Digital Forensics

A BASIC GUIDE FOR THE MANAGEMENT AND PROCEDURES OF A DIGITAL FORENSICS LABORATORY

www.coe.int/cybercrime

Version 1.1
June 2017

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Acknowledgement

The first edition of this Guide was published in October 2016 under the joint project of the Council of Europe and the European Union on Global Action on Cybercrime (GLACY). Work on this document was coordinated by Nigel Jones (United Kingdom) and Victor Voelzow (Germany). Valuable inputs were received from cybercrime experts from GLACY project countries and areas as well as a range of other international experts from Africa, Asia and Europe.

The authors were:

- Nigel Jones (United Kingdom)
- Victor Völzow (Germany)
- Andrea Bradley (United Kingdom)
- Branko Stamenkovic (Serbia)

This Guide will be improved and updated over time.
Comments on this version should be sent to cybercrime@coe.int.

CONTACT
Cybercrime Division
Directorate General of Human Rights and Rule of Law Council of Europe,
F-67075 Strasbourg Cedex (France)
Email cybercrime@coe.int

Table of Contents

Acknowledgement **2**

Abbreviations **5**

1 Introduction **6**

1.1 The purpose of the Guide **6**

1.1.1 What is included 6

1.1.2 What is not included 6

1.2 Who is the Guide for? **7**

1.3 How should the Guide be used? **7**

1.4 Symbols and explanations **8**

1.5 What is digital forensics **9**

1.6 Appendices **10**

1.7 Further tools and resources **11**

2 Management of a digital forensic laboratory **13**

2.1 Research **13**

2.2 Budgeting/capacity **14**

2.3 Premises **14**

2.3.1 Security 14

2.3.2 Location 15

2.3.3 Size 15

2.3.4 Air conditioning 16

2.4 Staff **17**

2.4.1 Recruiting 18

2.4.2 Police officers or police support staff? 18

2.4.3 Vetting 19

2.4.4 Staff development and human resources 19

2.4.5 Welfare 20

2.4.6 Health and safety 21

2.5 Physical laboratory requirements **22**

2.5.1 Office equipment 22

2.5.2 Software and hardware 23

2.5.3 Quality assurance/ review procedure 25

2.5.4 Streamlined examination and reporting 25

2.5.5 Retention of data 26

2.5.6 Education and training of all stakeholders 26

3 Digital forensics lab processes and procedures **27**

3.1 Overall process model **28**

3.2 Acquisition stage **30**

3.2.1 Acquisition of computer systems 31

3.2.2 Acquisition of mobile devices 35

3.3 Processing stage **42**

3.3.1 Processing of computer systems 42

3.3.2 Processing of mobile devices 44

3.4 Analysis stage **46**

3.4.1 Analysing computer systems 46

3.4.2 Analysing mobile devices 52
3.5 Presentation stage 54
3.5.1 Admissibility of electronic evidence 54
3.5.2 Report writing 55
3.5.3 Expert witness status 55
3.5.4 Alternative presentation methods 56

4 Appendices 60
Appendix A – Comparison of forensic software 61
Appendix B – Exemplary Device Carrying Case contents 67
Appendix C – Acquisition Process Flow Chart 68
Appendix D - Processing Flow Chart 69
Appendix E - Analysis Flow Chart 70
Appendix F - Presentation Flow Chart 71
Appendix G - Chain of custody record 72
Appendix H - Image Acquisition Worksheet 75
Appendix I – Digital Forensics Analysis Form / Spreadsheet 79
Appendix J – Digital Forensics Report Template 81

Abbreviations

AFF	Advanced Forensic Format
ATA	Advanced Technology Attachment
CCTV	Closed Circuit Television
COE	Council of Europe
DCO	Device Configuration Overlay
DNA	Deoxyribose Nucleic Acid
DVD	Digital Versatile Disk
GLACY	Global Action against Cybercrime
EU	European Union
EWF	Expert Witness Format
FSD	File System Dump
H & S	Health and Safety
HPA	Host Protected Area
IDEN	Integrated Digital Enhanced Network
IMEI	International Mobile Equipment Identify Number
iOS	iPhone Operating System
ISO	International Standards Organisation
IT	Information Technology
JTAG	Joint Test Action Group
LEA	Law Enforcement Agency
MD5	Message Digest 5
MEID	Mobile Equipment Identity Number
MFT	Master File Table
PDP	Personal Development Portfolio
RAM	Random Access Memory
RAR	Roshal Archive
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module

1 Introduction

This Guide has been produced as a follow on to the Council of Europe Electronic Evidence Guide[1], which was developed as a basic guide for police officers, prosecutors and judges. The Electronic Evidence Guide provides guidance on the steps to be taken to secure electronic evidence, for example at a crime scene and to ensure its evidential integrity is maintained until it is passed to digital forensics laboratory for further action. The present Guide takes the reader to the next stages of activity in the digital forensics arena. In addition to the practical processes and procedures to be followed in a laboratory environment, it deals with the management issues involved in the running of a laboratory and also the strategic considerations in establishing such a laboratory.

This Guide should also be at the disposal of prosecutors and judges. Although members of the judiciary are not obliged to be well acquainted or specialised in skills other than legal, contemporary criminal acts and their perpetrators are putting additional pressure on professionals both in prosecution services and courts to better understand and enhance their knowledge of cybercrime and raise their capabilities to render decisions in criminal cases on cybercrime or electronic evidence.

1.1 The purpose of the Guide

1.1.1 What is included

The purpose of the Guide is to provide support and guidance to managers and practitioners of digital forensics laboratories in the setting up and running of such laboratories in such a way that any evidence produced by them is dealt with in such a manner that will ensure its authenticity for later admissibility in court. Although the Guide is not intended to be an instruction manual with step-by-step directions, it does provide an overview of the kinds of issues that often arise when developing and running a digital forensics laboratory and offers advice on how to deal with them. Readers of this document should check if such advice already exists at the national level.

1.1.2 What is not included

The guide does not make any recommendations regarding hardware and software choices that may be available. Each country and organisation will decide what is appropriate given their needs and available funds. It should be remembered that digital forensics equipment and commercial software can be a very expensive long term commitment and is not easy to change once the initial decision is made. Details of the types of costs associated with forensic software purchases and information about some options to use open source software are dealt with elsewhere in this document.

[1] Available at the Cybercrime Octopus Community https://www.coe.int/en/web/octopus/home

This Guide and the information contained in it are considered valid until 31 December 2018. Where conditions permit the Guide will be updated before that date to reflect any relevant changes in technology, procedures and practices. Any person or organisation wishing to use the Guide after the above date should contact the Council of Europe to obtain the most recent version.

1.2 Who is the Guide for?

This Guide is designed for two specific categories of reader:

1. Those responsible for the development and management of their digital forensics laboratory that will form part of an overall digital forensics strategy,
2. Staff employed within a digital forensics laboratory, in technical roles relating to the digital forensics processes and procedures.

The guidance for the first group is designed to assist those responsible for developing digital forensic strategies, making decisions about building the capacity to deal with digital forensics and for those responsible for the management of laboratories. It is recognised that there is no single solution applicable to all countries or even different organisations within countries. The guide is designed to assist managers to make decisions about a subject with which many may not be familiar.

The second group consists of those with direct responsibility of laboratory activities and the staff that will carry out the function of acquisition, processing analysing and presenting electronic evidence. The guidance for this group will be more specific to the functions related to the electronic evidence process and will allow procedures to be adopted that will meet requirements of national and international criminal justice systems.

As aforementioned, prosecutors, judges, prosecutorial and court assistants and other staff included in criminal proceedings on substantive level, should be introduced to the contents of this guide in parts which are of vital interest for the cases in their competence.

1.3 How should the Guide be used?

This Guide should be seen as a template document that can be used by countries to consider when developing their digital forensics capability. The advice given is intended to be used at both strategic and tactical levels, according to their national legislation, practice and procedure.

The overarching principles described in the Electronic Evidence Guide are just as relevant to the procedures conducted in the laboratory environment and are in accordance with generally accepted good practice for dealing with electronic evidence. The principles are set out below to reinforce their importance:

Principle 1 – Data integrity

No action taken should materially change any data, electronic device or media which may

subsequently be used as evidence in court.

Principle 2 – Audit trail

A record of all actions taken when handling electronic evidence should be created and preserved so that they can be subsequently audited. An independent third party should not only be able to repeat those actions, but also to achieve the same result.

Principle 3 – Specialist support

If it is expected that electronic evidence may be found in the course of a planned operation, the person in charge of the operation should notify specialists/external advisers in time and to arrange their presence if possible.

Principle 4 – Appropriate training

First responders must have the necessary and appropriate training to be able to search for and seize electronic evidence if no specialists are available at the scene.

Principle 5 - Legality

The person and agency in charge of the case are responsible for ensuring that the law, the evidential safeguards and the general forensic and procedural principles are followed to the letter.

Further explanation of the principles is to be found in the Electronic Evidence Guide.

Readers should ensure that they are fully conversant with the laws of their own countries related to the digital forensics process and the admissibility of evidence adduced therefrom. National law should always be the primary point of reference. Advice given in the Guide is not expected or intended to contradict any national legislation and is at all times subject to national laws, rules and procedures.

1.4 Symbols and explanations

Various symbols are used throughout the Guide to indicate the importance or difficulty of the content of the section they accompany.

This symbol indicates the section contains information.

This symbol indicates important information.

This symbol indicates highly technical information

This symbol indicates the section contains basic knowledge

This symbol indicates advanced knowledge

This symbol specialised knowledge

The following information boxes indicate that there are specific considerations highlighted by the Prosecutor. This advice as with the remainder of the document is subject to local legislation, which will always take priority.

Prosecutor's considerations

Prosecutors' considerations are very important for criminal justice officials who are involved in the development and management of a digital forensics laboratory and for the technical staff employed of a digital forensics laboratory, since the outcome of the digital forensics process should be valid evidence representing a cornerstone for prosecutorial decisions in a criminal case.

Depending on the country's criminal law framework, the involvement of prosecutors will be needed at different stages of the criminal justice process. In some jurisdictions, the prosecution will only request a digital forensics expert opinion. In others, the prosecution will be more involved in the expertise processes, including involvement in particular phases of the process itself. In some jurisdictions, prosecutors have an advisory role or legal responsibility for the investigation process.

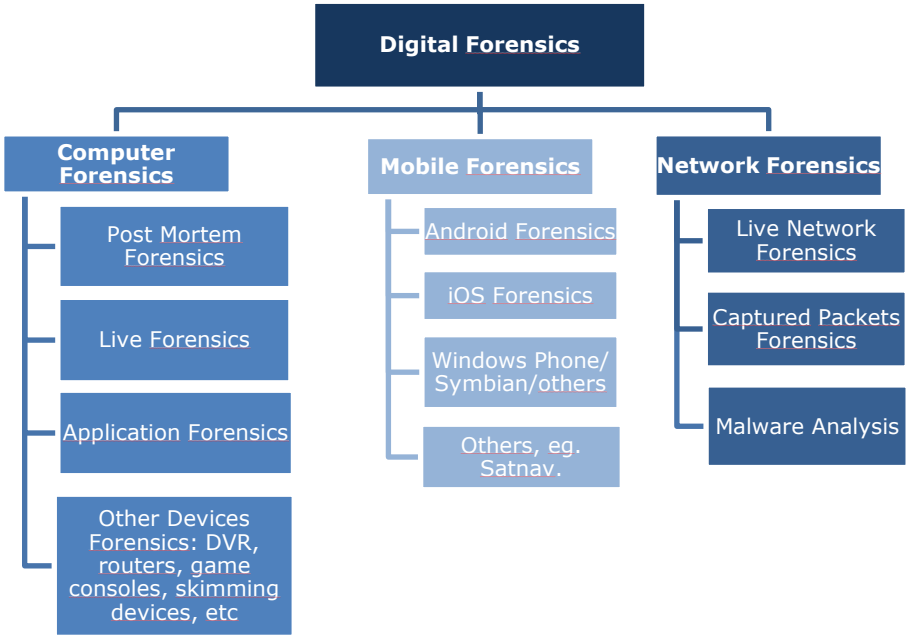
Irrespective of the legal framework, it is very likely that prosecutors will be first judiciary officials who are going to be presented with evidence resulting from the digital forensic process.

Therefore, this guide, together with the Council of Europe Electronic Evidence Guide, should be accessible to prosecutors and other parties involved in the criminal justice process.

1.5 What is digital forensics

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

Each and every branch of Digital Forensics requires extensive training and experience making it impossible for one forensic examiner to be expert in all areas. The following chart shows the main subcategories and subject areas of Digital Forensics.



In large countries, it is possible to have individual staff knowledgeable and skilled in each of the above disciplines. However in countries with a lower level of resources, it will be necessary to examine how the available resources may be put to best effect. This may involve outsourcing some activities or multi-skilling staff.

1.6 Appendices

A number of useful tools to assist the digital forensics practitioner are appended to this document:

- Appendix A - Forensic software comparison matrix
- Appendix B - Exemplary device carrying case content
- Appendix C – Acquisition process flow chart
- Appendix D – Processing flow chart
- Appendix E – Analysis flow chart
- Appendix F – Presentation flow chart
- Appendix G – Chain of custody record
- Appendix H – Image acquisition worksheet
- Appendix I – Digital forensics analysis form / spreadsheet
- Appendix J – Digital forensics report template

1.7 Further tools and resources

There is a wide range of resources and tools available to complement this Guide. For example:

- The Council of Europe Electronic Evidence Guide that has been referred to at various times in this publication. This may be used for example to provide information to those responsible for the search and seizure of electronic evidence that is to be brought to the Digital Forensics Laboratory.
- The Budapest Convention on Cybercrime[2] Parties to the Convention is expected to enact law enforcement powers for securing electronic evidence and for enabling efficient international cooperation. Under Article 14 these powers can be applied to electronic evidence in *any* offence. These powers include:
  - Expedited preservation of data at domestic (Article 16) and international (Article 29) levels, including the partial disclosure of traffic data (Articles 17 and 30);
  - Search and seizure of stored computer data (Article 19);
  - Real-time collection of traffic data and interception of content data at domestic (Articles 20 and 21) and international (Articles 33 and 34) levels;
  - Rapid mutual assistance to access data in foreign jurisdictions (Article 31);
  - Trans border access to data without the need for mutual assistance (Article 32).
- The proposal for law enforcement training strategies prepared under CyberCrime@IPA.
- The first responder training course pack prepared by the Council of Europe under CyberCrime@IPA project.
- The introductory cybercrime and electronic evidence training course for the judiciary, developed under the Cybercrime@IPA project.
- The advanced cybercrime and electronic evidence training course for the judiciary, developed under the Cybercrime@IPA project.
- The judicial training concept prepared by the Council of Europe and the judicial training materials developed under CyberCrime@IPA project.
- Guidelines for the delivery of Council of Europe judicial training courses on cybercrime and electronic evidence.
- The typology study on criminal money flows on the internet prepared by MONEYVAL and the Global Project on Cybercrime of the Council of Europe.

---

2 The Council of Europe Convention on Cybercrime (ETS No.185)

- The guidelines for law enforcement/Internet service provider cooperation adopted at the Octopus Conference of the Council of Europe in 2008.
- The good practice study on specialised cybercrime units prepared under CyberCrime@IPA project.
- Applicable rule of law safeguards and guarantees (Article 15 Budapest Convention) as documented under CyberCrime@IPA and Cybercrime@EAP projects.
- The Octopus Cybercrime Community, a forum linking up the many hundred public and private sector cybercrime experts from all over the world.

This list is not exhaustive. Countries and organisations should avail themselves of all relevant national and international resources to assist them in the development of their digital forensics strategies and capabilities, ensuring that the overarching principles associated with the subject are adhered to.

These resources and tools are available at www.coe.int/cybercrime.

2 Management of a digital forensic laboratory

In this day and age it is not uncommon to find that all types of criminal acts are being carried with the use of the Internet, mobile devices and computers. In some parts of the world this type of criminal activity accounts for the majority of criminal investigations. It is safe to say that as technology advances and becomes more affordable – so too will the use of digital data to research, facilitate and carry out various types of crime.

Digital forensic laboratories are being set up regularly by law enforcement agencies around the world. Some are professionally scoped and heavily invested in and others may be one officer with a computer and freely available forensic tools. Anyone who contemplates setting up and relying on a digital forensic laboratory should carefully research the requirements of their jurisdiction, ensuring they consult with the other players in the criminal justice system of the country.

2.1 Research

Initial research should be conducted to establish recent statistics on the seizure of digital devices, the types of crimes, the location, specialism of the seizing officers and what, if any digital forensic analysis has been carried out. This information should give a fair guide of how quickly this type of investigation is growing and where to start when considering the initial size of a digital forensic laboratory and identifying the need for investment. The research should establish if there are any legal or procedural requirements that cover the creation and management of forensics services within the criminal justice system. Comparison with countries of similar geography and demographics, that have already established a digital forensics capability, will be a beneficial exercise.

Finding the answer to the following questions will assist decision makers to understand and recognise the scope of the requirements of the digital forensic laboratory that is to be created:

- How many reported crimes have been facilitated with the use of digital data in the last 3 years, 2 years and 1 year?
- Is there an obvious and documented growth of this type of investigation?
- If digital forensic investigation has been required,
  - Who conducted the analysis?
  - Where procedures were followed?
  - What was the outcome?
  - What was the cost of the examinations?
  - Were some functions not able to be conducted with available resources?
- Are there other law enforcement agencies who have a similar requirement and could collaboration expedite the acceptance of any business case submitted?

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

2.2 Budgeting/capacity

There are many factors to consider when completing a Business Case, not least of which is the overall cost. This can be broken down into two main areas:

- The initial 'one off' outlay (capital costs) – Premises, refurbishment, security, office/lab equipment, hardware and software.
- Ongoing costs – staff, training, software licenses, counseling, etc.

The following chapters will assist with the specific considerations for each of these areas and will provide more detailed information to assist with the setting up of a digital forensic laboratory that is fit for purpose, scalable and resilient.

2.3 Premises

Demand and budgets will play a significant part in the availability, size and location of suitable premises. When identifying suitable premises the following factors should be considered:

2.3.1 Security

The premises will need to provide adequate security to store and investigate sensitive evidential data. It is not only the evidential data that needs to be secured, but managers must also consider the security of personal information, valuable software and hardware, actual exhibits and personal information pertaining to employed staff.

Preventing unauthorised entry and monitoring visitors to the premises should protect the access to the laboratory. Due to the sensitive data held within a digital forensic laboratory – it is advisable to have some form of record of entry and exit to assist with maintaining the continuity of the evidence within. The simplest way to do this is to have a witnessed signing in/out book but this requires a second person to be always present. Other types of access control include physical locks and keys, electronic keypads, swipe cards, CCTV and biometrics.

The premises should, ideally be alarmed with motion sensors in each room and at each entry point (external doors and windows). The windows and doors should be re-enforced to prevent non-authorised entry and theft and be covered to prevent observation of from external sources.

Fire detection and 'dry' fire quenching is also important and should be in place to protect people, property and evidence.

Off-site back up of electronic evidence held on servers should be considered mandatory and included in any security policy.

2.3.2 Location

Several factors will come into place when considering the location of any digital forensic laboratory. The availability of suitable premises will be a major factor in identifying the appropriate location. Ideally, a property in a central location would be a preferred choice. After identifying the business area that the laboratory will be service and the location from which the exhibits will be seized a more informed choice of location will be identified in the business case.

Ideally the Laboratory should be within another building as this provides additional security and resilience. It is better not to have windows or as few as possible, because these are a vulnerability to the security of the office and increase the possibility that the sensitive data could be observed from outside. If the identified location does have windows, they should be secured with bars or shutters and any glass should be frosted or opaque.

The delivery to and examination of evidence in the digital forensic laboratory should not be hindered by its physical location. Considerations about the physical location should include;

- If it is above the ground floor, is there a lift available to transport large quantities of computer evidence?
- If a large quantity of electronic evidence is to be delivered – how safe is the property in the vehicle.
- How far away is the car park to the laboratory?
- Is the building or office robust enough to ensure the security of the data and protect the people within?
- Are the walls, floor and ceiling strong enough to withstand physical or environmental damage?
- What is the risk from flood, fire, natural disasters and civil unrest?
- Incursion by terrorist or criminal organisations seeking to damage investigations.

2.3.3 Size

When considering the size of any laboratory, considerations that account for the various tasks that will be conducted within must be made. It is best practice to try and segregate the specific types of activities to prevent cross contamination and loss of exhibits.

A reception type area where evidence can be delivered or collected without allowing access to the actual laboratory should be incorporated in the planning of the digital forensic laboratory. A high priority is the need for a secure area to store exhibits and sensitive data. This should be a room located within the digital forensic laboratory. Alternatively a fixed metal cage could be used, depending on the amount of exhibits likely to be stored. Any access to and removal or return of exhibits to the storage room must be recorded. As with access to the laboratory, there are several different physical and virtual methods to achieve this.

There will need to be a laboratory, which is restricted to the forensic analysts of computers and mobile devices – or both. Each analyst will require a large desk for IT equipment, filing cabinets to hold their case files and comfortable chairs.

The digital forensic laboratory will need a server – this may be stored securely within the laboratory and if available, a separate room.

An area designated to imaging and processing will be required – this should be separate to the analyst's workstations and should, ideally, be close to the property store to reduce the amount of manual handling.

A breakout or rest area is important to provide the analysts with an area away from their investigations.

Considerations for an additional room for briefings or meetings as well as an additional office for the laboratory manager to utilise are advised.

Some laboratories have a separate 'viewing' room to allow for visiting officers/prosecutors to view their cases without causing distraction to the forensic analysts.

Ideally the office will have its own rest room facilities or there will be one situated in close proximity.

In addition to the above, areas dedicated to storage of non-evidential equipment like 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 in selecting the most appropriate place to locate a digital forensic laboratory.

The building or office selected should be large enough to expand if there is an anticipated increase in demand for digital forensic investigation.

Once you have established the required laboratory size, consider the longevity of such a facility. Many existing digital forensics facilities have found it necessary to relocate or expand in a short space of time due to exponential increases in workload. The information gathered during the research phase will give a good idea of the likely need for future expansion. It is extremely expensive to relocate or expand, so it may be beneficial to provide room for expansion in the initial business plan.

2.3.4 Air conditioning

Air conditioning is of vital importance, as a room with many working computers will generate a great deal of heat. If a server is positioned in its own area – this area should be cooled. Overheating can lead to loss of data and damage to hardware. Ideally an extractor unit should be purchased and installed in an area to provide greatest comfort to staff and to control the temperature and humidity of the laboratory. The exhibit storage facility should have its own air conditioning or climate control system to try to prevent deterioration of stored evidence.

2.4 Staff

It is likely that the person scoping and preparing the business case will be the laboratory manager or will be involved in the recruitment of such a Manager. Best practice shows that the laboratory manager should be involved in the recruiting of the staff that will be employed to carry out the different roles within the laboratory.

Depending on the size of the laboratory and the required number of staff they must consider the different functions that are required. Staff roles and responsibilities will need to be documented and detailed job descriptions should be prepared so that each member of the team has a clear understanding of their job profile. Where possible the structure of a digital forensics capability should incrementally allow for staff to be able to advance within the organisation, rather than leaving. It is accepted that this is only possible within a facility with plentiful resources, however it should always be an aim. There is strong anecdotal evidence that shows in many digital forensics laboratories highly qualified staff spend much of their time undertaking mundane tasks below their level of capability. To avoid this, it is important to recognise the activities to be undertaken should be clearly defined in the job profiles. The roles and responsibilities that should be considered include the following:

Laboratory manager

The manager must have some advanced technical knowledge and a strong understanding of the legislative requirements for electronic evidence as well as the procedures and processes to be followed. It is vital that the manager understands the overarching principles described in the Electronic Evidence Guide and reiterated earlier on in these operating processes. The laboratory manager should have control over the original set up, identifying the building, purchasing equipment and software and setting the procedures and functions of the laboratory. They should be responsible for leading the recruiting, training, mentoring, counselling and guidance of everybody employed within the unit.

Digital forensics analyst - computers

The analysts will require technical knowledge, and where possible appropriate qualifications. Ideally they should have some training in the use of digital forensic software. Alternately these staff members will require specific forensic training to bring them up to a suitable skill level. Digital forensic analysts must have knowledge of legislation and be aware of the points to prove when investigating different types of crimes. These roles require an analytical and investigative mind-set; the digital forensic analyst must be able to deliver their findings in a clear and understandable format. It is important that digital forensic analysts have good oral and written communication skills.

Digital forensics analyst – mobile devices

The analysts will require technical knowledge, and where possible appropriate qualifications. Ideally they should have some training in the use of mobile device acquisition. Alternately these staff members will require specific training to bring them up to a suitable skill level. Digital forensic

analysts must have knowledge of legislation and be aware of the points to prove when investigating different types of crimes. These roles require an analytical and investigative mind-set; the digital forensic analyst must be able to deliver their findings in a clear and understandable format. It is important that digital forensic analysts have good oral and written communication skills.

Forensic imaging technician

The role of the Imaging Technical is to take forensically sound copies (images) of computer hard drives and other storage media. Depending on the size of the laboratory, several technicians may be required. The Forensic Imaging Technician will need to have good technical knowledge and an understanding of the various methods of forensically acquiring digital data. A key skill requirement is attention to detail and the ability to clearly document all their actions, the verification of imaged data and the continuity of evidence.

Administration

An important role within any laboratory is continuity of the evidence and requisite recording of the chain of custody. Depending on the size of the laboratory and the amount of electronic evidence to be examined, an administrator role may need to be filled. The administrator would take responsibility for documenting each new case, checking the exhibit numbers/serial numbers and case files are all accounted for. Other considerations include

- Making decisions about the seriousness of the investigation.
- Prioritisation of cases.
- Entering the information onto a case management system.
- Liaison with outside agencies, police officers and the rest of the laboratory team.
- Strong oral and written communication and attention to details.

2.4.1 Recruiting

Recruitment should start as soon as the business case has been accepted and the premises are identified. Having key staff on hand to assist with the identification and selection of hardware and software would be beneficial. It may be that these key staff are already trained or are familiar with a certain type of forensic software and would rather work with this. Ideally the roles and responsibilities of each vacancy will be established prior to advertising.

2.4.2 Police officers or police support staff?

Some forensic laboratories will be staffed totally by serving police officers, some with only support staff and others with a combination of both. There are pros and cons for each option.

Police officers tend to have better investigative knowledge and are more familiar with legislation and points to prove criminal action. They will be less likely to move onto other job opportunities and will be more used to working unsociable hours.

Support staff may have more relevant technical qualifications and received more training. They may have practical experience in the investigation of digital data but may be more inclined to seek career progression and move to the private sector.

A mixture of both may improve your overall technical ability and provide a more diverse team.

2.4.3 Vetting

Whoever is recruited to work in the digital forensic laboratory will require some form of background check or security vetting. All staff within the laboratory will have access to sensitive data and evidence of serious criminal activity. It is important to establish that they or their close family have not been involved in any criminal activity previously, especially dishonesty offences. It is also prudent to identify if they have any financial difficulties that may make them susceptible to bribery or corruption. It is also worth considering any previous affiliation with extreme political groups. It may be that managers will have access to existing vetting material within their environment or alternately cover the Vetting criteria during the selection and interview processes.

2.4.4 Staff development and human resources

Once staff are recruited, it is important to continually develop their abilities, motivate and retain them. The establishment of an achievable staff development program can support this. This must commence with an induction to their new workplace. Initial documents should clearly illustrate their role and responsibilities, their reporting manager and their senior manager. These initial documents must identify any immediate training needs or desires and record arrangements that are agreed to address this plan. Such arrangements may send staff on training courses or arranging for them to shadow and learn from colleagues alongside a planned timeframe. For example, all Digital Forensic Analysts will require externally certificated training to provide them with the confidence to use the forensics tools and the credibility to deliver reliable evidence in a court. Consideration may be given to issuing each staff member with a Personal Development Portfolio (PDP), which will contain an ongoing record of their training and qualifications, as well as milestones achieved in their work place mentored activities. Managers may use PDP's to set targets for individuals that will collectively within the team create a more balanced and effective capacity.

Advancements in technology are moving at a very fast pace and digital forensics analysts need to be regularly trained and retrained to keep up to date with the advances in digital forensics science. Management will also need to set aside some time for these analysts to undertake research and development. As new tools and applications come onto the market – the analysts should evaluate them to identify artifacts of value to the digital forensic laboratory.

Staff retention will be key to managing a successful digital forensic laboratory. A great deal of time and money will be spent on training of staff, and it is vital they are retained, especially once they are trained and begin to become more experienced. Having robust personal development plans for each member of staff will give them objectives and a better understanding of their career path and future opportunities. It must always be remembered that retaining staff is not simply a matter of salary. Developing a working environment, where staff can flourish is equally if not more important.

There are some guides available, which relate to the desired competencies in the digital forensics arena:

- EU Training Competency Framework on Cybercrime by CEPOL, ECTEG, EuroJust and Europol EC3 - available via Europol EC3;
- A skills matrix being developed (and available in early 2017) as an output of the EU funded SENTER project.

2.4.4.1 Mentoring

Of equal importance to development and training is staff mentoring. Mentoring is the process whereby an experienced staff member offers support to a new member of staff during their probationary period. If appropriate, the probationary period should be set once the level of training and development of the individual is identified.

The role of mentor is as guide and support, possibly a friend and confidante, as well as source of information. It is envisaged that the need for a mentor will diminish as time goes by and will disappear completely as the new member of staff settles in to their new role.

Mentoring takes place alongside appraisal and the assessment of performance in relation to reappointment or confirmation of satisfactory completion of probation.

2.4.4.2 Appraisals

All staff will need regular appraisals with their line managers to discuss their progress as well as the staff members of their own progress. It is proposed that that these be conducted at 6 monthly intervals and should review their performance over the last 6 months and their needs/requirements and aspirations for the next 6 months. It is also useful to ensure that areas of development are achievable and staff progress is delivered, evidenced and recorded.

2.4.5 Welfare

Digital forensics Laboratories are often fast paced and stressful. When dealing with serious criminal investigations it is common that time pressures are encountered as investigators are pushing for evidential results in order to further detain, charge or release their suspect or to prevent further suffering to victims. Analysts work need to be monitored, as mistakes can be made under pressure. Break out areas should be provided so that analysts can walk away from the data and take a moment to refresh. Managers need to observe their analysts to assess individuals' workload and offer support and intervention if casework becomes stressful.

2.4.5.1 Subject matter tolerance

Time pressure is not the only issue for analysts, as many cases will contain distressing pictures, videos and text depicting child abuse, sexual abuse or terrorism subject matter. In some cases the quantity of this type of material will cause stress; occasionally the depravity depicted in the digital images will affect the analyst more. It is important that the manager aims to allocate a varied caseload to the analyst to provide a break from the more harrowing investigations. The demeanor

and behavior of laboratory staff should be monitored so any issues can be identified and dealt with before they have the opportunity to escalate and negatively impact upon the health of staff.

2.4.5.2 Counseling

Best practice shows that regular counseling should be offered to all laboratory staff that come into contact with concerning subject matter. This counseling should be provided at regular intervals of 3 to 6 months and may be more effective if it is compulsory, as staff may be reluctant to put themselves forward for counseling, for fear of a negative perception created among colleagues. It is important to remember that peer support is an additional powerful counseling tool that is freely available, if this working culture is encouraged.

2.4.5.3 Succession planning

It is widely accepted that technology will continue to grow and criminals will commit more crimes with the use of digital devices. It would therefore make sense to prepare for the growth of the laboratory by introducing a program that trains, supports and nurtures each member of the team to be willing and able to take on a more senior role as the need arises. Succession planning is an effective method of nurturing and retaining trained staff. The alternative method is replacement planning – where a totally new employee fills a vacancy. Experience shows that skilled, experienced and qualified digital forensic analysts are difficult to acquire. Creation of a succession plan has supported longevity and success in many digital forensic laboratories.

2.4.6 Health and safety

The laboratory manager should take responsibility to ensure the health and safety of all staff and the visitors to the laboratory. He should conduct risk assessments by examining current conditions and situations and addressing anything thought to be hazardous or potentially damaging to health or safety. The manager must also be aware of any legal health and safety requirements. Health and safety measures apply equally in respect of people that may visit the laboratory and measures must be put in place to ensure that they do not see or are subjected to illegal or distressing materials. The possibility of this can be mitigated by following the ideas previously provided with regard to the structure and set up of the laboratory.

These are some of the standard H&S features that are encountered in a digital forensics laboratory:

- Anti-static mats and wrist straps – reducing the risk of static damage to equipment and exhibits.
- Contaminated Substances – preventing exposure with the use of surgical gloves or other protective clothing.
- Handling/lifting - ensuring staff are aware of the correct way to lift heavy items to avoid injury.
- Rubber matting - to reduce the risk of electric shock
- Circuit breakers - to reduce the risk of electric shock or damage to data.

2.5 Physical laboratory requirements

Once the location of suitable premises has been identified and the initial recruitment processes for a digital forensics team are underway, it is important to consider the establishment of the physical laboratory.

2.5.1 Office equipment

The size of any laboratory will dictate the amount of office equipment required.

Administrator desk - Ideally you will have a reception area that will require a reception desk large enough to hold two monitors and two computers, a telephone and a significant amount of paperwork. In addition, it would be beneficial to have an adjoining clear surface to deposit incoming and outgoing exhibits and case papers to allow for the checking, documenting and recording of these exhibits by the administrator. A chair for the administrator and chairs for visitors could be considered. It is envisaged that this area would be less secure than the rest of the laboratory so no case papers or sensitive paperwork should be stored in this area.

Secure property store – This facility should be large enough to store various items of computer and mobile phone evidence for a significant period of time. Computers can come in all shapes and sizes and some servers are very large and heavy. Conversely, mobile phones and external storage devices could be easily damaged or lost if not stored securely. The property store should be a secure room with access control. It should be situated close to reception and close to the Imaging area to avoid the need to carry heavy items too far. Ideally you should install strong shelving and a numbering system to segregate the exhibits to allow easy identification of exhibits for each case. Consider purchasing plastic boxed to house the smaller exhibits. The exact location of the exhibits for each case should be noted in the case management system and exhibits returned to the same location once imaging has been concluded. It may also be worth considering isolating the secure store from radio waves by implementing Faraday shielding. This will ensure the isolation of devices with wireless communication capabilities. There have been reported instances of the contents of mobile devices being remotely deleted while in police custody. A Faraday cage is very expensive and the use of Faraday bags may be an alternative. As a last resort, completely enclosing the devices in strong silver foil as a temporary measure will prevent communication with devices.

Forensic imaging department – The imaging department will require a large, clean surface area preferably with raised edges to prevent the loss of screws and small components, whilst computers are being dismantled for acquisition. Anti-static mats should be on all work surfaces. An area for digital camera and battery chargers should be arranged, as all evidence should be photographed prior to imaging. Each imager will require a desk area large enough to hold two monitors and two computers, acquisition hardware, telephone and paperwork. A chair for each imager, preferably a comfortable operator's chair, with lumbar support and height adjustment should also be provided.

Analyst work station - The digital forensics analyst will require a large desk area big enough to hold several monitors, two computers, various paperwork, mobile devices and mobile device extraction hardware and tools. Again a comfortable chair would be beneficial due to the amount of time spent sat at the monitor. It would also be advisable to position the desks to avoid others from

accidentally viewing sensitive data on the screens – or put privacy screens between the workstations to provide a cubicle type environment.

Server room – The space allocated to central server will need to be secure due to the amount of sensitive data that may be stored within. It will need adequate air conditioning to prevent overheating and will need room for resilience like UPS.

2.5.2 Software and hardware

Hardware - The digital forensic laboratory should be a high tech environment with lots of sensitive data being analysed and stored. As such, it will require an examination network, which is isolated from any external connections. As all laboratory staff will use this network it will need to be resilient, secure and fast. When setting up any server or system, best practice would be to opt for the highest available processing power and a suitable data storage array.

This system must provide Internet access to the team, either individually supplied to all hosts or just to one dedicated computer within the laboratory. This should allow analysts and staff easy use for checking emails, researching, downloading patches, updates and tools.

Any analyst would prefer that two monitors make their work easier. When it comes to building their final reports it is much easier to have the report open on one screen and their investigation on the other. It can also assist when viewing a high quantity of thumbnails. Whilst this is extra expense, the benefits of having this viewing capability will provide time saving benefits along with a robust system that can support the analysts provide more accurate reports for evidence.

Those responsible for imaging computers will require sanitised storage disks and write blockers to prevent any changes in data and the integrity of the original evidence. There are numerous types of write blockers on the market and several software tools that can also be used.

In addition to backing up operating data, the laboratory will be dealing with three additional types of storage issues; the original evidence, the forensically created images and the data generated after the investigation. Consideration must be given as to how this is all to be stored, archived and backed up. A stringent back up and archive regime should be implemented to offer resilience.

If any of the digital forensic team are likely to assist with the execution of search warrants and engage in 'on site' acquisitions and analysis – they will require an 'on site' kit (see appendix B for an exemplary configuration of a device carrying case). In addition to a portable workstation or laptop and the imaging tools, consideration must be given for purchasing the following equipment:

- Property bags, security tags and exhibit labels
- Torch
- Screw drivers
- Sterile gloves and clothing
- Tape

- Communication devices
- Power extensions, leads and adaptors
- Camera, video recorder
- Storage boxes or suitable container for the carriage of equipment.

Software – It is important to consider that there is not only the initial purchase but also the ongoing cost of licensing, support and training, associated with most types of digital forensic software. The initial and ongoing cost of licenses can be significant and research should be undertaken before purchase to ensure the hardware and software being obtained correctly matches the laboratories requirements and the staff's preference. Appendix A shows an exemplary matrix that shows how a lab manager can create a comparison between different forensic software products taking into account the functionality as well as the cost of purchase, license renewal and training.

It is worthy of note that some digital forensics analysts can conduct entire investigations with the use of open source or free software – however there is a lack of support and training opportunities with these types of product. Many jurisdictions and standards will require 'dual tool verification' and additional software may need to be purchased in order for the analysts to compare and verify their findings.

A fundamental requirement for the smooth running of any laboratory is some type of case management system. This is a database that holds all the relevant administration information about the evidence and cases held at the laboratory and will be fundamental to the integrity of the analysts' processes.

The minimum entries for a case management system should be as follows:

- Date, time and person delivering and receiving the exhibit to the laboratory.
- Unique reference number – software generated.
- Case number or crime number.
- Exhibit reference numbers.
- OIC/ investigating officer/prosecutor name and contact details.
- Type of crime.
- All laboratory staff that have had contact with the exhibits.
- The points to prove or what is required from the investigation.
- Time factors – such as delivery dates and anticipated court dates.
- Date imaged – who by and details of the items imaged.

- Verification hash results.
- Date investigation commenced.
- Assigned forensic officers and staff involved in the investigation.
- Details of quality assurance by colleagues and managers.
- Date investigation completed.
- Result of the investigation.
- Record of communication with the officer in charge of the submission.
- Date and time exhibits/report were collected.

All this information is vitally important to show continuity, credibility and verification of actions and evidence. A software database should be created by a technically proficient person unless the forensic laboratory utilises on of the commercial software packages that are available.

2.5.3 Quality assurance/ review procedure

As with all types of evidence it is possible that digital findings will be questioned once they are presented to a court of law. Due to the volatile nature of electronic evidence it is imperative that steps are taken to ensure the integrity of the evidence and the validity of the findings.

It is very important that procedures to monitor the quality of the work undertaken by the laboratory are established and implemented from the outset. All staff and managers must be fully conversant with their role in quality assurance and should adhere to the procedures on all cases. Random QA checks, peer reviews and administrative reviews should be carried out before a case is labeled as completed.

Managers should consider the introduction of recognised, externally audited, standards to maintain quality, information security and validation of forensic techniques. These standards are described in ISO 9001 – Quality Management, ISO 27001 – Information Security and ISO 17025 - Laboratory Validation.

2.5.4 Streamlined examination and reporting

It is sensible to introduce responsible methods of prioritising workload from the beginning. By having a process that identifies the more serious or time critical cases and places them on a priority list, an effective system is created to support the efficient the staff throughput of urgent and non-urgent cases. Risk assessment should be undertaken and decisions recorded in all cases that are considered for streamlined activity or triage. A court should in the future be able to examine and consider the rationale behind such decisions.

Another consideration that will support the streamlining of examination is to put in place a form of triage. This triage will allow interim examinations to be conducted in order to establish the likelihood of a positive result. Several jurisdictions now use a form of streamlined reporting, so that

a reduced amount of evidence is produced initially, in the anticipation that the defendant will accept his guilt at court. Where this does not happen and the matter is to be subject of a full court trial, a more comprehensive examination should be carried out in good time for any trial.

2.5.5 Retention of data

In a busy digital forensics laboratory it is important to have a data retention policy in place. If this is not implemented and followed from the beginning, a situation may quickly arise where there is insufficient storage available at the laboratory to hold the data. This may be in breach of good practice and the laboratory may be breaching local data protection legislation. Once implemented there should be regular checks to make sure the laboratory is still compliant. In some jurisdictions there are legal requirements for the retention of data, particularly in serious cases. Any such requirements should be at the forefront of any policy.

2.5.6 Education and training of all stakeholders

At some time the preparation of the laboratory will be underway and the staff will commence their employment. At this time submissions will be made requiring the digital examination of data. It must be reinforced to staff and colleagues about what can be reasonably expected from examining a computer, tablet, phone, or any digital device.

To prevent errors at the time of seizure of electronic evidence, it will be necessary to circulate instructions and guidance to police officers, which gives them directions in order to fully consider the implications of their actions at the time of seizing digital devices. Prosecutors and judges should also be aware of the procedures that the police follow, in order to assure themselves that the correct procedures have been adopted in individual cases they may be prosecuting or adjudicating.

3 Digital forensics lab processes and procedures

This chapter covers the processes and procedures that typically are involved in a digital forensics examination. An overall, chronological process model is used in order to provide a better overview over the main processes.

During all phases of a digital forensics examination it is vital to remember the special characteristics of electronic evidence as laid out in the Electronic Evidence Guide.

Electronic evidence...

> **... is invisible to the untrained eye**: Electronic evidence is often found in places where only specialists would search or in locations reachable only by means of special tools.
>
> **... is highly volatile**: On some devices and under certain conditions computer memory (and the evidence it contains) can be overwritten (or altered) by the usual functioning or operation of the device. This might be caused, for instance, by a loss of power or where the system needs to lay (or 'write') new information over the top of the old due to lack of memory space. Computer memory can also be corrupted or lost through environmental factors such as excessive heat or humidity or through the presence of electromagnetic fields.
>
> **... may be altered or destroyed through normal use**: Computer devices constantly change the state of their memories, be it on user request ("save this document", "copy this file") or automatically by the computer operating system ("allocate space for this program", "temporarily store information to swap it between devices").
>
> **... can be copied without degradation**: Digital information can be copied indefinitely with each copy exactly the same as the original. This unique attribute means that multiple copies of the evidence can be examined independently and in parallel by different specialists for different reasons without affecting the original.

Please remember that this manual is not intended to be used as a step-by-step set of instructions. While it describes processes and procedures and provides indications of what should be considered in all phases of a digital forensics analysis, it does not explain which features of a certain software need to used or where exactly and in which format certain artefacts from all operating systems and applications need to be parsed.

In addition to the explanatory text a number of useful resources have been created in order to visually aid in the faster understanding and remembering of the processes and procedures.

Flowcharts:

- Appendix C – Acquisition Process Flow Chart
- Appendix D – Processing Flow Chart
- Appendix E – Analysis Flow Chart

- Appendix F – Presentation Flow Chart

Forms:

- Appendix G – Chain of custody record
- Appendix H – Image Acquisition Worksheet
- Appendix I – Digital Forensics Analysis Form / Spreadsheet
- Appendix J – Digital Forensics Report Template

These resources can be used as template documents and may be adapted as required.

3.1 Overall process model

In a case that involves digital forensics the standard procedure typically consists of four stages:

The following subchapters will explain these stages in more detail. Each stage consists of several procedures which are thoroughly explained.

As every case is different not all of the above stages are necessary any time. Laboratory managers can for example decide that in extremely urgent cases or cases that involve an unusually high amount of data the acquisition step can be skipped and a triage approach is followed in the processing phase while the analysis stage will be extremely shortened. Decisions like that should depend on the aim of the investigation and the characteristics of the case.

Prosecutor's considerations

Criminal procedure and substantive law vary through countries and continents. The usual division between "common law" and "civil law" criminal justice systems still exists, but the borderline is becoming less visible and hybrid systems emerge as time goes by and practitioners all over the world are demanding more unified and, above all, more expedited systems for criminal justice.

The position and role of prosecutors in a contemporary criminal justice system becomes more prominent. In most systems prosecutors are bridging points between suppression and litigation, between discovery and adjudication of criminal acts, and between the police and other law enforcement agencies as well as judges and courts.

Taking that into account, processes and procedures in the forensics laboratory may or may not be under scrutiny of the public or state prosecutor, but one thing should always

be on the mind of laboratory staff: facts discovered and evidence produced is always going to end in the hands of a prosecutors who will be responsible to render lawful decisions about the fate of the case and it's perpetrator.

The aim of the investigation should always be two-fold: acquisition of all existing evidence with regards to the case, and ability to reproduce and explain the forensic procedure which led to the acquisition.

Prosecutors should be interested in all stages of the process, but they will most probably focus on the acquisition and presentation stages.

On some occasions, the acquisition stage will be the first encounter of the prosecutor with the electronic evidence in a criminal case. Often, this contact will happen during the on call duty and maybe during late hours. With an increasing role of prosecutors within criminal law systems, they are in charge of decision making throughout the whole investigation process or a significant part thereof. Thus, a forensic examiner should expect important and expedited decisions about the acquisition of electronic evidence to be taken by the responsible prosecutor. In such cases it will be very important that information presented by examiners to prosecutors about the acquisition and actions needed includes all relevant facts in an understandable manner indicating clearly the connection with the crime under investigation.

Examiners should understand a prosecutor's questions and directions, comment on them, provide further information and be prepared to extend the acquisition to other hardware and software if technically and legally possible.

Presentation of extracted evidence and established facts represents the final stage and goal of the whole process and will be covered in more detail later on in this Guide.

3.2 Acquisition stage

Electronic evidence needs to be acquired in a forensically sound manner. Acquisition of data is typically conducted by collecting volatile data from a running computer system during a search, or by acquiring a storage medium from a seized computer or in any other stage during an investigation. The application of specifically defined and tested procedures at the acquisition step is crucial as there is an enormous scope for irreversible errors to be made. It is important to keep the chain of custody intact at any stage, to document all steps carefully and to verify all images and copies that were acquired.

The intangible nature of any data and information stored in electronic form makes it much easier to manipulate and more prone to alteration than traditional forms of evidence. This has created special challenges for the justice system, which requires that such data have to be handled in a special way to ensure the integrity of the evidence.

Similar to other types of forensic evidence, the correct acquisition and handling of electronic evidence are vital to the outcome of a case. Close attention must be paid to ensure that the general guidelines are followed at all times:

Handling by specialists: Every kind of electronic device has its own specific characteristics that require the correct and appropriate procedures must be applied. One of the greatest risks is the unintentional modification of the evidence. Failure to adhere to approved procedures is likely to lead to formal challenges in court about data integrity that can undermine or invalidate the evidence.

Rapid evolution of electronic evidence sources: New technologies are invented and develop very quickly. Consequently the procedures and techniques to be applied to them also need to be constantly reviewed and updated.

Use of proper procedures, techniques and tools: As in more traditional forensic disciplines, digital forensic specialists require special tools and knowledge to undertake their investigations properly. It is imperative that the correct techniques and tools are used for the situations encountered. The procedures must also be auditable and repeatable by other specialists if the information obtained is to have evidential value.

Admissibility: Since the ultimate goal is to use evidence to prove or disprove disputed facts, electronic evidence must be obtained in compliance with existing legislation and best practice to ensure admissibility at trial.

Before even considering starting the acquisition process either the laboratory manager or the exhibit officer must check whether the proper permission for a data acquisition exists.

If proper permission exists, special attention should be given to the correct handing over of the exhibits. Particular attention should be given to the following aspects:

- Are all exhibits tagged?
- Are all exhibits labels filled out completely and correctly?
- Is the exhibit register complete and correct?
- Is the chain of custody thoroughly documented?
- Are there any damages to the exhibits? If so, have they been documented?
- Are all security seals intact?
- All exhibits, including the internal storage media should be photographed.

An exemplary chain of custody record in included in Appendix G.

3.2.1 Acquisition of computer systems

In order to preserve the integrity of the original evidence, forensic imaging technicians and digital forensics analysts should acquire the storage media of a computer system in a forensically sound manner as described in this chapter. The aim of the acquisition of a computer system is to produce an identical copy or image of the original data without changing the original evidence. This forensic copy will then become the basis of all further steps in the forensic examination.

The acquisition process typically includes the following steps:

3.2.1.1 Exhibit handling

Electronic evidence, as with any other kind of evidence, must be handled carefully and in a manner that preserves its evidential value. This pertains not only to the physical integrity of an item or device, but also to the electronic data it contains. Certain types of electronic evidence will require special handling. Electronic evidence can be susceptible to damage or alteration from electromagnetic fields (such as those generated by static electricity, magnets, radio transmitters and other devices) and should be adequately protected. Such a protection should include but is not limited to wearing of antistatic wristbands, working in secured premises with access controls, storing evidence dry storage facilities, etc. More details on how to properly handle and store electronic evidence have already been mentioned in Chapter 4 of the Electronic Evidence Guide as well as Chapter 2 of this Guide.

3.2.1.2 Wiping imaging media

As the aim of the acquisition process is to produce a forensically sound copy/image of the computer's storage media the digital forensics analyst needs to ensure that this copy will be stored on a target medium which does not contain any other data that do not belong to the case being examined.

To avoid cross-contamination of the target copy/image with other data (e.g. from the examiner's files or from past cases) the medium that should hold the new copy or image has to be sterilised. This can be achieved by wiping (or overwriting) all data on the target medium.

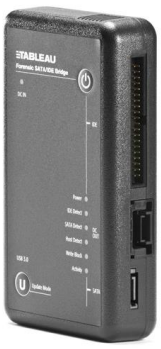
3.2.1.3 Write blocking

Analysing a computer device is similar to an investigator examining a physical crime scene in that evidence must be preserved intact, as close to the original condition as possible and free from contamination. While traditional crime scene investigators use gloves and overalls to avoid tampering with fingerprint and DNA evidence digital forensics examiners should safeguard the data integrity of the original storage media by using write-blocking mechanisms described in chapter 3.3.2.

Please note that using traditional write-blocking techniques it is not possible to avoid changes of data on a solid-state drive or flash-media which include a controller chip. As soon as the controller is attached to a power supply it will start to reorganise data on the flash chips. Techniques like wear-levelling, write-amplification and garbage collection are common tasks that are carried out by the controller even when attached to a write-blocking device. The only yet resource-intensive way to create a true forensic copy of flash-media is by disordering the chip(s) from the circuit board and then reassembles the data in the correct way where possible.

3.2.1.4 Hardware and software

There are typically two types of write-blocking methods; hardware write-blockers on the one hand side and software write-blockers on the other. Hardware write-blockers are typically available in two different varieties; write-blocking devices which are connected to a forensic workstation or imaging server or write-blocked disk duplicators which image onto an attached storage medium while not being connected to a computer system. Wherever possible hardware based write-blockers or disk duplicators should be used because they physically block write transactions to the exhibit and work very reliable in doing so.



Software write-blockers typically involve any combination of the following techniques:

- avoid mounting a file system
- mount a file system read-only
- change the operating systems parameters for handling external storage devices
- install their own drivers and background services

Software write-blockers are often used in forensic boot-DVDs where they are needed because there might be no way to physically get hold of the storage media of a computer system and attach it to a hard ware write-blocking device (e.g. flash media might be soldered onto the mainboard of Ultrabooks).

Depending on the techniques used some software write-blockers might not block write attempts to the disk under any circumstances (e.g. some techniques do not stop a corrupt file system from being repaired).

3.2.1.5 Imaging process

The imaging of a storage medium can be done using specialised imaging software. There are free as well as commercial products available which can aid in that process. Reliable and fast software should be chosen which can produce a bit-by-bit copy or an image in one of the forensic image formats (see section 3.2.1.7) and is able to verify the copy (see section 3.2.1.8).

The imaging software can include features like:

- recognition of hidden area (see below)
- imaging multiple devices simultaneously
- imaging to multiple destinations at the same time
- 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 to hardware errors

Finally, as part of the data integrity principle, an experienced examiner should always be alert to the possibility of anti-forensic techniques. Hidden areas like host-protected areas (HPA) or device configuration overlay (DCO), which are only addressable via special ATA commands can be recognised be some of the imaging software's.

3.2.1.6 Physical vs. logical copy

There are two types of copies; a physical and a logical one. While a physical copy includes all raw data, a logical copy typically only includes an allocated subset of all that data. On disk level for example a physical copy includes the whole disk including the partitioning scheme, all partitions and even unpartitioned areas while a logical copy on disk level is just a copy of one logical partition.

A digital forensic analyst should typically aim for a full physical copy of a whole disk because it includes deleted and formerly allocated areas. However, when dealing with encryption a logical copy of the unlocked data is preferred to a physical copy of the encrypted data. There can also be situations during a search and seizure operation where creating a physical copy might not be possible, out-of-scope or simply not covered by the warrant or other authority.

Both, the physical and the logical copy can be written in different ways. Either they are cloned, which means that the data is directly copied bit-by-bit from one storage medium to another, or they are written as an image file, which means that all data is copied bit-by-bit from one storage medium into one or more image files on a target medium. The latter technique is the more common one as writing the data into an image file offers some advantages as laid out in the following chapter.

3.2.1.7 Forensic image formats

Besides a raw image (raw/dd) that contains all data of the original medium within a raw file there are a few commonly accepted forensic image formats available. Those forensic imaging formats have in common that they are not able to be easily manipulated due to built-in checksums and case metadata. The most common formats are the Expert Witness Format (EWF(x)/E(x)01) and the Advanced Forensic Format (AFF). They include features like:

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

In addition to that, different forensic software solutions come with their own propitiatory image formats with similar features. However, a forensic image format should be chosen that is supported by the largest variety of software.

Special attention should be given to the image format when the image is to be analysed in a different forensic laboratory which might use different forensic software. This is especially important when the investigation involves multiple jurisdictions.

3.2.1.8 Verification / hashing

In the later stages of the digital forensics process all further processing and analysis is typically conducted on the forensic copy of the data. That is why it is crucial to verify that the original storage medium and the copy contain exactly the same data. In order to prove this a mathematical algorithm should be applied to both data sets. This algorithm produces a very complex number called a hash value. If the hash value for both files/devices is the same, then the files/devices are deemed to be identical. The slightest change will result in a large difference in the hash value. The

most commonly used hash algorithms are MD5, SHA-1 and SHA-256. Since single hash algorithms can be subject to hash collisions it is advised to use at least two hash algorithms to verify the copy/image.

It is good practise that hash verifications are done at two points at the imaging process. The first hash calculation should be done at the beginning of the imaging process in order to produce the hash value of the original medium. The second hash calculation should be done at the end of the imaging process. This second calculation should be done on both the original medium as well as the copy/image in order to prove that a) the data on the original medium has not changed during the imaging process and b) the data on the copy/image is exactly the same as on the original. In the forensic imaging formats the calculated hash sum is typically stored in the metadata area of the image. It can then be used in the later stages of the analysis to verify that the data in the image that is to be analysed is still the same as the data that has been acquired.

Even if the hash based verification returns a positive result, the digital forensics analyst should still pre-examine the data to ensure it looks authentic and does not exhibit any traits suggesting that the data may have been modified or tampered with before or during the imaging process. Devices can be self-encrypted or they can have a layer of protection that only allows communication when the device is attached to a certain trusted platform. Imaging such devices can produce a valid hash-verification even though the data that have been copied are not usable for a forensic analysis.

Please note that hash verification for solid-state drives and flash-media that has its own controller will most likely fail because the controller of the medium might have changed the data while connected to a power supply.

3.2.1.9 Copy storage / archiving / data retention

A forensic laboratory needs to have a storage facility to store backups of the forensic copies/images. It is good practice to not only have one backup but also another off-site backup. While the digital forensic analyst is conducting the analysis with his working copy of the image there should still be a backup stored on another system (e.g. an imaging server).

3.2.2 Acquisition of mobile devices

As with computer-based examinations, the aim during the acquisition of mobile devices is to produce the best possible copy, or image, of data stored on the mobile device. With mobile devices however, it may not be possible to make a full, exact copy of the original data due to the device's own limitations and limitations of available forensic solutions. It may be that in order to acquire the best image of a mobile device possible, changes may have to be made to the device to allow for the acquisition process.

The acquisition process typically includes the following steps:

Prosecutor's considerations

Mobile device acquisition and subsequent steps can present a legal challenge since mobile devices are, in the majority of the cases, mobile communication devices (e.g. smart phones). Depending on jurisdictions, different countries and their criminal law systems may impose additional rules when it comes to the above mentioned steps, especially the processing and analysis. Thus, there is a probability that additional legal instruments are needed to get permission to implement this procedure. Forensic experts should be aware of this and, when in doubt, consult with the authority leading the investigation, which is in most cases the prosecution service.

3.2.2.1 Exhibit Handling

Forensic officers must use extra care when handling mobile devices, as they contain batteries and can easily be powered on accidentally. This is likely to change evidential data in the process, such as time and date information for last use. Experts should pay special attention during initial handling to identify power buttons and to provide network isolation at all times.

The 'Isolation' phase is essential, as many devices require acquisitions to be conducted when it is 'Live.' This means that the examiner will be required to power the device on in order to use the device functioning throughout the acquisition. If the mobile device is not isolated and allowed to connect to external networks, such as the relevant mobile network or a wireless Internet connection, data may be changed on the device. One example is that it is possible to remotely wipe some mobile devices.

Isolation can be achieved through different forms:

- **Production of a 'Laboratory SIM/IDEN card'** – a SIM/IDEN card that appears to the device as the original SIM/IDEN card but lacks the capability to actually connect to the mobile network. A Subscriber Identity Module (SIM) / Integrated Digital Enhanced Network (IDEN) identifies the subscriber to the network which the mobile device wishes to connect to
- **Acquisition in a network shielded room** – a dedicated laboratory with Faraday shielding installed to prevent network isolation.
- **Use of wireless jamming equipment** – equipment can be acquired that can jam and prevent wireless signals from reaching the exhibit. These devices are illegal in some

jurisdictions.

The best method will depend on local laws, laboratory set up and on the device being examined. Consideration should also be applied to prevent connection to Wi-Fi and Bluetooth signals.

Before proceeding with acquiring the mobile device exhibit, it must be identified. The device will often have an equipment label affixed to the inside of the handset, if it is a mobile telephone, or printed on the back of the device. The label will include an International Mobile Equipment Identify Number (IMEI), a Mobile Equipment Identity Number (MEID) or Serial Number. This data can be used to uniquely identify the devices and is important for requesting billing records or conducting cell site analysis later. The make, model and IMEI/MEID can then be used to look up the device using your forensic packages to determine what level of support is available (for information regarding the different levels of support, see chapter 3.2.2.6).

Also at this stage, a review of the case paperwork supplied with the exhibit from the officer in charge should be undertaken to ascertain what evidence is required from the device. This can help the examiner make a decision in regards to what level of examination should be undertaken, i.e. if deleted data is required then a physical examination should be sort for. An attempt should also be made to gather any known passcodes, passwords or patterns from the device's owner prior to the full examination. This will ensure that no matter what level of support is available for the device, at least access can be granted to the data that is live and accessible to the user.

Once this information has been gathered, the forensic examiner should draw up a plan of action as to how they are going to examine the device and any associated additional media cards, i.e. SIM/IDEN cards or memory cards. This plan should include the acquisition of data from the SIM / IDEN card(s) and memory card(s) (if applicable) and what level of exam is going to be undertaken and why. The examiner should also plan a second level of exam in case the first level of exam is not successful due to various difficulties, i.e. a broken or ineffective power button (see chapter 3.2.2.6 for levels of examination).

3.2.2.2 Wiping imaging media / sterilising / cross-contamination

When producing images of the mobile devices, it is considered best practice to use a clean target medium, which does not contain any data relating to any previously examined exhibits. If using laboratory or cloned SIM cards, examiners must ensure that the laboratory SIM card contains the data from the last inserted SIM card.

3.2.2.3 Write blocking

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. Where possible write-blocking should be implemented, for example the extraction of memory cards, however it is widely acknowledged that this is not always possible or practical when working with 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 these actions in a coherent fashion.

3.2.2.4 Acquisition process

It is important that, at all stages of an examination, the mobile device under scrutiny is isolated from all external connections. This prevents the device from altering any stored data. A number of modern devices have the capacity to be remotely (and securely) wiped. Isolating the devices will help to prevent this from happening.

Mobile devices are presented with three distinct media that require separate handling and investigation techniques:

- SIM / IDEN Cards – Requires specialist mobile phone forensic tools and equipment.
- Memory Cards – Can be examined as a computer hard disk or flash drive.
- Device's Internal Memory – Requires specialist forensic tools and software.

The necessary forensic tools must be provided to the laboratory along with adequate hardware to support acquisition of these devices and examination of the data.

At this stage, the logical acquisition of the SIM/IDEN card and physical acquisition of the memory card should be undertaken. A physical examination is not possible for a SIM/IDEN card. This should always be carried out prior to the examination of the device itself. The memory card should only be returned to the device after it has been examined. This is due to some handsets having data stored on the memory card and if the memory card is not present, this could cause data loss from the handset. If time and resources allow, a bit-to-bit clone of the memory card should be created and that clone inserted into the handset. It is good practice that the SIM/IDEN card found in the device should remain outside of the exhibit for the duration of the examination so as to isolate the device from the mobile network. However, the majority of devices which contain SIM/IDEN cards require it to be present within them when they are powered on or they are susceptible to data loss. To combat this, a laboratory or cloned SIM/IDEN is created and used within the device so that the device notes the presence of a SIM/IDEN card, but yet is still not able to communicate with any mobile networks (for further isolation methods, see chapter 3.2.2.1). It is worth noting, if a device used an IDEN card, it is often necessary to further isolate the device with a Faraday Shield, especially if IDEN devices are common.

At this stage, if the device is supported by forensic solutions for a boot loader physical examination, this should be carried out. Often this can be carried out without the need for a SIM/IDEN card. This will allow the forensic solution to upload a boot loader to the device and boot the device in a particular way, which will allow for the full acquisition of the device's internal memory without making any changes or alterations to the user data on the device. A physical examination of this nature can also potentially recover any device lock codes, such as PINs or patterns, which will allow the forensic examiner to gain full access to the device once it has been powered on.

If the device being examined is not supported for this type of examination, the device should be powered on whilst isolated from any networks. If user protection is encountered, and the PIN, password or pattern has not been provided alongside the device, the forensic examiner should

attempt the best level of examination possible whilst bypassing the protection. If this is not possible, the user's PIN, password or pattern will be required prior to examination. If the PIN, password or pattern is already known prior to examination, then this should be entered so that full access can be gained to the device. Again, the best level of examination should be undertaken to get the most data extracted out of the device. If obtaining the correct solution for the protection is not possible it may be necessary to attempt typical PINs or patterns in order to access the data. This is not without risk, as many devices will implement secure data destruction should the wrong code be attempted too many times. Commercial tools are available that can "Brute-Force" passcodes, guessing all possible combinations until the correct one is found. When guessing passcodes, it is best to build a dictionary of probable passcodes from known facts (such as birthdates or other passcodes) or from known common passcodes (such as 1234, 1379, 0000 etc).

Depending on the extraction tool available and chosen, the acquisition process will vary. Most tools have a guide explaining the procedure that must be followed to create a successful extraction. It is important at all stages to minimise the effect on the electronic evidence and to attempt to preserve the integrity of the data to the highest standard possible. It is important to consider that for some mobile devices it may be necessary to modify system files or the operating system, or in some cases upload and install a dedicated application in order to successfully extract data from the devices. This process can cause some data to be irrecoverably lost; this is normally only system files with little to no evidential value. The knowledge of what is altered by any of these processes can be demonstrated by holding appropriate training certifications, such as training provided by the manufacturers of mobile forensics software, or practical experience involving the testing of what data, if any, on the device is altered by making these system changes.

3.2.2.5 Hardware and software

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

3.2.2.6 Levels of examination

There are five different levels of examination for mobile devices, with the best possible extraction being listed first:

- Physical
- File System Dump (FSD)
- Logical
- Manual
- JTAG / Chip-Off / Rooting / Jail Breaking

A physical copy of the device is the process of acquiring all of the raw binary data from the storage of the device. This raw data then needs to be analysed and processed at a later stage by software.

This method typically will allow the examiner to access live and deleted data, operating system files and areas of the device that are not normally accessible to the user.

Mobile devices, unlike computer devices, have further acquisition strategies. The other main strategy is a File System Dump (FSD). An FSD is like a hybrid of a Physical and a Logical acquisition. FSDs retrieve the devices file system and interpret the data during the processing stage. This allows examiners to retrieve, for example, databases holding deleted messages that may not be available at a logical acquisition and may not be accessible during a physical acquisition. However, not all deleted data that it would be possible to retrieve with a physical acquisition would be acquired during an FSD.

A logical acquisition of the mobile device will involve receiving information from the 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 typically will only make live data available to the examiner. If no other method is available, a method termed "manual examination" can be used. This method involves accessing the device and recording the data displayed on the screen, with photographs, video recording or transcribing the data. Care should be taken to ensure that data is not un-necessarily changed and information is recorded accurately. With this method, you can only recover the data which the mobile device displays, for example some mobile devices will not show full time and date information.

For mobile devices that are damaged or locked, two other methodologies can be utilised. These are JTAG and Chip-Off examinations. JTAG examination requires the stripping down of the device to the device's logical board and the soldering of connections to specified connections on the board. This enables the examiner to retrieve a full physical copy of the data stored on the device. A chip-off also allows the extraction of a full physical copy of the device, but requires the permanent removal of the device's memory chip from the memory board.

Another, less destructive modification that can be performed to some mobile devices is the process known as "Rooting" or "Jail Breaking" the device. This process involves leveraging features of the operating system to elevate the permissions of the running user (similar to the process of gaining "Root" access in a Linux computer). This process involves the modification of system files and can potentially damage the device and so should be low on the list of techniques leveraged.

The order of attempted extractions is important. Examiners should strive to conduct the examination method that is least destructive with the most yield first. 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 as, especially with Chip-Off, the process can be destructive and un-recoverable.

3.2.2.7 Forensic imaging formats

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

Another source of forensic evidence is a backup. Some users and devices will create backups of themselves on other devices, such as the subject's computer. These backups can assist in building a time line 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 the backups were a physical device. Allowing examiners to review data stored on a unusably damaged device or a device that cannot be accessed.

3.2.2.8 Verification / Hashing

Once the data has been extracted, this extracted data should be manually verified on the device. This will require the forensic examiner checking that the data that has been extracted by the forensic solution matches what is displayed on the device, such as the correct time/date information. This will identify any errors with the extracted data or if data is missing as often not all chat messages, such as Facebook Messenger chat threads, are extracted from the device. If there are any discrepancies then further extractions can be undertaken to try and acquire the missing or inaccurate data or a manual examination can be undertaken to manually record the data. Some additional data (like IMEI and application settings) are often best confirmed / acquired during this stage.

Once all the required data has been acquired from the device in an acceptable fashion, then the reports containing the desired data can be compiled and produced for the officer to review.

Prosecutor's considerations

Since the ultimate goal of a digital forensics process is to produce evidence to prove or disprove disputed facts, electronic evidence must be obtained in compliance with existing legislation and best practices to ensure admissibility at trials.

Compliance with the existing legal framework on cybercrime is of paramount importance and it does not include only well-known laws, acts, bills and regulations concerning criminal justice. It also includes other areas of legislation which, at a first glance, do not have much in common with criminal law.

Cybercrime is and will be an ever-growing area of criminality. New types of crime as well as traditional forms of crime increasingly take place in cyber space. If evidence is gathered without respect to criminal law rules and provisions, it may be dismissed.

The responsible prosecutor, and to a certain extent forensic managers and staff, must be aware not only of the applicable criminal law framework, but very often about laws and by-laws which are regulating telecommunications, service provider operations, information technology, as well as international law related to substantive criminal law, procedural law and mutual legal assistance. For example, grounds for the retention of data and rules for their acquisition for criminal investigation purposes are often stipulated by laws or acts on electronic communications.

3.3 Processing stage

During processing the forensic examiners may prioritise certain devices or data and will produce an exact copy or image of the content of any digital storage seized. Working on the duplicate (never the original) they can apply smart, case-specific filters (data mining) or they can just process the image (e.g. by recovering deleted files, mounting containers, breaking encryption, parsing application data like internet history, chat logs, etc.). Those processing steps are often times repeatable for specific categories of cases. Even though they are resource intensive needing a lot of computing power and time they can typically be run over-night, over the weekend or on a second forensic workstation that is not in use.

3.3.1 Processing of computer systems

Not only the number of computer systems per household and organisations, but also the amount of storage in these computer systems is rising. Managing large amount of data while keeping the backlog short is a big challenge for digital forensics laboratories. That is why different processing approaching should be considered.

3.3.1.1 Case-specific considerations

Before analysing a case it is important to ask the case officer what type of data is needed for this case. The information provided should include a scope of which data are relevant and which data can be filtered out. Based on that information the analyst can consider which processing options might be applicable. Depending on the case and the warrant it should also be considered which data might be subject to data protection, legally privilege or some other form of access restriction, for example journalistic material.

3.3.1.2 Triaging techniques

In cases that involve lots of computer systems and storage media it might not be possible for the digital forensics lab to analyses each and every exhibit within a reasonable amount of time. That is when a triaging technique could help. It can also be one model used in the digital forensic process to find out quickly which computer seems most promising to analyse.

Triage in the digital forensics context is the process by which cases or activities are prioritised to determine which case, which exhibit and which type to data are to be examined firstly, secondly, etc. This process can include the possibility that some exhibits or data are not examined at all (exclusive triage) or that some data will just be analysed at a later stage (prioritising triage). Triage considers the value of investigating, the complexity, the cost and the order in which the investigation should be accomplished.

While triaging offers some advantages there are also disadvantages that need to be addressed. A triage cannot replace a full examination. That is why triage should not be used on a daily basis. Using only automated techniques to retrieve evidence and/or only examining a small sub-set of all data comes with the risk to miss evidence. Those disadvantages need to be explained to the investigator, prosecutor or judge and based on that information they need to decide in favour or against the triaging process for that particular case.

However, triage remains a valid method in order to cope with a situation that could not be solved in any other way. Examples for such situations include:

- a huge amount of exhibits to be analysed in a very short time frame
- exhibits cannot be stored any longer because of legal issues
- getting information as quickly as possible is of highest priority (e.g. in terrorist cases)

A triaging process is typically conducted by booting up several exhibits at the same time using a forensic boot medium. The medium should ideally be configured to run several pre-defined tasks (e.g. search for child abuse material using hash comparison, other tasks see chapter 3.3.1.4) automatically without the need for the examiner to observe the process. It should then write the report with its' findings to an attached USB medium. This way a forensic examiner can process multiple exhibits at the same time, even overnight or on weekends. The analyst can concentrate his/her resources on the setup of the triaging process for the exhibits and can view the reports of previously processed computers while the new chunk of exhibits is being processed by the triage boot medium automatically.

3.3.1.3 Prioritisation of data

Prioritisation of data can be seen in close conjunction with triage. While due to time constrains or limited resources triaging excludes the analysis of each and every piece of evidence, priorisation would still allow analysis of all exhibits. It would however start with more relevant exhibits to see whether this might contain enough evidence for a conviction or acquittal. Examples for a prioritisation would be to analyze:

- the main suspect's computer before witness’s PC,
- urgent cases / high profile cases before low profile cases,
- encrypted data before unencrypted data, and
- certain data types (e.g. documents, emails) before others.

3.3.1.4 Automated processing

Automated processing is an important part of a digital forensic analysis. The scope of the automated processing is set by the forensic analyst in the beginning of the analysis. The steps are often times repeatable for specific categories of cases. Even though they are resource intensive needing a lot of computing power and time they can typically be run over-night, over the weekend or on a second forensic workstation that is not in use.

The automated processing includes tasks like:

- mounting of containers (e.g. ZIP, RAR, etc)
- extraction and parsing of various artefacts (e.g. mailboxes, internet history, etc)
- signature analysis

- recovering deleted files and folders
- recovering deleted partitions
- carving for certain file types
- indexing of keywords
- OCR of PDF files
- creation of thumbnail pictures for quicker viewing by the analyst
- extracting pictures from videos
- skin-tone detection for videos
- hash comparison (see chapter 3.3.1.6)

While a streamlined approach is possible it is not necessary in all cases.

3.3.1.5 Data recovery

Recovering deleted data can be essential if no evidential files have been found in the allocated areas of the disk. Data recovery is possible on different levels. First of all the forensic analyst should check whether all partitions of a disk are shown in the forensic software or if there are any notable partition gaps. Those gaps should be scanned for additional partitions. The next step is to undelete files and folders from a file system. After that, additional files can be recovered by scanning the unallocated areas for known file headers and footers (carving).

3.3.1.6 Filtering techniques

Applying filters to an image before it is being analysed can help to reduce the amount of data that the forensic analyst has to view and analyses. Popular filtering techniques are using hash sets to either filter out known operating system or program files (whitelisting) or to specifically search for hash matches with databases of known illegal materials (blacklisting).

Filtering can also be applied when only certain types of traces are relevant for the case. Files can be filtered by signature analysis, by size, by date, by owner, etc.

3.3.2 Processing of mobile devices

As with the processing of computer exhibits, the number and storage capacity of mobile phones per household is increasing. Along with this increase, the added functionality and reliance on mobile devices leads to a wealth of data available for forensic analysis. Examples of this data are locations and communication logs.

3.3.2.1 Automated processing

The processing of mobile devices often requires a different approach to computers due to the wildly 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.

3.3.2.2 Filtering techniques

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, such as sent and received SMS messages and call records to establish contact between suspects.

Prosecutor's considerations

The processing stage can be of vital importance to the prosecution. Although technical data (evidence) is very much needed, one should not forget that the complete picture of the case is and should be with prosecutor during the investigation phase. Forensic expert staff in the laboratory may or may not be acquainted with legal requirements, or may or may not be part of the law enforcement. The prosecutor, on the other hand, more often would not be specialised in questions of information and communication technologies.

Therefore, the prosecutor should, if necessary, consult directly with the laboratory already for provisional findings. The laboratory staff, police and prosecutors will should cooperate to discover and understand the full picture of the case.

Often prosecutors will not have enough time to take this approach because of everyday routines. Nevertheless, especially in more complex cases and in cases of higher public importance, prosecutors will need to be closely involved and closely lead forensic investigations within the limits of the law.

Prosecutors must be aware that given the equality of arms the defence will be examining forensic findings, including provisional conclusions, which may be challenged thoroughly at the trial stage.

3.4 Analysis stage

During the analysis phase the examiner actually searches for electronic evidence on the images. This step 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. A lot of different factors have an influence on the time and workload that is needed for the analysis phase. Those 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 usage of the operating system, the sophistication of the user, complexity of software and techniques being used by the computer user, etc.

3.4.1 Analysing computer systems

Computer systems are used by humans for all sorts of activities: writing documents, accounting, surfing the internet, chatting, writing e-mails, gaming, viewing and editing images and videos and so on. That is why they can hold a lot of evidential data. Analysing a computer system, the digital forensic analyst can typically not only find traces in relation to the case but could potentially also find evidence regarding the intention of a perpetrator (e.g. by finding internet searches on how to commit the crime).

3.4.1.1 Categories of digital traces

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".

To get a better idea of the kinds of digital traces that an examiner might discover during forensic analysis, it makes sense to distinguish between two types of digital traces:

Avoidable traces: These are traces that are stored by the operation system and applications by default, but which a system can be configured not to store. Take a web browser as an example. This software will store a suspect's browsing history as well as details of his or her downloads, form inputs, cookies, etc., but it can either be disabled or deleted by the suspect. Another example can be the "Start" menu and the suspect's Office programs that 'remember' which files the suspect has opened recently. There are various types of 'avoidable' traces automatically stored on the hard disk in this way (as shown in the table below). However, they can be prevented by someone who knows what they are doing.

Unavoidable traces: By contrast, unavoidable traces are, of course, those that cannot be disabled or those that require considerable effort to stop temporarily. The probability of finding such traces is correspondingly high even if a suspect has tried to cover his or her tracks.

The following table lists some examples for avoidable and unavoidable traces:

Avoidable traces	Unavoidable traces
Thumb caches	**Slacks**
Most recently used lists	**Unallocated space**
Log files	**MFT entries**
Browser histories	**RAM**
Browser caches	**Some application traces**
Most Used programs	
Form Data	
Pagefile.sys	
Hiberfil.sys	
Volume shadow copies	
…	

3.4.1.2 Procedures for different traces

Every case typically involves some particularly relevant traces. In a fraud case for example documents, spreadsheets and e-mails are typically more relevant while in child-abuse cases pictures, videos and communication traces are more relevant. But even within those categories of cases not every case is the same. That is why the following subchapters included information on procedures based on the type of type that is relevant rather than the type of case.

3.4.1.2.1 E-Mails

To analyse e-mail communication it is not only important to analyse mail clients like Outlook, Thunderbird or Mail but also webmail accounts. The former will be covered in this subchapter while the latter will be covered in section 3.4.1.2.4.

In order to analyse an e-mail client it is important to know which artefact that e-mail client produces. Outlook for example stores evidential data in personal folder files such as PST, OST and PAB files while Thunderbird stores messages in mbox files. The forensic software suites can usually parse those files. However, they do not necessarily extract all messages. Some forensic tools, for example, have problems extracting deleted messages from personal folder files.

3.4.1.2.2 Office documents

In cases in which office documents are of importance the digital forensics analyst should conduct a signature analysis and then afterwards filter for the files of interest (e.g. files with a docx signature). When the forensic analyst has found those files it is good practice depending on the policies of the office to extract all of those files and hand it over to the case investigator for a content analysis. When the case officer has identified the relevant documents the forensic analyst

can search for further evidence of when those documents have been produced, by which user they have been produced and whether they have been sent or received by other persons.

3.4.1.2.3 Pictures / videos

Most forensics software solutions offer support for analysing masses of pictures and videos. After an initial file signature analysis and setting a filter for pictures and video files, the forensics analyst can use a gallery view to inspect the thumbnails of all pictures for case relevant evidence. For a faster analysis of video files certain software offers the feature of extracting still pictures from the videos (e.g. every X seconds/minutes depending on the settings). These extracted images can then be viewed in a gallery view as well.

If the case requires searching for a set of known pictures (e.g. child abuse material or stolen blueprints, etc), hash comparison can be used to accomplish this task. There are even techniques available that enable searching for similar pictures with another hash value (fuzzy hashing, similarity hashes, PhotoDNA, etc.).

In cases where location data or production details of pictures and video files are important the analyst should consider extracting meta-data (e.g. exif data) for those files. In fact analysing meta data and putting evidence into context in the major task for the forensic analyst in cases that involve pictures or videos as evidence. The simple task of viewing the contents of the pictures/videos does not require any digital forensic expertise and could thus be done by responsible case investigator. Besides that the categorisation of images or further investigation may be carried out by the investigating officer if facilities are supplied.

3.4.1.2.4 Internet browser

Internet browsers are of evidential value for a lot of cases. They typically contain the following artefacts which need to be analysed:

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

Analysing browser artefacts can be important for suggesting purpose or intent (e.g. keywords used in search engines could prove intent). That is why those artefacts should be analysed in most cases.

The most popular browsers are Google Chrome, Microsoft Internet Explorer / Edge, Mozilla Firefox and Apple Safari. All of them store their data in all operating systems within the user home directory. Except for the Microsoft browsers they all use SQLite databases to store the artefacts mentioned above.

Even though most forensic software can parse these browser artefacts to some extent, they differ quite a lot in a) which versions of the browsers they can parse and b) which detail of information they can extract from each browser artefact. This is why it is important for the forensic examiner to understand the underlying structure of those artefacts. Most browsers nowadays work on the basis of SQLite databases. The forensic examiner should search for those artefacts and parse them manually using SQLite database browsers. This ability not only makes him/her independent of particular tools or the wait for updates to those tools but also allows him/her to create their own reports and to cross-check the result of the tools.

3.4.1.2.5 Software artefacts

Whenever certain software can add evidential value to the case, the artefacts of those programs need to be analysed. Examples of such software include communication software (e.g. Skype), steganography software (e.g. OpenStego), password safes (e.g. KeePass), file sharing software (e.g. uTorrent), crypto currency software (e.g. Bitcoin wallet), etc. It is not possible to describe procedures how to analyze all potential software. The basic approach is to research trusted sources for information on how to analyses that particular software. In a next step the findings and the interpretation of the data need to be verified

3.4.1.2.6 User activity

The operating system of a computer tracks user activity at many different places. Examples for that include:

- power on and shutdown times
- software settings
- most recently used files lists
- device usage
- user logins
- Wi-Fi connections
- preferred programs
- setup of user environment
- and many more.

Analysing this user activity helps getting a better understand of the user behavior and can even prove evidential activities. Depending on the operating system that has been used on the computer those artefacts are stored in various locations. In Microsoft Windows the Registry, Event Logs,

JumpLists and several other files need to be analysed by the examiner. On OS X systems the analyst will find most of the evidence in the Library and log folders while on Linux systems most of the data will wither be stored in the user home folder, the "/etc" and the "/var" directories.

3.4.1.2.7 Log files

Analysing log files is essential particularly in cases of attacks against systems. Digital forensics analyst should extract not only allocated log files but also traces of deleted/unallocated log files. Specialised software is available for log file analysis. The basis of such an analysis is to either search for particular keywords, to search for abnormal pattern or to search the logs that fall within a set time frame.

3.4.1.2.8 Encryption

All operating systems are offering built-in encryption facilities nowadays. It is easy for the user to activate a full disk encryption for a system drive. If possible passwords or encryption keys should either be obtained by the suspect or should be acquired by using live data forensics on scene. 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 specialised password cracking techniques.

3.4.1.2.9 Unallocated areas

Unallocated areas can contain artefacts of all of the types of evidence mentioned above. Searching and extracting of certain file types in unallocated areas can be automated by carving software. Digital forensics analysts should precisely 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 times data found in unallocated areas cannot be an associated with a certain user or even a location within a folder structure.

3.4.1.2.10 Cloud/remote storage

In situations where the forensic analysts finds traces of cloud services being used on a computer system this might mean that evidential data might not only be stored on that machine but also on a remote storage. In fact the data that is remotely stored might not just be stored on a single physical computer, but on multiple servers in the cloud. Most of the time, even the provider of a cloud service cannot tell on which particular server, in which data-centre, and which country certain parts of the data are stored.

The forensic analyst could even find situations where not a single byte of data can be retrieved from a company’s computers because they will merely be client computers without any storage media of their own, but using the resources of a virtual machine in the cloud. The advantage with this is that, technically, the virtual machine can be easily copied. Depending on the relevant and applicable legislation, however, identifying and obtaining the appropriate legal authorisation for intercepting such data might be a problem. 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 are likely to be far less recoverable data available to find. Indeed if a suspect were to create a temporary virtual machine for committing his or her crimes and then to delete that machine, there might be no evidence at all to recover.

The possibility to acquire and analyse data that is remotely stored is highly depending on the legislation and jurisdiction. In some jurisdictions for example the forensic analyst - under certain circumstances - is allowed to connect to the remote storage using the suspect's credentials from the computer in order to acquire the data from the cloud provider. Other jurisdictions will not accept such an acquisition. In those cases the official channels can be used in order to request preservation and access to the data from the provider.

3.4.1.2.11 Computer Memory (RAM)

When computer memory has been acquired while the seized computer was still running (as described in chapter 3.5 of the Electronic Evidence Guide), the memory dump can be analysed in the forensics laboratory.

Understanding memory structures of different operating systems in order to analyse RAM is a highly technical task. That is why it should only be done by examiners who are qualified for this work. Specialised software is requited to analyse RAM dumps. Examples for such software include "Volatility" and "Rekall". Typical artefacts that can be extracted from RAM dumps include:

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

3.4.1.3 Virtualisation

A picture is worth a thousand words - this is particularly true for virtualisation. The forensic analyst can view the operating system environment from a suspect's computer 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 data traces from the file system.

The forensic analyst should ensure that the image is mounted write-protect with a write cache allowing the virtual operating system to write log files and changes to that write cache without affecting the integrity of the image. Some operating systems refuse to start in virtual environments. This can typically be solved by replacing drivers and adapting configurations, using software like OpenGates and OpenJobs. Should the virtual operating system start with a password prompt the forensic analyst needs to either crack that password or blank it.

3.4.1.4 Process for handling mass data

Some cases involve lots of computer systems and storage media while the workload for the forensic laboratories is already very high. A separation between forensic analysis and content

analysis can spread the work more evenly between the digital forensics analysts and the case investigators. The forensic analysts can concentrate on recovering, parsing, mounting and processing of exhibits while the content analysis is being done by investigators with case knowledge. A process needs to be in place and the software and overhanding techniques supporting this process need to be in place (e.g. container file provided by forensic analyst to investigator, viewer component to be used by investigator, handing back the finding to the forensic analyst).

3.4.1.5 Visualisation aids

For aiding in visualisation of complex data structures, visualisation aids can be helpful. Examples for those aids are:

- Timelines: Indicating the behaviour of the user: When did the suspect log in, when did he connect a certain medium, when did he connect to which wireless lan, when did he view which website, etc.
- Relationship diagrams: Can give answers to the questions: Who has met whom at which point of time using which medium? Which information was sent/received? Who knows whom? Who is the main suspect who coordinated the others?
- Moneyflow diagrams: Can help to understand at which point of time which amount of money has been sent over which channel by which persons.
- Communication diagrams: Similar to a relationshop diagram but does not necessarily involve persons. It could show how often which IP addresses attacked a server from which country.

Graphical representations make it easier to understand the correlation between the data. They can also enable the investigator to find new links. Typically the basis for such diagrams are raw data which are stored in a structured way, e.g. csv/tsv files. Those files are loaded into specialised commercial or some free software. On Linux for example simple commands like awk, sort, uniq used in conjunction with Graphviz or dot can help drawing graphical representations.

3.4.2 Analysing mobile devices

Mobile devices contain records and logs of communications, along with times and dates of said communications. In addition to this, mobile devices will also contain media files and location data that can be utilised in an investigation.

3.4.2.1 Categories of digital traces

Digital traces found on mobile devices can be split into three distinct 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. Meta data on media files captured with a mobile phone, for example, is likely to contain geo-tags or other useful location data embedded within the file itself.

3.4.2.2 Procedures for different traces

3.4.2.2.1 Contacts

Contact lists make up the backbone of mobile phone usage. Care should be taken to cross-reference other artifacts of data back to contact lists to help identify subjects for investigation. Contacts can include other communication channels, identity information as well as pictures to assist in the identification of individuals. Contacts can also help to identify association between subjects and potentially identify how long such an association has been in place from the created dates of contacts.

3.4.2.2.2 Call logs

Call records often carry date/time stamps generated from the handsets internal clock. This can make recovered time/date stamps for call records unreliable. It is often best practice to obtain billing information from a mobile service provider to confirm time and date information for call records. This time stamp is obtained from the mobile service provider's servers and so can be considered accurate (or rather it is more likely to be accurate).

3.4.2.2.3 Application artifacts

Due to the amount of different applications and the multitude of application versions that are available, it is often necessary to analyse different artifacts unique to different applications. Many of these applications will, for example, store settings in database files. It may be the case that deleted database files are recovered and these can be used to ascertain the settings of an application at a given point in the past. Due to the closed nature of many applications and the lack of available information, it may often be necessary to obtain a test device and conduct some live research in order to identify the properties of some application artifacts.

3.4.2.2.4 E-mail messages

As with computer examinations, e-mail communications on mobile devices can be used within default Mail applications and through web mail accessed through the internet browser. On some devices, such as newer Apple iPhones, the extraction of email messages from the default Mail application is not supported. In these cases the examiner will have to manually record the data or attempt to gather this data from other sources.

3.4.2.2.5 Web history

Internet browsers on mobile devices typically store the following information that potentially has evidential value:

- Web history entries
- Web page visit counts
- Bookmarks / favorites
- Cookies

The majority of this information, such as visit counts and cookies, are not accessible on most devices.

Prosecutor's considerations

The analysis stage is of the vital importance for the identification and acquisition of evidence used for the investigation and trial phases of criminal proceedings. One of the most important things to be considered should be cataloguing of the steps and evidence which is gathered and secured.

Often evidence will be present in great numbers and their bulleting and listing can be time consuming. Nevertheless, one must be persistent in this process having in mind that this approach will lead to a logical explanation of the chain of evidence and the criminal act itself.

The interpretation of the evidence must be taken very seriously and its importance well understood. Forensic staff must be aware they will be summoned by the court and be in a position to explain their procedures and findings in detail; their statements will be examined both by the prosecution and defence, and, depending on the system, by the judiciary. This situation can be of crucial importance for the success or failure of the case and it must be taken seriously.

The analysis of the evidence should lead to clear and logical conclusions which should be able to sustain significant examination during the trial.

3.5 Presentation stage

After evidence has been found in the analysis stage, the examiner needs to create a report for the trial. The examiner's job is to illustrate and to 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.

3.5.1 Admissibility of electronic evidence

Although the details may differ from jurisdiction to jurisdiction (some might even not admit electronic evidence at all), the following criteria should generally be taken into account when evaluating electronic evidence for trial:

Authenticity: The evidence must establish facts in a way that cannot be disputed and is 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.

Believability: The evidence must be persuasive as to the facts it represents and the finders of fact in the court process must be able to rely on it as the truth.

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).

3.5.2 Report writing

The digital forensics report reflects all the procedures and outcomes of the steps that have been conducted before. It is the only one outcome of all the prior work and as such it is the key element for all other persons within the criminal justice system.

The nature of the report that it is being used in courts to help proving guilt or innocence of a person does not only make it an extremely important document but also causes some challenges for the forensic analyst. One of the biggest challenges is to make the report understandable for non-technical people. So a forensic report must be written in clear, understandable language and should have a summary indication in a compact format what has been found during the examination. All technical details can be listed in an appendix. It is important that the digital forensics analyst does not state something in the report that he cannot prove, e.g. "The suspect has done A, B, C"; it is only possible to state "With this computer, at this point of time, using user account XY, file A has been created, USB thumb drive B has been attached and in inbox of webmail account C has been visited."

A digital forensics report should consist of the following main chapters:

1. Information about the request and the mandate
2. Information about the exhibits
3. Information about the examination methods (persons/software/hardware)
4. Acquisition process
5. Analysis process
6. Result

An exemplary layout of a report has been attached to this document in appendix J.

In the digital forensics laboratory it should be clearly defined who is responsible for the report and who will be delivering the evidence in court. Typically that is the same person who's name is on the report and who signed it. In addition to that quality assurance measures should be followed before the report is completed and submitted.

3.5.3 Expert witness status

An expert witness, professional witness or judicial expert is a witness, who by virtue of education, training, skill, or experience, is believed to have expertise and specialised knowledge in a particular

subject beyond that of the average person, sufficient that others may officially and legally rely upon the witness's specialised (scientific, technical or other) opinion about an evidence or fact issue within the scope of his expertise, referred to as the expert opinion, as an assistance to the fact-finder. 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 has a more long lasting status, by virtue of appointment as, for example a court expert.[3]

Evidence involving complex issues of science and technology plays an increasing role in litigation. That is why some countries and courts maintain lists of appointed experts. Appointing an expert is often suggested as a means for the court to enhance its ability to deal with such issues.[4]

The rights and duties of an expert witness typically differ from country to country. It is important for the digital forensics analysts to make themselves familiar with their legislation, their court procedures, their role and their rights and duties in that role.

3.5.4 Alternative presentation methods

Some courts allow the usage of alternative presentation methods. Those can include explanatory media such as live demonstrations on computers with projectors, virtual machines, etc. If wanted, accepted and necessary, it is vital to discuss those possibilities with the judge before the hearing. It is also very important to be confident in the usage of those techniques and to have tested them before the hearing.

3 https://en.wikipedia.org/wiki/Expert_witness

4 http://www.fjc.gov/public/pdf.nsf/lookup/13.expert.pdf/$File/13.expert.pdf

Prosecutor's considerations

If the aim of the investigation was two-fold, to obtain all existing and qualitative evidence with regard to the case and to be able to reproduce and explain forensic procedures which led to the acquisition, the trial phase is the one confirming the quality or lack of quality of the acquired evidence.

Admissibility of evidence represents the key outcome of the digital forensic process. Prosecutors and judges are becoming increasingly comfortable with the existence and admission of such electronic evidence. In some jurisdictions, not only is it that electronic evidence is explicitly allowed by the criminal justice, but there are references and definitions of computers, computer networks, software, hardware and data in substantive and procedural parts of the legal framework. Also, in some jurisdictions, computer data is defined as a movable object, to which all legal rules for tangible items can apply (destruction, alteration, theft, alienation, exchange, etc.).

Some legal opinions about electronic evidence may consider it non-usable because of the possibility of alteration and forgery. Under this logic, any other evidence could be questioned as well. Forgeries of paper documents are widespread. Fingerprint forgery, alteration of photographic, video and audio materials is common. In that sense, electronic evidence should not be regarded as more volatile or unreliable, especially having in mind that as society, industry and technology advance, more and more of traces, facts and evidence will exist in digital form. Therefore, admissibility of electronic evidence as real evidence should not represent an issue for prosecutor or judiciary, provided that the procedures described in this Guide are followed.

The authenticity and reliability of electronic evidence must be ensured throughout the digital forensics process. Forensic staff should have knowledge or/and pay attention to the existence of an authentic search and seizure order (warrant) by a prosecutor or judge, records of searched and seized places, items and taken actions, acknowledgement (if applicable) of a suspect or person in possession of seized items, that records are authentic, and so forth. Photographic or video recordings from the place were a search was conducted and other documents and measures, if required by law, can also establish that understanding. Furthermore, the authenticity of electronic evidence is preserved only if digital forensic laboratory staff continue with actions which are carefully organised, executed and recorded.

Completeness of the evidence can also sometimes represent a difficult task, since some parts of the evidence can be missing due to different factors and reasons, including influence of the suspect and other persons involved in the actual case. On such occasions,

forensic staff should concentrate on best possible approach to existing items and their contents in order to extract the most comprehensive body of facts, without distortion or bias.

Credibility is closely connected to authenticity and reliability and must be ensured in writing. Written reports should provide clear explanations, logical connections and trustable outcomes of procedures and conclusions as a result of the process. The forensic examiner should always be aware that in case of court summoning, a verbal presentation of the findings and testing of the believability will most probably occur. In such a case, an examiner should possess thorough knowledge of the report, procedures and conclusions.

An examiner presenting and explaining findings in court or before the prosecution should have certain skills for verbal presentations. He/she must bear in mind that the judge and all parties present in the courtroom will carefully listen and follow not only the examiner's words, but his/her appearance and overall impression as well.

Of course, proportionality is expected. Any unauthorised intrusion or coercive measure will most certainly lead to the inadmissibility of evidence. Also, by following good practices of the rule of law, facts and evidence which are in favour of the defence should be presented and made available to the defence as well.

When it comes to report writing, it is of the outmost importance that the language is clear and understandable, but not diluted to the point where quality of the evidence will be lost. In most situations, defence attorneys will object to more complex language of the report and will try to advocate for additional examination for clarifying the initial report. This is one of the frequent techniques for prolonging the trial in cases when a prison sentence is expected. Any decision about this motion will be in the hands of the judge (rarely – prosecutors), and examiners should be ready such a development. In such a case, the content of the request should be carefully analysed and appropriate actions should be taken, without prejudice to the principal task of forensic analysis as requested by prosecutor or judge.

The forensic expert must take into account that not many prosecutors and even a smaller number of judges feel comfortable with cybercrime, electronic evidence, digital forensics reports and similare, and that in many cases the natural reaction is to reject the facts; in this case, such issues should be more thoroughly explained in person during the expert testimony. Forensic experts must be prepared and flexible on such occasions.

Te expert witness status will vary from country to country. In some systems, experts are engaged by the prosecution and defence, in some systems they are court-appointed, and there is number of mixed systems in which all parties and the court alike can appoint or hire expert at different stages of the proceedings.

However, it is a very likely scenario that expert witness coming from the forensics laboratory of the state authority will be engaged by the prosecution or court. This also

means that the defence is likely to engage expert witnesses of their own, who will challenge most, if not all, aspects of the expert examination. This kind of situation is becoming more and more frequent in courtrooms and forensic experts must be prepared for this.

Alternative presentation methods are depending on the technical facilities of the court but not only there. Plea bargaining and, in some countries, the growing popularity of "deferred prosecution" can lead to presentations in Prosecution Offices as well. Forensic experts must be aware that conditions for presentation are not always perfect. Many court and prosecution rooms are not equipped with hardware to support complex presentations. Expert must be prepared to present the same quality of evidence with less technical possibilities. Situations like this should be anticipated by the forensic laboratory and certified mobile equipment for such presentations can be a useful option.

In conclusion, the presentation stage should be a goal and outcome of all efforts of the forensic laboratory, examiners and support staff, and should always be on the mind of the personnel involved. The facts and evidence will serve the task for establishing the material or substantive truth, depending on the legal system. Thez will be used for the adjudication of the criminal case, for justice and for the compensation of victims.

The role and responsibility of digital forensic examiners are thus crucial for criminal justice.

4 Appendices

- Appendix A - Forensic software comparison matrix
- Appendix B - Exemplary device carrying case content
- Appendix C – Acquisition Process Flow Chart
- Appendix D – Processing Flow Chart
- Appendix E – Analysis Flow Chart
- Appendix F – Presentation Flow Chart
- Appendix G – Chain of custody record
- Appendix H – Image Acquisition Worksheet
- Appendix I – Digital Forensics Analysis Form / Spreadsheet
- Appendix J – Digital Forensics Report Template

Appendix A – Comparison of forensic software

All appendices in section A are templates and should aid laboratory managers to develop their own comparison matrix in order to make an educated decision about software, hardware and training purchases. In some tables, exemplary data are provided for better understanding. It is important to understand that each forensic laboratory might have its' own prerequisites, demands and maybe even legal framework (e.g. mandatory list of court-validated software). While one lab might have a majority of cases involving recovery of files and filesystems another lab might only have cases where large amounts of documents and e-mails might need to be analysed. While the first laboratory might choose one particular forensic software that suits their requirements (excellent data carving, file system support and recovery capabilities) the other laboratory might aim for another solution that fits their demands better. There cannot be one definite recommendation for a specific software that is the universal best solution for all digital forensic laboratories.

Please remember that results from each individual software should be double-checked. The ideal situation is that the results are double-checked by manually analysing the raw data. Depending on the data and on the knowledge of the examiner this might not be possible in any case. In this case the results of the first tool should be checked against the results of a second tool. Some legislations even require dual-tool verification legally. Thus, it is good practise to have more than one forensic software available at a forensic lab in order to cross-check the results.

A.1) Available software for digital forensics laboratories

A variety of different software is needed in order to run a digital forensics laboratory. This includes case management software as well as feature-packed suites for computer and mobile forensics. Depending on the tasks of the laboratory additional specialised software may be required. The number of forensic big and small software solutions is huge and very agile. Especially the open source community is publishing new tools nearly every day. It is not the aim of this guide to provide a full list of all available tools. However, to provide a better overview that can assist in the development of a comparison matrix a list of useful resources is given below.

Resource Name	URL
National Institute of Standards and Technology (NIST), Computer Forensics Tool Catalog	https://toolcatalog.nist.gov/index.php
National Institute of Standards and Technology (NIST), Computer Forensic Tool Testing (CFTT)	https://www.dhs.gov/science-and-technology/nist-cftt-reports
DFIR Training Website	http://www.dfir.training/index.php/tools/forensic-suites
Awesome Forensics list	https://github.com/Cugu/awesome-forensics
Forensicswiki	http://www.forensicswiki.org/wiki/Tools
Forensicfocus	http://www.forensicfocus.com/software

A.2) Cost overview of standard software for forensic analysis

Remember: All costs for software, hardware and training are reoccurring expenses. While the initial purchase of a forensic software is usually a one-time cost the reoccurring costs for annual license renewals should never be forgotten. Since the prices for license updates and service subscriptions may differ significantly depending on the product it is important to pay attention to those costs. Besides that, hardware needs to be renewed on a regular basis in order to maximise the performance of the evidence processing and to meet the requirements of updated forensic software. In addition to that even the training costs are reoccurring because digital forensics examiners need continuous professional education.

Product	**Manufacturer**	**Category**	**Software costs**	**Hardware costs**	**Training costs** (see table A.4)
Product A		e.g. Forensic Analysis Mobile Forensics Browser for investigator Case management	Purchase: **EUR** License Updates: **EUR / year**	<u>Requirements:</u> Operating system: CPU: RAM: GPU: Disks: Hardware costs: **EUR**	Preferred training option: Training: **EUR/day/person** Travel: **EUR/day/person**
Product B			Purchase: **EUR** License Updates: **EUR / year**	<u>Requirements:</u> Operating system: CPU: RAM: GPU: Disks: Hardware costs: **EUR**	Preferred training option: Training: **EUR/day/person** Travel: **EUR/day/person**
Product C			Purchase: **EUR** License Updates: **EUR / year**	<u>Requirements:</u> Operating system: CPU: RAM: GPU: Disks: Hardware costs: **EUR**	Preferred training option: Training: **EUR/day/person** Travel: **EUR/day/person**
Product D			Purchase: **EUR** License Updates: **EUR / year**	<u>Requirements:</u> Operating system: CPU: RAM: GPU: Disks: Hardware costs: **EUR**	Preferred training option: Training: **EUR/day/person** Travel: **EUR/day/person**

A.3) Forensic software functionality comparison matrix

Functionality	Product A	Product B	Product C	Product D
Signature analysis	e.g. +++	+	++	+++
Hash-Comparison				
Carving				
Imaging				
Mounting of container files				
File system support				
Partition recovery				
RAID recovery				
Encryption support				
Usability				
Indexing				
E-Mail analysis				
Internet traces (Browser, Messenger)				
Viewing of pictures				
Native view of file contents				
Bookmarking / Tagging				
Reporting				
Support for investigator analysis				
Timelining				
Categorisation				
Filter				
Mounting of images				
Extentability				
Easy of setup				
Skin tone detection				
Archiving of cases				
Support / Updates				
Low risk for discontinuation of product				

$ = optional Add-On with extra cost

A.4) Overview of training costs

Product	Training option	Cost per participant	Pros / Cons
Product A	Training by manufacturer	Training: Travel:	+ official training certificate and student handbook by manufacturer
	Training by manufacturer (in-house)	Training:	+ official training certificate and student handbook by manufacturer
	Training-Passports (Unlimited amount of trainings per passport)	Passport: Travel:	+ official training certificate and student handbook by manufacturer + unlimited amount of trainings for 10 employees for one year - Only cost-effective if used intensively
	Training by own personnel	Training:	+ Cheapest option + Trainer can adapt training to own personnel's needs - No official training certificate and student handbook by manufacturer - Trainers have to be educated in the usage of the product and working hours need to be dedicated for preparation of materials.
Product B	Training by manufacturer	Training: Travel:	+ official training certificate and student handbook by manufacturer
	Training by manufacturer (in-house)	Training:	+ official training certificate and student handbook by manufacturer
	Training-Passports (Unlimited amount of trainings per	Passport: Travel:	+ official training certificate and student handbook by

	passport)		manufacturer + unlimited amount of trainings for 10 employees for one year - Only cost-effective if used intensively
	Training by own personnel	Training:	+ Cheapest option + Trainer can adapt training to own personnel's needs - No official training certificate and student handbook by manufacturer - Trainers have to be educated in the usage of the product and working hours need to be dedicated for preparation of materials.
Product C	Training by manufacturer	Training: Travel:	+ official training certificate and student handbook by manufacturer
	Training by manufacturer (in-house)	Training:	+ official training certificate and student handbook by manufacturer
	Training-Passports (Unlimited amount of trainings per passport)	Passport: Travel:	+ official training certificate and student handbook by manufacturer + unlimited amount of trainings for 10 employees for one year - Only cost-effective if used intensively
	Training by own personnel	Training:	+ Cheapest option + Trainer can adapt training to own personnel's needs - No official training certificate and student handbook by

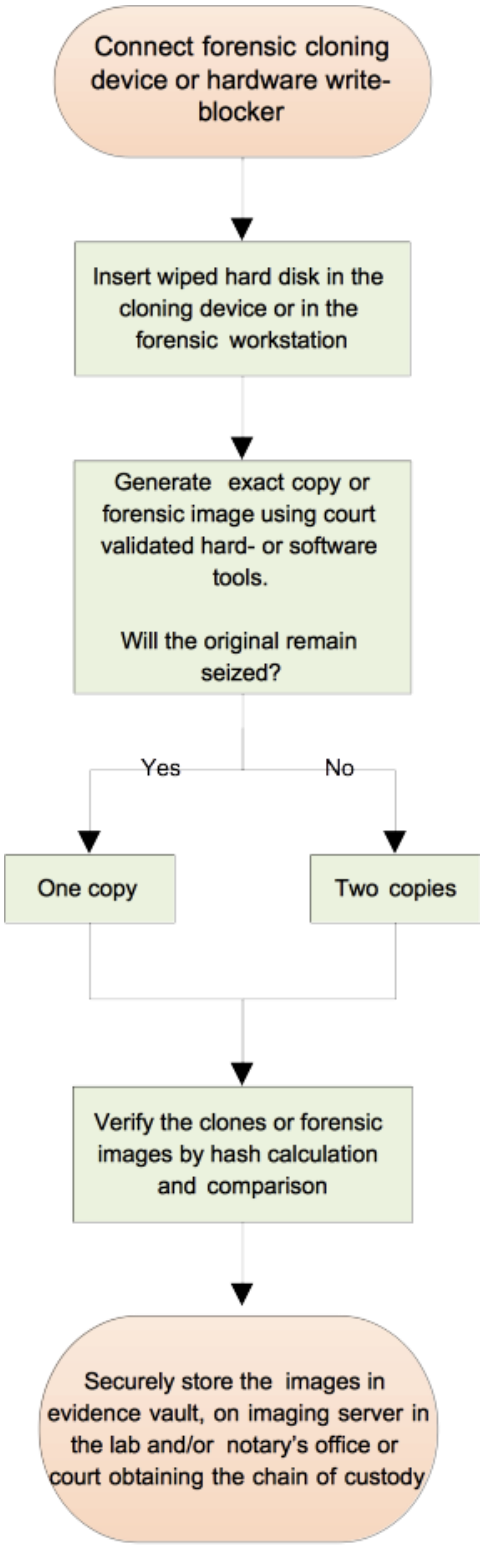
			manufacturer - Trainers have to be educated in the usage of the product and working hours need to be dedicated for preparation of materials.
Product D	Training by manufacturer	Training: Travel:	+ official training certificate and student handbook by manufacturer
	Training by manufacturer (in-house)	Training:	+ official training certificate and student handbook by manufacturer
	Training-Passports (Unlimited amount of trainings per passport)	Passport: Travel:	+ official training certificate and student handbook by manufacturer + unlimited amount of trainings for 10 employees for one year - Only cost-effective if used intensively
	Training by own personnel	Training:	+ Cheapest option + Trainer can adapt training to own personnel's needs - No official training certificate and student handbook by manufacturer - Trainers have to be educated in the usage of the product and working hours need to be dedicated for preparation of materials.

Appendix B – Exemplary Device Carrying Case contents

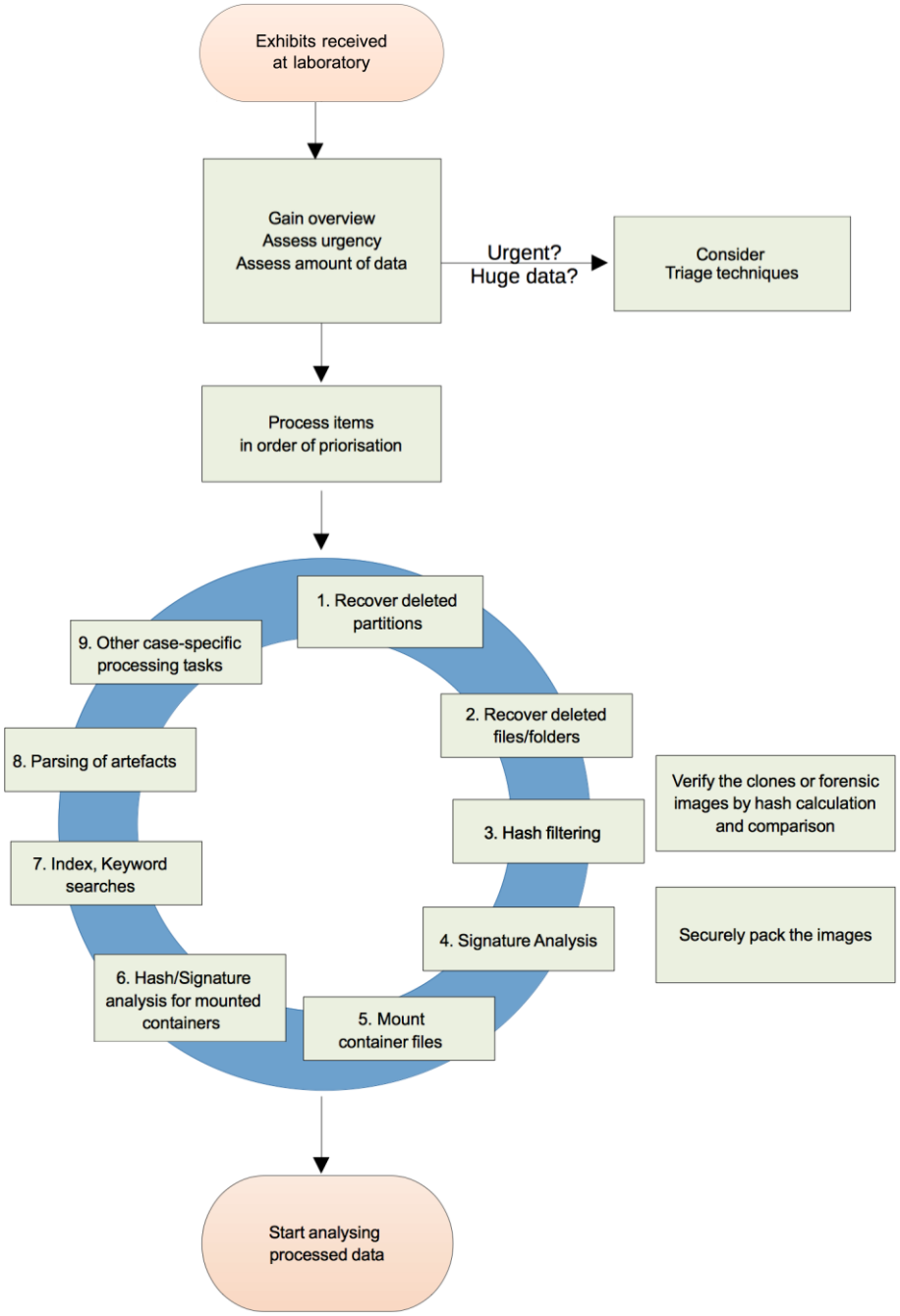
Exemplary Device Carrying Case Contents:

1. Two disk duplicators.
2. One disk duplicator USB protocol module
3. One IDE – SATA write-protection bridge
4. One USB Ultra write-protection bridge
5. One SCSI Ultra write-protection bridge
6. One SAS Ultra write-protection bridge
7. Four 3.5 inches harddrives
8. Two power supplies for disk duplicators
9. Four write-protection bridge power supplies
10. IDE, SATA, SCSI, USB, firewire data cables and adapters

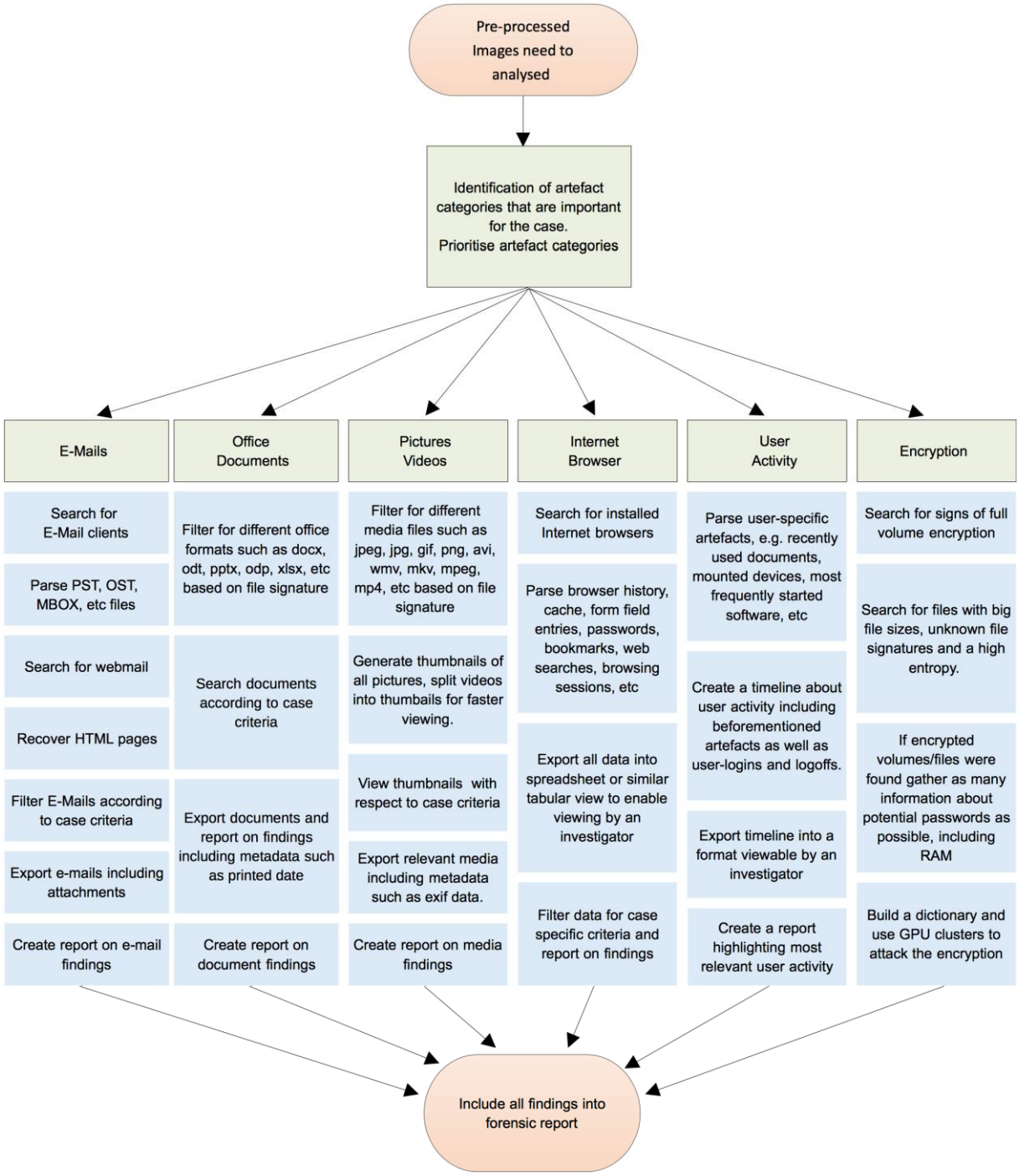
Appendix C – Acquisition Process Flow Chart



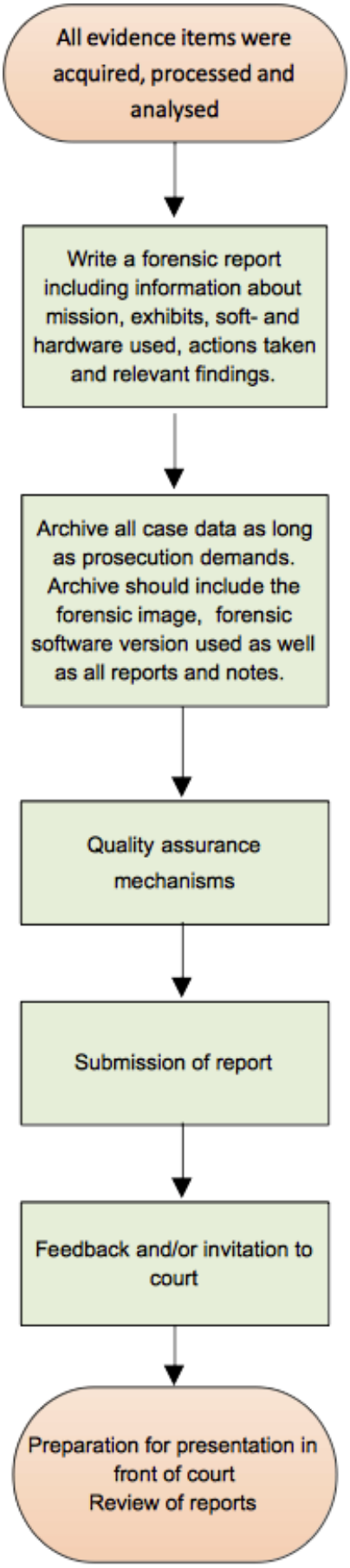
Appendix D - Processing Flow Chart



Appendix E - Analysis Flow Chart



Appendix F - Presentation Flow Chart



Appendix G - Chain of custody record

EXHIBITING INSTRUCTIONS

Each item seized will have an exhibit label attached which should be completed at the scene.

The first person to take possession of an article should exhibit that item. They will give it their exhibit reference number.

These exhibit reference numbers must be unique and should consist of the person's initials from their first name and given name followed by a sequential number starting at 1, *e.g.,* the first exhibit from Anne Browne would be AB/1. Each person who refers to or handles the exhibit must sign the exhibit label.

Each exhibit must have a unique reference number, which should be used by all people subsequently referring to that item.

An operative will need to show in court that an item seized at the scene is the same item produced at court. Therefore it is very important when an article is handed to another person or deposited, such transactions are fully documented.

Any person receiving an exhibited item must sign the relevant exhibit label, therefore maintaining the chain of custody.

Any person who refers to an exhibit in a subsequent report or statement must include the exhibit reference number.

If identical items are found at the same time and place they may be grouped together under the same exhibit reference number, however care should be taken to ensure that grouped items are correctly counted, *e.g.,* thirty-four (34) CDs.

QUESTIONING / INTERVIEWS

All questions and answers entries regarding exhibits must be recorded contemporaneously.

At the conclusion of a seizure any person questioned should be asked if they would initial each answer and sign the bottom of each page if correct and write after the final entry words such as "I agree that this is a correct record of what was said" and append his/her signature.

All persons seizing exhibits should initial relevant entries and sign the page.

In cases where a person refuses to initial or sign an entry the senior person present should initial each answer and sign each page.

If questions and answers cannot be written in one entry, continue into the next column below. A diagonal line should be drawn through the exhibit entry column.

Entry No.	Exhibits	i. Where found ii. Who found by	iii. Time seized iv. Exhibit Ref No.
		i. ii.	iii. iv.
		i. ii.	iii. iv.
		i. ii.	iii. iv.
		i. ii.	iii. iv.
		i. ii.	iii. iv.

Signature(s) of persons seizing item(s) ……
……
……

Questions and answers	v. Where sealed vi. Who by vii. Seal No.	viii. Place deposited ix. Person depositing x. Other reference
	v. **vi.** **vii.**	**viii.** **ix.** **x.**
	v. **vi.** **vii.**	**viii.** **ix.** **x.**
	v. **vi.** **vii.**	**viii.** **ix.** **x.**
	v. **vi.** **vii.**	**viii.** **ix.** **x.**
	v. **vi.** **vii.**	**viii.** **ix.** **x.**

I have initialled each answer, which has been correctly recorded.

Signature(s) of person(s) questioned ……

……

……

Appendix H - Image Acquisition Worksheet

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):				

(xx) *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.

Image Acquisition Worksheet Guidance Notes

The standard (enter agency name) Image Acquisition Worksheet is to be used during any forensic acquisition (imaging) of a hard drive or other type of media.

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 'stand alone 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, once 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, bootdisk, 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 I – Digital Forensics Analysis Form / Spreadsheet

Action	Date/Time started	Date/Time completed	Signature	Notes
Official request/order received				By whom: Notes:
Check for available resources				
Case assigned				To whom:
Exhibits received				By whom:
Exhibits photographed				
Exhibit register updated				
Exhibit forms and chain of custody record correct and complete				
Triage necessary				
Prioritisation completed				Priorities:
Forensic image acquired				Software&Configuration:
Forensic image verified				
Copy of image to backup server				Folder:
Parameters for case specific processing and searching defined				Parameters:
Automated pre-processing of images				
Partition recovery				
File recovery				
Mounting of containers				
Signature analysis				
Hash analysis				Hash sets used:
Other processing tasks				Other processing tasks:
Forensic analysis				Total GB/TB analysed:
Analysis of E-Mails *(if applicable)*				

Analysis of Office Documents *(if applicable)*				
Accounting data *(if applicable)*				
Analysis of Images *(if applicable)*				
Analysis of Videos *(if applicable)*				
Analysis of Internet Browsers *(if applicable)*				
Analysis of User-Activity *(if applicable)*				
Keyword search performed *(if applicable)*				Keywords:
Index created				
Analysis of Messenger *(if applicable)*				
Analysis of databases *(if applicable)*				
Analysis of log files *(if applicable)*				
Malware check? *(if applicable)*				
Encryption check? *(if applicable)*				
Virtualisation *(if applicable)*				
Analysis of other communication data *(if applicable)*				
Forensic Report				
QM of forensic report				
Report submitted				
Case data archived				

Appendix J – Digital Forensics Report Template

YOUR FORENSIC UNITS HEADER

Barcode
Case Ref.:
Lab Ref:
Report No:
Examiner:

DD/MM/YYYY

Forensic analysis report

1. Case information
   - 1.1. Case background
   - 1.2. Request
   - 1.3. Mandate
2. Exhibits
   - 2.1. Exhibit 1
     - 2.1.1. Photos
     - 2.1.2. Description
   - 2.2. Exhibit 2
     - 2.2.1. Photos
     - 2.2.2. Description
3. Examination methods
   - 3.1. Personnel
     - 3.1.1. Qualifications
   - 3.2. Hardware
     - 3.2.1. Write-Blocker
     - 3.2.2. Forensic Station
     - 3.2.3. Other Hardware used

3.3. Software

3.3.1. Imaging Software

3.3.2. Processing Software

3.3.3. Analysis Software

3.3.4. Other Software used

4. Acquisition process

4.1. Image of Exhibit 1

4.1.1. Actions taken

4.1.2. Result of hash verification

4.2. Image of Exhibit 1

4.2.1. Actions taken

4.2.2. Result of hash verification

5. Analysis process

5.1. Analysis of E-Mails (if applicable)

5.2. Analysis of Office Documents (if applicable)

5.3. Accounting data (if applicable)

5.4. Analysis of Images (if applicable)

5.5. Analysis of Videos (if applicable)

5.6. Analysis of Internet Browsers (if applicable)

5.7. Analysis of User-Activity (if applicable)

5.8. Keyword search performed (if applicable)

5.9. Analysis of Messenger (if applicable)

5.10. Analysis of databases (if applicable)

5.11. Analysis of log files (if applicable)

5.12. Malware check? (if applicable)

5.13. Encryption check? (if applicable)

5.14. Virtualisation (if applicable)

5.15. Analysis of other communication data (if applicable)

6. Results

Appendices

a) Printout of findings

b) Glossary

c) Report about technical details

Case Ref: Signature:

YOUR FORENSIC UNITS FOOTER

For further templates see: Streamlined Forensic Report Toolkit, http://www.cps.gov.uk/legal/s_to_u/scientific_evidence/sfr_guidance_and_toolkit/