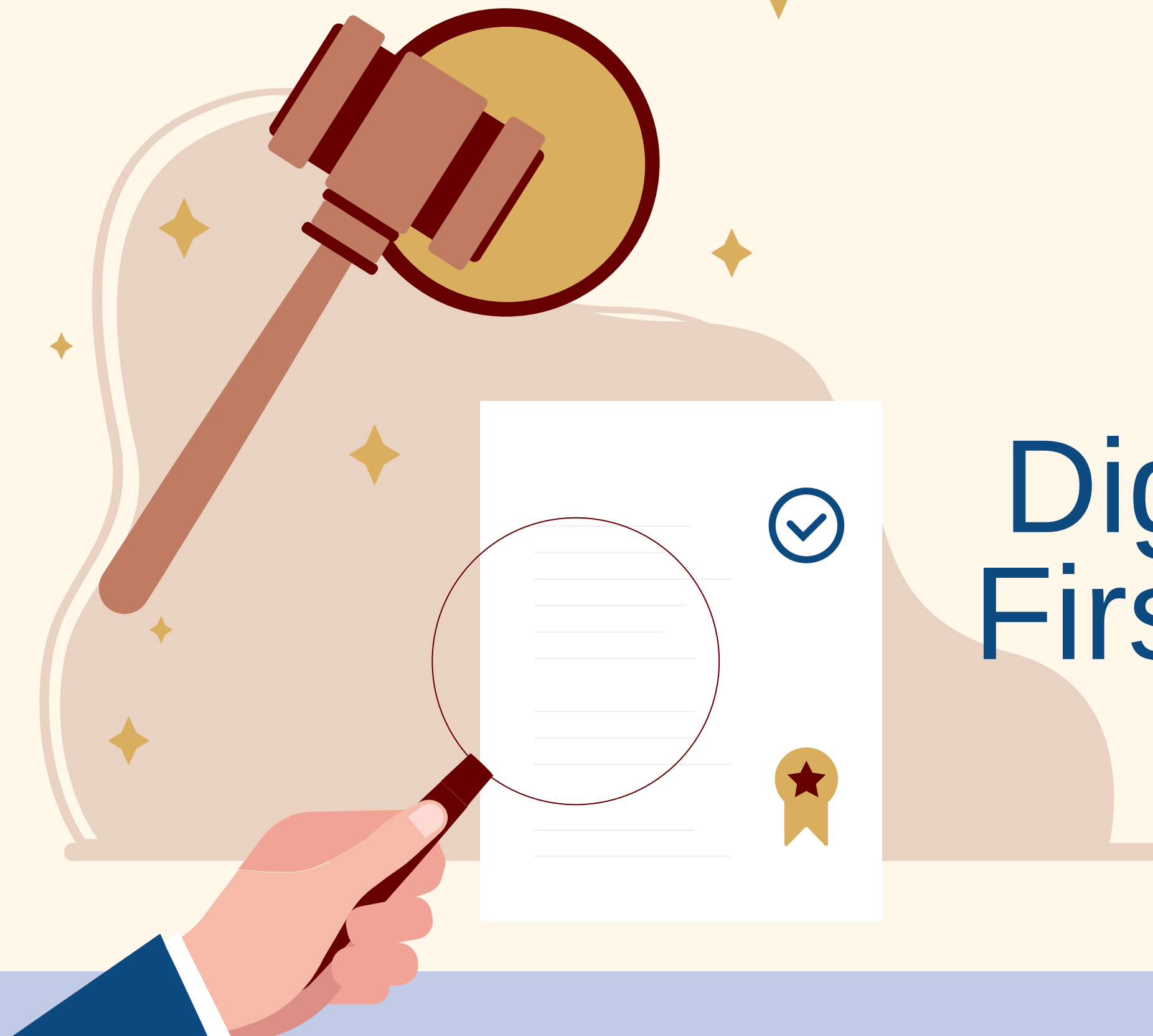
- It is an offence to cause a computer to perform any function with intent to gain unauthorised access to any program or data held in any computer. It will be necessary to prove the access secured is unauthorised and the suspect knows this is the case. This is commonly referred to as 'hacking'.
- The Police and Justice Bill 2006 amended the maximum penalty for Section 1 offences. The offence is now triable either way, i.e. in the Magistrates Court or the Crown Court. The maximum custodial sentence has been increased from six months to two years.

ACPO Limitations

Dated and Lacking Guidance on Emerging Technology

Appendix A	Network Forensic and Volatile Data Collection
Appendix B	Crimes involving Websites, Forums and Blogs

Interpol Guidelines for Digital Forensics First Responders



Interpol Strengths

Clear and Detailed Strategy and Technical Procedures with Numerous Examples

3.3. Document the scene

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

The following are examples for proper documentation of the scene:

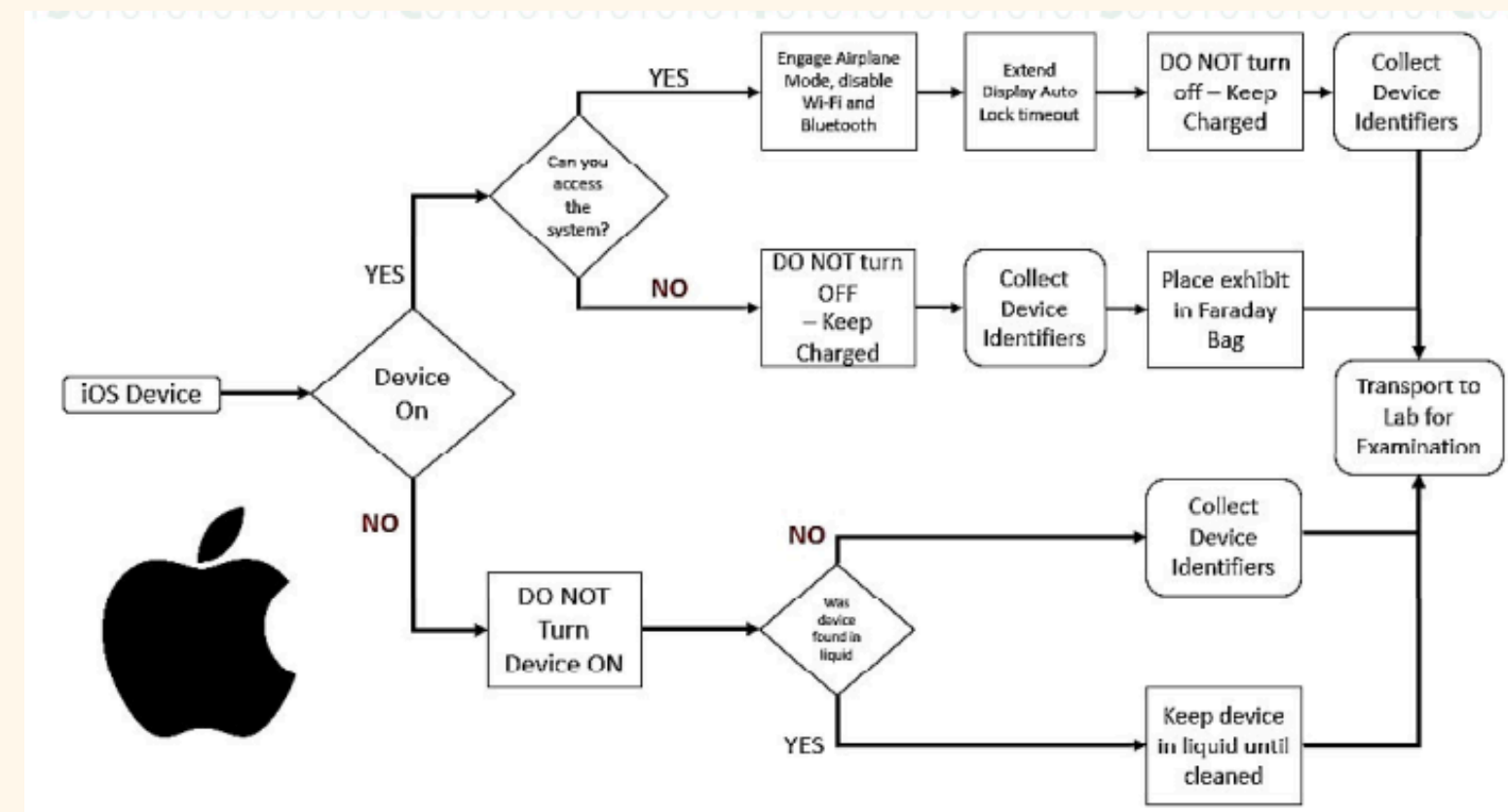
- Laptop computer: evidence number EVI001
- Internal hard drive: evidence number EVI001A
- USB Thumb drive: evidence number EVI001B
- DVD: evidence number EVI001C

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

For each device, the following data must be documented:

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

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



Interpol Strengths

Addresses Numerous Types of Devices and Emerging Technology

5.5. Storage media (memory cards, flash drives, external hard drives, optical discs, etc.)	34
5.6. Other devices (Digital cameras, GPS navigation systems, Dash Cameras, etc.)	36
5.7. IoT devices	36
5.7.1. Smartwatches	37
5.7.2. Smart TV	37
5.7.3. Home kits/Smart speakers	38
5.7.4. IP and concealed cameras	39
5.8. Gaming consoles	40
5.9. Drones	41
5.10. CCTV	43
5.11. Virtual assets devices	44
5.12 Automotive Vehicles	49
5.13 Shipborne Equipment	51

Interpol Limitations

No Specific Legal Requirements due to International Nature of Guide

5.1. Smartphones - Tablets

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

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

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

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



03

Analysis of Singapore Requirements

Two Categories of Cybercrime in Singapore



Cyber-dependent Crime

Offences under the **Computer Misuse Act (CMA)** in which **the computer is a target**. Includes offences such as ransomware, hacking and website defacements, etc.



Cyber-enabled Crime

Offences in which the computer is used to **facilitate the commission of an offence**. E.g. Online scams and cyber extortion, and other Penal Code offences committed via an online medium.

Two Categories of Cybercrime in Singapore



- Principles of digital evidence collection (e.g. chain-of-custody), remain the same in both cases and may not affect the operational aspect of digital forensics
- A practitioner in Singapore should be aware of how the Singapore police categorizes cybercrimes
- Moreover, the evidence present in cyber-dependent and cyber-enabled crime may be slightly different. **Cyber-dependent crimes** may involve malware and log analysis, while **cyber-enabled crimes**, e.g. cyber extortion could be done through a messaging service

Technology Neutrality

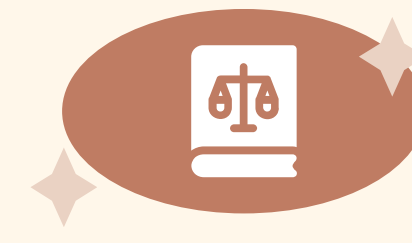
The United Nations Commission on International Trade Law Model Law on Electronic Transferable Records [‘UNCITRAL Model Law’] emphasizes that digital evidence should be treated the same way as other kinds of evidence. This is known as the **principle of digital equivalence**.



Technological Neutrality

Laws and regulations **should not favour, or discriminate against, any technology**

e.g. Singapore, Australia



Technological Specificity

Have special provisions for digital evidence within their statute

e.g. Malaysia, India

<https://law.asia/technology-neutrality/>

Relevant Legislations

- Computer Misuse Act 1993
- Criminal Procedure Code 2010
- Evidence Act 1893
- Telecommunications Act 1999
- Cybersecurity Act 2018
- Mutual Assistance in Criminal Matters Act 2000

Computer Misuse Act 1993

- Computer Misuse Act (CMA) criminalizes a wide range of computer-related activities
- Relevant sections that apply to **misuse of computers, cybersecurity incidents** and **police powers for investigations**

Computer Misuse Act 1993

“computer” - means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices

“data” - means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer, and as such covers electronic records, such as emails, digital files, computer logs and call logs

Computer Misuse Act 1993

✦ **Section 3 - Unauthorised access** to computer material

Section 4 - Access with intent to commit or facilitate commission of offence

Section 5 - Unauthorised modification of computer material

Section 6 - Unauthorised use or interception of computer service

Section 13 - Territorial scope of offences under this Act

- Defines jurisdiction, applying the CMA if the **offender** or **affected computer** is **in Singapore** during the offense

Section 18 - Saving for investigations by police and law enforcement officers

- Gives the digital forensics professionals the power to conduct their duties

Section 19 - Arrest by police without warrant

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

Criminal Procedure Code 2010

- Key legislation governing Singapore's criminal justice process
- Details the **procedure for the administration of criminal law in Singapore** and covers arrests, investigations, trials and appeals, and sentencing matters, among others
- Relevant sections that grant powers to the police with regards to digital forensics investigation focusing on **investigation, search and seizure**

Criminal Procedure Code 2010

Section 20 - Power to order production of any document or other thing

- Explicitly covers **documents in electronic form** or **documents contained in or available to a computer**
- When data is involved, the individual may be required to **authenticate the data**
- “Data” has the meaning given by the Computer Misuse Act 1993

Section 37 - List of all things seized to be made and signed

- Aligns with Principle 3 of ACPO - “An **audit trail** or other record of all processes applied to digital evidence should be created and preserved.”
- Applies to police officer or **any other person** making the search.
- In every case, the occupier or person in charge of the place search, must be given a signed copy of the list.

Criminal Procedure Code 2010

Section 39 - Power to access computer

- Grants powers to a **police officer** or an **authorised person** (a forensic specialist appointed under section 65A of the Police Force Act 2004) investigating an arrestable offence **access, inspection and checking of computers** (regardless if it is in Singapore or elsewhere) and to **search or make a copy of any data contained in computers**
- “Computer” here has a broad meaning, given by the Computer Misuse Act 1993

Section 40 - Power to access decryption information

- Similar to S39, a police officer or an authorised person may compel access to decryption information

*Obstruction of lawful exercise by a police officer or authorised person under S39 and S40 are arrestable offences

Criminal Procedure Code 2010

Section 364 - Order for Disposal of Property by Court

- Often consider the digital forensics process, up till the end of a trial
 - But what happens after?
- S364 empowers the court to issue orders for the disposal of property during or at the conclusion of an inquiry or trial
- Digital forensics investigators should handle the disposal of digital evidence in compliance with **PDPA Section 24** - Protection of personal data, to avoid causing a data breach
 - For example, equipment that holds storage media devices that contain the digital evidence should be physically destroyed, ensuring the data is unrecoverable, if directed by the court to dispose.

Evidence Act 1893

Admissibility

```
graph TD; A[Admissibility] --> B[How Evidence is Collected]; A --> C[How Evidence is Presented in Court];
```

**How Evidence
is Collected**

**How Evidence
is Presented in
Court**

Evidence Act 1893

How Evidence is Collected

★ **Section 64** - Primary Evidence

- Usually the original
- Copy of digital evidence is considered primary evidence. Use of hash is used to verify originality

Section 65 - Secondary Evidence

- Usually a copy of the original if the original cease to exist

Section 70 - Proof of execution of document required by law to be attested

- Attesting witness is required to ensure admissibility
- Recommend noting down relevant entities

Section 81 - Presumption as to genuineness of certified copies

- Assumed as genuine if accompanied with certs that meet legal standards such as digital signatures and hashes

Evidence Act 1893

How Evidence is Collected

★ **Section 88** - Presumption as to certified copies of foreign judicial records

- Relevant in dealing with overseas evidence
- Certification standards meet the originating country's standards

Section 100 - Evidence as to meaning of illegible characters

- Allows attachments of supporting explanations to clarify content

Section 116A - Presumptions in relation to electronic records

- Records are assumed to be genuine under standard circumstance unless challenged
- Note down the circumstance the records were retrieved under

Section 126 - Official Communications

- Official Secrets Act, confidential documents may be denied/not allowed

Evidence Act 1893

How Evidence is Presented in Court

Section 67 - Cases in which secondary evidence relating to documents may be given

Section 67A - Proof of documents in certain cases

Section 68 - Rules as to notice to produce

- Original document takes precedence over copies

Telecommunications Act 1999

Guidelines On Licensing And Regulatory Framework For IP Telephony Services In Singapore

- Telecommunication providers are required to maintain Call Detail Records (“CDRs”) for a period of not less than twelve (12) calendar months.
- Some data (e.g. call log or SMS data) may be better obtained from Telecommunication Providers, rather than to request a forensic examination of the mobile phones.
- Types of Data include:
 - (a) Assigned Source IP address and Date & Time stamps; and
 - (b) Assigned User ID/User Name (e.g., subscriber records associated with (a)).

International Collaboration

- **Mutual Assistance in Criminal Matters Act 2000**
 - Section 8 - Requests for taking of evidence
 - Specifies:
 - Requests for Taking Evidence
 - Requests for Obtaining Articles or Things
 - Admissibility of Evidence
 - Weight of Evidence
- **Mutual Legal Assistance Treaties (MLATs)**

Cybersecurity Act 2018

Section 14 - Duty to report cybersecurity incident in respect of Critical Information Infrastructure, etc

- Mandates CII owners to report prescribed incidents.

Section 19 - Powers to investigate and prevent cybersecurity incidents, etc

- Enables basic investigation of any cybersecurity threat or incident by authorizing officers to collect information, statements, and documents to assess impact and prevent harm.

Section 20 - Powers to investigate and prevent serious cybersecurity incidents, etc

- Grants enhanced investigative and intervention powers for severe cybersecurity threats that meet specific thresholds.




Cybersecurity Act 2018



Section 38 - Powers of investigation

- Establishes general investigative authority for any offense under the Act.

Section 39 - Power to enter premises under warrant

- Provides court-authorized access to premises when documents are withheld.
- 
- 
- 
- 

Cybersecurity Act - Supporting Sections

- ✦ • **Section 21 - Production of identification card by incident response officer** ✦
- **Section 22 - Appointment of cybersecurity technical experts**
- **Section 43 - Preservation of secrecy**



04

Key Recommendations and Trends

Key Recommendations

- Adoption of Best Practices
 - Combined strengths of both manuals (e.g. ACPO's principles, Interpol's technical depth)
- Legal contextualisation
 - Aligned with relevant Singapore legislation

Emerging Trend (Gen-AI X Law)

- AI may potentially disrupt the compliance field & digital forensics
 - Singapore's Supreme Court released a "Guide on the Use of Generative Artificial Intelligence Tools by Court Users" in September 2024
 - General principles - (1) The Court **does not prohibit the use of Generative AI tools to prepare Court Documents**, provided that this Guide is complied with
 - "For the avoidance of doubt, **Generative AI tools should not be used to generate any evidence that you wish to rely upon in Court.**
 - For example, you cannot use Generative AI to ask for evidence to be created, fabricated, embellished, strengthened or diluted. Asking a Generative AI tool to generate a first-cut draft of an affidavit/statement can be done (provided that this Guide is complied with), but it is not acceptable to ask a Generative AI to fabricate or tamper with evidence"

Conclusion

- Gap in Singapore's legislation and regulations regarding digital evidence investigation and handling
 - Our manual is a **guide to address these gaps**, especially regarding legality of investigation and admissibility of evidence
- Future work for our manual could include **country-specific case studies** (e.g. Singapore-Hong Kong) to handling digital evidence in cross-border cybercrime
 - Given the complexity of international cases and **varying national regulations**
 - Address civil cases - e.g. Hague Evidence Convention

THANK YOU

Questions welcome!

By: IFS4101 Group 2

