INTERPOL

GLOBAL GUIDELINES FOR DIGITAL FORENSICS LABORATORIES

These Guidelines were prepared by the Digital Forensics Laboratory at the INTERPOL Global Complex for Innovation.

Any inquiries can be directed to:

INTERPOL Global Complex for Innovation
18 Napier Road
Singapore 258510

E-mail: dfl@interpol.int
Tel: +6565503462

FOREWORD BY THE SECRETARY GENERAL

INTERPOL GLOBAL GUIDELINES FOR DIGITAL FORENSICS LABORATORIES

In today's complex international security environment, investigations more often require highly specialized and technical expertise.

To better address these challenges, one of the policing capabilities that INTERPOL focuses on is digital forensics, a rapidly changing discipline which requires robust policies and procedures.

An increasing number of connected devices – smartphones, watches, GPS – can store meaningful information which could potentially become pieces of digital evidence.

To meet this growing challenge, through our Innovation Centre's Digital Forensics Lab (DFL), INTERPOL is assisting member countries build national digital forensic capacity and develop e-evidence management processes to better support investigations and prosecutions.

As a neutral, global platform for law enforcement cooperation, INTERPOL continues its work to encourage and enhance communication and best practice development among our member countries.

This was one of the driving forces behind the creation of the INTERPOL Global Guidelines for Digital Forensics Laboratories which outlines the key principles and processes which are essential for practitioners.

These guidelines are also part of our ongoing commitment to make both the physical and virtual worlds, a safer place and I would like to thank everyone who contributed towards their development.

Jürgen Stock

INTERPOL Secretary General

A LETTER FROM THE DIRECTOR OF THE INTERPOL INNOVATION CENTRE

The dynamic history of digital forensics shows its strong interconnectivity with innovation. The rapidly evolving nature of digital space and technologies means that an enormous amount of digital traces and data can be produced in the blink of an eye. Continuous innovation in the field of digital forensics is a necessity, if not an obligation, for law enforcement.

On a global level, many pre-existing crimes are developing into a significant global threat by taking advantage of advances in technology and the borderless nature of our interconnected world. Further to this, we are witnessing unprecedented types of criminal activities suddenly appearing on the radar of law enforcement. These developments are adding another layer of complexity to the challenge.

Against this backdrop, INTERPOL created its Innovation Centre in Singapore in 2017 with a view to fostering innovation in global law enforcement. The Digital Forensics Lab (DFL) within the Innovation Centre has been leading the effort to enhance digital forensics capabilities in the member countries. I truly believe that the work of digital forensics laboratories is a crucial part of policing, particularly in combating digital crimes. Indeed, digital forensics specialists are obliged to constantly learn and to develop their expertise especially in the context of the emergence of Smart Cities/homes, connected cars, drones, mobile networks and cloud platforms.

To this end, the DFL has been organizing Digital Forensics Expert Group Meetings annually in recent years, bringing together forensics experts in law enforcement, industry and academia to share information, knowledge and best practices. Maintaining this global network of experts in digital forensics has been tremendously rewarding and useful in serving our member countries more effectively. Building on the active exchanges at the Expert Group meetings, I am pleased to present the INTERPOL Global Guidelines for Digital Forensics Laboratories.

The Guidelines aim to provide a universal framework for establishing and managing a digital forensics laboratory that is applicable anywhere in the world. It will also hopefully contribute to closing the gap between member countries in terms of their digital forensics practices and capacity. In the hope of creating momentum for the digital forensics field to become a very solid and important area of policing, the INTERPOL Innovation Centre will be at the forefront of instilling innovative spirit in the activities of digital forensics laboratories in the member countries with the aim of contributing to overcoming the complex global security challenges.

Anita Hazenberg

Director, INTERPOL Innovation Centre

ACKNOWLEDGMENT

Many parties have been involved in constructing the INTERPOL Guidelines for Digital Forensics.

First and foremost, INTERPOL would like to thank the Council of Europe for sharing the 'Basic Guide for the Management and Procedures of a Digital Forensics Laboratory' document. The Council of Europe's guide provided a strong foundation and has been used as a model for developing this document.

In addition, INTERPOL would like to express sincere gratitude to CyberSecurity Malaysia as the partner in making these guidelines a reality. CyberSecurity Malaysia's expertise and experience in an accredited digital forensics laboratory has been invaluable in completing this document.

Finally we want to thank our colleagues from

- BAHRAIN: Cybercrime Department, Digital Forensics Unit;
- GERMANY: OE 12 – IT Forensik, Federal Criminal Police (BKA)
- KUWAIT: Digital Forensic Department/General Department of Criminal Evidence of Kuwait,
- SINGAPORE: Technology Crime Forensics Branch. Criminal Investigation Department. Singapore Police Force (SPF)
- SPAIN: Computer Forensic Section, General Commissary of Scientific Police (CGPC) of Spanish National Police (CNP);
- THE UNITED STATES OF AMERICA: Department of Homeland Security, Homeland Security Investigations;

whose valuable input has helped to improve the quality of this document and make it a common effort to serve as a global reference for Law Enforcement Agencies worldwide.

Title of Document: INTERPOL Global guidelines for digital forensics laboratories
Date of publication: 13 May 2019
Original: English
Available in: English

CONTENTS Page

List of Figures

List of Tables

DEFINITIONS AND ABBREVIATIONS

AFF	Advanced Forensic Format
DCO	Device Configuration Overlay
DF	Digital Forensic
DFL	Digital Forensics Laboratory
EWF	Expert Witness Format
HPA	Host Protected Area
IDEN	Integrated Digital Enhanced Network
IMEI	International Mobile Equipment Identity Number
MEID	Mobile Equipment Identity Number
PDP	Personal Development Portfolio (PDP)
RAM	Random Access Memory
SIM	Subscriber Identity Module
SWGDE	Scientific Working Group on Electronic evidence

REFERENCES

1. A Basic Guide for the Management and Procedures of a Digital Forensics Laboratory, Council of Europe (COE), Version 1.1, June 2017

2. Scientific Working Group on Digital Evidence (SWGDE), https://www.swgde.org/

3. ACPO Good Practice Guide for Digital Evidence, Association of Chief Police Officers, version 5, 2012, https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

1. INTRODUCTION

1.1 Document purpose

INTERPOL Guidelines for Digital Forensics Laboratories outline the procedures for establishing and managing a Digital Forensics Laboratory (DFL), and provide technical guidelines for managing and processing electronic evidence.

These Guidelines should be seen as a template document that can be used by countries when considering developing their digital forensics capability. The advice given is intended to be used at both the strategic and tactical levels, in accordance with national legislation, practice, and procedures.

1.2 Intended audience

The document is intended for use by INTERPOL member countries. The objective of these Guidelines is to ensure that electronic evidence produced by the DFL is admissible in member countries' courts of law as well as in the international criminal justice systems.

The Guidelines focus mainly on two distinct groups: the first is the digital forensics strategists and managers who make decisions for the DFL; the second group includes the technical staff who deal with electronic evidence on a day-to-day basis.

In addition, prosecutors, judges and lawyers will also benefit from this document in understanding the digital forensics process, which may be vital for their cases.

1.3 Applying the document

The Guidelines are not intended to impose limits on the DFLs which have to follow the requirements of their national legal framework. The advice given in these Guidelines is not intended to contradict with any national legislation in any member country.

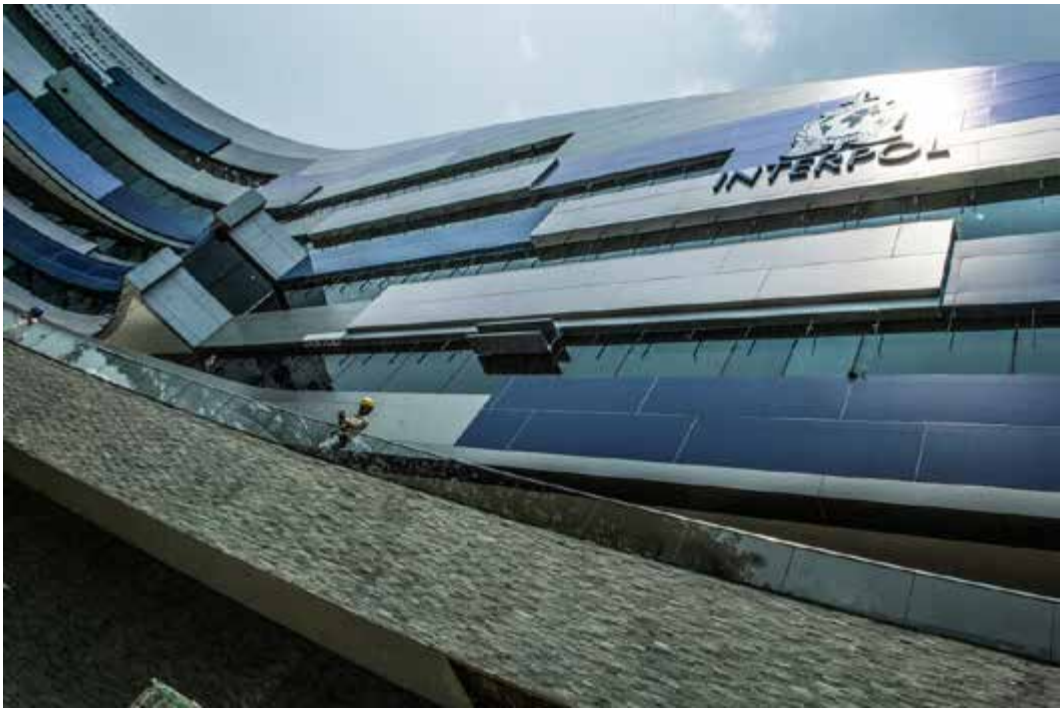
2. INTRODUCTION TO DIGITAL FORENSICS

2.1 Digital forensics

Digital Forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analysing and reporting on data stored on a computer, digital devices or other digital storage media.

The computer, digital device or other digital storage system which holds valuable data for investigation is known as electronic evidence. Such examples are laptops, smartphones, servers, Digital Video recorders, CCTV systems, drones, GPS systems, and game consoles.

The main goal of digital forensics is to extract data from the electronic evidence, process the data into useful information and present the findings for prosecution. All processes involved, therefore, should utilize sound forensic techniques to ensure that the findings are admissible in court.



The nature of the cases in which digital evidence is involved is generally borderless and the offence happens in a split second; the findings derived from electronic evidence must therefore follow a standard set of guidelines to ensure that it is admissible not only in a specific country's court of law, but also in the international criminal justice system. The INTERPOL Guidelines for Digital Forensics provide a baseline and a reference for the management of digital forensics.

2.2 Understanding electronic evidence

Electronic evidence, unlike any other evidence, such as fibre, hair and gunshot residue, is challenging to process due to the fact that:

a. The data can be scattered in several physical locations, sometimes across countries;
b. The data can be transferred across jurisdictional borders effortlessly and in a matter of seconds;
c. The data are highly volatile – easily altered, overwritten, damaged or destroyed by the single stroke of a key;
d. The data can be copied without degradation;
e. The lifespan of electronic evidence, unlike any other discipline of forensic evidence, is short before it is rendered useless. An example of this is a smartphone: after five years, it may not be able to switch on or function properly.

Based on these facts, therefore, electronic evidence must be processed and handled with due care.

2.3 Principle of electronic evidence

When dealing with electronic evidence, the following principles must be adhered to:

a. Electronic evidence must be obtained in a legal manner.
b. The Staff involved must complete the appropriate training programme, prior to handling electronic evidence.

c. Any actions taken on the electronic evidence must not change its data. If it is necessary to access the original data or change the system setting, it is recommended that only competent staff be able to do so, and that staff must be able to justify those actions.
d. Any action that requires the original data to be accessed or changed should be recorded and witnessed by a fellow practitioner if possible.
e. A record of all actions taken when handling electronic evidence must be created and preserved so that they can be audited. An independent third party should be able to repeat those actions and achieve the same results.

3. MANAGEMENT OF A DIGITAL FORENSICS LABORATORY

This section explains the process of establishing a DFL – creating a plan, acquiring the required resources, and the activities related to maintaining the DFL.

3.1 Conducting a plan

Initial research must be conducted to establish recent statistics on the seizure of electronic evidence, the types of crimes, location, specialization of the seizing officers and whether any digital forensic analysis has been carried out.

The information should provide a fair guide as to the growth of digital investigation and serve as an indication of where to start. This information should also help the agency to identify the need for investment as well as the size of the DFL.

Each agency must seek to understand legal or procedural requirements in the establishment of the DFL within its country's criminal justice system. This can be accomplished through comparison with countries of similar geographic and demographic size that have already established a DFL, to provide a firm understanding of the requirements for establishing a DFL.

Finding the answer to the following questions will help decision makers to understand and recognize the scope of the DFL:

a. How many investigations into reported crimes have been facilitated with the use of digital data in the last 3 years, 2 years and 1 year?

b. Is there an obvious and documented growth in this type of investigation?

c. If digital investigation was required;
   - Who conducted the analysis?
   - Which procedures were followed?
   - What was the outcome?
   - What was the cost of the examinations?
   - Was it not possible to conduct some functions due to a lack of resources?

d. Are there other law enforcement agencies in the country which have a similar requirement with which a collaboration may be initiated to expedite acceptance of the DFL proposal?

Establishing a DFL requires capital and operating cost. Capital costs include the cost of equipment and software and obtaining and refurbishing the appropriate facility. These are the "one-off" costs required for the infrastructure and equipment, before commencing to the operational stage. Operating costs will include the running expenditures such as building rental, software licence

fees, staff salaries, staff training, forensic equipment maintenance and the replacement of office equipment.

Once this initial research has been conducted, decision-makers should have a better idea about the role and the size of the DFL, as well as the number of staff required to provide an effective resource for all stakeholders.

3.2 Premises

When selecting the premises to build the DFL, several factors need to be considered to ensure its success. The following sections explain in detail the possible success factors when choosing and developing a DFL.

3.2.1 Location

Several factors need to be considered when selecting the location of the DFL. Some concerns that need to be addressed are:

	Considerations for Selecting DFL Location
1	Is there sufficient electrical power to run the required equipment, does additional equipment need to supplement the power facilities installed (backup generators/UPS)?
2	If the lab is above the ground floor, is there a lift available to transport large quantities of electronic evidence?
3	Is the building or office robust enough to ensure the security of the data and protect the people within?
4	Are the walls, floors, and ceilings strong enough to withstand physical or environmental damage?
5	What is the risk from flood, fire, natural disasters and civil unrest?
6	Is due care being taken to minimize the risks of incursion by a terrorist or criminal organization seeking to damage investigations?
7	Is the building suitable to provide the cooling required for the amount of equipment to be housed within the building, or can cooling facilities be retrofitted?

Table 1. Considerations for Selecting DFL Location

3.2.2 Physical Security

The DFL needs not only to secure electronic evidence but also to ensure the security of the staff, valuable software and hardware. The checklist for physical security is as follows:

Checklist for Physical Security		
1	**Surveillance system** The surveillance system is used to monitor the premises for unauthorized access and break-ins. Installation professionals should consider the best strategic place as well as the best resolution to ensure maximum security.	☐
2	**Access control** Access control can be in the form of physical locks and keys, electronic keypads, swipe cards, and/or biometrics, depending on the budget. 	☐
3	**Fire control system** A DFL must have a fire detection system and fire suppression system installed on the premises. The material used for the fire suppression system must not cause damage to the exhibits, equipment or personnel.	☐
4	**Windows, doors & walls protection** When required, windows should be reinforced with bars and locks to prevent break-ins. If the DFL has glass windows and walls, care should be taken that sensitive data are protected from view. Consider using a fireproof door in a location such as a stairwell or corridors to protect the premises from fire.	☐
5	**Sufficient power sockets, fuses, breakers and current load** Sufficient power sockets, fuses and breakers must be installed in the DFL to ensure smooth operation and prevent power overloads leading to fire hazards and posing risks to the safety of the staff.	☐
6	**Anti-static flooring** Anti-static flooring helps to reduce possible electrostatic discharge (ESD) that may cause harm to employees, equipment and evidence. 	☐
7	**Radio jamming system** It is recommended that the DFL install a system to block network signals, for example using a Faraday cage or a jamming device. A Radio jamming system will block any network signals and prevent any intrusion into the exhibit. With current wireless technology, the possibility exists for powered-on smart phones or laptops to automatically attempt to connect to existing wireless networks, hence modifying their data. National legislation must be checked to verify that the use of such systems is allowed and they do not interfere with other systems.	☐
8	**Cooling System** It is common for a DFL to have computers to conduct work, generating a considerable amount of heat within the lab. Overheating can lead to loss of data and damage to hardware. The DFL should install a cooling system to control its room temperature, including the evidence storage room and server room.	☐

9	**Off-site Data Storage Backup** A large amount of data is stored by the DFL once it is fully operational, and it can be sensitive in nature. The data are usually stored in a server. It is best practice for the data to be backed up to an offsite server, away from the DFL. In the event of a disaster where the DFL is affected, the offsite storage can be used to gain access to important data. Having an offsite data storage backup is part of a disaster recovery plan which ensures operations can be up and running in minimal time.	☐
10	**Archival Data Storage / Long Term Data Storage** After analysis, data should be stored such that they can be retrieved at a later date for the purpose of further judicial process, or in light of new evidence or findings pertaining to the case. Storage time should be adapted to national legal requirements.	☐

Table 2. Checklist for Physical Security

3.2.3 Size and Layout

At a minimum, a DFL must consist of desktop tables for Examiners to conduct analysis, a large table for evidence registration, labelling, imaging and sealing, a fireproof cabinet for electronic evidence storage, and a filing cabinet. This minimum setup is sufficient for a small-scale DFL, where small quantities of electronic evidence are submitted.

However, for an agency that deals with a large number of electronic evidence, this minimum setup may be insufficient. It is recommended that the DFL segregate the specific types of activities to prevent cross-contamination and loss of exhibits.

For example, there must be an area for receiving evidence. This can be done in the reception, where an Examiner will discuss case requests and the Requester and Technician will register the submitted evidence.

The laboratory, mobile phone lab or computer lab, for example, must be restricted to the DFL staff only. Each Examiner will require a large desk for IT equipment, filing cabinets to hold their case files and comfortable chairs. In addition, ergonomic keyboards, and padded mats can also provide more comfort for examiners.

If the DFL requires a server – this may be stored securely within the laboratory and if possible, in a separate room.

It is recommended to have a designated area for imaging and processing. It should be separated from the Examiner's workstations and should ideally be close to the evidence storage room to reduce the amount of manual handling.

The DFL may also consider having a space to conduct briefings or meetings, as well as an additional office for the laboratory manager.

In addition to the above, areas dedicated to the storage of non-evidential equipment such as media copiers, media production equipment, printers, scanners, files, property bags, tags, evidence labels, storage media, office equipment and personal belongings of staff, should be considered when selecting the most appropriate place to locate a digital forensics laboratory.

The building or office should be large enough to expand if there is an anticipated increase in demand for DFL work. Many existing DFLs have found it necessary to relocate or expand in a short time due to exponential increases in workload. It is considerably more expensive to relocate or expand, so it may be beneficial to provide room for expansion in the initial business plan.
The following is a suggestion for a basic floor plan for a DFL.

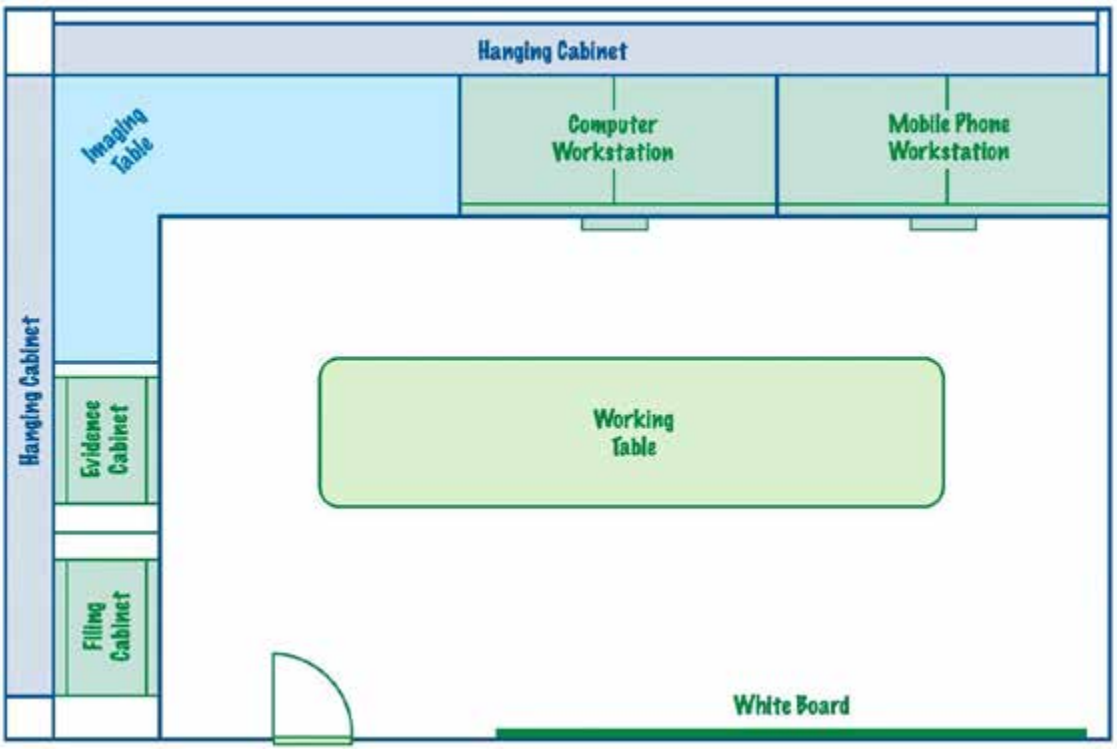


Figure 1. Basic Floor Plan for DFL Setup

If an agency decides to develop a moderate sized DFL, the following is a suggestion for the floor plan.

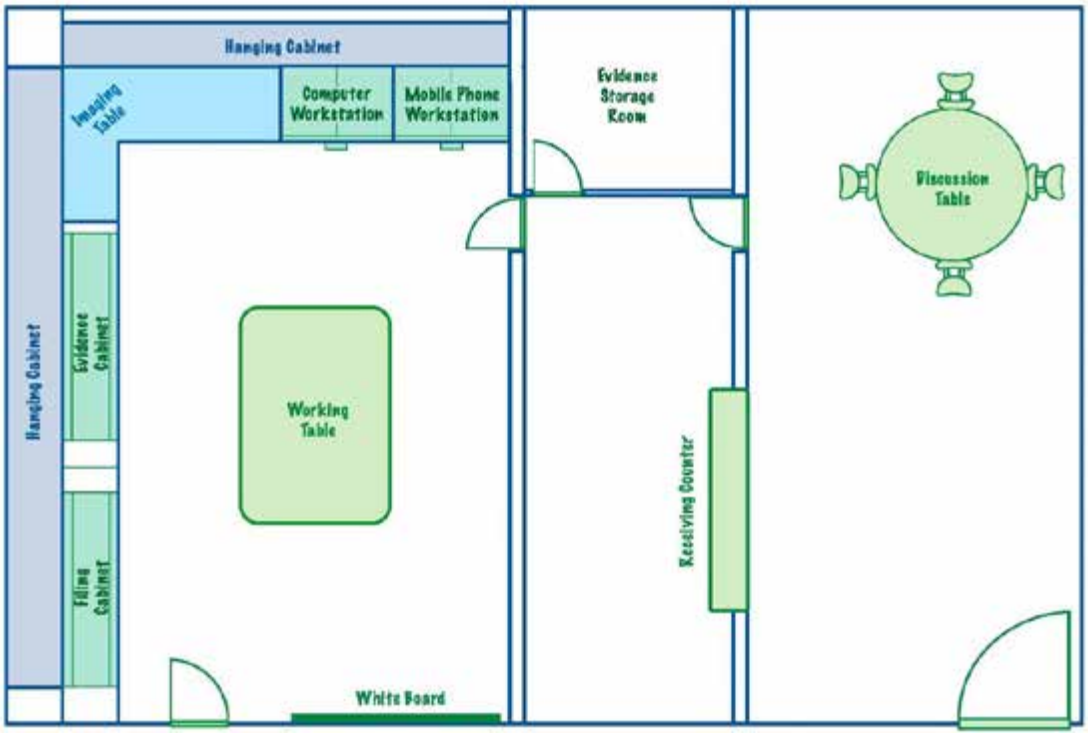


Figure 2. Floor plan for a moderate-sized DFL setup

3.2.4 Facility

Once the premises have been selected and security features have been installed, the Laboratory Manager needs to think of the facilities to be installed within the DFL.

Common facilities installed in a DFL are as follows.

Common Facilities in a DFL	
1	**Reception area** The area for delivering and collecting electronic evidence. It is best to separate this area from the labs with an access door. This is to prevent unauthorized access to the labs.
2	**Evidence storage room** The room is dedicated to storing electronic evidence. In some DFLs, this room is also used to store the server. Access to the room must be restricted to certain DFL staff only. Alternatively, if there are only a few exhibits, then a cost-effective solution is to have a safe box or fireproof cabinet to store all the electronic evidence instead of having a dedicated storage room.
3	**Evidence processing area** A designated area to dissemble, assemble, label and image the electronic evidence. This area should be separated from the Examiner's workstations and should be close to the evidence storage room to reduce the amount of manual handling.
4	**Laboratory** Depending on the types of DF cases received, a DFL can have several labs to segregate work based on types of evidence. Examples include a Computer Forensics Lab, Mobile Phone Lab, Audio or Video Lab.
5	**Personal space** In some DFLs, staff should have their own desk to conduct administrative tasks, write reports and create presentation slides. Labs are used solely for analysis work, whereas this personal space is used by the staff for other necessary work products.
6	**Briefing space** A briefing space is where Examiners can discuss a case and where the DFL manager/director can hold a briefing session about a case. The room can be either an open or closed space. It is good to equip the room with a display screen and a whiteboard to facilitate discussion or presentations.
7	**Isolated and unfiltered Internet access** Laboratories in the DFL commonly have their own isolated network from the organization's network. This is to prevent malware and viruses from entering the rest of the network. Furthermore, the DFL must have unlimited and unfiltered Internet access. Some cases require Examiners to access rogue websites, so they need to have Internet access which allows for this. This network should be provided with security and at minimum a basic intrusion detection and logging system which should be monitored and maintained periodically.

Table 3. Common facilities in a DFL

3.2.5 Visitors

Visitor access to the DFL must be restricted to prevent data leakage or any possible damage to the electronic evidence. Visitors can include maintenance workers, staff from other agencies, consultants or people delivering the electronic evidence.

The following table gives the basic checklist when receiving visitors.

Checklist for Visitor		
1	**Register** Visitors must be registered using a form or via an online system before entering the DFL premises. For a large group of visitors, the accompanying DFL staff must organize appropriate registration processes, noting the agency, size of the group and purpose of the visit.	☐
2	**ID Pass** A temporary ID pass may be issued to the visitor, especially for long visits. The ID pass must clearly distinguish the visitor from the DFL staff.	☐
3	**Escort** Visitors must be accompanied by DFL staff at all times when on the DFL premises.	☐
4	**Visitor Policy** Clear signs or a poster on Visitor Policy must be displayed in the DFL common area for visitors to read. Rules such as photographing, eating and drinking, touching forensic equipment and electronic evidence, etc. must be clearly stated to visitors. Instructions must be simple and easy to read for non-English speakers.	☐
5	**Viewing of Contraband** Clear signs should indicate that potentially illegal and inappropriate images are being analysed and viewed within the DFL.	☐

Table 4. Checklist for Visitor

3.3 Staff

Depending on the size of the laboratory and the number of staff required, the different functions that are required must be considered. Staff roles and responsibilities will need to be documented. Detailed job descriptions should be prepared so that each member of the team has a clear

understanding of his/her job profile. Where possible, the structure of a DFL should allow for staff career advancement within the organization.

Experience shows that highly qualified staff spend much of their time undertaking mundane tasks below their level of expertise. A job profile and a clearly set out career path at the early stage of the DFL development will provide direction for the organization's planning and budget forecasting.

3.3.1 Recruitment

Staff employed by the organization for DF work often depends on the type of DF cases and the total amount of electronic evidence submitted to the DFL. These staff may come from any educational background, but must have strong fundamentals and a high interest in the computing field and current advances in technology.

A DFL typically consists, at a minimum, of a Lab Manager and two Examiners. The Examiner works at the DFL, analysing the electronic evidence and sometimes may be required to go to the field site to conduct evidence preservation. If there is an increase in cases and more forensic equipment is obtained, it is often best for the DFL to employ a Technician. An Administrator may also be employed if the DFL deals with numerous administrative tasks such as managing various documents, training, visits, and talks.

A suggested organization chart at minimum level is as follows:

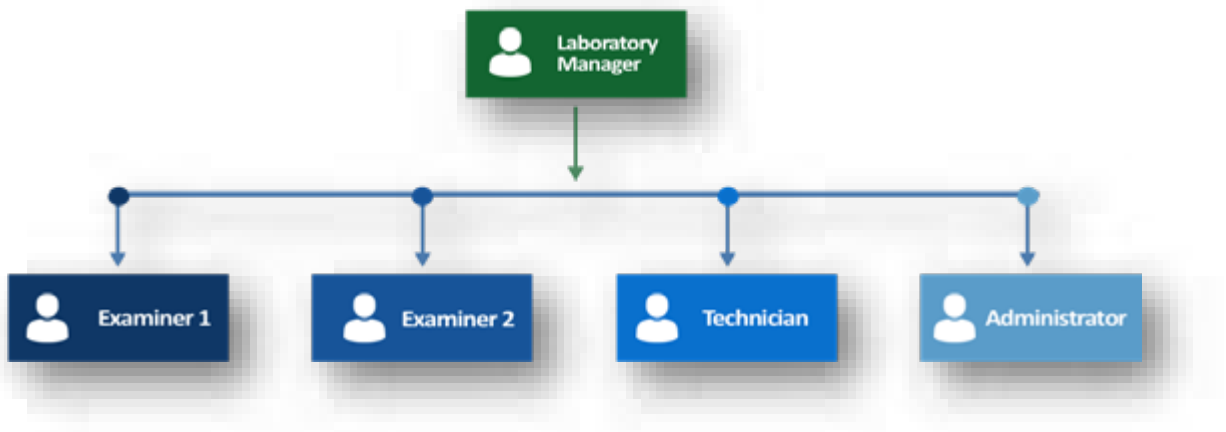


Figure 3. Organization chart for basic setup of Digital Forensic Laboratory

3.3.2 Security Clearance

Before DFL staff are hired, it is advisable for candidates to undergo a background check or security vetting. At a minimum, the DFL or the Human Resources Department must ensure that a candidate has no criminal record and has satisfactorily passed clearance by the authorities. While these clearances may not always be ideal, they at least provide an indication of any serious criminal offences in the past. It is common practice for the Human Resources Department or the DFL manager to have access to the vetting and the candidate's personal records prior to the interview process, or at least during the interview session.

3.3.3 Job Description

All staff must have a clear Job Description once they are employed by the DFL. Each individual's roles and responsibilities in the DFL must be explained in the Job Description. At a minimum, the roles and responsibilities of each staff member in the DFL should be explained as follows:

Description of Roles and Responsibilities
Laboratory Manager The Laboratory Manager must have technical knowledge and a strong understanding of legislative requirements for electronic evidence, procedures and processes. A Laboratory Manager must understand the overarching principles described in this guideline. He/She must have control over the original set up, and building oversight concerning the purchase of hardware and software or the DFL procedures and functions. He/she is responsible for leading the recruitment, training, mentoring, counseling and guidance of everybody employed within the unit. The Laboratory Manager is also responsible for decision making related to individual cases, including whether to accept or reject a case as well as the priority.
Examiner The Examiner must have the relevant technical knowledge and appropriate qualifications. Ideally he/she should have some training in the use of DF software. On being hired, the Examiner will be required to attend specific training to obtain a minimum set of skills. The Examiner must have knowledge of legislation and be aware of the elements of each offence in order to articulate those facts when investigating different types of crimes. These roles require an analytical and investigative mind-set. The Examiner must also be able to deliver his/her findings in a clear and understandable manner, therefore having good oral and written communication skills is essential.
Technician The Technician conducts evidence processing such as registration, acquisition and storage. Depending on the size of the laboratory, several technicians may be required. The Technician must have strong technical skills in the computing field and technical knowledge of the various methods of forensically acquiring digital data. A key skill requirement is attention to detail and the ability to clearly document all actions conducted on each item of evidence. The Technician is also responsible for maintaining forensic equipment. He/she needs to ensure that the hardware firmware is updated and software patches and updates are installed when released. The Technician is also responsible for handling the evidence in the Evidence Storage Room. He/she needs to maintain records of evidence as well as check in and check out exhibits in the Storage Room.
Administrator A DFL may also employ an Administrator to conduct the laboratory's administrative tasks. He/she is responsible for management of DFL documents, training and talks. He/she can also act as a liaison officer for internal as well as external stakeholders. The Administrator can also be responsible for handling the purchase of equipment for the laboratory.

Table 5. Description of Roles and Responsibilities

3.3.4 Staff Development

The DFL management must ensure that staff involved with DF tasks are adequately equipped and have the right skills.

The reason for this is that data contained in electronic evidence can be easily altered, damaged or destroyed by a single stroke of a key, so the staff must know how to handle the data without damaging them. Another reason is that the complexity of crime today can make it difficult to discover the right data; therefore the DFL staff must know how to find and extract them.

A. Training

Once staff have been recruited, it is important to continually develop their abilities to motivate and retain them, and establishing an achievable staff development programme can support this. This should begin with an induction to their new workplace. The Job Description must clearly indicate their role and responsibilities and their reporting manager. The manager must identify and plan for staff training needs and make the appropriate arrangements. The DFL may choose to send staff on training courses or it can arrange a session for staff to shadow and learn from colleagues, according to a planned timeline. For example, all Examiners will require externally certified training to provide them with the confidence to use the forensics tools and the credibility to deliver reliable evidence in court. A suggested skillset that may be helpful in determining the training needs is available at Appendix **A: DFL Skillset Checklist.**

B. Proficiency Maintenance

Advancements in technology require the staff to be regularly updated with the right knowledge and skills. In addition to the training programme, the DFL should consider having a proficiency maintenance programme, as part of which staff would be required to attend seminars on technology updates, attend technical-related meetings, continuously conduct electronic evidence analysis, attend product demonstrations, or attend retraining programmes. The programme is important to ensure that Examiners' skills are up to date with the current technology and that they are always able to perform DF tasks.

C. Personal Development Portfolio (PDP)

To effectively manage staff development, the DFL may consider issuing each member of staff with a Personal Development Portfolio (PDP). This portfolio should contain a training plan, training certificate, attendance record, as well as records of milestones achieved in the workplace. Managers may use PDPs to set targets for individuals and monitor their performance from time to time.

D. Research and Development Activities

Apart from the training and proficiency maintenance, management must also set aside some time for staff to undertake research and development activities. The staff should evaluate new tools and applications coming on to the market and decide whether there is a need for the DFL to use them.

E. Staff Retention

DFL should take note that the extensive training programme makes staff highly valuable for other organizations to hire, hence the high turnover rate in the DFL. A great deal of time and money will be spent on staff training, and it is vital they are retained, especially once they become more experienced. To minimize the risk of losing staff, the Organization should have a good staff retention programme in place. Having robust personal development plans for

each member of staff will provide them with personal objectives and a better understanding of their career path as well as future opportunities within the Organization. Factors that contribute to staff loyalty are not always limited to a salary; often a good and healthy working environment is a contributing factor.

3.3.5 Mentoring

For newly-hired staff it is recommended to have a mentoring session during their probation period. Mentoring is the process whereby an experienced staff member monitors the newly-hired staff member's work. The role of the mentor is to guide and support, as well as to share information in a friendly and confident environment. The need for mentoring sessions for newly-hired staff will diminish as they settle into their new roles.

Mentoring usually takes place alongside appraisal and the assessment of performance in relation to the probation period.

3.3.6 Health and Safety

The DFL Manager is responsible for ensuring the health and safety of all staff and visitors to the DFL. A risk assessment must be conducted by examining any current conditions in the premises that could potentially affect health or safety. Any hazardous material must be dealt with. There is often a dedicated staff or team within the agency to take care of health and safety matters, but when there is none, it is the responsibility of the DFL manager to be aware of any legal health and safety requirements.

Measures must be taken to ensure that visitors and staff from other departments do not see or are not subjected to illegal or distressing materials found in the DFL. This possibility can be mitigated by following the suggestions previously provided with regard to the structure and set-up of the DFL.

Several common safety features found in a typical laboratory are:

- Anti-static mats and wrist straps – to reduce the risk of static damage to equipment and exhibits.
- Dress code – proper footwear that covers the foot completely must be worn, long hair must be tied back, daggling jewellery and baggy clothes must be secured. If needed, surgical gloves should be worn to prevent exposure to contaminated substances.
- Handling/lifting – ensure staff are aware of the correct way to lift heavy items to avoid injury.

- Rubber mats - to reduce the risk of electric shock.
- Circuit breakers - to reduce the risk of electric shock or damage to equipment and evidence.

3.4 Equipment

A DFL must have access to forensic equipment that is required to produce the correct forensic results. Equipment can be in hardware form, software form, open source or commercial tools. Prior to use, the equipment must be tested and verified to ensure it is able to produce the correct results.

The recommended basic equipment for a DFL is available at Appendix **B: Checklist of Basic DFL Equipment.**

3.4.1 Software

When making a software purchase, the DFL must consider the initial price, yearly licence fees, maintenance fees and training fees.

The cost of licences can be significant, therefore the DFL must make a thorough study and include this in the planning of the budget for the subsequent yearly fees. It must be ensured that the software obtained correctly matches the DFL requirements.

Some open source software offers extensive features and can be used by the Examiners, but this software may be lacking in support and training opportunities.

Some jurisdictions and standards require 'dual tool verification', and it might be necessary to purchase additional software in order to conduct result comparison and verification.

The DFL must also consider having a Case Management System for its operation. This system will hold the database of cases, exhibits, Examiner's name and forensic results. Minimum entries for a Case Management System are as follows:

- Date, time and person delivering and receiving the exhibit to the DFL.
- Unique exhibit reference number.
- Unique case reference number.
- Requester's name and contact details.
- Type of crime and related act.
- The names of DFL staff that have had contact with the exhibits.
- The narrative for the case request.
- Time factors – such as delivery dates and anticipated court dates.
- Analysis process – Imaging, examination, extraction, calculated hash values, etc.
- Exact date and time of analysis conducted, as well as the Examiner's name.
- Details of quality assurance by colleagues and managers.
- Result of the analysis.
- Record of communication with the Requester.

All this information is vitally important to show continuity, credibility and verification of actions and evidence. The DFL can create the system internally, purchase an off-the-shelf solution, or hire a programmer to develop the system.

3.4.2 Hardware

Hardware must also be properly maintained periodically, for which it is recommended to have a scheduled plan and an equipment list.

An important element for the DFL to consider, apart from the storage and backup of operational data, is the storage of the electronic evidence. The three types of data that the DFL may need to deal with are the original evidence, the forensic copies and the data generated during the analysis. It is essential for the DFL to have a large, powerful and speedy server due to the volume of data and electronic evidence. Consideration must be given to how this is to be stored, archived and backed up. A stringent backup and archive regimen should be implemented to offer resilience.

A list of basic DFL equipment is available at **Appendix B: Checklist of Basic DFL Equipment.**

3.4.3 Tools and accessories

Tools and accessories such as cables, screwdrivers and power extensions are just as important as the software and hardware in a DFL. Some DF work requires electronic devices to be disassembled and reassembled, so the DFL needs to have access to good-quality tools and accessories. The following is a list of possible items that a DFL may need to perform day-to-day tasks:

- Power extension
- Leads and adaptors
- Screwdrivers
- Toolkit
- Camera, video recorder
- Magnetic tapes
- Communication devices
- Storage box or container for carrying equipment
- Torch
- Magnifying glass
- Evidence sealing or evidence bags
- Tamper-proof stickers
- Permanent markers
- Faraday bag

4. MANAGEMENT OF DIGITAL FORENSIC CASE

The DFL must establish a case management procedure before starting to receive cases. Generally, there are seven steps in managing a case, as illustrated in the following figure and further explained in the subsequent sections. Prior to conducting a case, the DFL must ensure that it is following and complying with relevant legislation. The Manager or Examiner must ensure that legal permission for processing the evidence exists through warrants or official documents. The aim of conducting DF work is to use evidence to prove or disprove disputed facts, hence electronic evidence must be obtained in compliance with the legislation. At the end of the DF work, it must be ensured that the electronic evidence is admissible and the forensic report is acceptable in court.

Figure 4. Case Management Procedure

4.1 Receiving a request

The DFL work starts on receipt of a formal request from a Requester. This formal request can be in the form of a letter, e-mail or fax. The information supplied in the formal request should include a description of the crime involved, the related act, electronic evidence details, the case objective and possibly the warrant.

The lab manager or appointed staff will then review the request and determine whether the case is feasible, based on the following criteria:

a. The case is within the scope of digital forensics, i.e. the evidence is electronic and not otherwise - such as DNA or fingerprints
b. Methods and tools that are available
c. Staff is available to conduct the case
d. The legal requirement is fulfilled

The DFL will then formally respond to the request as to whether or not it can accept the case. If the decision is to accept, the DFL will provide a date for delivery of the electronic evidence from the Requester.

4.2 Registering a case

Once the DFL decides that the case is feasible, the Requester will come to the DFL with the electronic evidence. The DFL creates a unique running case number for that case and fills out a case registration form. A sample of the case registration form is available at Appendix **C: Sample of Case Registration Form.**

In order to effectively examine electronic evidence, Examiners need to be supplied with a clear and specific case request by the Requester. Due to large amount and various types of data in a device, such as documents, videos, communications, health monitoring data, locations etc., it is impossible for an Examiner to examine the data without a clear and specific request.

Based on that information the Examiner can plan the methods and tools to be used to process the evidence.

Both parties, the Requester and the DFL staff, must sign the form. The work has now officially begun. The DFL will then create a folder in a storage medium to store all logical data related to the case.

4.3 Registering an exhibit

When electronic evidence (exhibits) is received, it is important for the exhibit to be sealed before custody can be transferred to the DFL. To eliminate any reasonable doubt about the integrity of the evidence, both the Requester and the Examiner must be able to demonstrate that no-one else has gained access to the evidence during the transfer process from one party to the other. This practice is new and costly for some agencies, the DFL will nevertheless provide constant awareness and provide a firm timeline to start practising this procedure with the agencies.

Each piece of electronic evidence that is submitted must be registered and assigned a unique exhibit label which is documented with the exhibit's details in the registration form. A sample of the exhibit registration form is available at Appendix **D: Sample of Exhibit Registration Form**.

This registration includes each exhibit's sub-items, such as sim cards and memory cards. The labels must be able to track the sub-items to the parent item. For example, if a mobile phone is labelled as 20190105(2)-MP01, then the sim card may be labelled as 20190105(2)-MP01-SIM01.

It is important to note that any defects on the exhibit must be documented in the exhibit registration form. This is to protect the DFL from any negative claims in the future.
Any forms of softcopy documents related to the exhibit must be uploaded to the case folder.

Now the chain of custody of the exhibits has started, and the form must be filled in by the staff receiving the exhibit.
While the exhibit is not in use it must be stored in an Evidence storage room, as explained in section 3.2.4

4.4 Photographing an exhibit

A Photograph of the exhibit is taken for the following reasons: to record the state of the exhibit and to effectively identify the exhibit in the future. Photograph the overall view of the exhibit as well as the close-up view. If the screen is active, photograph its screen display also. The pictures should then be uploaded to the case folder. It is advisable to photograph the exhibit before returning it to the Requester for future reference as to its condition.

4.5 Conducting analysis

The analysis must be conducted in accordance with the DFL Analysis Model. Refer to Section 5 for details of how to conduct the analysis. During the process, Examiners must maintain communication with the Requester and communicate any deviations or limitations that may arise during the examination. Some Examiners have years of knowledge in digital forensics, and so they are able to allocate the correct data when there are effective communications between Examiners and Requester.

4.6 Returning the exhibit

Once the analysis has been completed, the DFL contacts the Requester to pick up the evidence. Common practice in the DFL is to return the exhibit along with the forensic report to the Requester to save travelling time. Before returning the exhibit, the DFL must seal it. The seal must have the staff's initial, the exhibit's label and the date and time it was sealed. An example of exhibit sealing is available at Appendix **E: Sample of Exhibit Sealing.**

4.7 Closing the case

The process is then complete and the DFL can close the case. To close the case, both parties must agree that the work is complete and the report has been delivered to the Requester. This can be done by signing a form. An example is available at Appendix **D: Sample of Exhibit Registration Form,** where by signing the exhibit return section, both parties agree that the work is now complete.

After completion of the case, the way forward involves the Examiner appearing in court to provide expert testimony on the forensic results of the case if required. The Requester informs the Examiner when he/she is needed in court.

5. LABORATORY ANALYSIS PROCEDURE

This chapter covers the procedure for conducting analysis on electronic evidence at the DFL. An overall, chronological process model is presented to provide a better overview of the main processes.

There are typically four phases involved in the analysis of electronic evidence in the DFL: acquisition, examination, analysis, and presentation. Throughout the process, the chain of custody of the evidence must always be updated whenever it changes hands and its integrity must be secured at all times. Examination and analysis phases may be repeated until the work satisfies the case request.

It is commonly understood that conducting DF work in the DFL requires these four phases, however, not all cases will require all the phases. In certain cases, the acquisition phase can be skipped to conduct triage straightaway during the examination phase. An example of such a case

is when there are large sets of data, where conducting acquisition on each evidence item may be not feasible.

The following figure shows the laboratory analysis model:

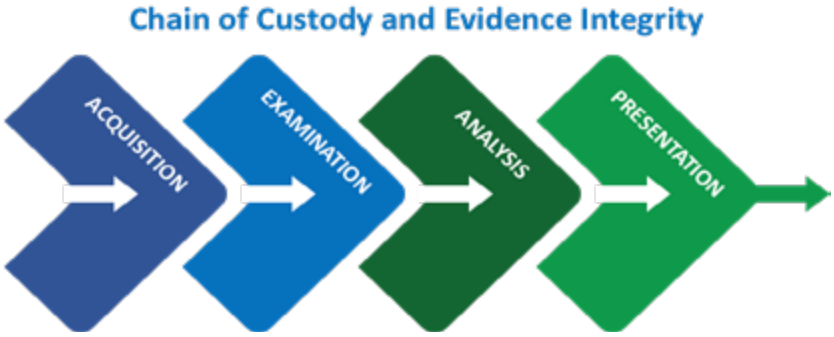


Figure 5. Digital Forensics Laboratory Analysis Model

The next section in this document explains in detail each phase involved in the DFL Analysis Model.

5.1 Acquisition

5.1.1 Overview

Acquisition or, as it is better known, data acquisition, is the process of creating a forensic copy of the electronic evidence (exhibit) such as hard disk, thumb drive or server in the form of an image file or files. The image file or files will then be used for the next stage of the process in analysing the evidence. The acquisition is made in order to preserve the integrity of the electronic evidence. It is to produce an identical copy of the data without changing the content of the electronic evidence in any way.

Electronic evidence needs to be acquired in a forensically sound manner. Data is typically acquired by collecting volatile data from a running computer during a search, or by acquiring a storage medium from a seized computer or at any other stage during an investigation. The intangible nature of data and information stored in electronic form makes it easy to manipulate and more prone to alteration than traditional forms of evidence. It is therefore important to have a defined and tested acquisition procedure.

Once an image file has been created, both the hash value of the exhibit and the image file must be recorded. Hashing is used to prove that the image file is exactly the same as the content of the exhibit. There are a lot of hashing algorithms used in DF, such as Sha-256. Most forensic software and hardware offer the hash-generating feature.

Examination and analysis must only be done on a forensic copy of the original evidence, unless circumstances prevent examiners from doing so. This is important in order to preserve the integrity of the evidence. The forensic copy of the electronic evidence must be stored on other storage media, never onto the evidence itself. The forensic copy must be clearly labelled to

ensure it is not mixed up with the original evidence or with forensic copies from other cases. The DFL must therefore prepare some storage media before receiving cases.

This document explains the process of conducting DF examination and analysis on two types of device:

(I) Computers
(II) Mobile Devices

5.1.2 Computer

Acquisition of computers is as follows:

5.1.2.1 Types of Data Acquisition

There are two levels of data acquisition: physical data acquisition and logical data acquisition. While physical data acquisition includes all raw data, a logical copy typically only includes an allocated subset of those data.

Physical data acquisition, at whole disk level, copies all data contained on the disk, including the partition scheme, partitioned area, and un-partitioned area. Logical data acquisition on disk level copies only a logical partitioned area.

The Examiner commonly chooses physical data acquisition of a whole disk because it includes deleted files and unallocated clusters. When dealing with encryption, however, a logical data acquisition of unlocked data is preferred to a physical acquisition of the encrypted data. In this cases physical acquisition is still recommended if the forensic software support the mounting of the encrypted imaged.

"There are two levels of data acquisition; physical data acquisition and logical data acquisition. While physical data acquisition includes all raw data, a logical copy typically only includes an allocated subset of all those data."

To create a copy, the Examiner first needs to choose the state of the exhibit. If the system is up and running, the Examiner may need to choose live acquisition.

However, if the system is powered off, the Examiner may then choose to conduct dead acquisition. The difference between these methods of acquisitions is described in the following table.

	Dead Acquisition	Live Acquisition
What?	Dead acquisition is conducted on a dead system. A dead system is a system that is not running; turned off, with no power. When the system is dead, volatile data in temporary storage areas such as RAM memory, running processes, cache or active application dialogues on a computer will no longer be available.	Live acquisition is conducted on a live system. A live system is a system that is up and running where information may be altered as data is continuously being processed. Because of the rich evidentiary value that could be discovered in a live system, switching it off may cause loss of volatile data, such as data stored on the cloud, encrypted data, running process, network connected and mounted file system.
How?	The process of conducting dead acquisition is straightforward as it is normally done automatically using forensic equipment. The hard disk must first be taken out of the computer before connecting it to the equipment, if possible. In some cases netbook computers or devices with soldered solid state drive storage cannot be extracted in dead acquisition. Other methods to perform extraction in such cases, like booting the system with a live CD/USB, should be considered.	Data on a system have different levels of volatility. These data will be lost if the system is switched off or rebooted. Whenever the Examiner acquires live data, it is sensible to collect from the most volatile data to the least volatile. The typical level of volatility, from the most to least volatile is as follows: • Memory • Swap File • Network Processes • System Processes • File System Information
When?	Dead acquisition is conducted when: • System is switched off • Deleted data is more important than volatile data	Live acquisition is conducted when: • The system is business-critical and cannot be shut down • Volatile data are more important than deleted data

Table 6. Method for conducting acquisition - Dead Acquisition and Live Acquisition

The Examiner then needs to choose whether to clone the exhibit or to create an image. The clone copies the data bit-by-bit from one storage medium to another. The image, on the other hand, copies the data bit-by-bit from one storage medium into an image file. This file can then be stored on another medium. The latter technique is the more commonly used as the image file can subsequently be read by most forensic software for forensic analysis processing. Cloning is commonly used for simulation purposes. Before that can be done, the Examiner must ensure that the exhibit is write blocked; a method which enables only reading and prevents any writing on the exhibit.

5.1.2.2 Write Blocker

A write blocker is a device that enables data to be acquired from a hard disk without modifying the disk's data. The device allows a read command, but does not allow write commands to be executed on the hard disk. Most imaging tools have a built-in write blocker that the Examiner can utilize while imaging a hard disk. While write blocking can also been achieved by software tools or changes in the Windows registry, hardware solutions will be preferred in DFLs.

5.1.2.3 Imaging Tools

The imaging of a storage medium can be performed using forensic software or hardware. There are free, as well as commercial, products available which can aid in the process. When purchasing a tool, the most important criteria to look for are the speed of conducting the image and the reliability. The imaging software can include features such as:

- recognition of hidden areas
- imaging multiple devices simultaneously
- imaging to multiple destinations concurrently
- imaging queues
- hash verification with common hash algorithms
- hash verification at different stages of the imaging process
- support the most common forensic image formats
- producing encrypted and compressed images
- resuming an interrupted acquisition process
- tolerance of hardware errors

The Examiner must always be alert to the possibility of anti-forensic techniques. Hidden areas like host-protected areas (HPAs) or device configuration overlay (DCO), which are only addressable via special ATA commands, can only be detected by some available imaging software solutions.

5.1.2.4 Imaging Format

There are several common image file formats, namely raw or dd. These formats store all data from the original medium in a raw file. Other formats include Expert Witness Format (EWF) and Advanced Forensic Format (AFF). They contain features such as:

- Compression of data
- Encryption of data
- Error-Checks
- Case Metadata
- Hash sums
- Splitting the image in chunks

Furthermore, different forensic software solutions come with their own proprietary image formats with similar features. When choosing an image format, always opt for one that is supported by most forensic software solutions. Some DFLs use different forensic software, and as a result there is the possibility that the image file may not be opened if the Examiner chooses a unique image file format.

5.1.2.5 Process Flow

The common process for conducting data acquisition is illustrated in the following figure:

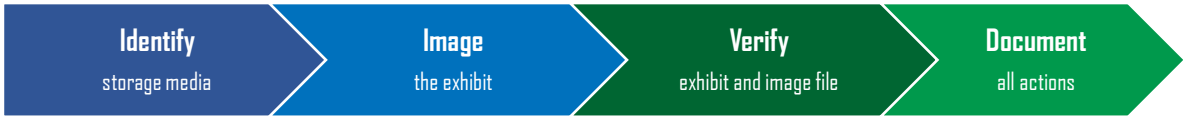


Figure 6. Data Acquisition Process on Computer

The method of conducting data acquisition is described in the following section. A detailed process flow is available at Appendix **G: Acquisition Process Flow Chart**.

A. Identify Storage Media

The Examiner must prepare a compatible storage media, with sufficient data size before handover. If the exhibit is large, the Examiner may need to prepare several storage media to store the image file.

B. Image the Exhibit

To image the exhibit, first connect it to a write-blocker to ensure the exhibit is not writable, thus protecting its integrity. Most forensic tools offer this feature.

The image file is then stored in the prepared storage media. To protect the storage media and the image file, use a standard labelling format by hashing all the evidence acquired with SHA256.

The Examiner needs to note that using an available write-blocking technique does not prevent changes to data on a solid-state drive or flash-media, which includes a controller chip. As soon as the controller is attached to a power supply it will start to reorganize data on the flash chips. Tasks like wear-levelling, write-amplification, and garbage collection are carried out by the controller even when it is attached to a write-blocking device. At this point in time, there is only a resource-intensive way to create a true forensic copy of the flash-media. This is done by unsoldering the chip(s) from the circuit board and then reassembling the data in the correct way where possible.

C. Verify Exhibit and Image File

After the image file has been created, the Examiner needs to check that it is able to run using forensic software, and that the hash values of both the exhibit and the image file are matched.

D. Document All Actions

The last step in examining and analysing the computer is to document the process, the tools used, the hash values, date and time, as well as the Examiner's initials in the case notes. A sample of case notes or worksheets is available at Appendix **F: Data Acquisition Worksheet.**

5.1.3 Mobile Devices

The following gives details of data extraction on mobile devices.

5.1.3.1 Types of Data Extraction

Before starting the DF work, the Examiner must review the case paperwork obtained from the Requester in order to ascertain the types of data required from the exhibit. This can assist the

Examiner in deciding the best extraction method for the case. An attempt should be made to gather all passcodes, passwords or patterns of the exhibit, prior to conducting the work. Using the manual method, for example, requires the phone to be unlocked. Almost all extraction methods require phones to be unlocked. It is therefore always a good practice to try to obtain the unlock code at the time of seizure.

There are five different levels of data extraction for mobile devices, which are described from the level where most data can be extracted to the level where the least can be extracted. Regardless of the method used, after the information has been extracted from the device (with the SIM and MicroSD inserted) the SIM card and Micro SD must be analysed separately.

A. Physical Extraction

A physical extraction is the acquisition of raw binary data from the media storage of the device. These raw data then need to be analysed and processed at a later stage by forensic software. This method typically allows the Examiner to access live and deleted data, operating system files and areas of the device that are not normally accessible to the user.

B. File System Dump (FSD)

The File System Dump (FSD) is a hybrid of Physical Extraction and Logical Extraction. FSD retrieves the device's file system and interprets the data during the processing stage. This allows the Examiner to retrieve, for example, databases holding deleted messages that may not be available at a logical extraction and may not be accessible during a physical extraction. However, a limitation of FSD is that it does not retrieve all deleted data the way a physical extraction is able to do.

C. Logical Extraction

Logical extraction involves receiving information from the mobile device and allowing the device to present the data for analysis. This is often the equivalent of accessing the data on the device itself. This method makes only live data available to the Examiner. Most mobile device forensic software offers this type of feature.

D. Manual

A limitation of forensic software is that sometimes it does not support the model of certain unique mobile devices, or recently launched models. In this case, it is commonly acceptable for the Examiner to use the manual method. This method accesses the device and records of the data displayed on the screen with photographs or video, or by transcribing its data. For

Android devices, the Examiner may consider doing screen captures using software tools. This method might require the phone to be connected via ADB command with developer mode enabled.

E. JTAG / Chip-Off / Rooting / Jail Breaking

For mobile devices that are damaged or locked with a password, JTAG and Chip-Off methods can be used to extract the data. JTAG extraction requires the stripping down of the device to its logical board, and soldering the certain cable to a certain connection on the board. This requires high technical skill. Using this method, the Examiner should be able to retrieve raw binary data from the media storage of the device.

Chip-Off also allows the extraction of raw binary data from the device's storage, but it requires the permanent removal of the device's memory chip from the memory board. When the Examiner conducts Chip-Off, the device will be damaged and can no longer be used. On top of that, expectations on the use of chip-off for mobile devices must be moderated. Recent devices store encrypted data on their memory chip. Devices operating on Android version 7.0 onwards are encrypted by default. Chip-off will still remain viable for other IOT devices which usually store data in clear text.

Another, less destructive, method that can be used with some mobile devices is "**Rooting" or "Jail Breaking**". This process involves leveraging features of the operating system to elevate the permissions and privileges of the running user (similar to the process of gaining "Root" access in a Linux computer). **This process cannot be considered as a forensic technique** as it involves the modification of system files, and can potentially damage the device and so should be low on the list of techniques used.

The order of attempted extractions is important. Examiners should strive to conduct the examination method that is least destructive but yields the most data. This allows examiners to capture areas that might be damaged or overwritten at later stages. Methods of extraction such as JTAG and Chip-Off should only be considered as a last resort, especially with Chip-Off, as the process can be destructive and unrecoverable.

5.1.3.2 Extraction Tool

Analysis of mobile devices typically requires the use of dedicated software, power cable and data cable. More advanced examination techniques, such as JTAG or Chip-Off, require further tools. These include soldering equipment and specialist jigs to read raw data from the device's memory chips.

5.1.3.3 Extraction File Format

Due to the requirement to use dedicated tools to extract data, mobile phone data are often extracted in a proprietary format. These formats can often be transferred between different tools to leverage the strengths of different decoding abilities. Other non-proprietary formats include bin files and raw files.

5.1.3.4 Process Flow

Figure 7. Data Extraction Process on Mobile Devices

A. Identify the Exhibit and Storage Media

The Examiner observes the exhibit at hand, before proceeding to the next process. The exhibit's label should be affixed on the inside of the mobile device, or printed on the back of it. The label must include International Mobile Equipment Identity Number (IMEI), a Mobile Equipment Identifier (MEID) or Serial Number. These data uniquely identify the device and are used to submit the request for billing records or to conduct cell site analysis in the later stages of the investigation. The make, model and IMEI/MEID, can also be used to determine the level of support from the forensic software.

Next, a storage media should be prepared to store the extracted data. If a cloned SIM card is required, a clean, empty SIM card should be prepared.

B. Isolate Exhibit from Network

When conducting mobile device extraction, the device needs to be switched on. To prevent any attempt to connect to a network and subsequently risk changes to any data, the exhibit needs to be isolated from a network. In some countries, some public networks are available everywhere and evidence must be configured to connect them by default.

Depending on budget, isolation can be achieved through different forms such:

Method to isolate networks	
Cloned SIM/IDEN card	A SIM/IDEN card appears in the exhibit as the original card but lacks the capability to connect to the mobile network. A SIM/IDEN card identifies the subscriber and makes a connection to the network. Some forensic tools offer the function of cloning the SIM/IDEN card. Latest mobile phones could be powered without SIM card, and there is no impact on the store data within the phone
Network shielded room	A laboratory installed with Faraday shielding to prevent network signals. However this is a very expensive solution and the use of smaller Faraday boxes can be considered as an effective alternative. If this is not available, proper containers such as Faraday bags or boxes can be used.
Wireless jamming equipment	This equipment blocks incoming network signals. In some jurisdictions, it is illegal to use this, as stated in Section 3.2.2
Manual method	This is the cheapest easily configured method. However, it needs the Examiner to access the exhibit. This poses some risk of changing the data. It is conducted by setting the mobile device to 'Flight Mode' and disabling the WiFi, Bluetooth, and any other network connections.

Table 7. Method to isolate networks

C. Extract Relevant Data

Due to some specific extraction techniques, such as iOS Boot loader extractions and rooting of Android devices, it is not always possible to implement write-blocking to a mobile device. Where possible, write-blocking should be implemented, for example on memory cards. However, it is widely acknowledged that the write-blocking method is not always possible or practical for mobile devices. For this reason, it is imperative that the examiner is fully aware of the consequences of their actions when handling mobile devices and is able to explain and justify these actions.

Mobile devices are presented with three distinct media that require separate handling techniques, as in the following table:

Media	Description
SIM/IDEN card	Requires mobile device forensic tools. Method to extract data is logical extraction. Physical extraction is not possible for this device. It is best that the SIM/IDEN card be removed from the exhibit during the DF work. However, some devices require the card to be inside the devices when they are switched on. The Examiner may produce a cloned SIM/IDEN card to overcome this.
Memory Cards	These can be examined as a computer hard disk. Both logical and physical extraction can be conducted on these cards, as long as the forensic tools support this feature. The Examiner has to the card, extract the data, and then put it back into the device before switching it on. Some devices store data in the memory card, and if it detects that the card is not available, it could cause data loss from the mobile device. If time and resources allow, a bit-to-bit clone of the memory card should be created and that clone inserted into the handset.
Internal Memory	This requires mobile device forensic tools. Some devices are supported by forensic tools for a boot loader physical extraction. This can often be carried out without a SIM/IDEN card. The forensic tools will boot the device in a particular way and conduct physical extraction without making any changes or alterations to the user data on the device. This method can potentially recover device lock codes, which allow the Examiner to gain full access to the exhibit, once it is switched on.

Table 8. Mobile Device Storage Media

The extraction process will vary depending on the extraction tool chosen. Most forensic tools have a guide explaining the procedure that must be followed for a successful extraction. In some cases, examining and analysing the mobile device requires modification to the system files or the operating system in order to extract the data. To some extent, it is necessary to upload or install applications to the mobile device. This process can cause some data to be irrecoverably lost, however it affects only the system files with little evidential value. Knowledge of what is altered by any of these processes can be gained by holding appropriate training certifications, such as training provided by the manufacturers of mobile forensics software, or practical experience involving the testing of mobile device extraction.

Another good source for forensic evidence is the mobile device's backup file. Some users and devices will create backups on other devices, such as in the computer or in the cloud. These backups can assist in building a timeline of evidence and can also be used to gain access to a passcode-locked device. It is also possible to analyse some backups as if they were a physical device.

D. Verify the Exhibit and the Extracted Data

Once the data have been extracted, the Examiner must verify the data against the displayed data on the exhibit. Information such as date and time must be cross checked by the Examiner, as sometimes it is converted to another date/time format during the extraction process.

E. Document All Actions

The last step in examining and analysing a mobile device is to document the process, the tools used, date and time and the Examiner's initials in the case notes.

5.2 Examination

5.2.1 General

Examination of original evidence should be avoided, where possible. The Examiner must always work on the forensic copy (image file) of the evidence. If this is inevitable, access to the data must be protected using a write blocker.

In certain cases, Examiners need to use an isolated environment or pre-set environment to conduct the examination. For example, conducting the simulation on a database system or gaming software. To achieve this, Examiners may use virtualization technology and encapsulate the case in a working container. When the examination is complete, the Examiner may revert the workstation to its previous state using a known image, or using a feature offered by the operating system.

5.2.2 Triage

Triage is the process of prioritizing cases, exhibits or data for analysis processes, according to their relevance to the case. Based on the result of triage, cases, exhibits or data will be analysed depending on their priority sequence from the most important to the least important. It is possible that some may not be analysed at all due to irrelevance to the case being investigated.

Triage is conducted in order to address situations such as:

- A huge amount of exhibits or mass data needs to be analysed in a short time frame;
- Exhibits cannot be stored any longer due to legal issues;
- It is a high priority case and results need to be produced immediately, i.e. in a case in which bodily harm or death is possible.

While triaging offers some advantages there are also disadvantages that need to be addressed. A triage cannot replace a full examination. Triage is conducted using automated processing, this is offered by forensic software or by running self-written codes to the exhibits or data. There is a risk that this automated processing only examines subsets of data, and some important data might be left out. This risk needs to be explained to the investigator, prosecutor or judge and based on that information they may need to decide in favour of or against the triaging process for that particular

case. However, triage remains a valid method to cope with a situation that could not be solved in any other way.

There is lots of software on the market that offers triage functions, some are commercial and some are open source. Triage can be conducted by running the software while the exhibit is still live or by booting up the exhibit using forensic bootable media. The Examiner then inputs keywords and lets the system run, before selecting relevant files and storing them in removable storage media. By doing this, multiple exhibits can be processed at the same time, even overnight or during weekends.

After triage has been conducted and the Examiner decides that the exhibit is relevant to the investigation, the Examiner can then proceed to the next process described in this document, and use more sophisticated methods to gather more data from the computer.

5.2.3 Methods for Computer Examination

There are many methods and techniques to examine a computer. Some require in-depth skill while others require minimal skill, such as conducting an automated process. A number of forensic softwares can be used by the Examiner. Depending on software capability, some are able to recover passwords, correlate data between electronic evidence, and conduct keyword searches.

The process flow for conducting an examination on a computer is available at Appendix **H: Computer Examination Flow Chart**. The flow chart is explained in the following section.

5.2.3.1 Examination on "Dead System"

A "dead system" is a system that is not running, turned off with no power. When the system is "dead", volatile data in temporary storage areas such as RAM memory, running processes, cache or active application dialogues on a computer will no longer be available.

Examination of a "dead system" must consider the following data:

- Active files, deleted files, file slack, partition slack, disk slack, and shadow files
- Device artefacts – operating system files, file registry, file metadata, encrypted files, log files and database files
- Browsing history, e-mail, social media, and peer-to-peer file sharing

5.2.3.2 Examination on "Live System"

A "Live system" is a system that is up and running, where applications may be running and can be updated as data are continuously being processed.

Because of the valuable evidence that could be discovered in a live system, switching it off may cause loss of volatile data such as data stored on the cloud, encrypted data, running processes, network connections and mounted file systems.

Examination of a live system should consider the following data:

- Random Access Memory(RAM)
- Running processes
- Network connections
- System settings
- Storage media
- Cloud services

Depending on the case request, examination of a live system may be conducted on any of the above data.

5.2.3.3 Automated Processing

Automated processing is often conducted using the readily-available features on forensic software. The scope of automated processing is usually set by the Examiner at the beginning of the examination. This scope can be repeated for other cases within a similar scope of investigation. An example is running a hash comparison on images in a child pornography case. The common activities and sequences for automated processing are:

i. Extraction of operating system and users data
ii. Mount containers such as ZIP, RAR, and encrypted containers.
iii. Extract and parse artefacts such as mailboxes and Internet history
iv. Signature analysis
v. Recover deleted files and folders
vi. Recover deleted partitions
vii. Carve certain file types
viii. Depending on case request, these analysis methods may be used:
    - Keyword search
    - Optical Character Recognition (OCR) of PDF files
    - Create pictures thumbnail for easy viewing
    - Extract pictures from videos
    - Skin-tone detection for videos
    - Hash comparison
ix. Processing operating system logs (e.g. windows event log, windows journal)

This step saves time as it can run over-night or over the weekend with minimal supervision, although it uses high computing power.

5.2.3.4 Data Recovery

Data recovery involves the recovering data on storage media that have been deleted, damaged, hidden or lost. In some cases, the storage media is damaged, corrupted or formatted, causing data to be inaccessible. Data recovery therefore also involves the process of fixing the storage media so that data can be extracted from the media.

There are two types of data recovery - logical recovery and physical recovery.

Logical recovery is conducted when storage media are accessible, but the data are formatted, corrupted, hidden or lost. The recovery process is usually conducted using forensic software.

Physical recovery is conducted when the storage media are inaccessible due to mechanical failure or electronic failure. The recovery process is fairly tedious and requires some advanced skill. In some cases, a special room is needed to conduct the physical recovery, for example replacing a head in a hard disk requires it to be conducted in a class 100 room. In other cases, special equipment is needed to recover the data. For example, a soldering machine is required when replacing a cable in a USB thumb drive.

Not all DFLs can afford to have a physical recovery facility since the cost is high and a highly-skilled Examiner is required to perform the tasks. Nevertheless, having a logical recovery facility is sufficient for the DFL. Most forensic analysis software comes together with a logical recovery feature, so the Examiner can make use of or upgrade to the offered feature to save on costs.

5.2.3.5 Filtering

Applying filters to an image file before it is analysed can help to reduce the amount of data that the Examiner has to view and analyse. Popular filtering techniques use hash sets to either filter out known operating systems or program files (whitelisting) or to specifically search for hash matches within the databases of known illegal materials (blacklisting).

Filtering can also be applied when only certain types of findings are relevant to the case. Files can be filtered by signature analysis - by size, date, owner and many more details located within the meta-data. This filtering feature is offered in most commercial forensic software.

5.2.4 Methods for Mobile Device Examination

Mobile devices pose a unique challenge to the Examiner as the diversity of operating systems, the innumerable brands and models, the abundance of data and the diversity of data types stored in the device is overwhelming.

The following describes common general methods conducted on mobile devices.

5.2.4.1 Automated Processing

The processing of mobile devices often requires a different approach to computers due to the greatly varying hardware and software used between devices. Applications are updated with a

much greater frequency, and changes can often be major. For this reason, dedicated forensic tools will automatically process much of the data, however manual verification of this processing is often necessary. A number of available tools use a form of "fuzzy processing", that is to say, the processing is implemented in such a way as to leverage logic and loose matches.

5.2.4.2 Filtering

Filtering of mobile data is typically performed on a data type level. Data is filtered by tools during processing into groups such as communication data and media files. These groups are then further divided; for example communication data can be divided into call records and messages. The level of filtering presented to the analyst depends on the tool being used, however, this filtering allows analysts to quickly review key data types. These can include sent and received SMS messages and call records to establish contact between suspects.

5.3 Analysis

During the analysis phase, the Examiner searches for electronic evidence on the images. This can be very time consuming and can require a lot of expert knowledge to interpret traces from a variety of file systems, operating systems, and applications. Many different factors have an influence on the time and workload that is needed for the analysis phase. These factors include the amount of storage media to be analysed, the size of the storage media, the complexity of the file systems being used, the level of use of the operating system, the sophistication of the user, complexity of software and techniques being used by the computer user, etc.

5.3.1 Analysing Computer

5.3.1.1 Categories of digital traces

"Computer can be configured not to store certain artefacts i.e. browsing history, log files and download history"

Just as a criminal leaves physical traces behind at a crime scene, the criminal that commits a crime by computer will leave traces at a "digital crime scene". Some of these traces are discoverable, some of them can be configured to not be discoverable by the Examiner.

The following table lists some examples for discoverable traces and configurations to avoid discoverable traces.

Traces that are discoverable	Traces configured to be undiscoverable
Artefacts that are stored on the computer by default. The probability of finding such traces is high, even if a suspect tries to cover his or her tracks.	Artefacts that can be configured not to be stored on the computer. For example, a web browser where the user can disable or delete download history.

Some of the discoverable traces:	Some of the undiscoverable traces:
• Slack space • Unallocated space • MFT entries • RAM	• Thumb caches • Most recently used lists • Log files • Browser histories • Browser caches • Most used programs • Form data • Pagefile.sys • Hiberfil.sys • Volume shadow copies • Download history

Table 9. Discoverable and undiscoverable traces from a computer

5.3.1.2 Procedures for different traces

Data and information that need to be extracted from a computer depends on the type of case. For example in a fraud-related case, data/information typically extracted from the computer is in the form of spreadsheets, e-mails and office documents. In a child-abuse case, the possible related data/information may be pictures, videos and communication messages.

The process of analysing various kinds of artefacts is illustrated at **Appendix I: Process of Analysing Exhibit's Artefacts.** The following sections explain in detail the types of data that can be extracted from a computer.

A. E-mails

Analysis of e-mails, which typically involve the mail clients such as Outlook, Thunderbird, and Mail as well as webmail accounts. Different mail clients will produce different types of artefacts. Outlook, for example, stores evidential data in personal folder files such as PST, OST, and PAB files. Thunderbird stores messages in inbox files. Usually, forensic software is capable of parsing these files, however they do not necessarily extract all messages. Some forensic software cannot retrieve deleted messages from personal folder files, so the data recovery method may be needed in this case.

B. Office Documents (Word Processor, Spreadsheet, presentation)

Analysis of office documents typically starts with file signature analysis and is followed by filtering the files of interest. File signature analysis compares the file header with its extension to ensure it is matched. If it does not match, there may be a possibility that the document header or extension is being modified to hide the content. Filtering files involves using a keyword search. Most forensic software is able to perform both tasks automatically.

Once the Examiner has discovered related documents, it is good to refer to the Requester for content analysis. This is to ensure that the extracted document is indeed related to the case being investigated. When the Requester has confirmed the documents, the Examiner can conduct further analysis on the document, document metadata, document maker, and identify whether it has been sent or received on the computer.

C. Pictures and Videos

To conduct analysis on pictures and videos, the Examiner first needs to have a clear idea from the Requester of what to look for. If it involves searching for identical photos, then the

Requester needs to supply the Examiner with the necessary photos. If it involves files with known hashes, then the Requester may need to supply the Examiner with the hashes, or the Examiner can use a list of hashes from known databases. If it involves a certain portion of a video, then the Requester needs to state its unique features. For example, to extract all pictures from the video that has a motorcycle.

Analysis of pictures typically starts with signature analysis. Next, the Examiner may sift through pictures in the gallery by using the thumbnail view.

If the case requires searching for a set of known pictures - for example in a child abuse case or stolen blueprints - a hash comparison can be used to accomplish this task. Some forensic software offers a feature of similar picture detection, The Examiner can use this feature by supplying the necessary picture to the software.

For video analysis, some software offers the feature of extracting still pictures from the videos. For example Y pictures, in every X second/minute. These extracted pictures can then also be viewed in a gallery view. This allows for the much more efficient previewing of video files.

In cases where location or production details of pictures and video files are important, the Examiner should consider extracting the metadata of those files. Metadata are sets of data that describe and give information about other data, for example GPS coordinates where the picture was taken, creation date and time as well as the device used to capture the picture.

Some exhibits may have thousands of photos and videos, and it is impossible for the Examiner to sift through and locate one specific video or pictures files. The best way of doing this is by extracting all pictures and then passing them to the Requester.

The simple task of viewing the contents of the pictures/videos does not require any digital forensic expertise and could therefore be carried out by the Requester. When the relevant photos/videos have been identified, further analysis can be conducted by the Examiner to extract more meaningful data, such as GPS coordinates and creation or modification data.

D. Internet Browser

Internet browsers are of evidential value in many cases. They typically contain the following artefacts:

- Website visit history
- Local cache / temporary internet files
- Bookmarks/favourites
- Sessions information
- Cookies
- Saved usernames and passwords
- Entries from form fields
- Internet keyword searches

Analysing browser artefacts can be important for suggesting purpose or intent, an example is the keywords used in search engines which could prove intent.

Popular browsers include Google Chrome, Microsoft Internet Explorer / Edge, Mozilla Firefox and Apple Safari. All of them store data within the user's home directory. With the exception

of the Microsoft browsers, all other browsers use SQLite databases to store the artefacts mentioned above.

Most internet analysis forensic software offers browser parsing. However, due to evolving technology where some browsers are frequently being updated, some forensic software may take some time to update its database. Therefore it is important for Examiners to understand the underlying structure of internet browsers. Since most browsers today work on SQLite databases, the Examiner may consider parsing the artefact manually by using SQLite database browsers, which can be downloaded for free.

This not only allows Examiners to be independent of a particular software, but also allows them to cross-check the results of the software against the SQLite database browsers.

E. Software

Whenever certain software needs to be analysed, most of the time it has to involve the extraction and understanding of the software artefacts. Examples of such software include communication software (e.g. Whatsapp and Skype), steganography software (e.g. OpenStego), password safes (e.g. KeePass), file sharing software (e.g. uTorrent) and crypto currency software (e.g. Cryptocurrency wallets).

Although there are no standard procedures for how to analyse all software artefacts due to their diversity, it is commonly done by conducting information gathering on reliable and trusted sources on the software artefacts. The findings can then be verified by conducting a simulation.

F. User Activity

The computer operating system tracks user activity at many different places. Examples include:

- power on and shutdown times
- software settings
- most recently used files lists
- device use
- user logins
- Wi-Fi connections
- preferred programs
- setup of user environment
- frequently accessed files

Analysing this user activity helps to get a better understanding of the user's behaviour and can even prove evidential activities. Depending on the operating system, the artefacts are stored in various locations. In Microsoft Windows, most of the artefacts are stored in the Registry, Event Logs and Jump Lists.

On OS X systems the artefacts are stored in the Library and log folders, while on Linux systems, most of the data will be stored in the user home folder, or the "/etc" or "/var" directories.

G. Log Files

Analysing log files is essential, particularly in cases of attacks against systems. The Examiner should extract not only the allocated log files but also traces of deleted/unallocated log files. Specialized software is available for log file analysis. The basis of such an analysis is to either

search for particular keywords, abnormal patterns or to search the logs that fall within a set time frame.

H. Encryption

Most common operating systems today offer built-in encryption facilities. It is easy for the user to activate full disk encryption for a system drive. It is recommended that the passwords or encryption keys are gathered at the crime scene using live data forensics before the exhibit is delivered to a DFL.

It can also be helpful to extract other passwords (e.g. browser passwords) from the disk where possible. These passwords and their permutations can be used to create a dictionary to conduct an attack using specialized password cracking techniques.

In addition, traditional law enforcement activities such as gathering physical evidence, including written passphrases, keys, or recovery strings should be conducted in an attempt to find passcodes.

I. Unallocated Space

Unallocated areas can contain artefacts of all of the types of evidence mentioned above. Searching and extracting certain file types in unallocated areas can be automated by using carving software. The Examiner should specify what kind of files they are searching for because data carving is a very time consuming task. Data carving does not work well on fragmented files. Most of the time data found in unallocated areas cannot be an associated with a certain user, time stamps, or even a location within a folder structure.

J. Cloud and Remote Storage

When an Examiner discovers traces of cloud services in a computer, it could indicate either of the following:

- Data is stored locally on the computer and remotely on the cloud; or
- Data is stored fully on the cloud. The computer may not contain any data at all.

In fact, the data that are stored remotely may not just be stored on a single server, but can be stored on multiple servers in the cloud. Most of the time, even the provider of a cloud service cannot tell on which particular server, data-centre or in which country certain parts of the data are stored.

The Examiner may even find situations where not a single byte of data can be retrieved from a company's computers because they are merely client computers without any storage media, but using the resources of a virtual machine in the cloud.

Although technically it is easy to make a forensic copy of the virtual machine which resides in the cloud, there are some legal matters that need to be considered. Depending on the applicable legislation, identifying and obtaining the appropriate legal authorization for intercepting such data may pose an issue. It may also be challenging to ensure that the data have been acquired in compliance with the legal procedures in the requesting country.

Another disadvantage is that there is likely to be far less recoverable data to be extracted. Indeed, if a suspect created a temporary virtual machine to commit his or her crimes and then deleted that machine, there may be no evidence at all to recover.

The possibility of acquiring and analysing remotely stored data is dependent on the legislation and jurisdiction. In some jurisdictions, for example, under certain circumstances the Examiner is allowed to connect to the remote storage using the suspect's credentials from the computer in order to acquire the data. Other jurisdictions may not accept such an acquisition. In these cases, official channels can be used to request preservation and access to the data from the provider.

K. Computer Memory (RAM)

When the computer memory has been acquired while the seized computer was still running, the memory dump can be analysed in the DFL.

Understanding memory structures of different operating systems in order to analyse the memory dump requires very high and technical skills, so only a qualified Examiner should do the work. Special software is required to analyse the memory dump. Examples of this are Volatility and Rekall, which are publicly available on the Internet for free.

Typical artefacts that can be extracted from memory dumps include:

- Running processes, including their memory
- Process information (e.g. handles)
- Encryption keys
- Opened files
- Usernames, passwords
- Unsaved documents

5.3.1.3 Virtualization

A picture is worth a thousand words - this is particularly true for virtualization. Using virtualization, the Examiner can view the operating system environment of an exhibit the same way as the suspect has seen it. Finding evidence from within a virtual machine can sometimes be faster and more expressive than reassembling traces of data from the image file. An example is viewing counterfeit gaming software.

When mounting an image, it should be mounted with write-protected or read only parameters with a write cache, allowing the virtual operating system to write log files, without affecting the integrity of the image file.

Some operating systems refuse to start in virtual environments. This can typically be solved by replacing some drivers and by configuring the system settings, using software like OpenGates and OpenJobs. If the virtual operating system starts with a password prompt, the Examiner needs to either crack the password or remove it.

5.3.1.4 Process for handling mass data

Some cases involve lots of computers with masses of data. To execute the forensic task, a strategy needs to be implemented in order to expedite the work. One way to do this is to separate the forensic analysis task from the content analysis task. The Examiners concentrate on the forensic analysis tasks such as recovering, parsing, mounting and processing of exhibits, while the Investigators with case specific knowledge do the content analysis.

The proper processes for handling and viewing extracted files may need to be developed and implemented between the Examiners and the Investigators to ensure smooth operation.

Another method for processing mass data is by conducting triage. Triage is explained in section 5.2.2 in this document.

5.3.1.5 Visualization aids

To aid the understanding of complex data and flows, visualization aids can be useful. Some examples of such aids are:

Methods for visual aids	
Timelines	These can be used to display user behaviour; when the suspect logged in, when he connected to a certain medium, when he connected to a certain wireless router and when he viewed a particular website.
Relationship diagrams	These can give answers to questions such as: Who has met with whom; at which point in time; using which medium? What information was sent/received? Who knows whom? Who is the main suspect that coordinated others?
Money flow diagrams	These can help to understand at which point in time an amount of money has been sent, over which channel, and by which individuals.
Communication diagrams	Similar to a relationship diagram, but these do not necessarily involve persons. They could show how often certain IP addresses attack certain servers from different countries.

Table 10. Method for Visual Aids

Graphical representations make it easier to understand the correlation between the data. They can also enable the investigator to find new relationships not previously noted. Typically the basis for such diagrams is raw data stored in a structured way, for example in CSV, TSV or XML format. These files are loaded into analytical software.

On Linux, for example, simple commands like awk, sort, and uniq used in conjunction with Graphviz or dot, can help to draw graphical representations.

5.3.2 Analysing Mobile Devices

Mobile devices contain records and logs of communications, along with times and dates of particular communications. In addition to this, mobile devices may also contain media files and GPS locations.

5.3.2.1 Categories of digital traces

Digital traces found on mobile devices can be split into three distinctive groups: communication data, media files, and other data. Communication data can include call records, SMS messages, and other messaging service messages. Media files, as with computers, can contain information beyond what is depicted by the file. Metadata on media files captured in a mobile phone, for example, are likely to contain geo-tags or other useful location and identification data embedded within the file itself.

5.3.2.2 Procedures for different traces

The following sections explain the types of data that can be extracted from a mobile device.

A. Call history

The call history provides insight into the call activity of the owner before the acquisition of the Smartphone device. The investigator can see incoming, outgoing and missed calls including the time and duration. This can help the forensics investigator to draw an indirect conclusion about the suspected activities, therefore assist the DFL in speeding up the analysis process by providing a concise and clear case request.

B. Contact list

The contact list not only provides contact names, but potentially also the home number, mobile number, and work number. Other types of information such as contact title, company, address, and associated e-mails can also be extracted from the contact list. Some smartphone devices store a picture of the contact in the contact list, which can assist in identifying a certain individual. The information stored in the contact list provides the investigator with the social and work relations of the owner of the Smartphone device. Besides this, many people store different types of account information and the passwords in the contact list.

C. Text messages and E-mails

Unlike the call history and contact list, which provide indirect information, text messages and e-mails give explicit information that can be used as evidence in court. This is because they contain the exact text intended/sent and received by the user of the device.

D. Media File (Pictures, videos, audio)

Media files such as pictures, videos and audio files can be used as potential digital evidence in court. Many smartphone devices such as iPhones embed GPS coordinates of the location into the metadata called Exchangeable File Format (EXIF) of the pictures. Other information embedded in the EXIF data can include the brand of smartphone, date and time in which pictures were taken, as well as the software that is used to modify the picture, if any. This provides the investigator with more insight into the activities of the owner of the smartphone.

E. Internet browsing history and keyword search

The Internet browsing history and keyword searches made in the smartphone device provide the investigator with a general understanding of the Internet activities of the owner. The investigator will discover the types of websites that the owner has visited and to some extent the user's favourite sites.

F. Chat logs and Messaging Apps

There are several available chat applications and messaging apps. Example include Whatsapp, Telegram, Skype, Line, Weebo, WeChat, QQ, Windows Live Messenger, Google Talk, and BlackBerry Messenger. Users of these applications usually choose to save the chat logs. The chat logs can be used as digital evidence in court as to what the owner communicated to others. Some chat logs are backed up in the cloud or local storage such as a computer, so analysing the computer may be useful to gain more data.

Messaging apps can also offer VoIP (Voice over IP) service. This enables the owner of the smartphone to communicate with many people using the IP protocol, without leaving a record in the call history of the device. The suspect may use this software to communicate

with a criminal or a victim. For example, in child abuse cases, the criminal may communicate with the child using these messaging apps.

G. Social network accounts

Social network accounts, such as Instagram, Facebook, Twitter and Tumblr store user credentials in the device itself. By storing the credentials locally, users do not have to log in each time they want to visit these sites. These credentials are valuable to the Examiner, as they can be used to gain access to suspect's social media account, enabling data to be extracted from the device.

A lot of data is stored in social media accounts, contact lists, messages between individuals and groups, pictures, videos, user activity – the list is endless. The Examiner needs to be supplied with a clear case request in order to extract the correct data and present analysis results completely and concisely in forensics reports.

H. Calendar and Notes

The calendar gives a picture of the previous, current and future planned activities of the owner of the smartphone. The calendar can be used to associate the owner of the smartphone with specific locations and times in order to look for possible witnesses. The owner of the Smartphone may also have saved notes that have valuable information that can be presented as evidence in court.

I. Connections (Mobile network, Wi-Fi, Bluetooth)

These will give the investigator an overview of the networking activities that were performed by the owner's smartphone device. The mobile network will give a picture of which country or region the owner has roamed in. Wi-Fi will give a picture of which Local Area Network (LAN) the smartphone has connected to. Bluetooth connections will give the Investigator information about the nicknames of the devices that were connected with the owner of the smartphone.

J. Maps (locations, directions help, favorites)

This will provide the Investigator with a geographical view of the owner's movements, which can be used as potential evidence in court. GPS coordinates of the user's movements can also be captured and analysed, such as in the case where applications that provide directions are used. These include, Google Maps, Bings Maps, and Apple Maps.

K. Software (Document processing, PDF, etc.)

Most smartphones offer the feature of creating and editing documents. Document processing software, such as Word To Go and Sheet To Go, may contain potential evidence related to the case.

5.4 Presentation

The Presentation phase requires putting together findings in a presentable and understandable way for stakeholders. When the analysis phase is completed, the Examiner needs to put the findings and results in a forensic report. The Examiner should illustrate and translate complicated technical contexts into facts that judges, prosecutors and other parties involved can easily understand. They may also be expected to interpret those facts, and to express an opinion on their meaning. In some cases when a large number of exhibits are analysed, it will be difficult for the examiner to present the outcome to the investigation team. It is recommended to adopt an analytic software, to facilitate matching digital evidence with other data from the investigations. This kind of tools can also be used to index and search all the exhibits, providing the investigation team with a global overview of the case

5.4.1 Admissibility of Electronic Evidence

The criteria for the admissibility of electronic evidence may differ from jurisdiction to jurisdiction. Generally, the Examiner should consider the following criteria when evaluating electronic evidence for trial:

General Criteria for the Admissibility of Electronic Evidence	
Authenticity	The evidence must establish facts in a way that cannot be disputed and be representative of its original state.
Completeness	The analysis of, or any opinion based on, the evidence must tell the whole story and not be tailored to match a more favourable or desired perspective.
Reliability	There must be nothing about the way in which the evidence was collected and subsequently handled that may cast doubt on its authenticity or veracity.
Convincing	The evidence must be persuasive as to the facts it represents, and must be able to convince the stakeholder of the truth in court.
Proportionality	The methods used to gather the evidence must be fair and proportionate to the interests of justice: the prejudice (i.e. the level of intrusion or coercion) caused to the rights of any party should not outweigh the probative value of the evidence (i.e. its value as proof).

Table 11. General Criteria for the Admissibility of Electronic Evidence

5.4.2 Report Writing

A forensic report must be written in clear and understandable language. The result must be properly summarized and it must also provide a concise answer to the case request, supplied by the Requester.

It is recommended that all technical details be listed in the appendix section, rather than put in with the main content. This is to facilitate the layman's understanding in reading the report.

The Examiner must also refrain from providing a statement that cannot be proven. For example, "The suspect has altered File A". An appropriate sentence would be "File A found in Computer B has been altered".

A common requirement for a forensic report is available at Appendix **J: Common Requirement for Forensic Report** of this document.

Due to the complexity of the case, sometimes it is difficult for the Examiner to express the findings in the report. The use of visual aids and visual representation such as animation, slides, pictures and live demonstrations are good methods of facilitating understanding.

5.4.3 Expert Witness

In some jurisdictions, a submitted forensic report is sufficient in court, in lieu of the Examiner attending the court session. However, in other jurisdictions, the Examiner is required to attend a court session and present his/her expert testimony related to the case.

An expert witness is a person who, by virtue of education, training, skill, or experience, has an expertise and specialized knowledge beyond that of the average person. The witness's knowledge is sufficient that others may officially and legally rely upon his/her specialized (scientific, technical or other) opinion about evidence or a fact within the scope of his/her expertise, referred to as the expert opinion.

In some jurisdictions, expert status is decided on each and every case by the trial judge and the person is only an expert in that case. In other jurisdictions, expert status is appointed by the legal institution, and the person is responsible for any case within his/her expertise.

The rights and duties of an expert witness differ from country to country. It is important for Examiners to familiarize themselves with their legislation, their court procedures, their role and their rights and duties in that role.

6. QUALITY ASSURANCE

When presenting the forensic report in court, examiners may not only be required to explain the analysis process. They will also be required to explain their proficiency, the equipment they used, the method they chose, the evidence handling method, and much more. It is important that procedures to address the above matters are established and implemented in the DFL.

The following section explains in further detail the components, as well as the accreditation which should be obtained.

6.1 Quality assurance component

The basic quality assurance that can be implemented in a DFL includes, but is not limited to:

Quality Assurance Components Checklist	
Laboratory	a. Create an Organization Chart at DFL level and at the organization level. b. Conduct an internal audit annually. c. Establish a procedure to address internal and external complaints. d. Establish a procedure to control documentation.
Facility and Environmental Condition	a. Establish lab premises – access and exits. b. Create an access list and limit access by using keys, individually assigned identification cards, or biometric devices. c. Monitor the lab environment regularly – temperature, humidity, cleanliness. d. Establish a Health and Safety programme. e. Establish visitor policy. f. Conduct regular housekeeping.
Equipment	a. Establish a procedure for handling, transport, storage, use, repair, disposal and planned maintenance for equipment. b. Before putting into use, ensure that the equipment is working according to specifications. c. Implement the maintenance programme. d. Update the firmware according to requirements. e. Maintain equipment documentation, manuals, and warranties.

Staff	a. Employment Qualifications: • Conduct background screening prior to hiring. • Prepare Job Descriptions for staff once hired - See section 3.3 Staff. b. Professional Development and Training: • Establish a training programme for staff - See section 3.3.4 Staff development. • Send staff for training. • Assign mentors for newly-hired staff. • Evaluate staff's competency by conducting Competency Tests for newly-hired staff. • Evaluate existing staff's proficiency by conducting annual Proficiency Tests. • Participate in external or inter-laboratory Proficiency Tests. • Obtain technical certifications. Establish a Continuous Education Programme for existing staff to maintain skills.
Forensic Method	a. Establish SOPs for conducting DF examinations. b. Keep a document of forensic methods, such as conducting a live acquisition, updated and available to Examiners. c. Conduct verification on methods introduced to ensure the DFL can use them properly. d. Conduct validation when using any method: non-standard method, lab-developed method or standard method used outside its scope. e. For ease of operation, use an internationally-accepted method in DFL, such as SWGDE.
Service Request	Establish and implement a policy and procedure on the service request. This should contain: a. The process for accepting or rejecting the request. b. The process for resubmission of the request. c. The requirement for having a concise request or case objective. d. Formal acknowledgment from the Requester and the Examiner, indicating that both parties agree with the work before the forensic work starts and after it has been delivered – by signing a form, replying to an e-mail or replying to a letter. e. Forms or other methods to be used to document the request. See **Appendix L: INTERPOL DFL Service Request Form** for a sample of the request form.

Evidence Handling	Establish and implement a policy and procedures on evidence handling. This should contain: a. Evidence preservation b. Evidence labelling c. Evidence sealing d. Items to document - including the chain of custody e. Evidence that is left unattended f. Precautions for securing and handling the evidence g. Storage and retention See Appendix K**: Electronic Evidence Handling** for details on evidence handling.
Forensic Result	a. Keep technical records to support the forensic result. The records must indicate the Examiners conducting the process, and the date. Amendments to previous records must be tracked. b. Conduct technical and administrative review of the forensic results. c. Authorize the forensic result before releasing to the Requester. d. Establish a common format for a forensic report. See **Appendix J: Common Requirement for Forensic Report** e. When providing an opinion, it must be clearly marked in the forensic report. f. Establish a process for amending a forensic report.

Table 12. Quality Assurance Components Checklist

6.2 DFL Accreditation

Forensic results impact the jurisdictional system, so they must be correct and reliable. The DFL can assure and demonstrate confidence in its forensic result by joining the accreditation programme. The accreditation body will evaluate the DFL process on an annual basis to ensure it is meeting the global standard.

Although joining the accreditation programme is recommended, in general it is voluntary and not mandatory in most countries. A DFL that is interested in the accreditation programme may refer to its own country's Accreditation Body for details of the process.

Some notable benefits of being accredited are:

Benefits of Lab Accreditation	
1	**Ensure confidence in the forensic result** When a DFL receives numerous cases in a year, it is generally difficult for the laboratory to monitor the performance of the forensic work and of the Examiners. The ISO 17025 standard defines the process of monitoring the quality aspect of the forensic result. With accreditation, this process will be assessed annually to ensure the laboratory continues to maintain its performance. In addition, the process of managing and examining the evidence must follow the international standard, providing confidence to the stakeholder in the forensic result produced by the DFL.

2	**More systematic with standardized processes** A DFL with several Examiners must ensure that each Examiner follows the same set of processes. This is to ensure that testimonies in court are coherent and consistent between each Examiner coming from the same DFL, thus facilitating immediate understanding by the prosecutors, judges and other court staff. Having this accreditation in place ensures that the DFL establishes the necessary standard processes, and also ensures that Examiners implement them.
3	**Produce quality results** One of the requirements in ISO 17025 is to conduct continuous improvements to the lab processes. The DFL can benefit from accreditation by implementing continuous improvements and ensuring the lab produces more quality results. An example of such implementation is court testimony monitoring. Examiners are able to continuously improve their methods of presenting the results in court if they are being monitored and provided with constructive feedback.

Table 13. Benefits of Lab Accreditation

7. SUMMARY

Electronic evidence has posed challenges to the investigation of certain cases, due to its nature, which is unique and different from traditional types of evidence. Therefore, it must be handled with due care. The aim of this document is to provide the standard guidelines for the management of a DFL, and for the examination of electronic evidence. This is to ensure that the electronic evidence and the result produced by INTERPOL member countries is accepted in other jurisdictions.

The Examiner and the management of the DFL must always strive to update methodologies, guidelines, and procedures with current advancements in technology. Only then can we together bring down criminals and serve justice as it should be served.

APPENDIX A: DFL SKILLSET CHECKLIST

The following is a recommendation of skillsets for the DFL Examiner. The reader shall take note that the list is non-exhaustive and needs to be updated from time to time.

Category	Topic	Skillset	
Foundation	Computer Foundation	Organization of computer; How computer stores data; Bits & bytes; Evolution of digital media and storage system.	☐
	File System	Decimal, hexadecimal, binary; Little endian, big endian; Sectors, cluster, slack space; Metadata, data, filename; FAT, NTFS, EXT, HFS.	☐
	Introduction to Investigation and Digital Forensics	Law enforcement and regulators; Introduction to forensic science, electronic evidence and its nature; Categories of electronic evidence; Methodology; Forensics terminologies.	☐
Identification	Information Gathering	Gather facts of the case online; Preserve the gathered facts.	☐
Collection and Examination	Collection and Examination	First responder roles and SOP; Dead acquisition and live acquisition; Choosing the best data acquisition method; Triage method; Triage tool.	☐
Analysis	Data Recovery	Storage technology; Damaged hard disk and flash drive symptoms; Logical and physical recovery; Data recovery tools; Recovery of data using tools.	☐
	Computer Forensics	Operating systems technology; Metadata, registry, artefact; Data Extraction; Data analysis; Data hiding technique; Analytics for large sets of data; Memory Analysis.	☐
	Mobile Phone Forensics	Mobile phone Technology and evolution, User, telecommunication provider technology, types of data, acquire and analysis tools, preservation of data.	☐
	Network Forensics	Network Types; Internet history files and Cookies; User Credentials; Network forensic tools; Reading packets.	☐
	Audio, Video and Image Forensics	Understanding the technology; Enhancement; File Authentication; Comparison.	☐
	Emerging Technology:	Understanding the technology; Accessing data from the device; Data Extraction; Data	☐

	- Social Media Forensic - Database Forensic - Drone Forensic - Vehicle Forensic - Shipbourne forensic - Cryptocurrency Forensic - Biometric Forensic	analysis; Data interpretation; Reporting the findings.	☐
Presentation	Report Writing	The format of the report; Effective result presentation to stakeholders.	☐
	Law & Mock Court	Laws related to cases; International Law; International Collaboration; Presenting expert testimony in court; Introduction to Court structure; Submitting electronic evidence in court.	☐
Etiquette	Etiquette	Professional Code of ethics, ethical & non-ethical code of conduct.	☐
Lab Management	Quality Management	Understanding standards; Conducting Audit; Quality Management System.	☐
	Health & Safety	Identify hazards; Health and Safety measures; Self-protection.	☐

APPENDIX B: CHECKLIST OF BASIC DFL EQUIPMENT

The following is a suggested list of basic equipment that a DFL should own. The reader should note that the list is non-exhaustive and more may be required depending on the nature of cases received.

No	Item	
1	Laptop	☐
2	Computer analysis software	☐
3	Data recovery software	☐
4	Mobile device analysis software	☐
5	Internet artefacts analysis software	☐
6	Virtual machine software	☐
c	Imaging Hardware	☐
8	Docking System	☐
9	Write blocker	☐
10	Empty storage media – to store data extracted from electronic evidence in the short and long term: • Pen drive • External hard disk • Hard disk • Server	☐
11	PC toolkit	☐
12	Power cable extension	☐
13	Printer	☐
14	Document shredder	☐

APPENDIX C: SAMPLE OF CASE REGISTRATION FORM

Requesting Agency Information	
Name:	Department/Unit:
Job Title:	Agency:
Tel Number:	Requestor Case Number:
Email:	DFL Case Number: fill in by DFL

Case Information
Case Background: Describe the background of the case that may help DFL with the analysis
Case Specific Request: List all keywords or analysis scope here

Terms and Conditions
1 Selection of Method: DFL shall select the best available method to conduct digital forensics analysis.
2 Statement of Confidential: DFL ensures that any information supplied by Requestor and any information gathered from the work performed will be treated with STRICTEST CONFIDENCE.
3 Damage or Loss of Profit: DFL shall not be held liable for any damaged exhibit or loss of profit caused by the Requestor in connection to the work performed. DFL,however, shall take reasonable precautions, care and steps in preserving the integrity of evidence at all times.
4 Abandoned or Unclaim Exhibit: Exhibit unclaimed or abandoned at DFL's location in excess of 30 days after communication has been made with the Requestor will be disposed of at DFL's discretion. DFL will not be responsible for exhibit left in its possession beyond 30 days. DFL, however,will inform the Requestor prior to disposing the exhibit.

Requestor	DFL
I have read, understood and agreed to the Terms and Conditions. Sign here Date :	Sign here Name: Date :

APPENDIX D: SAMPLE OF EXHIBIT REGISTRATION FORM

Section A: Exhibit Receive

No	DFL Exhibit Label	Manufacturer	Capacity	Description Include any defects of the item here	Serial Number

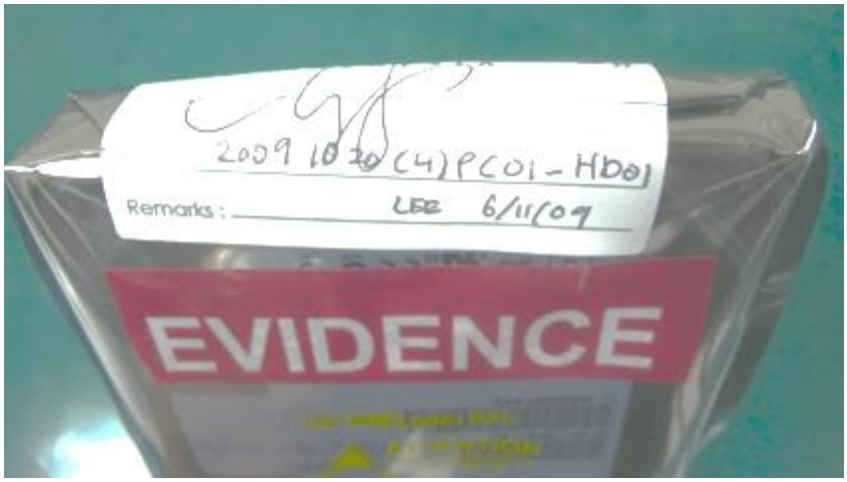
Requestor	DFL
Sender of the exhibit sign here Name: Date:	Sign here Name: Date:

Section B: Exhibit Return

I have agreed that DFL has returned all the exhibits listed in Section A to me. Upon signing the above column, both parties agreed that the work has completed and the case is signed off.

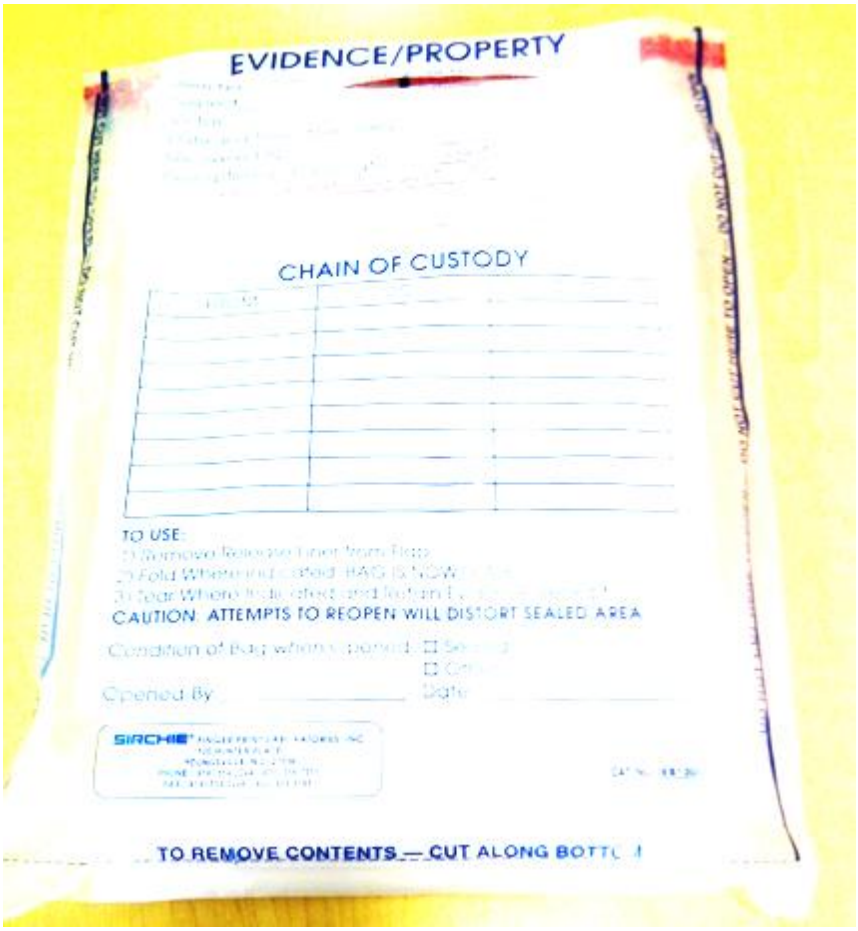
Requestor	DFL
Sender of the exhibit sign here Name: Date:	Sign here Name: Date:

APPENDIX E: SAMPLE OF EXHIBIT SEALING



The exhibit, a hard disk, is put in an anti-static plastic bag and a tamper-proof sticker is put at the opening of the bag. The Examiner then puts his/her initials on the sticker, along with the exhibit's label, date and time that the exhibit is sealed.

In this sample, the exhibit is put in a tamper-proof plastic bag. Details of the exhibit, the Examiner and the chain of custody are available on the plastic bag.



APPENDIX F: DATA ACQUISITION WORKSHEET

A standard Data Acquisition Worksheet is to be used during any forensic acquisition (imaging) of a hard drive or other type of media.

Image Acquisition Worksheet

CASE INFORMATION
Project ID (1):
Project / Matter Name (2):
Custodian Name (3):
Project Manager (5):

TARGET COMPUTER INFORMATION
Location of System (6):
System Type (7): ☐**Desktop** ☐**Laptop** ☐**Server** ☐**Other:**
Evidence Type (8): ☐***Hard Drive*** ☐**CD/DVD** ☐**Floppy** ☐**RAID** ☐**Other:**
System State (9): ☐**On** ☐**Off** ☐**Logged On** ☐**Other:**
BIOS Date /Time (10):
Current Date/Time (11):
Total Number of Hard Drives in CPU (12):
Hard Drive Removed by (13):
Photographs Taken (14): ☐**Yes** ☐**No – reason:**

CONSENT

I hereby authorize (enter agency name) (and their representatives) to take possession of all computer equipment necessary for their investigation. (4)

Signature Position

Print Name Date /Time

(xx) *See Guidance Notes*

	COMPUTER	HARD DRIVE/OTHER
Manufacturer:	(15)	(18)
Model Number:	(16)	(19)
Serial Number:	(17)	(20)

IMAGE ACQUISITION INFORMATION				
Acquired by (21):				
Imaging Location (22):				
Acquisition Method (23):	☐ **EnCase (v.)**	☐ **FTK (v.)**	☐ **X-Ways:**	
	☐ **dd Image**	☐ **Logical File Copy**	☐ **Other:**	
Acquisition Hardware (24):	☐ **Writeblocker**	☐ **Firewire W/B**	☐ **Bootdisk**	☐ **Direct Connection**
	☐ **SCSI-IDE W/B**	☐ **Xover Cable**	☐ **Other:**	
Evidence Media (25):	☐ **Hard Drive**	☐ **Other:**		
Serial Number (25):				
Evidence Disk Drive ID Number (25):				
Size of Hard Drive (26):		GB	MB	(indicate one)
Size of Image (27):		GB	MB	(indicate one)
Image Verified (28):	Yes	No	Errors (29): Yes	No
Hash Value (30):				

See Guidance Notes

NOTES
This section is available to add additional notes that are not included in the standard form, or to expand upon notes, i.e. types of errors received, problems encountered during imaging process.

Guidance Notes

CASE INFORMATION

1. Project ID - refers to the assigned number for the matter.
2. Matter Name - refers to the "code" name assigned by the project manager.
3. Custodian Name - refers to the end user assigned the computer.
4. Consent - if consent is required to obtain the machine, obtain a signature of the person releasing the machine.
5. Manager - refers to the assigned Project Manager leading the case.

TARGET COMPUTER INFORMATION

6. Location of System - address of site, may include office number if computer was taken directly from an office.
7. System Type - indicates whether the machine is a desktop, laptop, server, etc. If the device is a standalone drive, check 'other' and write in 'standalone drive'.
8. Evidence Type - mark the device to be imaged/copied.
9. System State - indicates whether the suspect machine was on, off, logged on, etc. If the machine is on, indicate who powered the machine down.
10. BIOS Date/Time - refers to the bios from the suspect machine.
11. Current Date/Time - refers to the date and time from the examiner's computer.
12. Total number of hard drives in the computer - self-explanatory.
13. Hard Drive Removed by - indicate who disassembled the computer.
14. Photographs Taken - please indicate whether photographs were taken of the computer and the hard drive. If the answer is no, you must explain why no photographs were taken.

COMPUTER

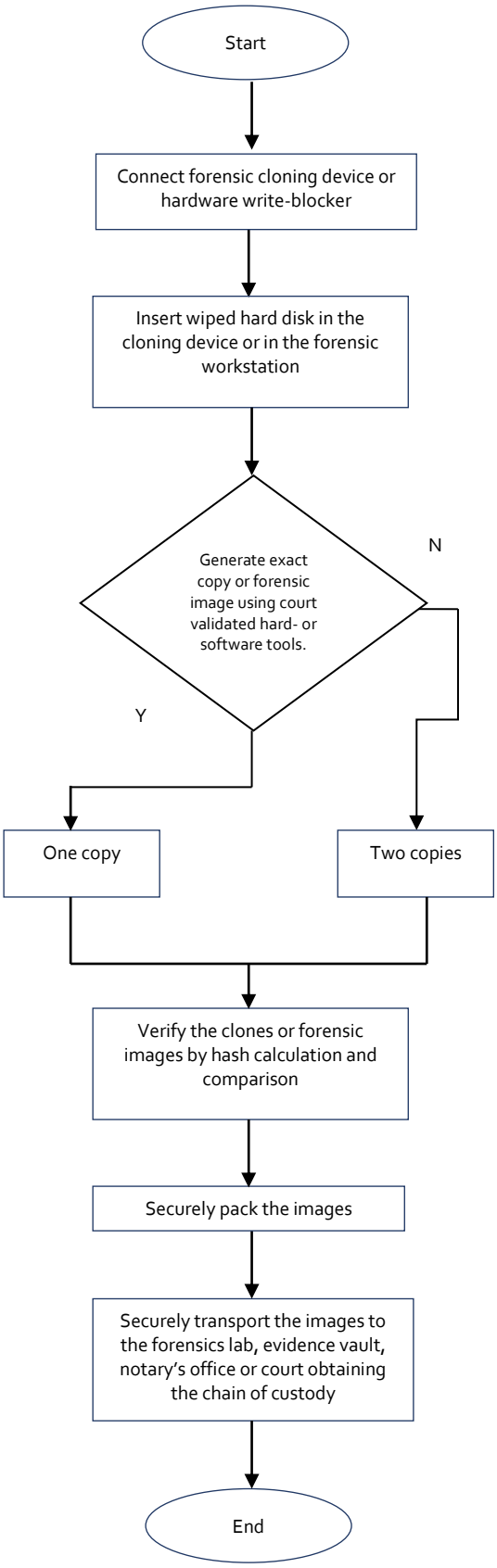
15. Manufacturer of Target Computer - type of machine and size of hard drive.
16. Model Number - model number of computer.
17. Serial Number - serial number from computer. If more than one serial number on the machine, copy them all HARD DRIVE/OTHER.
18. Manufacturer - type of hard drive.
19. Model Number - model number of hard drive.
20. Serial Number - serial number from the hard drive. If more than one serial number exists, copy them all.

ACQUISITION INFORMATION (this will be completed twice, one for each image).

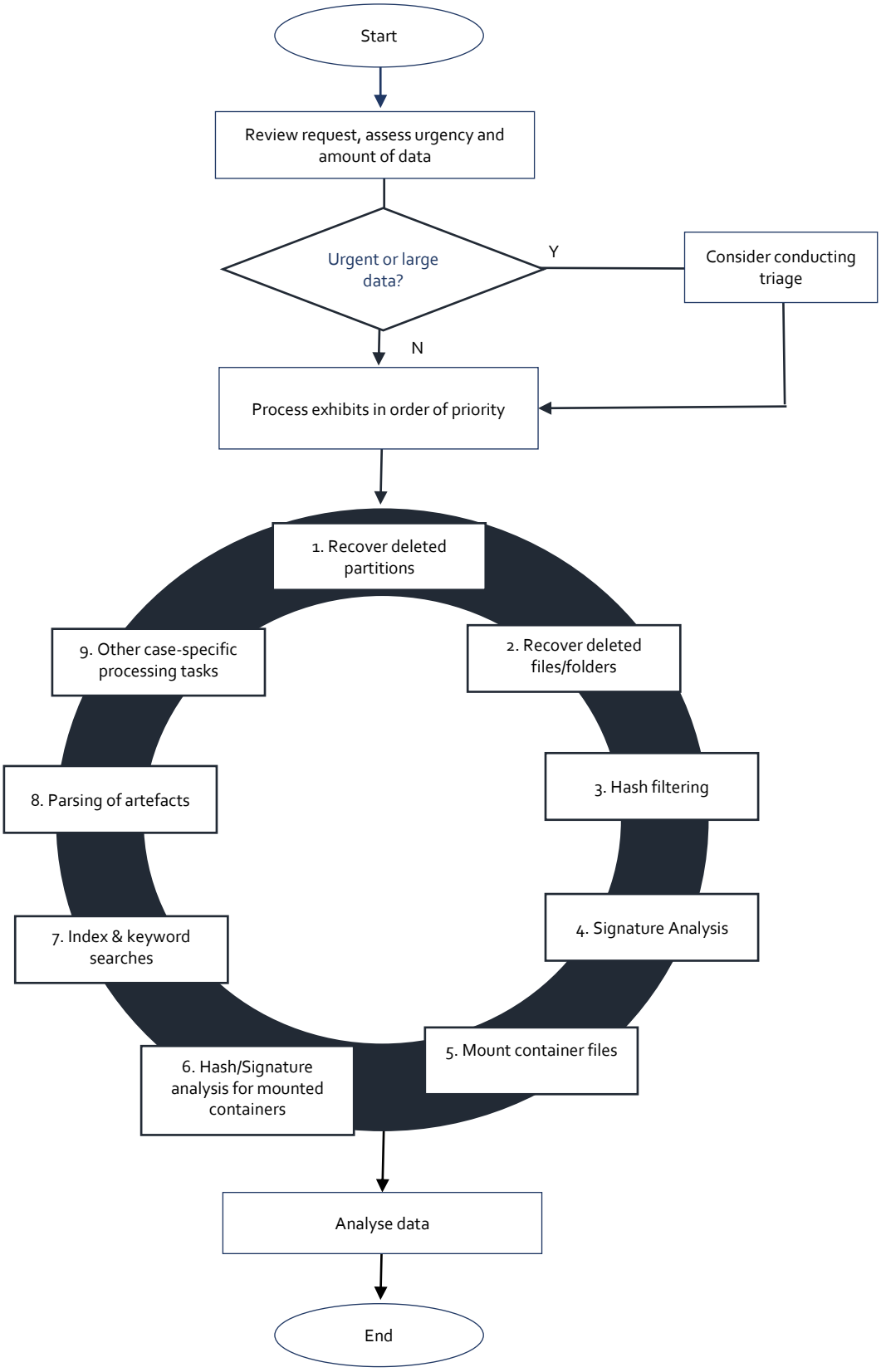
21. Acquired by - refers to the examiner who physically acquired the device.
22. Imaging Location – indicate whether the machine was imaged onsite, in the Lab - indicate which lab, etc.
23. Acquisition Method - indicates the type of software used to image the device. Make note of the version number of the software used.

24. Acquisition Hardware - indicate the type of acquisition it was, whether you used a write-block device, cross-over cables, boot disk, etc.
25. Evidence Media - refers to the drive where the image will be located. Indicate the Drive Label, serial number, and the Evidence Disk Drive ID Number.
26. Size of Drive - total size of hard drive in GB or MB.
27. Size of Image - indicate the total size of the image (NOT the size of the hard drive), indicate whether GB or MB.
28. Image Verified - when the image is completed and verified, check the YES box.
29. Errors - indicate if any errors were found during the verification process. If so, use the "Notes" section on the back of the sheet to record the specific errors.
30. Hash Value - record the hash value generated during the imaging process. Be sure to check that the acquisition hash value and the verification hash value match.

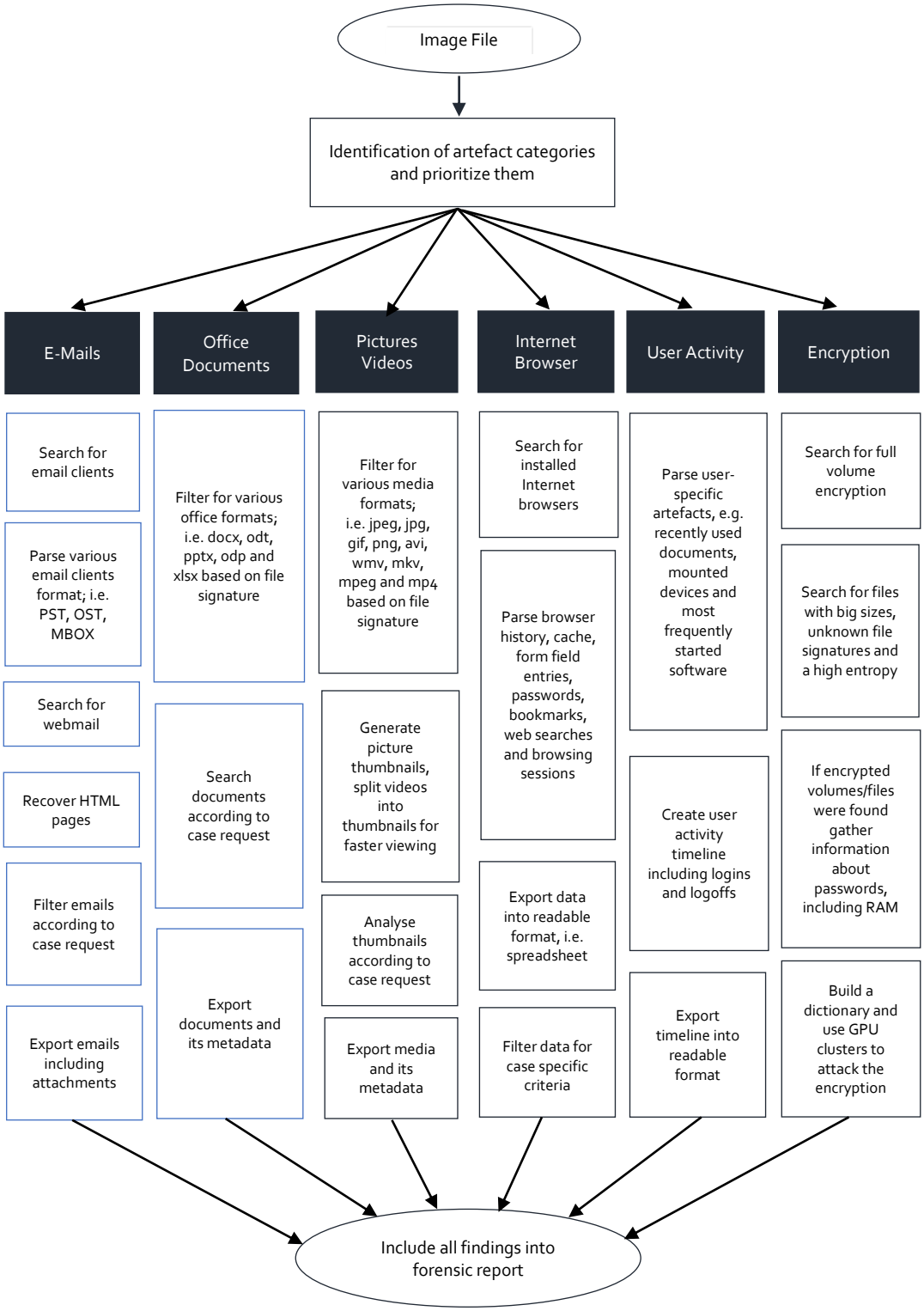
APPENDIX G: ACQUISITION PROCESS FLOW CHART



APPENDIX H: COMPUTER EXAMINATION FLOW CHART



APPENDIX I: PROCESS OF ANALYSING EXHIBIT'S ARTEFACTS



APPENDIX J: COMMON REQUIREMENTS FOR FORENSIC REPORT

Common Requirements for Forensic Report	
1	Title
2	Name and address of laboratory
3	Location where collection and examination take place
4	Page number and indication of page end
5	Requester name and contact information
6	Method used for the case
7	Description of electronic evidence
8	Date when evidence was received by DFL
9	Date of examination
10	Date of report issuance
11	Forensic result
12	Name and function of the person authorizing the report

APPENDIX K: ELECTRONIC EVIDENCE HANDLING

The following is a basic suggestion for the handling of electronic evidence.

Checklist for electronic evidence handling	
1	**Label** • Evidence must be uniquely labelled once it is delivered to the DFL. If it is difficult to put a label on the evidence, the DFL can put the label on the evidence's seal. • The label must stay throughout the lifetime of the evidence in the DFL. • Labels must also be able to track sub-items. Example: DFL-MP01 for a mobile phone and DFL-MP01-SIM01 for the Sim card contained in the phone.
2	**Seal** • Evidence must be sealed using a proper container. • The container must be able to detect any access made to the evidence. • The seal must be signed and dated by the Examiner. • Each time evidence is accessed, the person doing so must seal the evidence again, once the processing is complete, bearing his/her signature and dates.
3	**Document** • A full record of electronic evidence must be established. Items to be recorded include evidence type, serial number, manufacturer, any defects and any labels. • Evidence inventory list must also be established in the DFL. • A chain of custody record must be established for each piece of electronic evidence. At minimum it must contain a unique label, initials and date.
4	**Not Left Unattended** • Evidence not in the process of examination due to the Examiner's long leave or Examiners focusing on high-priority cases must not be left unattended in the DFL. It must be properly stored away to prevent contamination. • Evidence must also not be left unattended during the transportation process.
5	**Keep away from source of contamination** • Electronic evidence must be properly taken care of and be kept away from sources of contamination, such as water, heat, extreme humidity and electromagnetic field.
6	**Storage** • Electronic evidence must be stored in a secure place, with limited access. • A record of check-in and check-out of the evidence from Storage Room must be kept updated.
7	**Preservation** • A copy of the original electronic evidence must be made to preserve integrity of the original evidence. • Hash value of original evidence and its copy must be the same. • Examination and analysis must be conducted on the copy of electronic evidence.

APPENDIX L: INTERPOL DFL SERVICE REQUEST FORM

Form 01: DFL Request for Assistance

Use this form to formally request assistance from INTERPOL DFL. The form must be filled out completely and accurately by the NCB. A different criminal law enforcement agency authorized by the NCB ("Contact Agency") may fill out the form, however this request must be sent to INTERPOL by the NCB.

The information in this form will be assessed to determine whether the INTERPOL DFL is able to provide assistance. More detailed information will allow for a timely response.

In case of any questions, INTERPOL will liaise with the contact person(s) indicated in this form.

Requesting Member	
INTERPOL Member Country	
NCB	
Title/Rank of Contact Person	
Last Name	
First Name	
Contact email address (official)	
Contact phone	
Approval to coordinate directly with Contact Agency	(*) YES. NCB TO BE INFORMED ON ALL MATTERS RELATING TO THIS REQUEST. (*) YES. COORDINATE ONLY WITH CONTACT AGENCY. (*) NO. COORDINATION ONLY THROUGH THE NCB.

Contact Agency (if different from the NCB)	
Name of Agency	
Contact address	
Office phone	
Title/Rank of Contact Person	
Last Name	
First Name	
Contact email address (official)	
Contact Mobile phone	

Case Details	
Primary Offence	
Punishment upon conviction under Member Country law	
Other Countries Involved/International Character of the Offence	
Exhibit relates to (Tick all that apply)	(*) Suspect (*) Victim (*) Person of interest. Explain:

Brief Description of Case	

Reasons for requesting INTERPOL DFL assistance (Tick all that apply)
(*) Lack of expertise/knowledge (*) Lack of resources/funds (*) Lack of equipment/software (*) Others. Please specify:

Exhibits: General	
Will INTERPOL DFL Officers be required to interact with exhibits?	(*) YES (*) NO
If YES…	
(1) Will exhibits be "original" exhibits or "copies" *As far as possible, please restrict exhibits to copies.*	(*) ORIGINAL (*) COPIES
(2) Will INTERPOL staff have to visit the Member Country for the assistance?	(*) YES (*) NO
(3) Contact details of person(s) from Member Country who will be present during the assistance. Please note that INTERPOL will assist and guide this person to perform the task requested here, and to prepare a report for Member Country use.	(*) Same as Contact Agency (*) Different – Please specify:

Please indicate the nature of assistance required from INTERPOL DFL (Tick all that apply)
(*) Extraction of information from the exhibits. Please describe the information to be extracted (Choose all that apply): (*) Images/videos: Relating to: _____ (*) Files: Relating to: _____ (*) Text messages: Relating to: _____ (*) Technical details: _____ (*) Others: Please specify: _____ (*) Information on how to extract material from the exhibits, the extraction to be done by the Member Country (*) Information on available software or products to perform a task on the exhibits.

What is the task? _____ (Example unlocking a locked mobile device) Only open source/free software recommendations? (*) YES (*) NO Proprietary software recommendations welcome? (*) YES (*) NO

Exhibit Handling and Recording Instructions
IF Exhibits (including Original Exhibits) are required to be handled, please provide instructions in relation to the following:
(1) Please provide specific instructions or requirements on handling:
(2) Please list any specific activities or processes that MUST NOT be done:
(3) Please specify any particular instructions, with respect to recording of the assistance process, particulars of the Exhibit, or the chain of custody:
(4) Please provide any other information of relevance for the assistance: (*For example, is the Exhibit in 'switched off' mode? Were any prior attempts made to extract information?*)
(5) If INTERPOL considers that third party assistance is necessary to provide the assistance sought in this request, does the NCB agree to seek assistance from another Member Country, subject to both NCB's consent? (*) YES (*) NO

Assurances from Member Country	
The NCB and Contact Agency provide INTERPOL the following assurances:	
This request for assistance is lawful as tested against the laws of the applicable Member Country, applicable international laws and INTERPOL's Constitution and rules.	(*) YES

Specifically, Article 3 of INTERPOL's Constitution states: "*It is strictly forbidden for the Organization to undertake any intervention or activities of a political, military, religious or racial character.*" The assistance requested here will not any in manner cause an infringement of Article 3 of INTERPOL's Constitution.	(*) YES
Nothing in the Member Country's laws prevents the NCB or the Contact Agency from obtaining the information requested through this request for assistance.	(*) YES
The offence to which the request relates has an international link and is a serious offence within the Member Country's laws.	(*) YES
The NCB and Contact Agency understand that INTERPOL's provision of assistance is subject to the assessment of this request as per criteria applicable under INTERPOL's Constitution, rules and regulations.	(*) YES
If any information is sought to be extracted from Exhibits, the NCB and the Contact Agency endeavour to limit the request for extraction to information of relevance to the offence concerned, and proportionate to the purpose for which the extraction is sought.	(*) YES
Should INTERPOL agree to provide the assistance sought through this request, the Contact Agency/NCB shall sign an agreement in the form provided by INTERPOL, prior to the provision of assistance.	(*) YES
In case interaction with Exhibits is necessary, INTERPOL shall provide assistance and guidance to designated Member Country personnel to perform the request outlined in this request for assistance, and prepare necessary reports further to the same. Extractions will not be performed in the absence of Member Country personnel, other than in exceptional circumstances as INTERPOL may consider appropriate.	(*) YES
The Member Country personnel (whether from the NCB or Contact Agency) accompanying the Exhibit(s), if any, shall observe or ensure the observance of all requirements as per the Member Country's applicable criminal, procedural and evidentiary laws.	(*) YES
The Member Country personnel (whether from the NCB or Contact Agency) accompanying the Exhibit(s) shall certify that all requirements under the Member Country's laws were met, in extracting the relevant information from the Exhibit(s), in the report produced using INTERPOL's assistance or expertise.	(*) YES
The NCB and Contact Agency acknowledge that INTERPOL shall not be responsible with respect to the use of any information extracted from any Exhibits, or any reports produced with the assistance of INTERPOL. Any use of such information or reports in judicial proceedings or otherwise, is at the discretion and responsibility of the NCB/Contact Agency.	(*) YES

Exhibits: Specific	
Exhibit Type	Mobile Device/Hard Drive/ Other:_____
Physical Description	
Make/Model	

Serial #	
IMEI #	
Local Exhibit Identifier	
Passcode/Passwords	
Any other Relevant Information	
Exhibits: Specific	
Exhibit Type	Mobile Device/Hard Drive/ Other:_____
Physical Description	
Make/Model	
Serial #	
IMEI #	
Local Exhibit Identifier	
Passcode/Passwords	
Any other Relevant Information	

Exhibits: Specific	
Exhibit Type	Mobile Device/Hard Drive/ Other:_____
Physical Description	
Make/Model	
Serial #	

IMEI #	
Local Exhibit Identifier	
Passcode/Passwords	
Any other Relevant Information	
Exhibits: Specific	
Exhibit Type	Mobile Device/Hard Drive/ Other:_____
Physical Description	
Make/Model	
Serial #	
IMEI #	
Local Exhibit Identifier	
Passcode/Passwords	
Any other Relevant Information	

INTERPOL

INTERPOL General Secretariat
200, quai Charles de Gaulle
69006 Lyon
France
Tel: +33 4 72 44 70 00
Fax: +33 4 72 44 71 63

WWW.INTERPOL.INT

INTERPOL_HQ

@INTERPOL_HQ

INTERPOLHQ

INTERPOLHQ